FERDINAND PORSCHE
FERN FH

# Die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen in Österreich in Bezug auf Phishing Schulungsmethoden

## Masterarbeit


Eingereicht von: **Sharon Velikkakath, B.Sc. (WU)**

Matrikelnummer: 01451953


im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

## Master of Arts in Business

Betreuung und Beurteilung: Thomas Krabina, M.Sc.

Zweitgutachten: Daniela Wolf, Bakk. MSc MA MA

Wien, September 2022

# Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.
3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, 08.09.2022 _____

Unterschrift

**Kurzzusammenfassung:** Die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen in Österreich in Bezug auf Phishing Schulungsmethoden.

Sicherheitsforscher und Sicherheitsforscherinnen argumentieren, dass Unternehmen Programme zur Sicherheitsausbildung, Schulung und Awareness für Informationssicherheit benötigen, um die Awareness von Mitarbeiter und Mitarbeiterinnen für Sicherheitsrisiken zu schärfen und ihnen die erforderlichen Fähigkeiten und Kenntnisse zur Einhaltung der Sicherheitsrichtlinien zu vermitteln. Infolgedessen beschäftigt sich die Masterarbeit mit der Beantwortung der folgenden Forschungsfrage: Wie stellt sich derzeit die Phishing Schulung der Arbeitnehmer und Arbeitnehmerinnen in österreichischen Großunternehmen dar? Es wurde eine Literaturrecherche durchgeführt und mit einer quantitativen Online-Umfrage der Ist-Stand ermittelt. Die Ergebnisse der Umfrage zeigten, dass fast die Hälfte der Teilnehmer und Teilnehmerinnen noch nicht eine Phishing Schulung erhalten haben. Ein Drittel der Personen kennen den Unterschied zwischen „http://“ und „https://“ nicht. Knapp 50% der befragten Personen haben mehr als 50% der Beispiele zu legitimen- und Phishing-E-Mails bzw. -URLs richtig identifizieren können. Es wurden signifikante Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme bzw. Nicht-Teilnahme einer Phishing Schulung ermittelt. Es wurde ebenfalls festgestellt, dass es signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit der befragten Personen gibt. Außerdem würden die Teilnehmer und Teilnehmer der Umfrage die eingebettete- oder Achtsamkeitsschulung bevorzugen. Auf Basis der Erkenntnisse und Ergebnisse aus der Literatur und Umfrage wurde ein Leitfaden für eine Phishing Schulung entwickelt.

**Schlagwörter:**

Phishing-Angriff, Phishing-E-Mail, Phishing-URL, Anti-Phishing-Methoden, Phishing-Awareness, Phishing-Schulungen, SETA-Schulung, Phishing-Schulungsmethoden.

**Abstract:** The employees point of view in Austria regarding phishing training methods.

Security researchers argue that companies need security education, training, and information security awareness programs to raise employees' awareness of security risks and provide them with the necessary skills and knowledge to comply with security policies. As a result, this master thesis deals with answering the following research question: How does the phishing training of employees in large Austrian companies currently look like? A literature review was conducted and a quantitative online survey was used to determine the current state. The results of the survey showed that almost half of the respondents have not received phishing training. One-third of the individuals do not know the difference between "http://" and "https://". Almost 50% of the respondents were able to correctly identify more than 50% of the examples of legitimate and phishing email or URL. Significant differences were found between phishing susceptibility and participation or non-participation in phishing training. It was also found that there were significant correlations between phishing susceptibility and phishing familiarity of the respondents. In addition, survey participants would prefer embedded or mindfulness training. Based on the findings and results from the literature and survey, a guideline for phishing training was developed.

**Keywords:**

Phishing attack, Phishing email, Phishing URL, Anti-phishing methods, Phishing awareness, Phishing training, SETA-training, Phishing training methods.

# Inhaltsverzeichnis

1 Einleitung ..... 1

1.1 Ausgangssituation ..... 1

1.2 Problemstellung ..... 5

1.3 Zielsetzung ..... 6

1.4 Forschungsfrage ..... 6

1.5 Hypothesen ..... 6

1.6 Wissenschaftliche Methoden ..... 7

1.7 Aufbau ..... 9

2 Theoretischer Teil ..... 10

2.1 Einleitung ..... 10

2.2 Social-Engineering ..... 13

2.3 Phishing ..... 14

2.3.1 Definition ..... 16

2.3.2 Herkunft ..... 17

2.3.3 Kategorie ..... 18

2.3.4 Ablauf ..... 40

2.3.5 Technische Anti-Phishing Methoden ..... 44

2.3.6 Nicht-Technische Anti-Phishing Methoden ..... 55

2.3.7 Phishing Anfälligkeitsmerkmale ..... 77

3 Empirischer Teil ..... 102

3.1 Vorgehensweise ..... 102

3.1.1 Teil 1 ..... 103
3.1.2 Teil 2 ..... 104
3.1.3 Teil 3 ..... 106
3.1.4 Teil 4 ..... 107
3.1.5 Teil 5 ..... 107
3.2 Ergebnisse ..... 108
3.2.1 Demografische Merkmale ..... 108
3.2.2 Vertrautheit, Awareness und Sicherheitsgewohnheiten ..... 112
3.2.3 Phishing Definition ..... 115
3.2.4 Phishing Anfälligkeit – E-Mail ..... 115
3.2.5 Phishing Anfälligkeit – URL ..... 124
3.2.6 Phishing Anfälligkeit – Gesamt ..... 132
3.2.7 Durchgeführte Phishing Schulungen und Methoden ..... 134
3.2.8 Bevorzugte Phishing Schulungsmethoden ..... 136
3.3 Auswertung ..... 138
3.3.1 Cronbach´s Alpha ..... 138
3.3.2 Mann-Whitney-U-Test ..... 139
3.3.3 Korrelation ..... 141
3.4 Diskussion ..... 144
3.5 Leitfaden für Phishing Schulung ..... 157
4 Schlussfolgerung ..... 174
4.1 Zusammenfassung ..... 174
4.2 Limitation ..... 176

4.3 Forschungsbedarf ..... 177

5 Literaturverzeichnis ..... 178

6 Abbildungsverzeichnis ..... 189

7 Tabellenverzeichnis ..... 194

Anhang A ..... 1

# 1 Einleitung

## 1.1 Ausgangssituation

Zum gegenwärtigen Zeitpunkt der Informationstechnologie ist das Internet die am weitesten verbreitete Technologie und im Alltag nicht mehr wegzudenken (Adil, Khan and Nawaz Ul Ghani, 2020, p. 2). Die Analysen des „DataReportal - Global Digital Insights" zeigten Ende 2011, dass knapp über zwei Milliarden Menschen auf der ganzen Welt das Internet nutzten, was 30% der Weltbevölkerung entspricht. Zehn Jahre später ist diese globale Zahl der Nutzer und Nutzerinnen auf fast 4,9 Milliarden angewachsen, wobei Ende 2021 mehr als sechs von zehn Menschen auf der ganzen Welt das Internet benutzten (*A Decade in Digital*, 2021). Heutzutage sind das Internet und der Computer omnipräsent, was einen allgegenwärtigen Zugang zu Informationen mit sich bringt (Arduin, 2020, p. 9). Aufgrund dessen entstanden viele Anwendungen wie zum Beispiel Online-Banking (M. Alwanain, 2019, p. 480), Online Shopping und soziale Medien (Adil, Khan and Nawaz Ul Ghani, 2020, p. 2). Diese Allgegenwärtigkeit von Diensten bringt jedoch auch kritische Sicherheitsbedrohungen mit sich (M. Alwanain, 2019, p. 480). Eine Bedrohung in diesem Zusammenhang ist der „Phishing-Angriff" (Adil, Khan and Nawaz Ul Ghani, 2020, p. 2).

Der Begriff „Phishing" entstand in den 1990er Jahren und (Das *et al.*, 2019, p. 1) stellt seit über zwei Jahrzehnten noch eine weit verbreitete Bedrohung in der Cyberwelt dar (Chiew, Yong and Tan, 2018, p. 1). Cisco, eines der führenden Unternehmen für Netzwerke und Sicherheitsgeräte, beschreibt Phishing wie folgt: Phishing-Angriffe sind betrügerische Mitteilungen, die scheinbar von einer seriösen Quelle stammen (Patayo, 2021, p. 2). Phishing wird auch als Social-Engineering-Technik definiert, (Abroshan *et al.*, 2021a, p. 345) die menschliche Interaktionen miteinbeziehen. Diese Technik wird verwendet, um Benutzer und Benutzerinnen zu psychologischen Fehlern zu zwingen, so dass am Ende Sicherheitsfehler entstehen und daher (Kaushik *et al.*, 2021, p. 14) heikle Informationen preisgeben werden. Solche Fehler können Personen und Unternehmen großen Schaden zufügen wie zum Beispiel: Datenverlust, Reputationsverlust, Identitätsdiebstahl und Geldverlust (Abroshan *et al.*, 2021a, p. 345).

Ein wichtiger Angriffsvektor für Phishing sind der Gebrauch von E-Mails, die von Social-Engineers verwendet werden, um die allgemeine Bevölkerung, Organisationen und sogar Einzelpersonen anzugreifen (Burda, Allodi and Zannone, 2020, p. 2). Trotz des Wachstums von mobilen Messengern und Chat-Apps spielt E-Mail nach wie vor eine wesentliche Rolle in der Online-Kommunikation (Miranda, 2018, p. 5). Im Jahr 2020 belief sich die Zahl der

globalen E-Mail-Benutzer und -Benutzerinnen auf vier Milliarden und soll bis 2025 auf 4,6 Milliarden anwachsen. Mit einer Schätzung von 306 Milliarden E-Mails, die täglich weltweit gesendet und empfangen werden (*Number of e-mail users worldwide 2025*, 2021), sind E-Mails noch der am häufigsten von Angreifer und Angreiferinnen verwendete Vektor (Baki and Verma, 2021, p. 1). Ein Angreifer oder eine Angreiferin verleiten E-Mail-Benutzer und -Benutzerinnen dazu, auf einen Link zu klicken oder einen Anhang zu öffnen. Die Angreifer oder Angreiferinnen stehlen dann die sensiblen Daten des Opfers, kompromittieren den Computer oder das Konto und/oder kompromittieren das Unternehmensnetzwerk/-system (Abroshan *et al.*, 2021a, p. 345). Wie Kevin Mitnick, einer der berühmtesten Computerhacker aller Zeiten, sagte: Ein Unternehmen kann Hunderttausende von Dollar für Firewalls, Verschlüsselungen und andere Sicherheitstechnologien ausgeben, aber wenn ein Angreifer oder eine Angreiferin eine vertrauenswürdige Person innerhalb des Unternehmens erfolgreich kompromittiert, erlangt diese Person Zugang in das Unternehmen. Dann ist das ganze Geld, das in die Technologie investiert wurde, im Wesentlichen verschwendet (De Bona and Paci, 2020, p. 1).

Viele Forscher und Forscherinnen (Anwar *et al.*, 2017; Ovelgönne *et al.*, 2017; Sebescen and Vitak, 2017; Aldawood and Skinner, 2018; Yan *et al.*, 2018; Linkov *et al.*, 2019; Arend *et al.*, 2020; Younis and Musbah, 2020) auf dem Gebiet der Cybersicherheit sind sich einig, dass der menschliche Faktor das schwächste Glied in der Cybersicherheit darstellt (Papatsaroucha *et al.*, 2021, p. 2). Dennoch wenden Unternehmen, die sich mit Informations- und Datensicherheit befassen zunehmend mehr technologische Ressourcen für den Schutz ihrer Informationssysteme auf und vernachlässigen die Schulung von Mitarbeiter und Mitarbeiterinnen. Es ist für einen Angreifer oder Angreiferin oft einfacher, menschliche und soziale Schwächen eines Menschen auszunutzen, als die technologischen Gegenmaßnahmen des Unternehmens zu überwinden (Frauenstein and von Solms, 2013, p. 198). Technologische Lösungen können nur so weit gehen, dass das menschliche Urteilsvermögen die letzte Verteidigungslinie darstellt (Hakim *et al.*, 2021, p. 1342). Die Bemühungen der Organisation um Cybersicherheit hängen weitgehend von den Mitarbeiter und Mitarbeiterinnen ab, die sich innerhalb der Organisation aufhalten (Canham *et al.*, 2021, p. 1). Viele Mitarbeiter und Mitarbeiterinnen sind so sehr mit den primären Arbeitsaufgaben beschäftigt, dass diese Personen z.B. kaum (Frauenstein and von Solms, 2013, p. 198) auf den Text einer Phishing-E-Mail achten. Eine Phishing-E-Mail adressiert den Empfänger oder die Empfängerin meist mit Dringlichkeitshinweisen, oder mit Wörtern die Gefühle der Verwundbarkeit oder Bedrohung hervorrufen. Hiermit

zwingen sie diese Person sofort und impulsiv zu handeln. Diese Dringlichkeitshinweise sind äußerst trügerisch, weil die Aufmerksamkeit der Empfänger und Empfängerinnen somit abgelenkt werden, die jedoch möglich helfen könnten eine Phishing-E-Mail zu erkennen. Ein Angreifer oder eine Angreiferin können Benutzer und Benutzerinnen auch dazu verleiten, bösartige Malware herunterzuladen, nachdem auf einen in der E-Mail eingebetteten Link geklickt wird (Baillon *et al.*, 2019, p. 1).

In den letzten Jahren haben sich Phishing-E-Mails von qualitativ schlecht gestalteten und nicht zielgerichteten Texten zu hochgradig personalisierten und raffinierten Nachrichten weiterentwickelt, wodurch die Empfänger und Empfängerinnen eher glauben, dass der Inhalt legitim ist (Baillon *et al.*, 2019, p. 1). Diese Art von Nachricht wird auch als Spear-Phishing bezeichnet und wird auch mit Social-Engineering in Verbindung gebracht, das selbst für geschulte Mitarbeiter und Mitarbeiterinnen nur schwer zu erkennen ist (Thomas, 2018, p. 1). Social-Engineering Angriffe werden hinterhältiger. Das bedeutet, dass Vorschläge zur Bekämpfung von Social-Engineering, die noch vor zwei Jahren als wirksam erachtet wurden, heute nicht mehr verwendet werden können. Zum Beispiel wurde im Jahr 2018 von der Anti-Phishing Working Group dazu geraten, nach dem Hyper Text Transfer Protocol Secure (HTTPS) in einem Universal Resource Locator (URL) in mutmaßlichen Phishing-E-Mails zu suchen. Im Jahr 2020 jedoch, rief die Anti-Phishing Working Group dazu auf, sich nicht auf das Vorhandensein von HTTPS-Protokollen zu verlassen, da mittlerweile bis zu 75% der schädlichen Websites HTTPS-Protokolle verwenden (Antonucci *et al.*, 2020, p. 3).

Des Weiteren hat die Zahl der Phishing-Angriffe in den letzten Jahren zugenommen, insbesondere seit Beginn der COVID-19-Pandemie. Allein im März 2020 gab es eine Zunahme der Phishing-Angriffe von 600% (Abroshan *et al.*, 2021a, p. 345). Im April 2020 berichtete Google, dass täglich 18 Millionen Malware- und Phishing-E-Mails im Zusammenhang mit COVID-19 sowie 240 Millionen COVID-19-Spamnachrichten blockiert wurden (Frauenstein and Flowerday, 2020, p. 2). Die COVID-19-Pandemie hat für Angreifer oder Angreiferinnen die Gelegenheit geboten, die Angst der Menschen in Bezug auf Phishing und Arbeitssituation auszunutzen (Yanakiev *et al.*, 2020, p. 6). Dies ist darauf zurückzuführen, dass die meisten arbeitstechnischen Angelegenheiten von Regierungs- oder Unternehmensebenen, Bildungsaktivitäten und nichtkommerziellen Unternehmen vom traditionellen On-Premises-Ansatz auf Online und somit Homeoffice umgestiegen sind (Basit *et al.*, 2021, p. 150). Daher kann ein Angreifer oder eine Angreiferin die Angst von Menschen ausnutzen, was das Sicherheitswissen und die Awareness der Benutzer und Benutzerinnen überschatten könnte. Ein Beispiel wäre, dass

der Benutzer oder die Benutzerin ohne nachzudenken auf den Phishing-Link klickt, weil diese Person Nachrichten in Bezug auf COVID-19 erwartet oder allgemeine Informationen erhalten möchte (Abroshan *et al.*, 2021a, p. 348).

Während Technologie wichtig ist, spielen organisatorische und menschliche Faktoren ebenfalls eine entscheidende Rolle beim Erreichen von Informationssicherheit. Sowohl die organisatorischen als auch die technologischen Dimensionen hängen von menschlichen Faktoren ab. Der menschliche Faktor ist oft der Einstiegspunkt für Phishing-Angriffe. Daher erstellen Unternehmen Richtlinien und Verfahren, um die Informationssicherheit zu gewährleisten. Jedoch reicht es nicht nur aus, dass die Mitarbeiter und Mitarbeiterinnen diese einhalten. Denn die Schwachstellen des Menschen in der Informationssicherheit sind in der Regel auf unbeabsichtigtes Verhalten zurückzuführen. Einigen Nutzer und Nutzerinnen fehlen möglicherweise einfach die Kenntnisse und Fähigkeiten, um sich vor Bedrohungen zu schützen und bestehende Richtlinien einzuhalten (Frauenstein and von Solms, 2013, p. 199). Die effektivste Verteidigung gegen Phishing-Angriffe sind somit gut ausgebildete und aufmerksame Mitarbeiter und Mitarbeiterinnen. Jedoch sind viele Menschen nicht aufmerksam oder neugierig und werden Opfer eines Phishing-Angriffs. Aus diesem Grund sollten Unternehmen versuchen, ihre Mitarbeiter und Mitarbeiterinnen zu schulen, sodass diese eine Denkweise entwickeln, die es unterlässt auf verdächtige Links und Websites zu klicken (Basit *et al.*, 2021, p. 150). Viele Unternehmen haben bereits damit begonnen, den Mitarbeiter und Mitarbeiterinnen Phishing Schulungen anzubieten (Jampen *et al.*, 2020, p. 1). Es gibt zahlreiche wissenschaftliche Untersuchungen (Jansson and von Solms, 2013; Kearney and Kruger, 2013; Arachchilage and Love, 2014; B. Kim, 2014; Arachchilage, Love and Beznosov, 2016; Jensen, Durcikova and Wright, 2017; CJ *et al.*, 2018; Gupta, Arachchilage and Psannis, 2018; Meyers *et al.*, 2018; Akpon-Ebiyonare, 2019; Anawar *et al.*, 2019; Furnell, Millet and Papadaki, 2019; Gordon *et al.*, 2019; M. I. Alwanain, 2019; Alabdan, 2020; Brickley, Thakur and Kamruzzaman, 2021; Jayatilaka, Arachchilage and Babar, 2021; Yeoh *et al.*, 2021), die besagen, dass es Mitarbeiter und Mitarbeiterinnen an Awareness und Schulung mangelte, um einen Phishing-Angriff richtig zu erkennen und abzuwehren. Daher bleibt die Verbesserung der Schulung der Mitarbeiter und Mitarbeiterinnen einer der wirksamsten Abwehrmöglichkeiten gegen Phishing-Angriffe (Brickley, Thakur and Kamruzzaman, 2021, p. 28).

## 1.2 Problemstellung

Sicherheitsforscher und Sicherheitsforscherinnen argumentieren, dass Unternehmen Programme zur Sicherheitsausbildung, Schulung und Awareness für Informationssicherheit (Security, Education, Training and Awareness - SETA) benötigen, um die Awareness von Mitarbeiter und Mitarbeiterinnen für Sicherheitsrisiken zu schärfen und ihnen die erforderlichen Fähigkeiten und Kenntnisse zur Einhaltung der Sicherheitsrichtlinien zu vermitteln. Jedoch hat ein nicht mitarbeiter- und mitarbeiterinnen-orientiertes SETA-Programm mehrere Nachteile. In erster Linie kann das mangelnde Verständnis über die Motivation zur Einhaltung von Sicherheitsanweisungen von Mitarbeiter und Mitarbeiterinnen, die Wirksamkeit aller stattfindenden SETA-Programmen beeinträchtigen. Darüber hinaus ist es wichtig für die Entwicklung von Programmen die Bedürfnisse der Mitarbeiter und Mitarbeiterinnen in Bezug auf den Lernstil, ihre Arbeitsanforderungen und -prozesse zu verstehen. In den meisten Unternehmen werden diese Programme entwickelt, um Compliance-Anforderungen zu erfüllen, jedoch wird die Sichtweise der Mitarbeiter und Mitarbeiterinnen nicht berücksichtigt.

Die Studie von Alshaikh, Maynard und Ahmad (2021) konzentriert sich bei der Entwicklung von SETA-Programmen auf die Sichtweise der Mitarbeiter und Mitarbeiterinnen. Jedoch wird in dieser Studie nur ein Teil des SETA-Programms behandelt und zwar die Awareness für Informationssicherheit. Die Autoren und Autorinnen haben die Sicherheitsausbildung und Schulung nicht behandelt, weil die meisten Unternehmen diesen Prozess an externe Anbieter und Anbieterinnen auslagern (Alshaikh, Maynard and Ahmad, 2021). Jedoch kann nicht jedes Unternehmen diese Möglichkeit nutzen, weil die Auslagerung mit höheren Kosten verbunden ist. Aus diesem Grund wird sich ein Teil der Masterarbeit mit der Sicherheitsausbildung und Schulung aus der Sicht der Arbeitnehmer und Arbeitnehmerinnen befassen. Es gibt noch zwei weitere Studien, die die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen behandeln. Die erste Studie von Rastenis et al. (2020) befasst sich jedoch mit einer speziellen Schulungsmethode und zu dieser Schulungsmethode wurde die Befragung durchgeführt (Rastenis *et al.*, 2020). Die zweite Studie von Williams, Hinds und Joinson (2018) befasst sich mit Spear Phishing-Attacken und im Zuge dessen wurde auch eine Befragung zur Wahrnehmung zu Sicherheitsschulungen durchgeführt. Jedoch wurde hier eine qualitative wissenschaftliche Methode verwendet (Williams, Hinds and Joinson, 2018). Die Masterarbeit wird eine quantitative wissenschaftliche Methode verwenden.

## 1.3 Zielsetzung

Die Masterarbeit hat zum Ziel die derzeitige Situation in Bezug auf Phishing-Schulungen in Großunternehmen in Österreich zu untersuchen. Ein weiteres Ziel dieser Masterarbeit ist es, den aktuellen Stand der Forschung hinsichtlich dem Thema Phishing zusammenzufassen, um eine theoretische Grundlage für die Durchführung der Studie dieser Masterarbeit zu bieten. In der Studie wird mittels eines Fragebogens festgestellt, wie viele Personen eine Phishing-Schulung erhalten haben, welche Schulungsmethoden verwendet wurden und wie weit die letzte Schulung in Bezug auf Phishing zurückliegt. Zusätzlich wird im Rahmen der Umfrage die Phishing Anfälligkeit der Arbeitnehmer und Arbeitnehmerinnen in Großunternehmen in Österreich untersucht. Außerdem wurde in bisherigen Forschungsarbeiten die Sichtweise der angestellten Personen in Bezug auf Phishing-Schulungen vernachlässigt. Daher ist ein weiteres Ziel der Arbeit, herauszufinden, welche Schulungsmaßnahmen Mitarbeiter und Mitarbeiterinnen in österreichischen Großunternehmen bevorzugen. Das soll dazu beitragen, den Großunternehmen in Österreich einen Überblick über die verschiedenen Schulungsmöglichkeiten zu geben und das Ergebnis zur bevorzugten Schulungsmethode zu liefern. Des Weiteren wird auf Basis der Ergebnisse der Literaturrecherche in Kapitel 2 und der Auswertung des Fragebogens in Kapitel 3 ein Leitfaden für Großunternehmen in Österreich erstellt die für die Gestaltung einer Phishing-Schulung helfen soll. In diesem Leitfaden werden zudem die wichtigsten Erkenntnisse der Forschung für Phishing-Schulungen aus der Literaturrecherche zusammengefasst.

## 1.4 Forschungsfrage

Wie stellt sich derzeit die Phishing Schulung der Arbeitnehmer und Arbeitnehmerinnen in österreichischen Großunternehmen dar?

## 1.5 Hypothesen

Die Hypothesen wurden anhand des erworbenen Wissens der Literrecherche definiert und werden im Zuge der quantitativen Analyse überprüft.

Hypothese 1:

- Nullhypothese: Es gibt keine signifikanten Unterschiede zwischen der Phishing Anfälligkeit und dem Geschlecht.

- Alternativhypothese: Es gibt signifikante Unterschiede zwischen der Phishing Anfälligkeit und dem Geschlecht.

Hypothese 2:

- Nullhypothese: Es gibt keine signifikanten Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme einer Phishing Schulung.
- Alternativhypothese: Es gibt signifikante Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme einer Phishing Schulung.

Hypothese 3:

- Nullhypothese: Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit.
- Alternativhypothese: Es gibt signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit.

Hypothese 4:

- Nullhypothese: Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Awareness.
- Alternativhypothese: Es gibt signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Awareness.

Hypothese 5:

- Nullhypothese: Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Sicherheitsgewohnheit.
- Alternativhypothese: Es gibt signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Sicherheitsgewohnheit.

## 1.6 Wissenschaftliche Methoden

Für die Masterarbeit wurden zwei wissenschaftliche Methoden verwendet, die nachfolgend näher erläutert werden.

Im ersten Teil dieser Arbeit wurde hauptsächlich auf bestehende wissenschaftliche Literatur zurückgegriffen. Eine ausführliche Recherche zu dem Thema Phishing und den Schulungsmethoden werden Aufschluss über den Status quo und aktuelle Studien geben. Bei der Auswahl der Literatur für die Masterarbeit wurde vor allem auf die Aktualität der

Literatur geachtet. Es wurden dabei unter anderem internationale Fachbücher und wissenschaftliche Fachzeitschriften herangezogen. Außerdem wurde themenspezifische Journale und facheinschlägige, wissenschaftlich fundierte Internetquellen untersucht. Die Literaturrecherche wurde nach der bekannten Methodik von Vom Brocke et al. (2009) durchgeführt. Diese Methodik versucht, die relevanten Quellen zu einem bestimmten Thema zu finden, indem die Schlüsselwörter-, Rückwärts- und Vorwärtssuche angewandt wird, um so eine umfassende Überprüfung verwandter Studien zu ermöglichen (López-Aguilar and Solanas, 2021, p. 1364). In dieser Masterarbeit wurde jedoch die Suche nur auf Schlüsselwörter begrenzt.

Bei der Auswahl der Literatur wurden folgende Datenbanken verwendet: Google Scholar, EBSCO, ScienceDirect, Emerald Web of Science, IEEE, ProQuest, Springerlink. Die Literatursuche wurde im November 2020 gestartet und es wurden zuerst nach folgenden Schlüsselwörtern gesucht: Phishing, Phishing-Angriff, Phishing-Attacks, Phishing-E-Mail/-Mail, Phishing-Website, Phishing-Website, Phishing-URL, Phishing-Link. Im Laufe der Recherche wurde festgestellt, dass Phishing oft als Teil von Malware-Angriffen untersucht worden ist. Aus diesem Grund wurde die Suche auf die folgenden Schlüsselwörter erweitert: Phishing-Malware, bösartige/Malware-URL, bösartiger/Malware-Link, bösartige/Malware-Website, bösartige/Malware-E-Mail/Mail. Es wurde Aufnahmekriterien verwendet, um nützliche Literatur aus den Suchbegriffen zu identifizieren und zu extrahieren. Quellen, die folgende Informationen enthalten, wurden miteinbezogen: Allgemeine Information zu Phishing, Phishing-Angriffe, Phishing-Awareness, Phishing-Schulungen, Rahmenbedingungen für Phishing-Schulungen, Studien in Bezug auf Phishing, Bestehende Phishing-Taxonomien und Präventionsmethoden. Es wurden nur deutsch- und englischsprachige Quellen, die im Zeitraum von 2005-2021 erschienen sind, in der Suche beachtet. Es wurden auch Ausschlusskriterien verwendet, um irrelevante Studien aus der gesammelten Literatur auszuschließen. Es wurden Quellen ausgeschlossen die für die Masterarbeit irrelevant sind, wie zum Beispiel: Keine Phishing- und Anti-Phishing-Techniken. Schlussendlich wurden 181 relevante Quellen auf Deutsch und Englisch gesammelt. Bei den 181 Quellen wurden die Abschnitte: Titel, Zusammenfassung, Einführung, Diskussion und Schlussfolgerung gelesen, um Studien zu finden, die folgende Themenbereiche in Bezug auf Phishing beinhalten: Experimente, Schulungen, Awareness und Lösungsmöglichkeiten. Die 181 Quellen wurden mit einer Notenskala von 1 (Sehr Gut) bis 5 (Nicht Genügend) eingestuft. Die Quellen mit den Noten 1-2 wurden vollständig gelesen (114 Quellen).

Der zweite Teil dieser Arbeit stellt die Erhebung von statistischen Daten dar. Dies wurde auf Basis der bereits erarbeiteten Literaturrecherche in Form einer quantitativen Online-Erhebung mittels Fragebogen durchgeführt. Mithilfe des Fragebogens wird der Ist-Stand in Bezug auf Phishing-Anfälligkeit, Phishing-Schulungen und -Methoden ermittelt. Der Fragebogen gliedert sich in vier Teile. Der erste Teil des Fragebogens beschäftigt sich mit dem Wissen und Awareness hinsichtlich dem Thema Phishing. Hierbei werden folgende Punkte analysiert: Phishing Vertrautheit, -Awareness und Sicherheitsgewohnheiten. Im zweiten Teil wurden Beispiele zu E-Mails dargestellt und Teilnehmer und Teilnehmerinnen müssen legitime E-Mails von Phishing-Mails unterscheiden. Den Teilnehmer und Teilnehmerinnen werden auch URL-Beispiele gezeigt und auch hier müssen sie erkennen, ob es sich um einen legitimen oder bösartigen Link handelt. Der dritte Teil der Befragung bezieht sich auf die durchgeführten Schulungen der Teilnehmer und Teilnehmerinnen. Im vierten Teil der Befragung werden die in der Literatur besprochenen Schulungsmethoden vorgestellt und Arbeitnehmer und Arbeitnehmerinnen entscheiden welche Schulungsmethode sie bevorzugen würden. Durch diese Art der Befragung kann die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen in Österreich festgestellt werden. Der letzte Teil bezieht sich auf personenbezogene Daten. Dazu zählen unter anderem das Geschlecht, die höchste abgeschlossene Ausbildung, der Arbeitsbereich, die Arbeitsdauer und die vertraglich festgelegten Arbeitsstunden pro Woche. Die genaue Vorgehensweise und Fragestellungen werden im Kapitel 3.1 näher erläutert.

## 1.7 Aufbau

Die Masterarbeit ist in vier Kapiteln unterteilt. Das erste Kapitel (Einleitung) befasst sich mit der Ausgangslage, Problemstellung, Forschungsfrage, Hypothesen, Wissenschaftliche Methoden und der Zielsetzung. Das zweite Kapitel (Theoretischer Teil) besteht aus dem theoretischen Teil. Hierbei wird der Begriff Social-Engineering näher erläutert. Der Rest des Kapitels setzt sich mit dem Thema Phishing auseinander. In diesem Zusammenhang wird auf die Herkunft von Phishing, die Kategorien von Phishing-Angriffen, den Ablauf einer Phishing-Attacke, die technischen Anti-Phishing Methoden, die nicht-technischen Anti-Phishing Methoden und die Phishing Anfälligkeitsmerkmale näher eingegangen. Das dritte Kapitel (Empirischer Teil ) umfasst den empirischen Teil der Masterarbeit. Dabei werden die Punkte Methodik, Vorgehensweise, Ergebnisse, Auswertung, Diskussion (Beantwortung der Forschungsfrage) und Leitfaden für Phishing Schulung genauer betrachtet. Das letzte Kapitel (Schlussfolgerung) beschäftigt sich mit der

Schlussfolgerung der Masterarbeit, hier wurde eine Zusammenfassung erstellt und die Limitation und den weiteren Forschungsbedarf erörtert.

# 2 Theoretischer Teil

## 2.1 Einleitung

Die digitale Welt ist für viele Menschen nicht mehr wegzudenken. Die Menschen erledigen ihre Geschäfte im Internet, tauschen Wissen online aus, tätigen elektronische Bank- und Zahlungsüberweisungen, handeln mit Kryptowährungen und führen eine Reihe anderer Aktivitäten aus, die früher nur in der physischen Welt möglich waren (Abroshan *et al.*, 2021c, p. 44928). Das Rückgrat dieser digitalen Welt ist die Internettechnologie, die es den Menschen ermöglicht, über ihre PCs und mobilen Geräte wie Smartphones einzukaufen, Kontakte zu knüpfen, zu kommunizieren, sich zu vernetzen und sich unterhalten zu lassen (Arachchilage, Love and Beznosov, 2016, p. 185). Die digitale Welt macht unser Leben viel einfacher. Gleichzeitig bringt dieser Wandel aber auch eine Reihe neuer Herausforderungen und potenzieller Probleme mit sich. Viele Angreifer und Angreiferinnen nutzen technische Schwachstellen aus, die im Design von Anwendungen vorzufinden sind und/oder im Netzwerk eine Sicherheitslücke darstellen. Dadurch verschaffen sich die Angreifer und Angreiferinnen unbefugten Zugang zu sensiblen und kritischen Daten der Opfer. Wiederrum andere Angreifer und Angreiferinnen nutzen psychologische Tricks, um Menschen zu täuschen und das Vertrauen zu gewinnen, ähnlich wie Betrüger und Betrügerinnen in der physischen Welt vorgehen (Abroshan *et al.*, 2021c, p. 44928). Mit der zunehmenden Abhängigkeit der Menschen vom Internet steigt auch die Möglichkeit von Angriffen und anderen Sicherheitsverletzungen. Zu den Cyber-Bedrohungen gehören Computerviren und andere Arten wie beispielsweise bösartige Software (Malware), unerwünschte E-Mails (Spam), Abhörsoftware (Spyware), orchestrierte Kampagnen, die darauf abzielen, Computerressourcen für die beabsichtigten Benutzer und Benutzerinnen unzugänglich zu machen (Distributed-Denial-of-Service-Angriffe (DDoS)), Social-Engineering und Phishing (Arachchilage, Love and Beznosov, 2016, p. 185).

Die Cyber-Bedrohungslandschaft hat sich von rein technischen Methoden (z.B. automatisierte Verbreitung von Malware, Ausnutzung von Schwachstellen aus der Ferne) zu sozio-technischen Methoden wie Social-Engineering entwickelt. Da es sich hierbei um eine technologisch billige und dennoch leistungsstarke Ausnutzungstechnik handelt, ist sie zur bevorzugten Methode von Angreifer und Angreiferinnen geworden (Burda, Allodi

and Zannone, 2020, p. 1). Phishing ist die häufigste Art von Social-Engineering-Angriffen (Sumner *et al.*, 2021, p. 1). Phisher und Phisherinnen nutzen technische, soziale und/oder psychologische Schwachstellen der Menschen aus, um an die sensiblen Daten der Opfer zu gelangen. Diese Informationen werden dann genutzt, um finanzielle Vermögenswerte zu stehlen oder andere Angriffe zu starten (Abroshan *et al.*, 2021c, p. 44928). Phishing ist wird auch als Online-Identitätsdiebstahl bezeichnet, da es darauf abzielt sensible Informationen zu stehlen (Arachchilage, Love and Beznosov, 2016, p. 185). Beim E-Mail-Phishing nutzen Phisher und Phisherinnen Social-Engineering und Identitätsimitation Techniken, um die Passwörter legitimer Benutzer und Benutzerinnen für betrügerische Zwecke zu stehlen (Aleroud and Zhou, 2017, p. 161). Ein Phishing-Angriff wird in der Regel über E-Mails eingeleitet (Chaudhry and Rittenhouse, 2015, p. 28). E-Mail ist ein Kommunikationskanal der als vertrauliches Kommunikationsmittel für den Austausch von Informationen zwischen Einzelpersonen und Organisationen gilt (Wosah and Win, 2021, p. 63). E-Mail ist nach wie vor ein wichtiger Dienst, den Benutzer und Benutzerinnen (vor allem Geschäftskunden) regelmäßig nutzen, um offizielle geschäftliche Aktivitäten durchzuführen, denn (Miranda, 2018, p. 6):

- Die meisten modernen IT-Dienste verlassen sich ausschließlich auf E-Mail, um offiziell mit Kunden und Kundinnen zu kommunizieren (Miranda, 2018, p. 6).
- Die Bereitstellung und Verwaltung von Berechtigungsnachweisen erfordert in der Regel ein E-Mail-Konto als Teil des Prozesses (Miranda, 2018, p. 6).
- Eine E-Mail ist die bequemste Methode, um die Kommunikation mit mehreren Diensten in einer einzigen Identität zusammenzufassen (Miranda, 2018, p. 6).
- Die Hürden und Gesamtkosten für das Senden und Empfangen von E-Mails sind sehr niedrig, wenn nicht sogar kostenlos (Miranda, 2018, p. 6).
- Eine E-Mail-Adresse wird als Synonym für die Online-Identität einer Person wahrgenommen (Miranda, 2018, p. 6).

Eine Phishing-E-Mail enthält meist einen Link zu einer bösartigen Website. Der Trick besteht darin, das Opfer dazu zu verleiten, die gefälschte Website zu besuchen. Daraufhin wird versucht Besucher und Besucherinnen dazu zu bringen, einen Benutzer- bzw. Benutzerinnennamen und ein Passwort oder andere persönliche Daten einzugeben. Eine Phishing-Website wird in der Regel erstellt, um Malware zu installieren oder um an persönliche Daten wie Kreditkartennummern, persönliche Identifikationsnummern (PINs), Sozialversicherungsnummern, Banknummern und Passwörter zu gelangen (Chaudhry and Rittenhouse, 2015, p. 28).

Es wird deutlich, dass Social-Engineering in hohem Maße auf menschlicher Interaktion beruht und oft psychologische Tricks beinhaltet (Aleroud and Zhou, 2017, p. 161), die bei dem Opfer Neugier, Empathie, Aufregung, Angst und/oder Gier auslösen können (B. Kim, 2014, p. 117). Dies führt dazu, dass die Opfer zu Taten bewegt werden, die sie normalerweise nicht getan hätten (Aleroud and Zhou, 2017, p. 161). Indem sie das begrenzte Sicherheitswissen oder Awareness der Menschen ausnutzen, vermeiden Phisher und Phisherinnen nicht nur den Einsatz komplexer und kostspieliger Angriffe (Burda *et al.*, 2020, p. 1), sondern verleiten Online-Nutzer und Nutzerinnen auch dazu, ihre sensiblen Daten preiszugeben oder verdächtige Inhalte in ihre Systeme einzuschleusen (Aleroud and Zhou, 2017, p. 161). PayPal, eBay, American Online, Google und Microsoft sind einige bekannte Unternehmensfälle, wo die Kunden und Kundinnen durch Phishing-Angriffe geschädigt wurden (Frauenstein and von Solms, 2013, p. 197). Phishing spielte auch eine Rolle bei dem ersten erfolgreichen Cyberangriff auf ein Stromnetz, der im Dezember 2015 in der Ukraine stattfand. IT- und Netzwerk-Administratoren und -Administratorinnen bzw. -Mitarbeiter und -Mitarbeiterinnen in diesen Bereichen aus verschiedenen Unternehmen, die für die Stromverteilung in der Ukraine zuständig waren, wurden mit Phishing-Attacken angegriffen. Der Angriff erfolgte über ein bösartiges Microsoft Word-Dokument, das eine Aufforderung zur Aktivierung von Makros enthielt. Sobald das Makro angeklickt wurde, installierte es die Malware BlackEnergy auf dem System und verschaffte den Angreifer und Angreiferinnen eine Hintertür. Dies führte schließlich zur erfolgreichen Abschaltung von 30 Umspannwerken und ließ 230.000 Menschen für bis zu sechs Stunden ohne Strom. Dieses Beispiel zeigt, wie mächtig und verheerend ein gut geplanter und gut durchgeführter Phishing-Angriff sein kann. Es ist auch klar, dass selbst geschulte IT-Experten und IT-Expertinnen diese Art von Angriffen oft nicht erkennen können (Alabdan, 2020, p. 3). Laut der britischen Cybersicherheitsstrategie 2016-2021 und weltweiten Statistiken haben fast alle erfolgreichen Cyberangriffe einen menschlichen Einfluss. Das bedeutet, dass es bei der Cybersicherheit nicht nur um die Technologie geht, sondern dass auch menschliches Wissen über Sicherheit für die Stabilität der Cybersicherheit erforderlich ist. Wird eine bösartige E-Mail vom Benutzer oder Benutzerin ignoriert, ist der Angriff sofort und ohne Verlust beendet (Wosah and Win, 2021, p. 63). Cybersicherheit ist der Schutz von Netzwerken, Informationen und Software im Cyberspace. Ein Informationssystem gilt als anfällig für Angriffe, wenn die Verteidigungsmaßnahmen schwach sind. Die schwache Verteidigung kann von Menschen, Maschinen oder Software ausgehen (Akpon-Ebiyonare, 2019, p. 88).

Phisher und Phisherinnen nutzen die von ihnen gesammelten Informationen, um an vertrauliche Informationen zu gelangen, die das gesamte System eines Unternehmens umfassen und dessen Ruf gefährden können. Selbst etwas so Einfaches wie eine Unternehmenswebsite kann sich als Quelle nützlicher Informationen für Phishing-Angriffen erweisen. Der Zugang zu bestimmten Details über das Unternehmen können Phisher und Phisherinnen nutzen, um sich besser als potenzielle Kollegen und Kolleginnen oder Geschäftskontakte auszugeben, wodurch es einfacher wird ihre Opfer zu täuschen (Rutherford, 2018, p. 6). Um die Informationen und Systeme der Benutzer und Benutzerinnen zu schützen, ist nicht nur die richtige Technologie erforderlich, sondern auch die menschliche Seite der Sicherheit sollte beachtet werden, denn Technologie allein reicht nicht aus, um Informationssicherheit zu gewährleisten (B. Kim, 2014, p. 116). Cybersecurity Awareness bedeutet nicht nur die Bereitstellung von Schulungsprogrammen für Benutzer und Benutzerinnen oder Mitarbeiter und Mitarbeiterinnen, sondern auch die Steigerung der Awareness dieser Personen für das Thema Cybersecurity und für die richtige Reaktion auf Cyberbedrohungen oder Cyberangriffe (Miranda, 2018, p. 4). Daher ist es für Unternehmen von entscheidender Bedeutung, ihre Mitarbeiter und Mitarbeiterinnen in Bezug auf ihre Verantwortung für die Sicherheit des Unternehmens zu schulen. Die Unternehmensleitung muss nicht nur Geld in die Infrastruktur und in technische Kontrollen investieren, sondern auch dafür sorgen, dass ein positives Sicherheitsverhalten Teil des Geschäftsprozesses wird und die Mitarbeiter und Mitarbeiterinnen zur ersten Verteidigungslinie des Unternehmens werden (Sebescen and Vitak, 2017, p. 2237). Um dies zu erreichen, ist ein tieferes Verständnis der Opferprofile, der Angriffsarten, der Phishing-Tools, der Methoden und der Studien unerlässlich, um herauszufinden, was Phishing-Angriffe so erfolgreich macht (Ferreira and Vieira-Marques, 2018, p. 225). Aufgrund dessen werden die nächsten Kapitel sich mit diesen Themenbereichen auseinandersetzen.

## 2.2 Social-Engineering

Social-Engineering ist ein Akt der Manipulation einer Person, um eine Aktion freiwillig oder unfreiwillig auszuführen. Wie der Begriff Social-Engineering schon besagt, ist dieser Vorgang mit der Sozialwissenschaft verbunden. Social-Engineering-Angriffe sind nicht auf High-Tech-Ausrüstung angewiesen, um einen Angriff zu starten. Sie werden vielmehr durch einen geschickten Angriff auf den Verstand des Opfers ausgeführt (Anawar *et al.*, 2019, p. 2867). Phishing und Spear-Phishing sind Formen des Social-Engineering, bei denen sich der Angreifer oder die Angreiferin als vertrauenswürdige Person ausgibt, um

an sensible Informationen zu gelangen (Sebescen and Vitak, 2017, p. 2238). Social-Engineers verkaufen die erworbenen sensiblen Informationen, um aus den wertvollen Daten Kapital zu schlagen. Social-Engineering-Angriffe bestehen aus einer Reihe von Schritten. Es gibt vier gängige Phasen (Mashtalyar *et al.*, 2021, p. 417) und Kaabouch (2019) definiert die vier Phasen als (Antonucci *et al.*, 2020, p. 3):

(1) Informationsbeschaffung (Antonucci *et al.*, 2020, p. 3).
(2) Kontaktaufnahme (Antonucci *et al.*, 2020, p. 3).
(3) Ausnutzung und Ausführung (Antonucci *et al.*, 2020, p. 3).
(4) Ausstieg (Antonucci *et al.*, 2020, p. 3).

In der Phase der Informationsbeschaffung werden Informationen über ein Opfer gesammelt, auch bekannt als Reconnaissance. In der Phase der Kontaktaufnahme wird das Opfer geködert. In der Ausnutzung- und Ausführungsphase führt der Angreifer oder die Angreiferin den Angriff aus, während in der Ausstiegsphase Maßnahmen ergriffen wird, um alle Spuren des Angriffs zu beseitigen (Antonucci *et al.*, 2020, p. 3).

Social-Engineering-Angriffe können entweder als menschliche oder als computerbasierte Angriffe kategorisiert werden. Computergestützte Angriffe basieren auf Technologie, um eine Person dazu zu verleiten, vertrauliche Informationen preiszugeben. Die einfachsten und beliebtesten Social-Engineering-Angriffe sind menschengestützt (Younis and Musbah, 2020, p. 1). Dabei erhalten Benutzer und Benutzerinnen in der Regel eine E-Mail von einer scheinbar etablierten Organisation und werden aufgefordert, ihre Daten preiszugeben. Diese E-Mails sind in der Regel mit authentischen Bildern und Logos versehen die vortäuschen, dass diese Nachrichten von einem bekannten Unternehmen oder einer Organisation stammen (Zielinska *et al.*, 2014, p. 1466). Um glaubwürdige Social-Engineering-Artefakte zu erstellen, müssen Angreifer und Angreiferinnen verschiedene Aspekte der menschlichen Kognition und Psychologie berücksichtigen. Diese Aspekte stehen oft im Zusammenhang mit bestimmten Merkmalen des Angriffsopfers. Menschen können manipuliert werden, indem ihre Gewohnheiten, Motive und kognitiven Neigungen ausgenutzt werden (Allodi *et al.*, 2020, p. 2). Im Folgenden wird speziell auf Phishing näher eingegangen.

## 2.3 Phishing

Die Zahl der Phishing-Angriffe ist seit des COVID-19-Ausbruchs stetig gestiegen (Abroshan *et al.*, 2021b, p. 121916). Phisher und Phisherinnen nutzten die COVID-19-Pandemie, um die Auswirkungen von Phishing-Angriffen auf die Welt zu verstärken

(Patayo, 2021, p. 2). Das Auftreten der COVID-19-Pandemie hat auch die Geschäftsmodelle, das Verhalten und den Lebensstil der Menschen drastisch verändert, was dazu geführt hat, dass sie von zu Hause aus arbeiten und sich aus der Ferne mit der IT-Infrastruktur ihres Unternehmens verbinden (Chigada and Madzinga, 2021, p. 1). Während der Pandemie, haben Personen beispielsweise E-Mails mit wichtigen und aktuellen Informationen über die Coronavirus-Situation erhalten. Diese E-Mail-Flut konnten sich Cyber-Angreifer und -Angreiferinnen in der Pandemie zunutze machen und anfällige Opfer anvisieren (Abroshan *et al.*, 2021b, pp. 121916–121917). Die Angreifer und Angreiferinnen gaben sich als Weltgesundheitsorganisation (WHO) oder Seuchenkontrolle aus (Patayo, 2021, p. 2), um die Menschen dazu zu bringen auf Phishing-Links zu klicken oder bösartige Anhänge zu öffnen. So erhielten die Benutzer und Benutzerinnen während der Pandemie sowohl die üblichen Phishing-E-Mails als auch COVID-19 Phishing-E-Mails (z.B. Angebote für schnelle Infektionstests, Produkte zur Behandlung oder Prävention der Krankheit) (Abroshan *et al.*, 2021b, p. 121917).

Laut dem Sicherheitsunternehmen Barracuda Networks, haben seit Anfang Januar 2020 die COVID-19-bezogenen E-Mail-Phishing-Angriffe stetig zugenommen, gefolgt von einem plötzlichen Anstieg um 667% bis Ende Februar (Frauenstein and Flowerday, 2020, p. 2). Zwischen Februar und April 2020 haben Cyberangriffe auf Finanzinstitute weltweit um mehr als 238% zugenommen, zu einer Zeit als die Weltwirtschaft unermüdlich an der Bekämpfung der COVID-19-Infektionen arbeitete (Chigada and Madzinga, 2021, p. 4). In der ersten Aprilwoche 2020 meldete Google täglich 18 Millionen Malware- und Phishing-E-Mails mit Bezug zu COVID-19 (Desolda *et al.*, 2021, p. 6). Palo Alto Networks stellte fest, dass von Januar bis März 2020 116.357 neue Domänen mit COVID-19-bezogenen Schlüsselwörtern registriert wurden. Das Unternehmen stellte fest, dass 34% dieser Domänen ein hohes Risiko darstellten (Mashtalyar *et al.*, 2021, p. 418). Das australische Institut für Kriminologie stellte fest, dass zwischen Februar und März 2020 die Zahl der bösartigen URLs (Universal Resource Locators) weltweit um mehr als 260% gestiegen ist. Die WHO, das World Economic Forum (WEF), Google und das Center for Disease Control and Prevention (CDC) gaben an, dass es mehr als 86.000 neue aktive, riskante und bösartige Domänen im Zusammenhang mit der COVID-19-Pandemie gibt (Chigada and Madzinga, 2021, p. 6). Die Anti-Phishing Work Group meldete eine Gesamtzahl von 298.012 Phishing-Vorfällen mit 122.092 Phishing-Angriffen vom 1. Mai bis 31. Juli 2020 (Manoharan *et al.*, 2021, p. 2). Aus dem Internet Crime Report des FBI geht hervor, dass im Jahr 2020 allein durch die Kompromittierung von Geschäfts-E-Mails Verluste in Höhe

von über 1,8 Milliarden Dollar entstanden sind, weit mehr als bei jeder anderen Art von Internetkriminalität (Jayatilaka, Arachchilage and Babar, 2021, p. 1).

Wie auch bei der COVID-19 Pandemie passen Angreifer und Angreiferinnen ihre Kampagnen oft an aktuelle Ereignisse an, um die vermeintliche Legitimität von Phishing-E-Mails zu erhöhen. So begannen beispielsweise russische Hacker und Hackerinnen, kurz nach der Veröffentlichung der Wahlen in den Vereinigten Staaten von Amerika im Jahr 2016, mit gefälschten E-Mail-Adressen der Harvard University bösartige Zip-Dateien im Anhang zu versenden, in denen angeblich erklärt wird warum amerikanische Wahlen fehlerhaft sind (Jampen *et al.*, 2020, pp. 1–2). Berichten zufolge gab es auch Phishing-Angriffe auf die US-Regierung. Während des Wahlzyklus 2016 wurde die Democratic National Convention (DNC) Opfer eines Cyberangriffs. Die Hacker und Hackerinnen haben das E-Mail-Konto des Vorsitzenden der Präsidentschaftskampagne von Hillary Clinton, John Podesta gehackt. John Podesta erhielt eine Phishing-Mail an sein persönliches Gmail-Konto (Gupta, Arachchilage and Psannis, 2018, p. 249), in der er durch Social-Engineering Techniken dazu aufgefordert wurde (Adil, Khan and Nawaz Ul Ghani, 2020, p. 2) auf einen Link zu klicken. Die Phishing-E-Mail warnte ihn sein Passwort sofort zu ändern. Die URL innerhalb der E-Mail führte jedoch nicht zu einer sicheren Google-Website (Gupta, Arachchilage and Psannis, 2018, p. 249). Nachdem er das Passwort seines Kontos geändert hat, wurden die aktuellen Anmeldedaten seines Kontos für die Hacker und Hackerinnen offengelegt und später stellte er fest, dass sein Konto gehackt wurde. Dies war ein einfaches Beispiel für einen Phishing-Angriff, bei dem John Podesta durch Social-Engineering überzeugt wurde seine Kontodaten freizugeben (Adil, Khan and Nawaz Ul Ghani, 2020, p. 2).

### 2.3.1 Definition

Das Oxford English Dictionary definiert Phishing als, die betrügerische Praxis des Versendens von E-Mails, die vorgeben von seriösen Unternehmen zu stammen, um Personen dazu zu bringen, persönliche Informationen wie Passwörter und Kreditkartennummern preiszugeben (Jansson and von Solms, 2013, p. 584). Das National Institute of Standards and Technology definiert Phishing als den Vorgang, bei dem Personen durch betrügerische Mittel zur Preisgabe persönlicher Informationen verleitet werden (Gordon *et al.*, 2019, p. 547). Die Anti Phishing Working Group definiert Phishing als den Diebstahl von sensiblen persönlichen Daten wie Benutzer- und Benutzerinnennamen, Passwörtern, Kreditkarteninformationen und Online-Banking-Daten (Fernando and Arachchilage, 2020, p. 2). Der Begriff Phishing ist auch eine

Abwandlung des Wortes "fishing" (Qabajeh, Thabtah and Chiclana, 2018, p. 45), wobei der Akt des Phishings dem des Angelns in folgender Weise ähnelt. Der Angreifer oder die Angreiferin lockt das Opfer (Chiew, Yong and Tan, 2018, p. 1), um vertrauliche Informationen zu erlangen, wobei meist gefälschte E-Mails und Websites (Frauenstein and von Solms, 2013, p. 197) als Köder eingesetzt werden, um nach persönlichen oder vertraulichen Informationen des Opfers zu fischen (Chiew, Yong and Tan, 2018, p. 1). Es gibt einen kleinen Unterschied zwischen Spam-Mails und Phishing-Mails. Spam-Mails sind unaufgeforderte Nachrichten die zu kommerziellen Zwecken verschickt werden, oft in großen Mengen. Zum Beispiel ein Gesundheits- und Medizinunternehmen, das für die eigene Produkte wirbt. Phishing-Nachrichten hingegen sind eine Untergruppe von Spam-Nachrichten, wo sich Angreifer und Angreiferinnen sich als jemand anderes ausgeben (Bhadane and Mane, 2018, pp. 1–2).

### 2.3.2 Herkunft

Der Ausdruck "Phishing" kommt von "Phone Phreaking", einer in den 1970er Jahren sehr verbreiteten Technik mit der Telefonsysteme angegriffen wurden (Gupta *et al.*, 2017, p. 3629). Damals bezeichnete Phone Phreaking ein elektronisches Gerät namens "Blue Box", das in der Lage war dieselben Frequenzen wie die Telefongesellschaften auszusenden und damit kostenlose Anrufe zu ermöglichen (M. Alwanain, 2019, p. 480). Der Begriff Phishing tauchte erstmals in den späten 1990er Jahren auf (Mitchell, 2020, p. 3), als Phisher und Phisherinnen versuchten an die Kontodaten registrierter Online-Nutzer und -Nutzerinnen des Internetanbieters America Online (AOL) zu gelangen. Damals nutzten Phisher und Phisherinnen häufig Instant Messages (IM) in AOL-Chaträumen oder E-Mails, um ihre Opfer zu erreichen, damit diese ihre Passwörter preisgeben. Diese wurden dann von den Phisher und Phisherinnen verwendet, um die Konten der Opfer zu übernehmen und Spam-Mails an andere Online-Benutzer und -Benutzerinnen zu versenden. Offensichtlich haben die Phisher und Phisherinnen erkannt, dass sie ihre Opfer noch weiter betrügen können, wenn sie in den IMs und E-Mails aufgefordert werden ihre Rechnungsdaten zu aktualisieren. Mit dieser Erkenntnis weiteten die Angreifer und Angreiferinnen das Ziel aus und versuchten mit denselben elektronischen Mitteln (IMs und E-Mails) an andere Finanzdaten der Opfer heranzukommen, wie z.B. Sozialversicherungsnummern, Adressen und Kreditkarteninformationen (Qabajeh, Thabtah and Chiclana, 2018, p. 46).

Obwohl es Phishing mindestens seit 1995 gibt (der Begriff Phishing wurde 1996 zum ersten Mal verwendet (Baki and Verma, 2021, p. 1) und 1997 erstmals in den Medien

abgedruckt (Alabdan, 2020, p. 1)), ist es nach wie vor eine weit angewandte und beliebte Angriffsmethode. Der Grund für diesen Erfolg ist, dass diese Angriffe auf den menschlichen Empfänger und Empfängerinnen abzielen und keine technischen Abwehrmechanismen wie Firewalls durchdringen müssen (Baki and Verma, 2021, p. 1). Die akademischen Forscher und Forscherinnen haben jedoch erst 2004 damit begonnen, Studien über Phishing zu veröffentlichen. Die erste nutzer- bzw. nutzerinnenzentrierte Studie stammt aus dem Jahr 2005 (Das *et al.*, 2019, p. 4). Die ersten Fälle von Phishing-Schulungen wurden als "The West Point Carronade Exercise" bezeichnet. Diese Übung zur Awareness Steigerung für E-Mail-Sicherheit sollte sicherstellen, dass die Kadetten der U.S. Militärakademie gute E-Mail-Sicherheitspraktiken ausüben (Arduin, 2020, p. 12).

### 2.3.3 Kategorie

Es gibt verschiedene Arten von Phishing-Angriffen, die derzeit weit verbreitet sind (Damodaram, 2016, p. 701), dabei können Angriffstechniken in zwei Kategorien eingeteilt werden: Angriffsstart und Datensammlung. Für die Kategorie Angriffsstart wurden mehrere Techniken identifiziert, wie z.B. E-Mail-Spoofing, URL-Spoofing und Website-Spoofing (Basit *et al.*, 2021, pp. 140–141). Die Kategorie Datensammlung wird verwendet, um Daten von Opfern zu sammeln. Dieser Prozess kann während und nach der Interaktion des Opfers stattfinden. Die Datensammlung kann entweder manuell oder automatisch erfolgen. Automatisierte Techniken stützen sich hauptsächlich auf die Erstellung gefälschter Webformulare, Key Logger, aufgezeichneter Nachrichten, automatisierter Social-Engineering Bots und gefälschter Veranstaltungseinladungen (Aleroud and Zhou, 2017, p. 167). Bezüglich der automatisierten Datenerfassung kann festgehalten werden, dass gefälschte Webformulare die am häufigsten verwendete automatisierte Technik zur Datenerfassung beim Web-Spoofing sind. Andere Techniken wie Recorded Messages sammeln Daten aus Benutzer- bzw. Benutzerinneninteraktionen, wenn Angriffe über Telefone oder andere Voice-over-IP-Angriffe initiiert werden. In sozialen Netzwerken werden die öffentlichen Daten über Benutzer und Benutzerinnen genutzt, die für die Initialisierung von Social-Engineering-Angriffen erforderlich sind. Der Social-Engineering-Prozess beginnt in der Regel mit dem Sammeln von Hintergrundinformationen über die potenziellen Angriffsziele. Trotz der verschiedenen Online-Quellen, die in der Regel zum Sammeln von Informationen über potenzielle Opfer verwendet werden, nutzen Angreifer und Angreiferinnen heutzutage Social-Networking-Sites, aufgrund der explosionsartigen Verbreitung dieser Dienste. Außerdem erleichtern soziale Netzwerke die Automatisierung von Angriffen, da sie Daten in maschinenlesbarer

Form bereitstellen. Darüber hinaus dienen soziale Netzwerke auch als Kommunikationsplattformen, indem Dienste wie private Nachrichten und Chats von automatisierten Social-Engineering-Bots zur Datensammlung genutzt werden können. Mithilfe dieser Daten können Angreifer und Angreiferinnen beispielsweise Mitglieder und Mitgliederinnen von LinkedIn (einer professionellen Networking-Website) gefälschte Jobangebote senden und fordern sie im Zuge dessen auf, private Informationen anzugeben. Die manuelle Datenerfassung erfolgt durch menschliche Täuschung oder andere einfachere Techniken wie Beziehungen in sozialen Netzwerken. Die menschliche Täuschung sammelt sensible Daten über die Opfer durch direkte Interaktion (Aleroud and Zhou, 2017, p. 167). Phishing-Angriffe können wie folgt gruppiert werden (Papatsaroucha *et al.*, 2021, p. 13):

- Technikbasierte Angriffe, bei denen Informationen über das Opfer über das Internet gesammelt werden (z.B. über kompromittierte Websites) (Papatsaroucha *et al.*, 2021, p. 13).
- Sozial basierte Angriffe, bei dem der Angreifer oder die Angreiferin eine Beziehung zum Opfer aufbaut und das Vertrauen und die Emotionen des Opfers ausnutzt (Papatsaroucha *et al.*, 2021, p. 13).
- Physisch basierte Angriffe, bei denen Informationen über das Opfer durch physische Aktionen erlangt werden (Papatsaroucha *et al.*, 2021, p. 13).

Die gesamte Technik des Phishings kann in drei Komponenten unterteilt werden: Das Medium, der Vektor und der technische Ansatz (Alabdan, 2020, pp. 5–6). Alle Phishing-Angriffe erfordern eine Interaktion des Opfers, damit ein Phishing-Angriff erfolgreich ist, und für die Interaktion ist ein Medium erforderlich. Phisher und Phisherinnen können sich den potenziellen Opfern über diese drei Medien nähern: Internet, Sprache und Kurznachrichtendienst (SMS) (Chiew, Yong and Tan, 2018, p. 3). Jedes Medium kann einen Vektor verwenden (d.h. das Medium mit dem der Angriff durchgeführt wird) (Desolda *et al.*, 2021, p. 5). Der Vektor ist der Weg des Angriffs und wird oft durch das Medium begrenzt (Alabdan, 2020, p. 6). Die meisten dieser Vektoren stehen mit dem Internet in Verbindung. Daher ist das Internet das beliebteste Medium für Phishing-Angriffe. E-Mail, eFax, Instant Messaging, soziale Netzwerke und Websites sind Vektoren, die mit dem Internet verbunden sind (Chiew, Yong and Tan, 2018, p. 4). Die letzte Komponente ist der technische Ansatz und enthält alle technischen Lösungen, die zur Durchführung eines Phishing-Angriffs zur Verfügung stehen. Jeder Vektor kann sich einen oder mehrere der technischen Ansätze zunutze machen, um den Angriff durchzuführen (Desolda *et al.*, 2021, p. 5). Die technischen Ansätze für Phishing-Angriffe

lassen sich in zwei Kategorien unterteilen: Social-Engineering und Malware-basierte Phishing-Angriffe. Beim Social-Engineering werden die Emotionen der Benutzer und Benutzerinnen ausgenutzt, so dass diese Personen die persönlichen Daten preisgeben. Beim Malware-basierten Phishing-Angriff werden heimlich bösartige Programme installiert, um dem Phisher oder Phisherin Zugriff auf den Computer der Benutzer und Benutzerinnen geben (Apandi, Sallim and Sidek, 2020, p. 2).

#### 2.3.3.1 Medium

Es gibt drei wichtige Medien, über die eine Interaktion mit dem Opfer stattfinden kann, nämlich (Alabdan, 2020, p. 6):

##### 2.3.3.1.1 Sprache

Die Sprache, d.h. das Sprechen und der Gebrauch von Sprache, ist eine der ältesten und effektivsten Methoden, mit denen Menschen interagieren und Informationen übermitteln (Alabdan, 2020, p. 6).

##### 2.3.3.1.2 SMS

In seiner modernen Form ist SMS (Short Messaging Service) als "Texting" bekannt. Dabei handelt es sich um die Kommunikation über kurze Textnachrichten, die über ein Mobilfunknetz verschickt werden. Daraus entwickelte sich später MMS (Multi-Media Messaging Service), mit dem neben Text auch Inhalte wie Fotos, Videos oder Audioclips übertragen werden können (Alabdan, 2020, p. 6).

##### 2.3.3.1.3 Internet

Das letzte betrachtete Medium ist das Internet. Von seinen Anfängen als ARPANET bis hin zu der Masse an Websites, die heute zur Verfügung stehen, bedeutet die sich ständig verändernde und weiterentwickelnde Natur des Internets, dass ständig neue Kommunikationsmethoden entwickelt werden. Diese Sammlung von Kommunikationsmethoden ist an einem einzigen Ort verfügbar und reicht von E-Mail über Instagram bis hin zu Snapchat (Alabdan, 2020, p. 6).

#### 2.3.3.2 Vektor

Im Folgenden werden auf einige Vektoren näher eingegangen.

#### 2.3.3.2.1 Sprache/SMS

Diese beiden Medien haben zu den Phishing-Vektoren Vishing bzw. Smishing geführt. Phisher und Phisherinnen kontaktieren ihre Opfer per Anruf (beim Vishing) oder per Textnachricht (beim Smishing) (Chiew, Yong and Tan, 2018, p. 4).

#### 2.3.3.2.2 E-Mail

Die elektronische Post (E-Mail) ist ein weiterer Vektor, den es zu berücksichtigen gilt (Alabdan, 2020, pp. 7–8).

#### 2.3.3.2.3 EFAX

Internet-Fax, eFax oder Online-Fax unterscheidet sich vom herkömmlichen Fax dadurch, dass das Fax über das Internet-Protokoll (IP) und nicht über das Telefonnetz gesendet wird (Chiew, Yong and Tan, 2018, p. 4). Der Vorteil dieser Methode besteht darin, dass Faxe als E-Mails an das Gerät der Empfänger und Empfängerinnen gesendet werden können und somit kein Faxgerät mehr benötigt wird (Alabdan, 2020, p. 8).

#### 2.3.3.2.4 Website

Websites sind ein weiterer beliebter Vektor für Phisher und Phisherinnen. Es ist nämlich inzwischen üblich, dass Benutzer und Benutzerinnen ihre persönlichen Daten wie z.B. Anmeldedaten angeben, um Zugang zu einem bestimmten Dienst zu erhalten. Daher nutzen Phisher und Phisherinnen diesen Vektor aus, um ihre Opfer dazu zu bringen, die persönlichen Daten so zu übermitteln, wie es die Opfer normalerweise auf einer legitimen Website tun (Chiew, Yong and Tan, 2018, p. 4).

#### 2.3.3.2.5 Wi-Fi

Wi-Fi-Phishing findet in der Regel an öffentlichen Hotspots statt und ist daher normalerweise eine nicht zielgerichtete Form des Phishing-Angriffs. Allerdings könnte dieser Vektor auch für einen Spear-Phishing-Angriff verwendet werden, bei dem ein bestimmter öffentlicher Hotspot ausgewählt wird, weil eine bestimmte Zielperson diesen regelmäßig besucht und nutzt. Wi-Fi-Phishing kann verschiedene Formen annehmen. Die übliche Form ist die Installation von Malware auf dem Gerät des Opfers, um Anmeldedaten abzufangen oder auf gefälschte Websites umzuleiten. Es gibt auch Methoden, die den Verkehr der Nutzer und Nutzerinnen in diesen Netzwerken abfangen, um persönliche Daten zu stehlen (Alabdan, 2020, p. 9).

#### 2.3.3.2.6 Soziales Netzwerk

In den 2000er Jahren wurden die sozialen Medien beliebter, da sie es den Menschen ermöglichten (Chiew, Yong and Tan, 2018, p. 4), mit anderen Menschen in Kontakt zu treten, sich zu vernetzen und ihre Erfahrungen auszutauschen (Alabdan, 2020, p. 8). Dieser Bereich der sozialen Medien wird oft als soziales Netzwerk bezeichnet (Chiew, Yong and Tan, 2018, p. 4). Beispiele dafür sind Twitter, Facebook und LinkedIn, die es Nutzer und Nutzerinnen ermöglichen, sich mit anderen Nutzer und Nutzerinnen zu verbinden. Dadurch können die User und Userinnen andere User und Userinnen identifizieren, die dieselben Interessen, Lebensansichten oder Hobbys teilen. Diese Art des Austauschs von persönlichen Details im Internet ist eine hervorragende Ressource für Phisher und Phisherinnen, um Zielgruppen zu identifizieren und potenzielle Opfer anzusprechen (Alabdan, 2020, p. 8).

#### 2.3.3.2.7 Sofortnachricht

Sofortnachricht ist auch unter dem Begriff Instant Messaging (IM) bekannt. IM war eine der ersten Formen der Online-Kommunikation und wurde zunächst als IRC (Internet Relay Chat) eingeführt. Später wurden Instant-Messaging-Systeme wie MSN Messenger und Yahoo! Messenger entwickelt. Heutzutage werden diese Formen von Instant Messenger in der Regel mit anderen sozialen Medien kombiniert, wie z.B. Facebook Messenger. Es gibt auch Instant Messenger-Clients, die nicht direkt mit sozialen Medien verbunden sind, wie WhatsApp und Telegram. Des Weiteren sind Nachrichten nicht mehr nur textbasiert, sondern können auch Emojis, Fotos, Gifs, Dateien und Hyperlinks enthalten. Außerdem kann der IM-Client auch Funktionen für Audio- und Videoanrufe bieten. Diese Art der Kommunikation ist inzwischen weitaus beliebter als SMS-Nachrichten, was sie zu einem idealen Umfeld für Phisher und Phisherinnen macht. Online-Chats in Echtzeit ermöglichen es Phisher und Phisherinnen, ein Opfer anzusprechen und es mit Hilfe von Betrügereien dazu zu bringen, persönliche Daten preiszugeben (Alabdan, 2020, p. 8).

#### 2.3.3.2.8 Blog und Forum

Betrug bei der Online-Jobsuche und Spendenbetrug sind eine von wenigen Beispiele für Phishing-Angriffe, die auf Blogs und Foren abzielen. Online-Job-Betrügereien werden beispielsweise eingesetzt, um die Anmeldedaten von Arbeitssuchenden zu sammeln. In der Regel handelt es sich bei diesen Anzeigen um die Namen gefälschter Organisationen, die auf verschiedenen Stellensuch-Websites angezeigt werden. Wenn ein Benutzer oder

Benutzerin Interesse an einer Anzeige zeigt, wird diese Person aufgefordert z.B. die Anmeldedaten anzugeben. Beim Spenden-Phishing werden soziale, politische oder natürliche Ereignisse ausgenutzt, um nach Spenden zu bitten. Dabei werden Benutzer aufgefordert Informationen über ihre Kreditkarten anzugeben (Aleroud and Zhou, 2017, pp. 164–165).

#### 2.3.3.3 Technischer Ansatz

Es gibt einige technische Ansätze, die für die Durchführung von Phishing-Angriffen genutzt werden können und diese werden näher erläutert.

##### 2.3.3.3.1 Telefon Phishing

Telefon-Phishing ist eine kriminelle Aktivität, bei der böswillige Angreifer und Angreiferinnen einen Social-Engineering-Angriff über ein Telefon oder Mobiltelefon durchführt, um an sensible und private Informationen zu gelangen. Dies passiert entweder durch Anrufe, Nachrichten oder durch das Versenden von bösartiger Links an das Opfer (Arshad *et al.*, 2021, p. 166). Beim Telefon-Phishing gibt es mehrere Angriffsformen: Sprach Phishing, SMS Phishing und App Phishing (Alabdan, 2020, p. 20). Phishing-Versuche auf mobilen Geräten sind für Benutzer und Benutzerinnen schwieriger zu erkennen, weil die Geräte meist einen kleineren Bildschirm haben. Dadurch werden z.B. die URLs nicht vollständig angezeigt und die Überprüfung der Legitimität wird demzufolge schwieriger (Aleroud and Zhou, 2017, pp. 165–166).

##### 2.3.3.3.2 Sprach Phishing

Sprach bzw. Voice Phishing (Vishing) ist eine Phishing-Methode, bei der die Stimme benutzt wird (Alabdan, 2020, p. 7). User und Userinnen erhalten z.B. eine Sprachnachricht: Das Microsoft Windows-Lizenzschlüssel ist abgelaufen, bitte rufen Sie 866-978-7540 an. Es handelt sich dabei um eine betrügerische Sprachnachricht, in der die betroffenen Personen nach den Anmeldedaten gefragt werden (Arshad *et al.*, 2021, p. 167). Vishing verwendet gefälschte Daten, um den Anschein zu erwecken, dass die Anrufe von einer vertrauenswürdigen Organisation kommen (Damodaram, 2016, p. 702). Mit Hilfe von Voice over IP wird der tatsächliche physische Standort, von wo der Anruf ausgeht, verschleiert (Alabdan, 2020, p. 7).

#### 2.3.3.3.3 SMS Phishing

Phishing-Angriffe finden nicht nur per E-Mail statt, sondern auch per SMS (Jakobsson, 2018, p. 6). Das Medium SMS/MMS ist für den Vektor des Smishings verantwortlich. Es gibt zwei Hauptansätze, die diese Methode verwenden. Bei der ersten Methode wird eine SMS verschickt, die vorgibt eine vertrauenswürdige Behörde (z.B. eine Bank) zu sein. Das Opfer wird dann auf eine betrügerische Website weitergeleitet. Daraufhin wird die Person aufgefordert sich auf der Seite anzumelden oder bestimmte Identifikationsdaten anzugeben. Sobald dies geschehen ist, können die Angreifer und Angreiferinnen die gesammelten Informationen zum eigenen Vorteil nutzen. Die andere Methode besteht darin, dem Opfer eine SMS zu schicken, die entweder direkt Malware enthält oder einen Link zu einer Website mit Malware enthält (Alabdan, 2020, p. 7).

Eine besonders wirkungsvolle Phishing-Technik ist der Verifizierungscode-Weiterleitungsangriff. Bei diesem Ansatz greifen die Angreifer und Angreiferinnen auf einen Dienstanbieter oder eine Dienstanbieterin zu und fordern einen SMS-Code an, um das Passwort für einen bestimmten Benutzer oder Benutzerin zurückzusetzen. Unmittelbar danach senden die Angreifer und Angreiferinnen eine gefälschte Textnachricht an die Benutzer und Benutzerinnen, in der vorgegeben wird der Dienstanbieter oder die Dienstanbieterin zu sein und fordern das Opfer um Zusendung des Codes als zusätzliche Überprüfungsmaßnahme (Jakobsson, 2018, p. 6).

Die Einfachheit einer Textnachricht bedeutet auch, dass diese viel leichter zu fälschen ist als eine E-Mail. Es gibt keine Schriftarten oder Farben, die angepasst werden müssen. Ebenso werden sich nur sehr wenige Personen dafür interessieren oder bemerken, dass die SMS von einer anderen Nummer stammt. Dahingegen kann eine andere E-Mail-Adresse für aufmerksame Benutzer und Benutzerinnen ein Indikator für einen Betrug darstellen. Anders als bei E-Mails werden die gefälschten Nachrichten nicht routinemäßig abgefangen oder herausgefiltert (Jakobsson, 2018, p. 6).

#### 2.3.3.3.4 APP Phishing

Ein Beispiel für APP Phishing: Kürzlich wurde eine mobile Anwendung namens CovidLock (Ransomware) von Angreifer und Angreiferinnen entwickelt. Die Angreifer und Angreiferinnen behaupteten, dass die App entwickelt wurde, um COVID-19-Fälle zu verfolgen. Es stellte sich jedoch als gefälschte Anwendung heraus, da die Telefone der Opfer gesperrt wurden und diese 48 Stunden Zeit hatten, um 100 Dollar in Bitcoin zurückzuzahlen. Wenn die Opfer das Lösegeld nicht zahlten, drohten die Angreifer und

Angreiferinnen damit die Anmeldedaten zu stehlen und für böse Absichten zu verwenden (Chigada and Madzinga, 2021, p. 8).

#### 2.3.3.3.5 Graphical User Interface Squatting

Graphical User Interface (GUI) Squatting ist eine Art von Phishing-Angriff, der auf mobile Geräte abzielt. Dabei handelt es sich um eine automatisierte Methode zur Generierung plattformunabhängiger Phishing-Apps. Die echte App wird zunächst analysiert und die interaktiven Komponenten der Anmeldeseite werden extrahiert. Auf der Grundlage dieser Analyse wird eine grafische Oberfläche generiert, um die reale Anwendung so gut wie möglich zu imitieren. Anschließend wird ein Täuschungscode eingeschleust, der die persönlichen Daten der Benutzer und Benutzerinnen an einen entfernten Server weiterleitet. 61 Antivirenprogramme waren nicht in der Lage, die generierte App als bösartig zu erkennen. Mit dieser Methode werden hochwertige Kopien bestehender Apps erstellt, die in der Lage sind, bestehende Phishing-Präventions- und Erkennungstechniken zu umgehen, um die Anmeldedaten von Benutzer und Benutzerinnen zu stehlen (Alabdan, 2020, p. 21).

#### 2.3.3.3.6 Quick Response Code Phishing

Ein Quick Response (QR) Code ist eine Matrix mit einem Layout aus schwarzen und weißen Pixeln, die zum Speichern und Übermitteln komprimierter Informationen verwendet werden. Zweidimensionale QR-Codes ersetzen schnell die veralteten eindimensionalen Barcodes, da sie besser lesbar sind und mehr Informationen enthalten. Um auf die in einem QR-Code gespeicherten Informationen zuzugreifen, werden diese mit einem Scan gelesen. Anschließend dekodiert ein QR-Code-Lesegerät die im QR-Code enthaltenen Informationen und verarbeitet diese, indem es z.B. einen App-Store öffnet, wenn der QR-Code eine neue Anwendung für mobile Geräte bewirbt. Aufgrund der wachsenden Zahl intelligenter mobiler Geräte werden QR-Codes von Unternehmen häufiger sowohl intern (z.B. zur Nachverfolgung, Bezahlung und für Rabatte) als auch extern verwendet, um Menschen auf ihre Websites, Apps und Produkte zu leiten. QR-Codes sind inzwischen häufig auf Produktverpackungen, Zeitungen und Plakatwänden zu sehen. Leider hat die Leichtigkeit, mit der QR-Codes hergestellt und verbreitet werden können, die Codes zu einer idealen Methode für Phishing-Angriffe gemacht. Dies wird noch dadurch verstärkt, dass Menschen den Inhalt eines QR-Codes nicht verstehen können, bevor dieser mit einem QR-Code-Lesegerät entschlüsselt werden. Außerdem führen viele QR-Code-Lesegeräte die Aktion zum Lesen des Inhalts ohne vorher die

Zustimmung der Benutzer und Benutzerinnen einzuholen, z.B. das Öffnen einer URL in einem Browser. Um bei diesem Beispiel zu bleiben: Ein Phisher oder eine Phisherin könnte in einem Gebiet QR-Codes platzieren, die vorgeben Werbung für ein seriöses Produkt oder Unternehmen zu sein. Dann leiten die QR-Codes die Benutzer und Benutzerinnen zu einer bösartigen URL weiter, wo ein Drive-by-Download stattfindet. Das Gerät des Opfers wird somit infiziert, bevor es auf die legitime Website weitergeleitet wird. Das Opfer merkt nichts von dem Angriff, hat aber nun ein kompromittiertes Gerät, das die persönlichen Daten an den Phisher oder Phisherin übermittelt (Alabdan, 2020, p. 12).

#### 2.3.3.3.7 E-Mail Phishing

Phishing-Angriffe sind in der Regel "hit-or-miss"-Angriffe, bei denen der Angreifer oder die Angreiferin nur einen Versuch unternimmt (Allodi *et al.*, 2020, p. 4). Es wird auch als Bulk-Phishing bezeichnet, weil der Ansatz nicht speziell auf Empfänger und Empfängerinnen zugeschnitten sind und der Erfolg des Betrugs davon abhängt das genügend Personen erreicht werden (Furnell, Millet and Papadaki, 2019, p. 11). Eine Phishing-E-Mail leiten Benutzer und Benutzerinnen in der Regel auf eine Website weiter, auf der aufgefordert wird, persönliche Daten zu aktualisieren, z.B. ein Passwort, Kreditkarten-, Sozialversicherungs- oder Bankkontonummern. Das Absenderfeld bzw. Absenderinnenfeld scheint, von dem in der E-Mail erwähnten legitimen Unternehmen zu stammen. Es ist jedoch wichtig zu wissen, dass es sehr einfach ist, dieses Feld für jeden E-Mail-Client zu ändern. Die E-Mail enthält einen Link oder Hyperlink zu einer Website mit einem ähnlichen URL-Namen wie der des echten Absenders oder der echten Absenderin (Damodaram, 2016, p. 702).

#### 2.3.3.3.8 Spear Phishing

Spear-Phishing-Kampagnen werden speziell für eine Einzelperson oder eine bestimmte Gruppe wie zum Beispiel eine Organisation oder ein Unternehmen erstellt (Arshad *et al.*, 2021, p. 166). Zu diesen Personen gehören Mitglieder und Mitgliederinnen des Finanzteam, des IT-Sicherheitsteams oder sogar neu eingestellte Mitarbeiter und Mitarbeiterinnen (Bhardwaj *et al.*, 2020, p. 16). In diesen Fällen ist es wahrscheinlicher, dass die Angreifer und Angreiferinnen zuvor eine gewisse Aufklärung betrieben haben (Furnell, Millet and Papadaki, 2019, p. 12) (iterative Informationssammlung) (Allodi *et al.*, 2020, p. 4)), um die Nachricht zu formulieren (Furnell, Millet and Papadaki, 2019, p. 12) und die Chancen für eine erfolgreiche Übermittlung des Angriffs zu maximieren

(Allodi *et al.*, 2020, p. 4). Soziale Medien und Open Source Daten können zur Aufklärung genutzt werden. Eine weitere Möglichkeit ist das Browser-Sniffing, dass die von der Zielperson häufig genutzten Websites aufdeckt, indem die Zugriffszeit durch die Analyse von Cookies, des Domain Name System (DNS)-Caches oder von URLs ermittelt wird. Wenn die Zugriffszeit für eine bestimmte Website kurz ist, dann ist es wahrscheinlich, dass die Zielperson diese Website häufig besucht. Um diese Informationen auszuspionieren, muss der Angreifer oder die Angreiferin zunächst eine Website mit Werbung oder eine andere Möglichkeit zur Einbettung von JavaScript nutzen. Die ist notwendig, damit der Phisher oder die Phisherin das Skript installieren kann, dass den Angreifer oder die Angreiferin über die Zugriffszeiten von Websites informiert (Alabdan, 2020, p. 10). Spear-Phishing-E-Mail Angreifer oder Angreiferinnen geben sich dann zum Beispiel als ein bestehender Kontakt des Opfers aus (Meyers *et al.*, 2018, p. 136). Die Spear Phishing-Technik verwendet auch E-Mail-Spoofing-Angriffe (Adil, Khan and Nawaz Ul Ghani, 2020, p. 4), bei dem sich der Absender oder die Absenderin als jemand von einer höheren Behörde oder einer bekannten Organisation ausgibt (Arshad *et al.*, 2021, p. 166). Damit wird versucht, bestimmte Benutzer und Benutzerinnen oder eine bestimmte Organisation von der Legitimität zu überzeugen und Zugang zu den Unternehmensdaten zu erhalten (Adil, Khan and Nawaz Ul Ghani, 2020, p. 4).

#### 2.3.3.3.9 Whaling

Whaling ist ein Phishing-Angriff (Arshad *et al.*, 2021, p. 166) und eine Untergruppe des Spear-Phishing-Angriffs (Antonucci *et al.*, 2020, p. 3). Die einzigen Ziele sind leitende Personen (oder andere hochrangige Mitarbeiter und Mitarbeiterinnen) (Furnell, Millet and Papadaki, 2019, p. 12) wie Personalleiter und Personalleiterinnen, C-Level-Führungskräfte wie CISO, CTO, CFO oder Vorstandsmitglieder und Vorstandsmitgliederinnen (Bhardwaj *et al.*, 2020, pp. 15–16), die aufgrund ihrer Position privilegierten Zugang zu Daten in ihrem Unternehmen haben. Da es sich um einen sehr gezielten Angriff handelt, nehmen sich die Phisher und Phisherinnen Zeit für den Angriff. Das Whaling selbst kann möglicherweise nur die Vorstufe des Gesamtangriffs sein, wobei der so genannte Business E-Mail Compromise (BEC) zunimmt (Alabdan, 2020, pp. 10–11).

#### 2.3.3.3.10 Business E-Mail Compromise

Die Kompromittierung von Geschäfts-E-Mails ist eine Form des Phishing-Angriffs (eine Unterart des Spear-Phishing) (Alabdan, 2020, p. 11), auch bekannt als CEO-Betrug, bei

dem Phisher und Phisherinnen die Namen von Mitarbeiter und Mitarbeiterinnen oder Geschäftspartner und Geschäftspartnerinnen verwenden, um eine E-Mail oder eine Direktnachricht legitim aussehen zu lassen (Binks, 2019, p. 10). Diese Art von Betrug wurde in den Statistiken des FBI im Jahr 2017 noch nicht registriert. Aber in den ersten acht Monaten des Jahres 2018 erhielt die Behörde 1.164 Beschwerden mit Verlusten von mehr als eine Millionen Dollar. (Mansfield-Devine, 2018, p. 18). In den letzten Jahren wurden bei dieser Art von Betrug zunehmend Geschenkkarten als Methode zur "Auszahlung" verwendet. Im dritten Quartal 2019 stellte die Anti-Phishing Working Group (APWG) fest, dass in 56% der Fälle Geschenkkarten verwendet wurden. Die zweithäufigste Methode war die Abzweigung von Gehaltsabrechnungen (25%) und in den verbleibenden 19% wurde eine direkte Überweisung verwendet. Die am häufigsten angegriffene Position bei dieser Art von Angriffen ist die CEO Position. Diese spezielle Phishing-Methode ist mit automatisierten Tools schwieriger zu erkennen. Daher ist die einzige wirkliche Verteidigung gegen diesen Angriff derzeit die Aufklärung der Benutzer und Benutzerinnen (Alabdan, 2020, p. 11).

#### 2.3.3.3.11 Klon Phishing

Klon-Phishing ist eine Art von Phishing-Angriff, bei dem eine legitime, zuvor an einem Benutzer oder Benutzerin zugestellte E-Mail, die einen Anhang oder einen Link enthält, vom Hacker oder Hackerin durch eine bösartige Version ersetzt wird. Um legitim zu erscheinen und den Empfänger oder die Empfängerin davon zu überzeugen, den Link oder den Anhang zu öffnen, behaupten die Hacker und Hackerinnen, dass die neue E-Mail die aktualisierte Version der ersten oder ursprünglichen E-Mail ist (Patayo, 2021, p. 4).

#### 2.3.3.3.12 Social-Engineering

Social-Engineering ist die Manipulation der Emotionen, die Leichtgläubigkeit, die Nächstenliebe oder das Vertrauen einer oder mehrerer Personen. Ein sehr bekanntes Beispiel ist der klassische "Nigerian Prince", die die Gier der Zielpersonen ausnutzen. Bei diesen Angriffen wird versucht die Zielperson beispielsweise mit einer Geschichte über eine reiche Person die Geld überweisen möchte und dafür Hilfe benötigt, zu manipulieren. Als Gegenleistung für diese Hilfe wird dem Opfer eine beträchtliche Entschädigung versprochen, allerdings erst nachdem das Opfer der vermeintlich wohlhanden Person etwas zur Verfügung gestellt hat, z.B. eine kleine Zahlung oder eine Kontonummer, eine Adresse für eine Hintergrundprüfung. Die Gier des Opfers nach der großen Geldsumme verleitet das Opfer dazu, den Anweisungen Folge zu leisten (Alabdan, 2020, pp. 13–14).

Es gibt verschiedene Arten von Social-Engineering-Angriffen, zum Beispiel: Tailgating oder Piggybacking, Schultersurfen oder Dumpster Diving (Mashtalyar *et al.*, 2021, p. 420).

- Tailgating oder Piggybacking: Hier tricksen die Angreifer und Angreiferinnen autorisierte Mitarbeiter und Mitarbeiterinnen aus, um sich Zugang zu eingeschränkten Bereichen (z.B. Firmengelände) zu verschaffen. Die Angreifer und Angreiferinnen verwenden verschiedene Strategien z.B. indem die sie den Mitarbeiter und Mitarbeiterinnen folgen, um sich Zugang zu verschaffen, gefälschte Ausweise tragen, oder durch die Türen von Parkplätzen eindringen (Mashtalyar *et al.*, 2021, p. 420).
- Shoulder Surfing: Bei dieser Methode geht es darum, durch Beobachtung sensible Informationen von einem Opfer zu erhalten. Die Angreifer und Angreiferinnen beobachten ihre Zielpersonen aus der Nähe, wenn die Opfer Passwörter, Identifikationsdaten und andere wertvolle persönliche Daten eingeben. Die Angreifer und Angreiferinnen beobachten und belauschen auch Gespräche zwischen Mitglieder und Mitgliederinnen von Unternehmen (Mashtalyar *et al.*, 2021, p. 420).
- Dumpster Diving: Bei diesem Angriff versuchen die Angreifer und Angreiferinnen, die Informationen der Opfer auf physischem Wege zu erhalten. Die Angreifer und Angreiferinnen versuchen, an persönliche Informationen wie IP-Adressen und Bankkontodaten zu gelangen, indem sie z.B. Abfallstücke aus den Mülleimern des Unternehmens einsammeln (Mashtalyar *et al.*, 2021, p. 420).

Reverse-Social-Engineering ist eine gefährliche Methode des Social-Engineering und erfordert einen erheblichen Aufwand bei der Vorbereitung und Planung. Das Ergebnis ist, dass der Angreifer oder die Angreiferin den Anschein erweckt, in einer Macht- oder Autoritätsposition zu sein, sodass die Opfer sich dem Angreifer oder Angreiferin von sich selbst aus nähern. (Alabdan, 2020, p. 13).

#### 2.3.3.3.13 Social Network Phishing

Es gibt derzeit keinen allgemein akzeptierten Begriff für Phishing auf Social Network Sites (SNSs). Daher wird Phishing in SNSs auch als Social Phishing, Social Media Phishing oder Social Network Phishing bezeichnet (Frauenstein and Flowerday, 2020, p. 2). Phisher und Phisherinnen können auf verschiedene Weise die Kontrolle über das Social Media Konto von Benutzer und Benutzerinnen erlangen. Erstens, indem die Angreifer und Angreiferinnen eine echt aussehende E-Mail oder Nachricht von der Website senden,

die Benutzer und Benutzerinnen auffordert, den Namen und das Kennwort für die Konten in sozialen Netzwerken über eine angehängte URL zu bestätigen. Sobald der Phisher oder die Phisherin die Kontrolle über das Konto des Benutzers oder der Benutzerin erlangt hat, kann der Angreifer oder die Angreiferin das Passwort ändern. Zweitens können gefälschte Profile erstellt werden, die den Anschein erwecken, von Bekannten des Opfers zu stammen. Von diesen Profilen werden dann gefälschte Nachrichten an die Benutzer und Benutzerinnen gesendet. Drittens nutzen die Angreifer und Angreiferinnen Pinnwände sozialer Netzwerke oder offizielle Seiten, um Phishing-URLs zu veröffentlichen. Viertens nutzen Angreifer und Angreiferinnen die Empfehlungsliste von Freund*innen und Freundinnen bei Social Media Plattformen aus, um die Opfer einzuladen, sie als Freunde und Freundinnen hinzuzufügen. Sobald sie von den Opfern hinzugefügt wurden, können die Angreifer und Angreiferinnen diese Freundschaften ausnutzen (Aleroud and Zhou, 2017, pp. 166–167).

#### 2.3.3.3.14 Website Phishing

Website-Phishing sind sehr einfach zu bewerkstelligen, da es für den Angreifer und Angreiferinnen kein Problem darstellt, eine Phishing-Website zu erstellen, die eine exakte Kopie einer legitimen Website ist (Gupta *et al.*, 2017, pp. 3636–3637).

#### 2.3.3.3.15 Browser Schwachstelle

Browser sind Softwareanwendungen die Inhalte hosten, die im World Wide Web angezeigt, abgerufen und verändert werden können. Diese Inhalte bestehen aus Text, Bildern, Videos und anderen Dateien wie z.B. ausführbaren Dateien. Browser verwenden ein Client-Server-Modell: der Browser, der auf einem Computer oder einem mobilen Gerät verwendet wird, fungiert als Client, und der Webserver, der die Informationen für die Benutzer und Benutzerinnen bereitstellt, fungiert als Server. Der Webserver sendet die entsprechenden Informationen an den Client und die Ergebnisse werden in der Browser-Anwendung auf dem Client-Rechner oder mobilen Gerät angezeigt. Eine Browser-Schwachstelle dient als Möglichkeit für einen Angreifer oder eine Angreiferin diese Schwachstelle auszunutzen und dann können unbefugte Aktionen auf dem Rechner des Opfers durchgeführt werden. Browser-Schwachstellen entstehen unter anderem aufgrund von Designproblemen und -fehlern des Browsers, der Häufigkeit mit der diese Probleme aktualisiert und gepatcht werden, dem Grad der Integration des Browsers in das System und den zugewiesenen Berechtigungen (Alabdan, 2020, pp. 16–17). Die

Wahrscheinlichkeit einer Sicherheitslücke in einem System steigt, wenn eine neue Funktion oder ein neues Modul hinzugefügt wird (Arshad *et al.*, 2021, p. 166).

Im Jahr 2003 ermöglichte es eine Sicherheitslücke im Microsoft Internet Explorer Phisher und Phisherinnen die URL der Phishing-Website als legitime Website zu verschleiern, indem sie ein 0x01-Zeichen nach dem "@"-Zeichen einfügten. Der Rest der URL nach dem 0x01-Zeichen wurde in der Adressleiste nicht angezeigt, so dass der wahre Domänenname der URL verborgen blieb. Ein weiteres Beispiel für eine Sicherheitslücke ist die Methode window.createPopup(), von der Microsoft Internet Explorer im Jahr 2004 betroffen war. Diese Methode erstellt ein randloses Popup-Fenster und kann über alle Fenster gelegt werden. Die Phisher und Phisherinnen können dieses randlose Popup-Fenster verwenden, um die URL der Phishing-Website zu verschleiern oder das HTTPS-Vorhängeschloss-Symbol anzuzeigen, um dem Opfer vorzutäuschen, dass es sich um eine sichere Website handelt. Phisher und Phisherinnen können die in den meisten Browsern verfügbare Auto-Fill-Funktion nutzen, um an die persönlichen Daten des Opfers zu gelangen. Die Phisher und Phisherinnen können jedoch Formularfelder einfügen, die für das Opfer nicht sichtbar sind. Wenn Sie die Funktion zum automatischen Ausfüllen verwenden, werden diese versteckten Formularfelder automatisch ausgefüllt (Chiew, Yong and Tan, 2018, pp. 4–5).

#### 2.3.3.3.16 Bösartige Browsererweiterung

Browser-Erweiterungen sind zusätzliche Software, die innerhalb der Browser-Anwendung installiert werden. Es handelt sich dabei um Codestücke, die dem Code der Browseranwendung hinzugefügt werden. Diese Erweiterungen werden wie andere Softwareanwendungen ausgeführt. Jedoch werden diese nicht direkt auf dem Computer installiert, sondern der Browseranwendung hinzugefügt. Ein Problem mit Erweiterungen ist, dass diese über Webshops veröffentlicht und nicht angemessen überprüft werden. Daher ist es für Hacker und Hackerinnen einfach, bösartige Browser-Erweiterungen zu veröffentlichen. Da der Browser eine vertrauenswürdige Anwendung ist, ist es für Antiviren-Software schwierig, diese bösartigen Erweiterungen zu erkennen und zu bekämpfen. Obwohl diese Erweiterungen in der Regel die Erlaubnis der Benutzer und Benutzerinnen benötigen, um zu funktionieren, gewähren und bestätigen die meisten Browser standardmäßig die Berechtigungen für Erweiterungen, ohne den Benutzer oder die Benutzerin zu fragen. Sichere und legitime Erweiterungen erfordern jedoch, dass der Benutzer oder die Benutzerin der Erweiterung die Erlaubnis erteilt (Alabdan, 2020, p. 19).

#### 2.3.3.3.17 Tab Napping

Der Begriff leitet sich von den Worten "Tab" und "Kidnapping" ab, wobei Tabs einzelne Websites sind, die gleichzeitig in einem Browserfenster geöffnet werden können. Bei dieser speziellen Angriffsmethode nutzen die Angreifer und Angreiferinnen die Tatsache aus, dass potenzielle Opfer unbeaufsichtigte Tabs in ihrer Browser-Anwendung haben. Bei dieser Gelegenheit versuchen bösartige Hacker und Hackerinnen, die unbeaufsichtigten Websites des Opfers auf bösartige Websites umzuleiten, ohne dass der Benutzer oder die Benutzerin dies bemerkt. Im Folgenden wird ein Beispielszenario für einen Tab-Napping-Angriff betrachtet. Ein Opfer meldet sich beim Facebook-Konto an und gibt die relevanten Daten ein. Wenn die Person den Feed durchsucht, sieht sie einen interessanten Link zu einem Thema. Das Opfer klickt auf den Link, der sich dann in einem anderen Tab öffnet. Während der Benutzer oder die Benutzerin diese zweite Registerkarte ansieht, wird ohne das Wissen der Anwender oder Anwenderin ein Skript ausgeführt, das die vorherige Registerkarte (d.h. die bei Facebook angemeldete Registerkarte) auf eine gefälschte Facebook-Anmeldeseite umleitet. Wenn der Benutzer oder die Benutzerin zur ersten Registerkarte zurückkehrt, nimmt die Person an, dass er oder sie abgemeldet wurde, weil die Sitzung abgelaufen ist, und gibt die Daten erneut in das Anmeldeformular ein. Das Anmeldeformular aktualisiert den Benutzer oder die Benutzerin einfach und/oder leitet sie zu der vorherigen Sitzung zurück, ohne dass die Person weiß, dass der Angreifer oder die Angreiferin nun Zugriff auf die gültigen Anmeldedaten des Opfers hat. Die einzige Möglichkeit, sich vor einem solchen Angriff zu schützen, besteht darin, die URL in der Adressleiste des Browsers zu überprüfen. Wenn die URL aus irgendeinem Grund verdächtig erscheint, sollte der Benutzer oder die Benutzerin die Registerkarte schließen, eine neue Registerkarte öffnen und die gewünschte URL eingeben (Alabdan, 2020, p. 17).

#### 2.3.3.3.18 Click Jacking

Click Jacking, auch bekannt als Angriff auf die Benutzer- bzw. Benutzerinnenoberfläche, ist die Manipulation der User Interface (UI) einer Website, die dazu führt, dass der Benutzer oder die Benutzerin bei der Interaktion mit der kompromittierten UI unwissentlich eine Aktion ausführt (Chiew, Yong and Tan, 2018, p. 5). Bei dieser Technik wird der Benutzer oder die Benutzerin gezwungen, auf bösartige Links zu klicken, indem die Person zum Beispiel eigentlich einen Browser schließen wollte (Arshad *et al.*, 2021, p. 166). Weitere Beispiele für Aktionen, zu denen der Benutzer oder die Benutzerin verleitet werden kann, sind das das Durchführen einer Kaufabwicklung bei PayPal, das Zulassen

des Zugriffs auf Webcam und Mikrofon oder das Stehlen persönlicher Daten (Chiew, Yong and Tan, 2018, p. 5).

#### 2.3.3.3.19 404 Fehler Manipulation

Bei dieser Art von Angriff verwendet ein Hacker oder eine Hackerin eine Ressourcenzuordnungstechnik. Die Ressourcenzuordnung wird verwendet, um Informationen zu identifizieren und die Methoden zu ermitteln, mit denen der Hacker oder die Hackerin diese Ressourcen erhalten kann. Websites wie http://intranet werden ausschließlich von Unternehmensnetzwerken genutzt und sind für die Allgemeinheit nicht zugänglich. Wenn eine Website den 404-Fehler "Seite nicht gefunden" implementiert, kann der Angreifer oder die Angreiferin eine seitenübergreifende Verlaufsmanipulation durchführen (Alabdan, 2020, p. 18).

#### 2.3.3.3.20 URL Verschleierung

Die Studie von Garera et al. (Garera et al., 2007) hat prominente Verschleierungstechniken kategorisiert, indem sie die Liste der Phishing-URLs untersuchte, die von Google im Jahr 2007 geführt wurde (Fernando and Arachchilage, 2020, p. 3).

- Typ I: Verschleierung mit IP-Adresse: Der Hostname der URL wird vom Phisher und Phisherinnen mit einer IP-Adresse verschleiert. Zum Beispiel: http://67.210.122.222/apple/login (Fernando and Arachchilage, 2020, p. 4).
- Typ II: Verschleierung mit anderer Domäne: Ein gültig aussehender Domänenname wird in der URL verwendet und täuscht Benutzer und Benutzerinnen vor, dass es sich um eine Weiterleitungs-URL handelt. Zum Beispiel: https://recovery-confrim-paqe.cf/?facebook.com=chekpoint (Fernando and Arachchilage, 2020, p. 4).
- Typ III: Verschleierung mit großen Hostnamen: Bei dieser Art der Verschleierung hängen Phisher und Phisherinnen eine große Wortfolge an das Ende eines echt aussehenden Domänennamen an (Fernando and Arachchilage, 2020, p. 4).
- Typ IV: Unbekannte oder falsch geschriebene Domäne: Die Phishing-URL kann einen Domänennamen enthalten, der sich von dem einer Zielorganisation unterscheidet. Zum Beispiel: http://www.g0og1e.com (Fernando and Arachchilage, 2020, p. 4).

#### 2.3.3.3.21 Typo Squatting

Typo Squatting ist eine Art von URL-Hijacking, welches auf Benutzer und Benutzerinnen abzielt, die bei der Eingabe einer Website-Adresse einen Tippfehler machen (z.B. Facebok.com statt Facebook.com). Wenn potenzielle Opfer einen Tippfehler machen, werden sie auf eine bösartige Website geleitet und wie die ursprüngliche Website aussieht. Typo Squatting ist nicht nur auf einen falsch geschriebenen Domänennamen beschränkt, sondern kann auch genutzt werden, wenn der Benutzer oder die Benutzerin eine falsche Domänenerweiterung eingibt, z.B. .com statt .org. Einige vorbeugende Maßnahmen, die ein Benutzer oder eine Benutzerin ergreifen kann, sind: Lesezeichen für häufig besuchte Websites, Verwendung von Spracherkennungssoftware und Verwendung von Websuchen (Alabdan, 2020, pp. 17–18).

#### 2.3.3.3.22 Homoglyphen Substituierung

Es können Homoglyphen in E-Mails verwendet werden, um die tatsächlichen Zeichen durch ein ähnlich aussehendes Zeichen zu ersetzen. Es gab einen Angriff, bei dem die Website von Virgin Atlantic imitiert wurde, indem das „r“ durch ein „r̥“ ersetzt wurde, so dass die URL für Besucher und Besucherinnen identisch mit dem Original aussah. Dasselbe wurde bei einer Nachahmung der Rolex-URL beobachtet, bei der das „l“ durch den Homoglyphen „ι“ ersetzt wurde (Boddy, 2018, p. 10).

#### 2.3.3.3.23 Fast Flux

Systemeindringungstechniken werden verwendet, um Systemressourcen auszunutzen, welche im Zuge dessen die Initialisierung von Phishing-Angriffen erleichtern soll. Es gibt zwei Haupttechniken für das Eindringen in das System: Fast-Flux (FF) und Cross Site Scripting (XSS). Fast-Flux ist kein direkter Angriff, sondern eine Domain-Name-Service (DNS) bezogene Technik, die Phishing-Websites vor dem Herunterfahren schützt, indem der Hosting-Rechner der Phishing-Websites verborgen wird (Aleroud and Zhou, 2017, pp. 167–168). Fast-Flux ist eine Methode, bei der einer Domänenname verschiedene IPs zugewiesen werden. Dies wird häufig von echten Websites verwendet, um die Nachfrage auszugleichen. Dies passiert indem die Last auf die Server verteilt wird, wodurch die Leistung und Zuverlässigkeit verbessert wird. Phisher und Phisherinnen verwenden Botnets, um die Phishing Websites zu verstecken, so dass es schwieriger wird, diese zu finden und abzuschalten. Dadurch können Angriffe länger andauern und kann fortgesetzt werden, selbst wenn einige der Bots ausgeschaltet werden. Das ist dadurch möglich, dass die Domäne auf die IP eines anderen Bots geändert werden kann. Das einzige Kriterium

für die Aufrechterhaltung des Angriffs ist, dass die Bots schneller rekrutiert werden als sie ausgeschaltet werden (Alabdan, 2020, p. 15).

#### 2.3.3.3.24 Cross-Site Scripting

Die zweite Haupttechnik für das Eindringen in ein System ist Cross-Site-Scripting (XSS). Die Einschleusung bösartiger Inhalte kann durch Cross Site Scripting (XSS) erfolgen (Aleroud and Zhou, 2017, pp. 167–168). Moderne Websites verwenden häufig clientseitige Skripte, um die Benutzer- und Benutzerinnenfreundlichkeit zu verbessern. Leider ist der Client dadurch offen für einen XSS-Angriff. XSS ist ähnlich wie SQL-Injection eine Form der Code-Injection. Im Gegensatz zu SQL, das auf die Abfragefunktion von Datenbanken abzielt, zielt XSS jedoch auf die HTML-Ausgaben ab (Alabdan, 2020, p. 11).

#### 2.3.3.3.25 Botnet

Ein Botnet ist eine Form von Malware, die es einem Angreifer oder einer Angreiferin ermöglicht, das Gerät des Opfers durch Fernzugriff für die eigenen Zwecke zu nutzen z.B. Installation zusätzlicher Malware, Aktualisierung aktueller Malware, Scannen nach Schwachstellen, Überwachung, Versand von Spam- und Phishing-E-Mails, Umleitung zu Phishing-Websites und Distributed Denial of Service (DDOS) Angriffen (Alabdan, 2020, pp. 14–15).

#### 2.3.3.3.26 Malware Phishing

Malware Phishing-Angriffe verwenden eine Vielzahl von bösartigen Programmen, bei denen es sich in erster Linie um unerwünschte Software handelt, die auf dem System des Opfers läuft. Diese Angriffe lassen sich in folgende Kategorien unterteilen: Key Logger/Bildschirm-Logger, Session Hijacking, Host File Poisoning, DNS-Phishing und Content Injection. Key Logger stellen eine ernsthafte Bedrohung für die Systeme dar, da Menschen nicht in der Lage sind, ihre Anwesenheit zu erkennen. Key Logger können in folgende Kategorien eingeteilt werden: Hardware Key Logger und Software Key Logger (Gupta *et al.*, 2017, pp. 3635–3638).

- Hardware Key Logger zeichnen Daten auf, die über die Tastatur eingegeben werden. Diese Daten werden im Hardware Key Logger und nehmen somit keine Systemressourcen in Anspruch, daher können sie von keiner Antivirensoftware erkannt werden (Gupta et al., 2017, p. 3638).

- Software Key Logger untersuchen die Daten des Betriebssystems und die über die Tastatur eingegeben werden. Software Key Logger zeichnen die Daten an entfernten Orten auf, die später an den Angreifer oder der Angreiferin gesendet werden (Gupta *et al.*, 2017, p. 3638).

Es gibt eine Vielzahl von Malware wie z.B. Viren, Trojaner und Rootkits (Desolda *et al.*, 2021, p. 7). Bei Malware-Angriffen auf Unternehmen kann auch Ransomware zum Einsatz kommen. Die Betreiber und Betreiberinnen von Ransomware verlangen hohe Lösegeldsummen als Gegenleistung dafür, dass die gestohlenen Daten nicht preisgeben werden (Basit *et al.*, 2021, p. 151). Bei Ransomware werden die Daten von Angreifer und Angreiferinnen verschlüsselt (Papatsaroucha *et al.*, 2021, p. 13). Ransomware präsentiert sich im Allgemeinen auf drei verschiedene Arten: Sperrung des Bildschirms, Verschlüsselung von Dateien, falsche Warnungen (Thomas, 2018, p. 8).

#### 2.3.3.3.27 Malvertizing

Malvertizing unterscheidet sich von Adware. Es nutzt Online-Werbung als Mittel zur Verteilung von Malware an die Opfer. Diese Form des Angriffs ist weniger zielgerichtet und kann weitreichende Auswirkungen haben. Bei diesem Ansatz nutzt der Phisher oder die Phisherin einen Werbehosting-Dienst, um eine Anzeige zu hosten. Diese Anzeige enthält dann eine Malware, die aktiviert wird (Alabdan, 2020, p. 15), wenn das Opfer auf diese Anzeige klickt. Mit diesem Klick gelangen dann Viren in das System des Opfers (Arshad *et al.*, 2021, p. 166). Der Hauptvorteil für Phisher und Phisherinnen besteht darin, dass Malvertizing schwer zu erkennen und zu verhindern ist, insbesondere weil die Malware auf einer legitimen Werbe-Website gehostet wird (Alabdan, 2020, p. 16).

#### 2.3.3.3.28 Session Hijacking

Session Hijacking kann entweder auf Netzwerkebene oder auf Anwendungsebene stattfinden. Beim Session Hijacking auf Netzwerkebene werden TCP- und UDP-Sitzungen gestört, während beim Session Hijacking auf Anwendungsebene HTTP-Sitzungen gestört werden (Gupta *et al.*, 2017, p. 3638).

- Entführung von TCP-Sitzungen: In diesem Fall wird eine bestehende TCP-Verbindung zwischen zwei beliebigen kommunizierenden Systemen abgefangen und der Angreifer oder die Angreiferin gibt sich als eines der beiden Systeme aus. Anschließend wird der TCP-Verkehr zu dem Angreifer oder der Angreiferin umgeleitet. Die Sitzung zwischen den tatsächlich kommunizierenden Hosts wird

de-synchronisiert. Die Authentifizierung erfolgt nur zum Zeitpunkt des Verbindungsaufbaus. Daher kann eine bereits bestehende Verbindung ohne Authentifizierung gekapert werden (Gupta *et al.*, 2017, p. 3638).

- Entführung von UDP-Sitzungen: Es ist einfacher, eine UDP-Sitzung zu kapern als eine TCP-Sitzung, da keine Synchronisierung und keine Reihenfolge der Pakete erforderlich sind. In diesem Fall sendet der Angreifer oder die Angreiferin im Namen des Servers eine gefälschte UDP-Antwort an den Host, bevor der Server antworten kann (Gupta *et al.*, 2017, p. 3639).
- Entführung auf Anwendungsebene: Auf der Anwendungsebene wird entweder eine neue Sitzung unter Verwendung gestohlener Daten initiiert oder eine bestehende Sitzung gekapert. Es werden IDs für eine Sitzung erlangt. Die IDs sind die einzigen eindeutigen Bezeichner für eine HTTP-Sitzung und können aus der URL, die der Browser für die HTTP-GET-Anfrage erhält, den Cookies auf dem Client-System und den Formularfeldern extrahiert werden (Gupta *et al.*, 2017, p. 3639).

#### 2.3.3.3.29 Host File Poisoning

Host-File-Poisoning bedeutet, dass neue Einträge für Websites in die Host-Datei eines Rechners eingefügt werden, wodurch die Websites auf eine andere Website umgeleitet werden. Wenn ein Client eine URL eingibt, wird diese in eine IP-Adresse umgewandelt, bevor sie über das Internet gesendet wird. Hacker und Hackerinnen lassen gefälschte Adressen übertragen, indem sie die Hostdateien manipulieren und den Benutzer oder die Benutzerin auf eine betrügerische Website umleiten (Gupta *et al.*, 2017, p. 3639).

#### 2.3.3.3.30 Domain Name Service Phishing

DNS Phishing ("Pharming") nutzt Internet-Schwachstellen, die auf einem DNS-Server und DNS-Resolver basieren. Bei diesem Angriff wird die DNS-Infrastruktur kompromittiert, so dass die DNS-Anfragen für die angeforderte Domänenadresse des Opfers eine vom Angreifer oder Angreiferin kontrollierte IP-Adresse zurückgeben (Purkait, Kumar De and Suar, 2014, p. 197).

#### 2.3.3.3.31 Drive-by Download

Drive-by-Download ist eine Phishing-Technik, bei der bösartige Codes und Viren in ein System eingeschleust werden (Arshad *et al.*, 2021, p. 167). Es handelt sich dabei um eine Methode zur Verbreitung von Malware, die Wege wie E-Mails oder besuchte Websites nutzt. Wenn ein Drive-by-Download auf einem Webserver gehostet wird, hat der Angreifer

oder die Angreiferin zwei Optionen. Die erste besteht darin, die Ziele auf einen Webserver umzuleiten, der dem Angreifer oder der Angreiferin gehört. Die zweite und effektivere Option besteht darin, legitime Webserver zu sabotieren, sodass diese Exploits von dort aus gehosted werden. Diese Methode erhöht die Erfolgschancen des Angriffs, da der Verdacht des Opfers nicht geweckt wird, da dies über eine legitime Website stattfindet (Alabdan, 2020, p. 14).

Die häufigste Form von Malware, die durch einen Drive-by-Download installiert wird ist entweder ein Trojaner oder ein Botnet (Alabdan, 2020, p. 14). Ein Trojaner ist ein bösartiges Programm, das als legitime Software getarnt ist und das Opfer dazu verleitet, es zu installieren oder auszuführen. Anschließend verschafft es sich Zugang zum Rechner des Opfers. Trojaner können von Phisher und Phisherinnen dazu verwendet werden, Key Logger zu installieren (Chiew, Yong and Tan, 2018, p. 7). Session Hijacking kann auch mit Malware durchgeführt werden, die per Drive-by-Download eingeschleust wird. Dies ermöglicht es dem Phisher oder der Phisherin, den Internetverkehr des Opfers zu überwachen. Die Malware wartet zunächst darauf, dass sich der Benutzer oder die Benutzerin über eine sichere Sitzung authentifiziert und kapert dann die Sitzung (Alabdan, 2020, p. 15).

#### 2.3.3.3.32 Wiphishing

Wiphishing (auch als Böser-Zwilling-Angriff bekannt) ist eine Phishing-Methode, bei der drahtlose Netzwerke als Angriffsvektor genutzt werden. Der Phisher oder die Phisherin schiebt sich zwischen die Opfer und den echten Zugangspunkt (Access Point - AP). Dies geschieht mit Hilfe eines betrügerischen Zugangspunkts, der den gleiche Netzwerknamen und Frequenz wie das echte Netzwerk verwendet. Indem dieser Zugangspunkt so platziert wird, dass das Signal des bösartigen AP stärker ist als das des echten Netzwerks, wird das Gerät des Opfers dazu verleitet, sich mit dem bösartigen AP zu verbinden. Dann ist der Phisher oder die Phisherin in der Lage den Netzwerkverkehr zu überwachen. Diese Art des Angriffs ist bei kostenlosen Wi-Fi-Hotspots an Orten wie Cafés, Hotels oder Reisezentren üblich (Alabdan, 2020, p. 16).

#### 2.3.3.3.33 Suchmaschine Phishing

Phishing-Websites können über Suchmaschinenergebnisse an potenzielle Opfer übermittelt werden. Der Phisher oder die Phisherin erstellt eine Phishing-Website und optimiert sie für die Indizierung durch die Suchmaschine. Potenzielle Opfer, die mit Hilfe von Suchmaschinen nach der Website eines bestimmten Dienstleistungs- oder

Produktanbieters suchen, klicken möglicherweise auf den Phishing-Link in den Suchergebnissen und gehen davon aus, dass der Link auf die gewünschte Website führt. Blackhat SEO kann von Phisher und Phisherinnen eingesetzt werden, um den Seitenrang des Phishing-Links in den Suchmaschinenergebnissen zu erhöhen. Dies geschieht durch das Einfügen von Schlüsselwörtern beliebter Trends oder Ereignisse in ihre Website. Dadurch wird sichergestellt, dass die bösartige Website unter den ersten Suchergebnissen rangiert. Das erhöht die Wahrscheinlichkeit das potenzielle Opfer auf den Link klicken (Chiew, Yong and Tan, 2018, p. 13).

#### 2.3.3.3.34 Man-in-the-Middle

Beim Man-in-Middle-Phishing positioniert sich der Phisher oder die Phisherin zwischen dem Benutzer oder der Benutzerin und einer echten Website (Damodaram, 2016, pp. 701–702) und stiehlt dann die Daten und die Anmeldedaten des Opfers (Arshad *et al.*, 2021, p. 166). Man-in-the-Middle-Angriffe umfassen zwei Formen. Bei einem normalen Man-in-the-Middle-Angriff (MITM) fängt ein Angreifer oder eine Angreiferin eine direkte Kommunikation zwischen zwei Parteien ab, während ein Man-in-the-Cloud-Angriff (MITC) die Kommunikation zwischen Benutzer und Benutzerinnen und den Cloud-Diensten abfängt (Alabdan, 2020, p. 19).

- Bei einem MITM-Angriff fängt ein Angreifer oder eine Angreiferin die von einem Dienstanbieter und einer nutzenden Partei verwendeten Daten ab und konfiguriert sie neu. Der Angreifer oder die Angreiferin nimmt dann Kontakt mit dem Service Provider auf und gibt sich als der Nutzer oder die Nutzerin aus (Alabdan, 2020, p. 19).
- Bei einem MITC-Angriff nutzen die Angreifer und Angreiferinnen eine Schwachstelle im Synchronisations-Token-System der Cloud aus. Wenn eine Verbindung zwischen dem Benutzer oder der Benutzerin und der Cloud hergestellt wird, wird beiden Parteien ein Synchronisations-Token zugeteilt, das als Schlüssel für die Kommunikation zwischen ihnen dient. Bei jeder Verbindung zwischen dem Benutzer oder der Benutzerin und der Cloud wird ein neues, eindeutiges Synchronisierungstoken für diese spezielle Verbindung erstellt. Wenn ein Angreifer oder eine Angreiferin die Verbindung zwischen Benutzer und Benutzerinnen und der Cloud abfängt, kann der Synchronisierungstoken ermittelt werden. Nachdem der Token identifiziert wurde, kann sich der Hacker oder die Hackerin als der Cloud-Dienst ausgeben. Wenn ein Benutzer oder eine Benutzerin einen MITC-Angriff entdeckt hat, sollte das aktuelle Cloud-Konto gelöscht und

neues erstellt werden. Das dient zur Sicherstellung, sodass der Angreifer oder die Angreiferin nicht mehr in der Lage ist, das Synchronisierungs-Token zu nutzen. (Alabdan, 2020, pp. 19–20).

#### 2.3.3.3.35 Zero Day Phishing

Der Zero-Day-Phishing-Angriff ist eine Sicherheitslücke, die von Phisher und Phisherinnen ausgenutzt wird. Die Daten des Zero-Day-Angriffs sind nicht verfügbar, bis der Angriff entdeckt wird (Adil, Khan and Nawaz Ul Ghani, 2020, p. 4).

#### 2.3.3.3.36 Phishing Kits

Phishing erfordert ein gewisses Maß an technischen Kenntnissen, da es sich um ein Cyberverbrechen handelt (Alabdan, 2020, p. 22). Jedoch gibt es Phishing-Kits und das sind Tools, mit denen Phishing-Websites, E-Mails und Skripte erstellt werden können, ohne fortgeschrittene Programmierkenntnisse zu verfügen. Diese Kits können auf dem Marktplatz für Cyberkriminelle gegen Bezahlung oder von Entwickler und Entwicklerinnen des Kits in Untergrundkreisen erworben werden. Die meisten dieser kostenlosen Phishing-Kits haben jedoch Hintertüren, durch die die Benutzer und Benutzerinnen des Phishing-Kits gesammelten persönlichen Daten an den Entwickler oder Entwicklerin zurückgegeben werden. Phishing-Kits spielen keine direkte Rolle beim Phishing persönlicher Daten der Opfer, helfen aber bei der Durchführung von Phishing-Angriffen (Chiew, Yong and Tan, 2018, p. 13). Phishing Kits sind in der Lage, das exakte Design legitimer Websites zu spiegeln, um eine gefälschte Website authentisch aussehen zu lassen. Es wurden moderne Phishing-Kits entwickelt, die die IP-Bereiche der weltweit größten Sicherheitsunternehmen wie Kaspersky, McAfee und Symantec blockieren (Alabdan, 2020, p. 22).

### 2.3.4 Ablauf

Phishing-Angriffe bestehen in der Regel aus drei Komponenten: dem Haken, dem Köder und dem Fang (Anawar *et al.*, 2019, p. 2867).

- Der Haken ist ein Werkzeug, mit dem die Angreifer und Angreiferinnen vertrauliche Informationen des Opfers sammeln, z.B. über E-Mail, Social Media Websites oder Unternehmens-Websites (Anawar *et al.*, 2019, p. 2867).
- Der Köder ist der Anreiz, den die Angreifer und Angreiferinnen den Benutzer und Benutzerinnen bieten, um sie dazu zu bringen, die gewünschten Informationen

preiszugeben. Beispiele für einen Köder sind das Gefühl der Dringlichkeit oder Autorität in der E-Mail (Anawar *et al.*, 2019, p. 2867).

- Der Fang sind die Informationen, die von den Angreifer und Angreiferinnen abgerufen werden, um in das private Profil des Opfers einzudringen (Anawar *et al.*, 2019, pp. 2867–2868).

Die Phasen eines Phishing-Angriffs (Gupta *et al.*, 2017, p. 3632):

- Phase 1: Vorbereitung: Im ersten Schritt identifizieren die Angreifer und Angreiferinnen die Zielorganisation oder -person. Dann ist es ihre Aufgabe, Einzelheiten über die Organisation und das Netzwerk zu erfahren. Dies kann durch einen Besuch vor Ort oder durch die Überwachung des Datenverkehrs geschehen. Der nächste Schritt besteht darin, die Angriffe mit einem geeigneten Mittel zu starten, z.B. über eine Website oder E-Mails mit bösartigen Links, die das Opfer auf eine betrügerische Website umleiten können (Gupta *et al.*, 2017, p. 3632). Als Nächstes wählen die Angreifer und Angreiferinnen Angriffstechniken aus, wie z.B. Website-Spoofing, und bereiten schließlich das Angriffsmaterial für die spätere Verbreitung vor. Die Angriffsvorbereitung kann entweder manuell oder mit Hilfe einiger automatisierter Tools wie Phishing-Kits erfolgen. Die Vorbereitung des Angriffsmaterials hängt von der Zielumgebung ab. Im Falle von E-Mails wäre das Angriffsmaterial beispielsweise der E-Mail-Text (Aleroud and Zhou, 2017, pp. 162–163). Die Täuschung basiert auf dem Erscheinungsbild der E-Mail (z.B. Struktur der E-Mail-Adresse, Betreffzeile und Inhalt) und wird durch die Verwendung von Institutslogos legitimiert, um Authentizität zu erzeugen (Frauenstein and von Solms, 2013, p. 197).
- Phase 2: Phishing: Im nächsten Schritt werden diese gefälschten E-Mails, z.B. getarnt als eine Bank, über die gesammelten E-Mail-Adressen an das Opfer geschickt, in denen der Benutzer oder die Benutzerin aufgefordert wird, dringend einige Informationen zu aktualisieren, indem sie auf einen bösartigen Link klicken (Gupta *et al.*, 2017, p. 3632). Die E-Mail kann auch einen freundlichen Eindruck erwecken, z.B. indem sich für die Mitarbeit bedankt wird. Durch Reverse Social-Engineering fühlt sich die Zielperson dem Angreifer oder der Angreiferin gegenüber verpflichtet, sich zu melden. Der Benutzer oder die Benutzerin kann auch durch die gefälschte Warnung angelockt und dazu verleitet werden, auf einen Link zu klicken, der in der Regel als Text oder Bild getarnt ist, z.B. Klicken Sie hier für die Überprüfung. Der Text wird zusammen mit Psychologie eingesetzt, z.B. wenn der Benutzer oder die Benutzerin befürchtet, dass das Konto automatisch

gelöscht wird, wenn sie sich nicht umgehend verifizieren. Es liegt in der "menschlichen Natur", keine unerwünschten Konsequenzen zu wollen (Frauenstein and von Solms, 2013, pp. 197–198).

- Phase 3: Einbruch/Infiltration: Sobald das Opfer den betrügerischen Link öffnet, wird entweder eine Malware auf dem System installiert, die es dem Angreifer oder der Angreiferin ermöglicht, in das System einzudringen. In anderen Fällen führt der Link zu einer gefälschten Seite, die nach Zugangsdaten fragt (Gupta *et al.*, 2017, p. 3632).
- Phase 4: Datenerfassung: Sobald sich die Angreifer und Angreiferinnen Zugang zum System des Benutzers oder der Benutzerin verschafft haben, werden die erforderlichen Daten extrahiert. Wenn der Benutzer oder die Benutzerin die Kontodaten an die Angreifer und Angreiferinnen weitergegeben hat, können diese auf das Konto zugreifen, was zu finanziellen Verlusten führen kann. Im Falle von Malware-Angriffen hat der Angreifer oder die Angreiferin Fernzugriff auf das System (Gupta *et al.*, 2017, p. 3632).
- Phase 5: Ausbruch/Exfiltration: Nachdem die Angreifer und Angreiferinnen die erforderlichen Informationen erhalten haben, entfernen sie alle Beweise (Gupta *et al.*, 2017, p. 3632).

Ein Beispiel für den Weg einer Phishing-Mail zum Opfer: Die von einem Hacker oder einer Hackerin über das Internet gesendete Phishing-Mail erreicht zunächst den ersten Router, der die E-Mail je nach Konfiguration blockieren kann, so dass der Angriff nicht stattfinden kann. Falls der Hacker oder die Hackerin IP-Spoofing verwendet hat, um den Router zu ködern, steht eine spezielle Firewall für die weitere Analyse zur Verfügung. Wenn die Firewall diesen Angriff nicht erfolgreich abwehren kann, sendet diese die E-Mail zunächst an den Mailserver, der die gesendete E-Mail und den Inhalt prüft. Der Mailserver stuft die E-Mail auf der Grundlage der verschiedenen auf dem Server implementierten Algorithmen für maschinelles Lernen entweder als legitim oder als Spam ein, d.h. der Angriff könnte auch an diesem Punkt gestoppt werden. Wenn jedoch der Hacker oder die Hackerin auf dem Weg zum internen Mailserver Wörter oder Adressen verwendet, die der Klassifizierungsalgorithmus nicht als Spam klassifizieren konnte, muss die Phishing-E-Mail noch das Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) passieren, das je nach Konfiguration den Angriff stoppen kann. Der interne SMTP-Server (Simple Mail Transfer Protocol) wiederum muss die E-Mail genauer prüfen, bevor entschieden wird, ob die E-Mail an den Endbenutzer oder die Endbenutzerin zugestellt werden kann. Sobald die Phishing-E-Mail im Posteingang vom Endbenutzer oder

Endbenutzerin angekommen ist, wird der Host Intrusion Prevention System (HIPS) / Host Intrusion Detection System (IDS) die E-Mail noch prüfen, bevor der Benutzer oder die Benutzerin die E-Mail öffnet. Wenn die E-Mail noch nicht als Phishing erkannt wird, ist die letzte Verteidigungslinie der Endbenutzer oder die Endbenutzerin, die aufgrund der Bildung und Schulung in der Lage sein können, die E-Mail als Phishing zu erkennen (Patayo, 2021, pp. 12–13).

Intrusion Detection Systems (IDS) sind Geräte, Werkzeuge und Software, die zur Erkennung bösartiger Aktivitäten im Netz, auf Websites und Servern eingesetzt werden. IDS erkennen bösartige Websites und Datenverkehr auf der Grundlage ihrer Installation und Konfiguration. Es gibt verschiedene Arten von IDS, z.B. Host-basierte IDS (HIDS) und netzwerkbasierte IDS (NIDS). Netzwerkbasierte IDS werden auf der Routerseite mit der Konfiguration verwendet, um den gesamten Datenverkehr zu filtern, der durch das Netzwerk geht (IN/OUT). Das NIDS stoppt den Datenverkehr von Websites, E-Mail-Servern und DNS-Servern durch Verhaltenserkennung, Sicherheitsauthentifizierung und -ereignisse, wenn diese nicht mit der Konfiguration der Geräteauthentifizierung übereinstimmen. Darüber hinaus ist netzwerkbasiertes IDS effektiver und für große Organisationen kostengünstiger in der Anwendung. Host-basiertes IDS ist ein weiterer effektiver Weg, um bösartige Aktivitäten auf einem bestimmten Host-Server entsprechend der Konfiguration zu erkennen, zu stoppen und einzuschränken, wie z.B. die Einschränkung von E-Mails durch E-Mail-Analyse, von Websites durch Blacklist. Hostbasierte IDS sind teuer, aber effektiver, um einzelne Server oder Hosts vor Phishing-Angriffen zu schützen (Adil, Khan and Nawaz Ul Ghani, 2020, pp. 4–5).

Intrusion Prevention System (IPS) sind Geräte, Werkzeuge und Software die nicht nur bösartige Websites und E-Mail-Server erkennen, sondern auch Websites mit bösartigen Informationen blockiert und meldet. Bei der Phishing-Prävention werden die Websites vor der Autorisierung durch maschinelles Lernen überprüft, um die Sicherheitsparameter zu verifizieren. Darüber hinaus vergleichen IPS den Netzwerkverkehr (IN/OUT) mit ihrer Konfiguration, wie z.B. (Profil, Signaturübereinstimmung), um nur legitime Informationen zuzulassen und die Informationen, Websites und E-Mail-Server einzuschränken, die nicht mit den definierten Parametern übereinstimmen. IPS ist in der Lage, den Datenverkehr während der Analysephase zu erkennen und zu stoppen, wenn dies nicht mit dem Profil, der Signatur oder dem Schwellenwert übereinstimmt. Phishing-Filter ist eine weitere präventive Anti-Phishing-Technik, die zur Überwachung bösartiger Websites durch Filterung des Datenverkehrs (IN/OUT) im Netzwerk eingesetzt wird. Der Phishing-Filter verwendet auch URLs mit IP-Adressen, Attributen, Domänennamen und

Linktexten, um jede empfangene E-Mail mit der internen Konfiguration zu vergleichen, um den Sicherheitsstandard zu überprüfen, und wenn eine Abweichung oder ein Ähnlichkeitsindex mit den Blacklist-Informationen in der internen Konfiguration auftritt, zu stoppen, zu protokollieren und zu melden (Adil, Khan and Nawaz Ul Ghani, 2020, p. 5).

### 2.3.5 Technische Anti-Phishing Methoden

Unternehmen sollten Maßnahmen ergreifen, um zu verhindern, dass Phishing-Attacken die Benutzer und Benutzerinnen erreichen. Unternehmen können dies erreichen, indem sie in ihrem Netzwerk gut konfigurierte Firewalls, Intrusion-Prevention-Systeme, E-Mail-Filterung mit einer Whitelist für zugelassene Adressen und einer Blacklist zum Blockieren von Adressen, die bereits als Phishing erkannt wurden, sowie die Verwendung von SSL (Secure Socket Layer) auf den kritischen Serversystemen einsetzen (Patayo, 2021, p. 10). Die Zugriffskontrolle dient dazu, den Zugriff der Mitarbeiter und Mitarbeiterinnen auf die Ressourcen zu beschränken, die sie für ihre arbeitsbezogenen Tätigkeiten benötigen. Diese Kontrolle kann die Angriffsmöglichkeiten verringern, indem die Angriffsfläche minimiert wird. Organisationen setzen auch Informationsschutzverfahren ein, um zu beschränken, welche Informationen Mitarbeiter und Mitarbeiterinnen, Auftragnehmer und Auftragnehmerinnen und Lieferanten und Lieferantinnen über die Organisation preisgeben dürfen (Allodi *et al.*, 2020, p. 3). Unternehmen sollten auch Aufdeckungsmaßnahmen ergreifen (Patayo, 2021, p. 10). Dieser Prozess bietet kontinuierliche Überwachungsfunktionen, um anomales Verhalten innerhalb des Unternehmensnetzwerks zu erkennen (Allodi *et al.*, 2020, p. 3). Zu den Aufdeckungsmaßnahmen gehören unter anderem Intrusion-Detection-Systeme, die sowohl netzwerk- als auch hostbasiert sind, Antiviren-Software und andere Anti-Malware-Software (Patayo, 2021, p. 10). Die in diesem Prozess eingesetzten Netzwerküberwachungstools und Netzwerkfilterungstools zielen darauf ab, Angriffsartefakte zu erkennen und Spoofing-Versuche und betrügerische Websites zu identifizieren. Die Fähigkeit, rechtzeitig auf Social-Engineering-Angriffe, vor allem Phishing, zu reagieren, ist für Unternehmen entscheidend. Die Meldung von Vorfällen bietet die Möglichkeit, interessierte Parteien umgehend über eingehende Angriffe zu informieren (z.B. durch Warnmeldungen), um deren Auswirkungen zu verringern (Allodi *et al.*, 2020, p. 3). Es gibt verschiedene Phishing-Erkennungsmöglichkeiten basierend auf E-Mail, Website, Regel, Heuristik, Inhalt, Visuell, Authentifizierung, Honeypot, Künstliche Intelligenz, Machine Learning, Data Mining und Text Mining. Auf die einzelnen technischen Methoden wird nun näher eingegangen.

#### 2.3.5.1 E-Mail

Folgende Merkmale werden häufig zur Erkennung von Phishing-E-Mails verwendet (Gupta *et al.*, 2017, p. 3641):

- Körper-basierte Merkmale: Diese Merkmale werden aus dem E-Mail-Text extrahiert. Sie umfassen binäre Merkmale wie das Vorhandensein von Formularen, HTML oder bestimmten Phrasen und Links im Text (Gupta *et al.*, 2017, p. 3641).
- Betreff-basierte Merkmale: Einige Merkmale werden aus dem Betreff einer E-Mail extrahiert, z.B. ob es sich um eine Antwort auf eine frühere E-Mail handelt (Gupta *et al.*, 2017, p. 3641).
- URL-basierte Merkmale: Mit diesen Merkmalen wird geprüft, ob eine IP-Adresse anstelle des Domänennamens verwendet wird, ob „@“ in den Links vorhanden ist, wie viele Bilder, externe und interne Links im E-Mail-Text enthalten sind, wie viele Punkte in den Links vorkommen (Gupta *et al.*, 2017, p. 3641).
- Skript-basierte Funktionen: Diese Funktionen überprüfen das Vorhandensein von JavaScript und Pop-up-Fenster-Code in der E-Mail (Gupta *et al.*, 2017, p. 3641).
- Absender- und Absenderin-basierte Funktionen: Diese Funktionen beinhalten die Details des Absender oder der Absenderin, wie z.B. den Unterschied zwischen der Adresse des Absender oder Absenderin und der Adresse des Empfängers oder der Empfängerin (Gupta *et al.*, 2017, p. 3641).

#### 2.3.5.2 Website

Phishing-Gegenmaßnahmen, die auf einer Profil-Abgleichstrategie beruhen, können in vier Kategorien eingeteilt werden: Nutzungsverlauf-Abgleich, Muster-Abgleich, Visueller-Abgleich sowie Whitelist- und Blacklist - Abgleich. Phishing-Gegenmaßnahmen zum Profil-Abgleich nutzen Informationen über den Domänennamen und URLs von Domänen auf die Benutzer und Benutzerinnen kürzlich zugegriffen haben. Des Weiteren die Anmeldeinformationen der Nutzer und Nutzerinnen in diesen Domänen und andere Merkmale der aufgerufenen Domänen (z.B. Layout und Bilder). Danach werden merkmalbasierte Profile erstellt und diese zur Erkennung von Phishing verwendet. Die Komponenten des Profilabgleichs können einfach sein (z.B. URL-Abgleich) oder ausgefeilte Techniken beinhalten (z.B. Bildabgleich) (Aleroud and Zhou, 2017, pp. 172–173).

- Nutzungsverlauf-Abgleich: In den Benutzer- und Benutzerinnenprofilen werden Informationen über die Medien und die Authentifizierung des Benutzers oder der Benutzerin gespeichert, die für jedes Medium verwendet werden. Wenn solche Informationen in einem bestimmten Medium angefordert werden, das vorgibt, eines der im Profil gespeicherten legitimen Medien zu sein, verwendet die Anti-Phishing-Komponente die im Profil gespeicherten Informationen, um den Phishing-Versuch zu erkennen (Aleroud and Zhou, 2017, pp. 172–173).
- Muster-Abgleich: Anstatt Informationen über Benutzer- und Benutzerinnenaktivitäten aufzuzeichnen, werden Profile über andere Entitäten erstellt (z.B. legitime Websites, legitime E-Mail-Muster) (Aleroud and Zhou, 2017, pp. 172–173).
- Visueller-Abgleich: Die visuelle Ähnlichkeit wird auf Grundlage der visuellen Aspekte von Webschnittstellen wie Bildern, Blöcken und Layout berechnet, um zwischen Phishing- und legitimen Seiten unterscheiden zu können (Aleroud and Zhou, 2017, pp. 172–173).
- Whitelist- und Blacklist - Abgleich: Bei dieser Art liegt der Schwerpunkt auf der Erstellung einer Datenbank mit vertrauenswürdigen und verdächtigen Domänen. Sobald Anomalien mit Hilfe von Domänen-Filtertechniken erkannt werden, kann ein Abgleich mit einer Blacklist und/oder einer Whitelist durchgeführt werden. Basierend auf der Art und Weise, wie Blacklists erstellt werden, haben Virvilis et al. (2015) die vorhandenen Browser in drei Kategorien eingeteilt (Aleroud and Zhou, 2017, pp. 172–173):
    - 1. Browser, die das Google Safe Browsing nutzen, wie Chrome, Firefox und Safari (Aleroud and Zhou, 2017, pp. 172–173) .
    - 2. Browser, die ihre eigenen Blacklist verwenden, wie Internet Explorer und Edge (Aleroud and Zhou, 2017, pp. 172–173).
    - 3. Browser, die Blacklists von Drittanbietern zusammenstellen. Opera beispielsweise verwendet die Blacklists von Phishtank und Netcraft, um eine eigene Liste verdächtiger URLs zu erstellen (Aleroud and Zhou, 2017, pp. 172–173). PhishTank bietet über eine API eine Blacklist an (Alsharnouby, Alaca and Chiasson, 2015, p. 70). Die PhishTank-Website speichert die von den Nutzer und Nutzerinnen gemeldeten Phishing-Daten und können über eine API abgerufen werden (Gupta *et al.*, 2017, p. 3634).

Phishing-Gegenmaßnahmen, die auf Anti-Phishing-Symbolleisten beruhen, wurden entwickelt um zu erkennen ob eine Website legitim ist. Es gibt mehrere Methoden, die

diese Toolbars verwenden, um legitime Websites von Phishing-Websites zu unterscheiden: Benutzer- und Benutzerinnen-basiert, Whitelisting, Black Listing und heuristische Methoden. Die Art und Weise, wie Toolbars konfiguriert sind, spielt eine große Rolle für ihre Wirksamkeit bei der korrekten Erkennung potenzieller Bedrohungen. In einer von Cranor et al. (2007) durchgeführten Studie wurden zehn verschiedene Anti-Phishing-Toolbars miteinander verglichen. In dieser Studie wurde festgestellt, dass die Hälfte der getesteten Anti-Phishing-Symbolleisten 15% der Phishing-Websites falsch erkannten und vier der anderen Symbolleisten weniger als die Hälfte der betrügerischen Phishing-Websites erkannten. Alle zehn Anti-Phishing-Toolbars wiesen Probleme mit der Benutzer- und Benutzerinnenfreundlichkeit auf (Brickley, Thakur and Kamruzzaman, 2021, pp. 29–31). Symbolleisten die auf dem Webserver basieren umfassen den Schutz der Opfer durch SSL- (Secure Socket Layer) und TLS- (Transport Layer Security) Protokolle (Adil, Khan and Nawaz Ul Ghani, 2020, pp. 5–6).

- SSL (Secure Socket Layer) und TLS (Transport Layer Security) verwenden beide ein fortschrittliches kryptographisches Protokoll mit öffentlichem Schlüssel. Die Funktionsweise von TLS und SSL basiert auf dem Handshake, bei dem die Authentifizierung zwischen Benutzer und Benutzerinnen und Server durch einen Handshake erfolgt. Wenn der Authentifizierungs-/Handshake-Prozess abgeschlossen ist, wird ein sicherer Kanal zwischen Client und Server eingerichtet, um Daten zwischen Client und Server zu übertragen (Adil, Khan and Nawaz Ul Ghani, 2020, p. 6).
- HTTPS und IPSec sind weitere Protokolle, die zum Schutz der Opfer vor Phishing-Angriffen eingesetzt werden. IPSec (Internet Protocol Security) verwendet Authentication Header (AH) und Encapsulation Security Payload (ESP) zur Authentifizierung und Verschlüsselung von Daten. Authentication Header (AH) wird als Authentifizierungsprotokoll verwendet, während Encapsulation Security Payload (ESP) als Authentifizierungs- und Verschlüsselungsprotokoll verwendet wird, um einen sicheren Kommunikationskanal zwischen Client und Server zu schaffen und Authentifizierung, Vertraulichkeit und Datenintegrität zu erreichen (Adil, Khan and Nawaz Ul Ghani, 2020, p. 6).

Der Zweck der Anti-Phishing-Symbolleisten ist die Erkennung und Blockierung von Phishing-Websites. Der Benutzer oder die Benutzerin kann diese Symbolleisten als Webbrowser-Erweiterung sehen. Eine Sicherheitswarnung wird angezeigt, um den Internetnutzer oder die Internetnutzerin zu warnen, wenn eine Phishing-Website besucht wird. Es gibt zwei Arten von Sicherheitswarnungen: die passive und die aktive Warnung.

Bei der passiven Warnung wird der Inhalt der Website nicht blockiert, sondern nur die Warnung angezeigt, um den Benutzer oder die Benutzerin über den Phishing-Angriff zu informieren. Bei einer aktiven Warnung wird der Inhalt der Website blockiert, so dass der Benutzer oder die Benutzerin die Website nicht mehr aufrufen kann (Apandi, Sallim and Sidek, 2020, p. 4).

#### 2.3.5.3 Regel

Die regelbasierten Ansätze gehören zu den frühesten Lösungen, die für die Spam-Erkennung vorgeschlagen wurden. Zu den regelbasierten Lösungen gehören Blacklist- und Whitelist-Technologien und werden verwendet, um Phishing-Angriffe zu verhindern, indem ein Datensatz mit vertrauenswürdigen und nicht vertrauenswürdigen Websites und E-Mail-Adressen geführt wird (Wosah and Win, 2021, p. 66). Die Aufnahme in die Blacklist kann einer Phishing-Website schweren finanziellen Schaden zufügen, da der Datenverkehr um bis zu 95% zurückgeht (Alabdan, 2020, p. 24), was die Einnahmekapazität der Website und schließlich den Gewinn beeinträchtigt (Qabajeh, Thabtah and Chiclana, 2018, p. 49). Blacklists blockieren Inhalte auf der Grundlage von vordefinierten bösartigen IP-Adressen, Universal Resource Allocator (URL), E-Mail-Adressen und einigen Schlüsselwörtern sowie Benutzer- und Benutzerinnenverhalten wie Klicken, Aktualisieren, Bereitstellen, Folgen und Verlinke. Wenn ein Internetnutzer oder eine Internetnutzerin versucht, eine gefälschte Website zu besuchen, die bereits auf der Blacklist steht oder bekannt ist, verhindert der Webbrowser den Besuch, indem der Zugriff verweigert wird. Zudem werden unerwünschte E-Mails von der Blacklist auf Basis von gefälschten Absender- und Absenderinnenadressen blockiert (Wosah and Win, 2021, p. 66). Benutzer und Benutzerinnen, Unternehmen oder Computersoftwarefirmen können ihre eigenen Blacklists erstellen (Qabajeh, Thabtah and Chiclana, 2018, p. 49). Webbrowser können ihre eigenen Blacklist und Heuristiken zur Erkennung von Phishing führen (Alsharnouby, Alaca and Chiasson, 2015, p. 70). Derzeit gibt es einige hundert öffentlich zugängliche Blacklist, darunter die ATLAS-Blacklist von Arbor Networks, die OpenPhish-Liste, die Google-Blacklist und die Microsoft-Blacklist. Da jeder Benutzer oder jede Benutzerin oder jede kleine bis große Organisation Blacklist erstellen kann, weisen die derzeit öffentlich verfügbaren Blacklist unterschiedliche Sicherheitsniveaus auf, insbesondere im Hinblick auf zwei Faktoren (Qabajeh, Thabtah and Chiclana, 2018, p. 49):

- 1. Zeit: Die Blacklist wird aktualisiert und ist ständig verfügbar (Qabajeh, Thabtah and Chiclana, 2018, p. 49).

- 2. Ergebnisse: Qualität in Bezug auf die genaue Phishing-Erkennungsrate (Qabajeh, Thabtah and Chiclana, 2018, p. 49).

Benutzer und Benutzerinnen und Unternehmen tendieren dazu, Google- und Microsoft-Blacklists im Gegensatz zu anderen öffentlich zugänglichen Blacklists zu verwenden, da diese eine geringere Falsch-Positiv-Rate aufweisen. Die Blacklist von Microsoft wird normalerweise alle neun Stunden bis sechs Tage aktualisiert, während die Blacklist von Google alle zwanzig Stunden bis zwölf Tage aktualisiert wird (Qabajeh, Thabtah and Chiclana, 2018, p. 49). Ein großer Nachteil der Blacklist ist, dass eine neu erstellte Phishing-Adresse nicht auf die Blacklist gesetzt wird, sodass die URLs unentdeckt bleiben und der Zugang gewährt wird (Glăvan *et al.*, 2020, p. 3). Dieser Nachteil von Blacklists führte zu einem heuristischen Ansatz. Die heuristischen Ansätze waren in der Lage, neue Phishing-Websites zu erkennen (Wosah and Win, 2021, p. 69). Die Wirksamkeit von Blacklist basierenden Methoden wurde umfassend untersucht (Ludl et al., 2017, Sheng et al., 2009, Zhang et al., 2006), und eine hohe Falsch-Negativ-Rate (d.h. nicht erkannte Phishing-URLs) ist ein häufiges Problem. Eine gute Blacklist kann mehr als 90% der aktiven Phishing-URLs abdecken, aber die Erkennungsrate für eine neue Phishing-Site kann weniger als 20% betragen (Sheng et al., 2009). Daher sind Blacklist in der Anfangsphase von Phishing-Angriffen für den Schutz der Nutzer und Nutzerinnen unwirksam (Yang *et al.*, 2017, p. 2).

Whitelists enthalten in Gegensatz zu Blacklists eine Liste vertrauenswürdiger Websites. Der Benutzer oder die Benutzerin kann nur auf eine Website zugreifen, die als legitim eingestuft ist. Whitelists erkennen auch vertrauenswürdige Absender- und Absenderinnen-E-Mail-Adressen. Eine vertrauenswürdige Website, die nicht in der Whitelist aufgeführt ist und auf die ein Benutzer oder eine Benutzerin zuzugreifen versucht, wird von der Whitelist als Phishing-Website eingestuft, da sie der Whitelist nicht bekannt ist, so dass die Falsch-Negativ-Rate bei diesem Ansatz sehr hoch ist (Wosah and Win, 2021, p. 66). Diese Methode der Phishing-Erkennung ist nicht praktikabel, da es nahezu unmöglich ist vorherzusagen, welche Websites der Benutzer oder die Benutzerin besuchen wird, und jede neue Website würde als verdächtig eingestuft werden (Alabdan, 2020, p. 25). Eine der früh entwickelten Whitelists wurde von Chen und Guo (2006) vorgeschlagen, die auf dem Besuch vertrauenswürdiger Websites durch die Benutzer und Benutzerinnen basiert. Die Whitelist überwacht die Anmeldeversuche des Benutzers oder der Benutzerin, und wenn eine wiederholte Anmeldung erfolgreich durchgeführt wurde, fordert diese Methode den Benutzer oder die Benutzerin auf, diese Website in die Whitelist aufzunehmen. Eine klare Einschränkung der Methode von Chen

und Guo besteht darin, dass sie davon ausgeht, dass die Benutzer und Benutzerinnen mit vertrauenswürdigen Websites zu tun haben, was leider oft nicht der Fall ist (Qabajeh, Thabtah and Chiclana, 2018, p. 50)

#### 2.3.5.4 Heuristik

Heuristiken beziehen sich auf eine Reihe von Regeln, die auf früheren Ergebnissen und Erfahrungen basieren, um ein Problem zu lösen oder um zu lernen (Gupta, Arachchilage and Psannis, 2018, p. 257). Phishing-Heuristiken sind Merkmale die bei Phishing-Angriffen zu finden sind, wobei nicht garantiert ist, dass diese Merkmale in jedem Fall vorhanden sind (Gupta *et al.*, 2017, p. 3646). Auf Heuristiken basierende Phishing-Erkennungstechniken erweisen sich bei Zero-Day-Phishing-Angriffen als wirksam. Browser wie Mozilla Firefox und Internet Explorer verwenden heuristische Lösungen für die Phishing-Erkennung (Gupta, Arachchilage and Psannis, 2018, p. 259). Bei der heuristischen Methode wird der Inhalt der Website untersucht. Es gibt drei Arten von heuristischen Ansätzen, nämlich Oberflächeninhalte, Textinhalte und visuelle Inhalte. Die Heuristik des Oberflächeninhalts bedeutet, dass die URL der Website untersucht wird. Die Heuristik der Textinhalte bedeutet, dass die Begriffe oder Wörter auf der Website untersucht werden. Die Heuristik des visuellen Inhalts schließlich bedeutet, dass das Layout der Website untersucht wird (Apandi, Sallim and Sidek, 2020, p. 4). Die auf Heuristiken basierende Methode zur Erkennung von Phishing ist derzeit stark eingeschränkt, da heuristische Merkmale auf Phishing-Websites möglicherweise nicht vorhanden sind. Zudem muss beachtet werden, dass wenn Phisher und Phisherinnen die Erkennungsmerkmale oder die verwendeten Algorithmen kennen, können sie die Erkennung leicht umgehen (Alabdan, 2020, p. 25). Die folgende Heuristik wird verwendet, um die Zahl der Fehlalarme zu verringern (Gupta, Arachchilage and Psannis, 2018, p. 259):

- Eine Domäne, die älter als zwölf Monate ist, ist wahrscheinlich legitim (Gupta, Arachchilage and Psannis, 2018, p. 259).
- Das Vorhandensein eines „@“ im Link oder in der URL weist darauf hin, dass es sich um eine Phishing-Seite handelt (Gupta, Arachchilage and Psannis, 2018, p. 259).
- Das Vorhandensein von mehr als fünf „.“ zeigt an, dass es sich um eine Phishing-Seite handelt (Gupta, Arachchilage and Psannis, 2018, p. 259).
- Eingebettete HTML-Formulare deuten darauf hin, dass es sich um eine Phishing-Seite handelt (Gupta, Arachchilage and Psannis, 2018, p. 259).

#### 2.3.5.5 Authentifizierung

Obwohl Passwörter zu den meistgenutzten und stärksten Authentifizierungsmechanismen gehören, stellen sie aus Sicht der Nutzer und Nutzerinnen aufgrund der komplexen Anforderungen (z.B. Länge, Zeichenverwendung, Ablaufdatum, Wiederverwendung) eine Herausforderung dar. Darüber hinaus müssen die Benutzer und Benutzerinnen nicht nur diese Anforderungen erfüllen, sondern auch mehrere Passwörter verwalten, was zu einer hohen kognitiven Überlastung führt. Dieses Problem wurde zum Beispiel von Abroshan et al. (2018) angesprochen. Sie führten eine Reihe von Studien in realen Organisationen durch, um das Verhalten von Mitarbeiter und Mitarbeiterinnen im Umgang mit den Passwortrichtlinien ihrer Organisation zu untersuchen. Diese fanden heraus, dass Mitarbeiter und Mitarbeiterinnen schwache Passwörter generierten, dieselben oder ähnliche Passwörter wiederverwendeten und in den schlimmsten Fällen das Passwort aufschrieben (z.B. auf einem Klebezettel). Selbst bei strengen Sicherheitsrichtlinien bleibt ein Unternehmen also aufgrund dieser menschlichen Fehler anfällig für Cyberangriffe (Desolda *et al.*, 2021, p. 13).

Riley, S. (2006) hebt zwei wichtige Faktoren über Passwortpraktiken hervor. Erstens: Selbst wenn die Benutzer und Benutzerinnen wissen welche Kriterien ein sicheres Passwort haben sollte, wenden sie diese Kriterien in der Praxis nicht an. Zweitens hat eine Verbraucherumfrage im Jahr 2012 von CSID, dem führenden Anbieter von Technologien und Lösungen für den globalen Identitätsschutz und die Betrugserkennung, eine Diskrepanz zwischen den Absichten und Handlungen der Nutzer und Nutzerinnen bei der Erstellung von Passwörtern festgestellt. So gaben beispielsweise 89% der amerikanischen Verbraucher und Verbraucherinnen an, dass sie sich mit den derzeitigen Passwortverwaltungsgewohnheiten und Passwortverwendungsgewohnheiten sicher fühlen, obwohl viele von ihnen riskante Verhaltensweisen an den Tag legten z.B. 61% der Personen verwendeten ihre Passwörter auf mehreren Websites wieder und bei 21% waren ihre Konten zuvor kompromittiert worden (Sebescen and Vitak, 2017, p. 2238).

Um Phishing-Angriffe zu verhindern, sollte eine zusätzliche Sicherheitsebene geschaffen werden, sobald sich der Benutzer oder die Benutzerin auf einer Website anmeldet. Diese zusätzliche Sicherheitsebene wird durch die Zwei-Faktor-Authentifizierung (2FA) erreicht (Apandi, Sallim and Sidek, 2020, p. 3). 2FA hat sich für viele Dienste und Unternehmen zu einer der am meisten akzeptierten Sicherheitsüberprüfungen entwickelt (Jakobsson, 2018, p. 6). Ein One-Time-Passwort (OTP) ist eine häufig verwendete Methode für die 2FA-Methode. Ein OTP ist im Wesentlichen ein Kurzzeit-Passwort, das

bei Bedarf generiert wird und nach der ersten Verwendung nicht mehr gültig ist. Es ist in der Regel eine zufällig aussehende Zusammenstellung von Zahlen und/oder Buchstaben und läuft automatisch ab, wenn es nicht innerhalb einer kurzen Zeitspanne verwendet wird. Ein OTP zwingt den Benutzer oder die Benutzerin, zusätzlich zur Eingabe von Benutzer- und Benutzerinnennamen und Kennwort einen weiteren Schritt zu absolvieren. Selbst wenn ein Betrüger oder eine Betrügerin in der Lage ist, das Kennwort eines Benutzers oder einer Benutzerin zu erlangen, ist es in der Regel nicht möglich, den zweiten Authentifizierungsschritt zu umgehen. Daher ist eine zweite Authentifizierung eine der besten Methoden, um Benutzer- und Benutzerinnendaten zu schützen. Heutzutage ist es bei Transaktionen mit Banken, Aktien und Steuern üblich, dass ein Institut ein OTP zur Überprüfung sendet (Miller *et al.*, 2020, p. 3).

Es gibt zwar verschiedene 2FA-Methoden, aber die einfache SMS hat sich als favorisierter Option herauskristallisiert, da es unglaublich allgegenwärtig und leicht zu verstehen ist. Sei es ein iPhone oder ein altes Nokia oder eine junge bzw. ältere Person, alle mobilen Geräte unterstützen SMS und selbst die unerfahrensten oder technikfeindlichsten Nutzer und Nutzerinnen können eine Textnachricht lesen. Dennoch weist die SMS als Sicherheitsüberprüfungsmethode eine Reihe Schwachstellen auf. Eine Schwachstelle wird d oft ignoriert, der Endnutzer bzw. die Endbenutzerin (Jakobsson, 2018, p. 6). So könnte ein Kunde oder eine Kundin beispielsweise das OTP falsch lesen und gezwungen sein, den Bestätigungsvorgang zu wiederholen. Wenn der Kunde oder die Kundin das OTP zu langsam eingibt, könnte das System eine Zeitüberschreitung verursachen, so dass der Vorgang wiederholt werden muss. Manchmal entscheiden sich Unternehmen wegen der Unannehmlichkeiten, die sie den Kunden und Kundinnen bereiten, gegen die Verwendung von OTP. Das OTP bietet jedoch extreme Systemsicherheit mit einer minimalen Wahrscheinlichkeit, dass es gehackt werden kann. Die Kunden und Kundinnen müssen zwar die Unannehmlichkeit in Kauf nehmen, haben aber die Gewissheit, dass ihre Daten sicher sind (Miller *et al.*, 2020, p. 3). Ein Problem des 2FA ist jedoch, dass sie nicht die Identität des Benutzers oder der Benutzerin überprüft, sondern nur, ob er oder sie Zugang hat. 2FA ist auch anfällig für Phishing aus der Ferne. Der klare Nachfolger bzw. die klare Nachfolgerin ist der Wechsel von einem textbasierten numerischen Code zu einer Authentifizierungs-App wie Google Authenticator. Während solche Codes von einem Angreifer oder einer Angreiferin angefordert werden können, wird es für den Angreifer oder der Angreiferin jedoch schwieriger mit dem Angriff. Zur weiteren Stärkung der Abwehr von Angriffen durch unbefugte Nutzer und Nutzerinnen mit Zugang

zum Gerät wären Authenticator-Apps, die den Zugang über biometrische Daten kontrollieren (Jakobsson, 2018, pp. 6–8).

Die Multi-Faktor-Authentifizierung (MFA) bietet eine wertvolle zusätzliche Sicherheitsebene für IT-Netzwerke von Unternehmen. Darüber hinaus bietet MFA in einer Umgebung, in der Mitarbeiter und Mitarbeiterinnen routinemäßig Heimnetzwerke nutzen, die oft weniger sicher sind als Unternehmensnetzwerke, die Gewissheit, dass der Zugriff auf Unternehmensanwendungen und -systeme zuverlässig geschützt ist. Weitere Ansätze zum Schutz von Unternehmensdaten, die von Mitarbeiter und Mitarbeiterinnen im Außendienst bearbeitet werden, sind Ende-zu-Ende-Verschlüsselung und VPNs (Virtual Private Network). Die Verschlüsselung kann in Verbindung mit einem VPN oder allein verwendet werden, ist aber in der Regel auf einen bestimmten Dienst oder eine bestimmte Anwendung beschränkt. Ein VPN schützt die Daten vom Gerät bis zum Server. Um eine zusätzliche Sicherheitsebene zu schaffen, können einige VPNs so konfiguriert werden, dass sie mit einem Sicherheitsschlüssel für den Fernzugriff arbeiten. Für Mitarbeiter und Mitarbeiterinnen, die aus der Ferne arbeiten, ist die einmalige Anmeldung bequem, aber sollten diese Zugangsdaten kompromittiert werden, kann dies den Zugriff auf mehrere Anwendungen und Informationsquellen ermöglichen. Auch hier hilft MFA, um das Risiko zu mindern, dass Daten in die falschen Hände geraten und Cyberangreifer und Cyberangreiferinnen Zugang zu einer Reihe von Diensten erhalten. Bessere MFA-Methoden, wie eine mobile Authentifizierungs-App oder ein Hardware-Sicherheitsschlüssel erhöhen die Sicherheit, ohne die Nutzer und Nutzerinnen übermäßig zu belästigen (Sarginson, 2020, pp. 11–12).

#### 2.3.5.6 Honeypot

Anti-Phishing-Honeypots ist ein Tool zum Schutz der Opfer vor fortgeschrittenen Phishing-Angriffen, wie Malware und Würmern. Anti-Phishing-Honeypots sind sehr effektiv bei der Erkennung von Phishing-E-Mails und Websites (Adil, Khan and Nawaz Ul Ghani, 2020, p. 6). Honeypots (Netzwerkköder) können von Forscher und Forscherinnen und Organisationen als Köder für Angreifer und Angreiferinnen eingesetzt werden. Die Köder werden absichtlich als verwundbar gehalten, damit Angreifer und Angreiferinnen gelockt werden. Diese Honeypots sind isoliert und werden überwacht. Sie können verwendet werden, um die Aktivitäten von Phisher und Phisherinnen zu erfassen, die dann zu Forschungszwecken genutzt werden können, um ein besseres Verständnis der Angriffsflüsse und -trends zu erhalten (Bhadane and Mane, 2018, p. 5). Der Kerngedanke besteht darin Phisher und Phisherinnen aktiv Honigtoken zur Verfügung zu stellen.

Honey-Token können in fast jeder Form vorkommen wie z.B. ein gefälschtes Konto oder ein Datenbankeintrag, der nur für böswillige Abfragen ausgewählt werden würde. Auf Honey-Tokens basierende Ansätze können dabei helfen, Phishing-Aktivitäten zu verfolgen und dann zur Schließung von Websites verhelfen (Aleroud and Zhou, 2017, p. 173).

#### 2.3.5.7 Künstliche Intelligenz

Bei der Methode der künstlichen Intelligenz (KI) werden Algorithmen des überwachten Lernens zur Klassifizierung von Websites verwendet, um festzustellen, ob es sich um legitime Websites oder Phishing handelt. Zu den verwendeten Algorithmen gehören maschinelles Lernen und Deep Learning. Das maschinelle Lernen (Machine Learning - ML) hat im Vergleich zu anderen Lösungen vielversprechende Ergebnisse erbracht, da es in einigen Fällen die Phishing-Angriffe der Zero-Day fast vollständig vereitelt hat. ML-Filtertechniken sind inzwischen Stand der Technik und der Klassifizierung von Phishing-Websites und können für Blacklist verwendet werden (Jampen *et al.*, 2020, pp. 3–6). Es wurde eine Reihe verschiedener maschineller Lerntechniken erforscht, darunter Entscheidungsbäume und Support-Vector-Maschinen (SVM) (Alabdan, 2020, p. 25). Support-Vector-Machine (SVM) wird verwendet, um ein Klassifizierungsmodell zu entwickeln, das die strukturellen Eigenschaften von Mail Transfer Agent (MTA) und Mail User Agent (MUA) nutzt. Der SVM Ansatz fängt jede laufende E-Mail ab und überprüft sie mit Hilfe des trainierten SVM-Klassifikators auf Phishing-Attribute und -Merkmale. K-Nearest Neighbour (KNN) wird verwendet, um E-Mails entweder als Spam oder Phishing einzustufen. Es erkennt E-Mails auf der Grundlage von Ähnlichkeiten. Der Entscheidungsbaum-Algorithmus (Decision Tree Algorithm, DTA) wird eingesetzt, um bösartige Anhänge im E-Mail-Text zu erkennen. Natürliche Sprachverarbeitung (Natural Language Processing - NLP) wird verwendet, um Phishing-E-Mails zu erkennen (Wosah and Win, 2021, pp. 66–67).

Diese maschinellen Lerntechniken wurden für eine Vielzahl von Anti-Phishing-Techniken eingesetzt, von der Erkennung von Phishing-E-Mails bis hin zur Identifizierung von Diskrepanzen zwischen den Strukturen von Websites und den HTTP-Transaktionen. Die Methoden des maschinellen Lernens zur Erkennung von Phishing sind wesentlich vielseitiger. Sie sind in der Lage, Änderungen auf Phishing-Seiten zu erkennen. Die ML-Methode ist zwar leistungsfähig, hängt aber in hohem Maße von der Größe und Qualität des Trainingsdatensatzes ab, um eine optimale Genauigkeit zu erzielen (Alabdan, 2020, p. 25). Der Algorithmus des maschinellen Lernens hat jedoch die Einschränkung, dass er

bei großen Datensätzen unwirksam wird. Um die Leistung der Phishing-Erkennung zu verbessern, wurde der Deep-Learning-Algorithmus eingeführt. Im Vergleich zu maschinellen Lernalgorithmen ist der Deep-Learning-Algorithmus in der Lage, große Datensätze zu verarbeiten. Allerdings benötigt der Deep-Learning-Algorithmus mehr Zeit für das Training (Apandi, Sallim and Sidek, 2020, pp. 5–6). Barracuda Sentinel ist ein Beispiel für ein KI E-Mail Schutz Tool. Durch den Einsatz der KI zum Lesen interner, externer und historischer E-Mails kann die KI Trends und Muster erkennen, die es dann ermöglicht Anomalien und Phishing-Angriffe in Echtzeit zu blockieren. In einer von Cranor et al. (2007) durchgeführten Studie ergab sich für Barracuda Sentinel eine Effizienz von 98,2% bei der korrekten Erkennung von Angriffen aus dem Datensatz (Brickley, Thakur and Kamruzzaman, 2021, pp. 30–33).

### 2.3.6 Nicht-Technische Anti-Phishing Methoden

Der wichtigste nichttechnische Ansatz für die Cybersicherheit in Unternehmen ist die Entwicklung und Umsetzung von Programmen zur Sicherheitsausbildung, Schulung und Awareness für Informationssicherheit (Security Education, Training, and Awareness - SETA) für Mitarbeiter und Mitarbeiterinnen. SETA-Programme zielen darauf ab, die Mitarbeiter und Mitarbeiterinnen für die verschiedenen Cyber-Bedrohungen zu sensibilisieren und ihnen Informationen darüber zu geben, wie sie ihre täglichen Aufgaben im Hinblick auf diese Risiken sicher ausführen können. Im Allgemeinen sind diese Programme ein wesentlicher Bestandteil bei der Entwicklung einer allgemeinen Sicherheitskultur, fördern die Wahrnehmung der Benutzer und Benutzerinnen hinsichtlich der Zweckmäßigkeit und Wirksamkeit der Cybersicherheitsbemühungen des Unternehmens und helfen Mitarbeiter und Mitarbeiterinnen, sich der gezielten Phishing-Angriffe bewusst zu werden. Ein wichtiges Element, das von Sicherheitsexperten in SETA-Programmen eingesetzt wird, um Mitarbeiter und Mitarbeiterinnen gegen Phishing-Anfälligkeit zu schulen, sind simulierte Phishing-Attacken. Mehrere Unternehmen haben damit begonnen Phishing-Simulationsplattformen zu nutzen, welche simulierte Phishing-E-Mails anbieten und diese dann an die Benutzer und Benutzerinnen des Unternehmens zu senden (Canham *et al.*, 2021, p. 3). Ein weiterer Ansatz zur Verringerung der Auswirkungen von Phishing auf Online-Nutzer und Online-Nutzerinnen und Organisationen ist der Aufbau einer Anti-Phishing-Community, die die jüngsten Phishing-Aktivitäten überwacht und die verschiedenen Interessengruppen mit Nachrichten versorgt. Diese Anti-Phishing-Communities ermöglichen es Benutzer und Benutzerinnen, Phishing-Inhalte zu melden und andere Benutzer und Benutzerinnen und Organisationen zu warnen. PhishTank wurde 2003 als Tochtergesellschaft von OpenDNS

gegründet (Qabajeh, Thabtah and Chiclana, 2018, p. 48) und ist die beliebteste Datenbank über gemeldete Phishing-Websites. Die Datenbank bietet ein gemeinschaftsbasiertes Phishing-Verifizierungssystem, bei dem Nutzer und Nutzerinnen verdächtige Phishing-Websites melden und andere Nutzer und Nutzerinnen darüber abstimmen, ob es sich bei den Meldungen um Phishing oder um legitime Websites handelt (Aleroud and Zhou, 2017, p. 172). Eine weitere Möglichkeit, Phishing-Angriffe zu verhindern, besteht darin, sich rechtlich gegen diese Angriffe zu wehren. Entsprechende Rechtsvorschriften haben sich jedoch nur langsam durchgesetzt (Alabdan, 2020, p. 24). Einer der Hauptgründe dafür, dass rechtliche Maßnahmen nicht so wirksam sind wie erwartet, weil eine Phishing-Website oft nur eine kurze Lebensdauer hat, was die Strafverfolgung erschwert (Qabajeh, Thabtah and Chiclana, 2018, p. 48). Die Aufrechterhaltung der Informationssicherheit ist eine wichtige Herausforderung für Unternehmen und auch für den staatlichen und öffentlichen Verwaltungssektor (Reinheimer *et al.*, 2020, p. 259).

Nutzer- und Nutzerinnenorientierte Phishing-Interventionen sind über eine vielfältige Forschungslandschaft verstreut, die bisher nicht systematisiert wurde. Dies macht es schwierig, sich einen Überblick über die verschiedenen Ansätze früherer Arbeiten zu verschaffen. Aus diesem Grund haben Franz et al. (2021) auf der Grundlage einer systematischen Literaturanalyse eine Taxonomie von Phishing-Interventionen vorgelegt. Sie folgten dabei dem Ansatz von Jansen & van Schaik (2019), die vier verschiedene Kategorien von Nutzer- und Nutzerinnenorientierten Phishing-Interventionen beschrieben: Bildung, Awareness, Design und Schulung. In ihrer reinen Form fördern Bildungs- und Schulungsmaßnahmen typischerweise ein nachhaltiges, langfristiges sicheres Verhalten, mit dem zentralen Ziel, dass die Anwendung von Wissen und Fähigkeiten auf die reale Welt übertragen wird und die Nutzer und Nutzerinnen somit sichere Praktiken ausüben. Währenddessen zielen Awareness- und Designmaßnahmen darauf ab, die Sicherheit der Nutzer und Nutzerinnen bei bestimmten Aktivitäten (wie dem Einloggen auf einer Website oder dem Lesen einer E-Mail) kurzfristig zu verbessern (Franz *et al.*, 2021, pp. 339–342). Im Folgenden werden auf die vier Kategorien näher eingegangen und im Zuge dessen werden auch die wichtigsten Ergebnisse und Erkenntnisse vergangener Studien zusammengefasst.

#### 2.3.6.1 Bildung

Rein pädagogische Maßnahmen konzentrieren sich auf die Entwicklung von Wissen und Verständnis für Phishing-Bedrohungen und Phishing-Möglichkeiten z.B. durch die Bereitstellung von Bildungsmedien wie Texten oder Videos oder durch die Erörterung von

Online-Bedrohungen im Rahmen von Schulungen (Franz *et al.*, 2021, p. 342). Die Veröffentlichung von Artikeln zur Awareness im Internet ist ein gängiger Schulungsansatz (CJ *et al.*, 2018, p. 171). Bildungsinitiativen, die die Awareness für Phishing schärfen und gleichzeitig Phishing-Bedrohungen mit konkreten negativen Folgen in Verbindung bringen, können die notwendigen Fähigkeiten vermitteln, um Phishing-Angriffe zu vermeiden. Die bisherige Forschung unterstützt den Einsatz von Bildung als Interventionsstrategie und Mittel zur Verringerung der Anfälligkeit (Gavett *et al.*, 2017, p. 12). Die wirksamste Methode zur Verhinderung von Phishing-Angriffen besteht darin, den Benutzer und Benutzerinnen beizubringen, wie sie Phishing-E-Mails erkennen können (De Bona and Paci, 2020, p. 3).

Eminağaoğlu et al. (2009) haben gezeigt, dass die Bildung durch interaktive Inhalte die Awareness für die Phishing-Sicherheit wirksam erhöht (Yeoh *et al.*, 2021, p. 6). Kirlappos und Sasse (2012) vertraten die Ansicht, dass Sicherheitsbildung die Endnutzer- und Endnutzerinnenverhaltens berücksichtigen sollte, anstatt die Nutzer und Nutzerinnen vor Gefahren zu warnen (Arachchilage, Love and Beznosov, 2016, pp. 186–187). Goel et al. (2017) haben herausgefunden, dass die Bildung über gängige Phishing-Praktiken die Wahrscheinlichkeit verringert Opfer eines Phishings zu werden (Goel, Williams and Dincelli, 2017, p. 26). In der Arbeit von Reynolds et al. (2020) wird festgestellt, dass eine bessere Sicherheitsbildung den Nutzer und Nutzerinnen helfen könnte, sich vor URL-Verschleierungen in Acht zu nehmen (Desolda *et al.*, 2021, pp. 21–22). Sun et al. (2016) stellten fest, dass die Erhöhung des Sicherheitswissens der Nutzer und Nutzerinnen die Wahrscheinlichkeit verringern kann durch Phishing-E-Mails getäuscht zu werden. Reinheimer et al. (2020) stellten fest, dass die Bildung das Verständnis der Menschen dafür verbessern kann, wie und warum sie ihre Netzwerke schützen müssen und die Wahrscheinlichkeit erhöht, dass sie eine Bedrohung der Cybersicherheit erkennen und melden (Yeoh *et al.*, 2021, pp. 1–6).

#### 2.3.6.2 Awareness

Die Awareness zielt darauf ab die Aufmerksamkeit der Nutzer und Nutzerinnen auf potenzielle Bedrohungen und deren Gegenmaßnahmen zu lenken (Franz *et al.*, 2021, p. 343). Die mangelnde Awareness zur Sicherheit kann von Angreifer und Angreiferinnen missbraucht werden. Es wurde festgestellt, dass eine Vielzahl von Faktoren die Awareness der Menschen beeinflusst, darunter Erfahrungsfaktoren wie das Sicherheitswissen und Interneterfahrung, Selbstwirksamkeit im Umgang mit Computern (Aleroud and Zhou, 2017, p. 171) (d.h. das Vertrauen der Menschen in die Fähigkeit ein

Verhalten auszuführen) (Kwak *et al.*, 2020, p. 4), Faktoren wie Vertrauensbereitschaft, wahrgenommene Risiko und Misstrauen gegenüber Menschen (Aleroud and Zhou, 2017, p. 171). Abbasi et al. (2016) bestätigen, dass Awareness ein wichtiger Faktor ist, aber nur einer von vielen. Fast zwei Drittel der Nutzer und Nutzerinnen in ihrer Studie fielen von den Autoren und Autorinnen erstellten Phishing-Mails zum Opfer. Eine Analyse der über einen Fragebogen und eine Phishing-Simulation gewonnen Daten ergaben, dass unter anderem übermäßiges Selbstvertrauen und ein hohes Vertrauen in die Technologie seitens der Nutzer und Nutzerinnen nachteilig waren (Jampen *et al.*, 2020, p. 18). Williams et al. (2017) betonten, dass verschiedene menschliche Aspekte (z.B. Selbsttäuschung, Selbstkontrolle, Selbstbewusstsein, Vertrauen, Motivation, Fachwissen) und kontextbezogene Faktoren (z.B. Emotionen, Kultur, Organisation) die Awareness der Nutzer und Nutzerinnen beeinflussten. In ähnlicher Weise untersuchten Asfoor et al. (2018) Bankkunden und Bankkundinnen, um zu verstehen, welche menschlichen Faktoren die Awareness für Phishing-Angriffe am meisten beeinflussten. Die resultierenden menschlichen Faktoren waren Sicherheitsbedenken, Sicherheitsaufmerksamkeit, Kompetenz, IT-Wissen, jahrelange PC-Nutzung und Geschlecht (Desolda *et al.*, 2021, pp. 14–15).

Metalidou et al. (2014) haben einen vorläufigen Rahmen entwickelt, der die Korrelation zwischen menschlichen Faktoren und die mangelnde Awareness für Informationssicherheit aufzeigt. Die erste Dimension ist der "Mangel an Motivation", d.h. die Mitarbeiter und Mitarbeiterinnen müssen motiviert werden, sichere Verhaltensweisen und Praktiken anzuwenden, und die Unternehmensleitung muss herausfinden, was ihre Mitarbeiter und Mitarbeiterinnen motiviert. Die zweite Dimension ist der "Mangel an Awareness", der sich auf einen Mangel an Allgemeinwissen über Cyberangriffe bezieht. Beispielsweise wissen die Benutzer und Benutzerinnen nicht, wie wichtig es ist, ein starkes Passwort zu verwenden, um Phishing-Angriffe zu verhindern. Die dritte Dimension ist die "Risikogläubigkeit der Benutzer und Benutzerinnen". Ein Beispiel dafür ist, dass die Benutzer und Benutzerinnen glauben, dass die Installation von Antivirensoftware für ihre Daten nicht entscheidend ist. Die vierte Dimension ist das "Verhalten", beispielsweise das risikoreiche Verhalten der Benutzer und Benutzerinnen oder das fehlende Präventionsverhalten. Ein Beispiel dafür ist die Generierung schwacher Passwörter oder das Aufschreiben von Passwörtern auf physischen oder digitalen Blättern. Die fünfte Dimension ist der "unzureichende Einsatz von Technologie", der darauf abzielt, dass selbst die beste Technologie in Sicherheitsfragen ohne menschliche Mitarbeit nicht erfolgreich sein kann (Desolda *et al.*, 2021, p. 19).

Des Weiteren stellten Vishwanath et al. (2011) fest, dass die wahrgenommene Selbstwirksamkeit in Bezug auf das Wissen über die E-Mail-Nutzung und Phishing-Versuche per E-Mail die Wahrscheinlichkeit, auf eine Phishing-E-Mail zu reagieren, negativ beeinflusste. In ähnlicher Weise fanden Wang et al. (2017) heraus, dass eine Person mit hohem Selbstvertrauen in die Fähigkeit eine Phishing-E-Mail zu erkennen, eine stärkere Absicht zeigt, Bewältigungsmaßnahmen zu ergreifen, wie z.B. die sorgfältige Analyse von Hinweisen in einer E-Mail, um deren Legitimität zu bestimmen. Rhee et al. (2009) fanden heraus, dass die Selbstwirksamkeit in Bezug auf die Informationssicherheit nicht nur die Verwendung von Sicherheitssoftware beeinflusste, sondern auch das sicherheitsbewusste Verhalten wie die Nichtweitergabe sensibler Informationen per E-Mail oder die Verwendung schwer zu erratender Passwörter (Kwak *et al.*, 2020, p. 4).

Unter anderem führten Steyn et al. (2007) eine Phishing-Übung in einem akademischen Umfeld als Teil eines laufenden Projekts zur Awareness für Informationssicherheit durch. Sie kamen zu dem Schluss, dass Bildung- und Awareness-Aktivitäten in Bezug auf E-Mail-Umgebungen für die Bewältigung der zunehmenden Bedrohung durch Identitätsdiebstahl von entscheidender Bedeutung waren (Jampen *et al.*, 2020, p. 17). Darüber hinaus fanden Alnajim und Munro (2009) heraus, dass die Awareness einen erheblichen Einfluss auf die Effektivität der Nutzer und Nutzerinnen bei der Unterscheidung zwischen legitimen Websites und Phishing-Websites hatte (Abbasi *et al.*, 2021, p. 412). Halevi et al. (2015) bestätigten, dass die Awareness die häufig durch Schulungen erhöht wurde, den Teilnehmer und Teilnehmerinnen dabei half, nicht Opfer von Phishing zu werden, da die Testpersonen mehr darauf bedacht waren sich zu schützen (Jampen *et al.*, 2020, p. 12). Außerdem führte Alwanain (2019) ein reales Experiment durch, um die Phishing-Awareness der Nutzer und Nutzerinnen einer Organisation zu analysieren und ihre Awareness zu verbessern. Die Experimente richteten sich an 1500 Nutzer und Nutzerinnen im Bildungssektor. Die Ergebnisse zeigten einen hohen und signifikanten Effekt auf die Phishing Awareness der Nutzer und Nutzerinnen. Die Nutzer und Nutzerinnen waren in der Lage Phishing-E-Mails korrekt zu identifizieren dadurch einen Phishing-Angriff zu vermeiden. Dies führte zu einer höheren Phishing-Vermeidungsrate bei den Nutzer und Nutzerinnen mit Phishing-Awareness im Vergleich zu denen mit weniger Awareness (M. I. Alwanain, 2019, p. 327).

Daengsi et al. (2021) konzentrierten sich auf die Awareness von 20.000 landesweit tätigen Mitarbeiter und Mitarbeiterinnen eines großen Finanzinstituts in Thailand. Die Studie bestand aus drei Phasen: einem Phishing-Angriff, dem Wissenstransfer und einem zweiten Phishing-Angriff mit anderem Inhalt. Nach der Validierung der Daten und der

Analyse der Ergebnisse wurde festgestellt, dass sich die Awareness der Mitarbeiter für Cybersicherheit deutlich verbessert hatte. Die Zahl der Mitarbeiter und Mitarbeiterinnen, die die Phishing-E-Mail öffneten, ging um 71,5% zurück. Außerdem wurde festgestellt, dass das Geschlecht eine wichtige Rolle für die Awareness für Cybersicherheit spielt, da weibliche Angestellte in Thailand eine höhere Awareness für Cybersicherheit haben als männliche Angestellte (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 1). Die Ergebnisse des Experiments von Alwanain (2020) zeigten, dass Phishing-Awareness-Schulungen einen signifikant positiven Effekt auf die Fähigkeit älterer Nutzer und Nutzerinnen hatten, Phishing-Nachrichten zu erkennen und dadurch Angriffe zu vermeiden (Alwanain, 2020, p. 114).

Daneben untersuchten Alsharnouby et al. (2015), ob verbesserte Browser-Sicherheitsindikatoren und eine erhöhte Awareness für Phishing zu einer verbesserten Fähigkeit der Nutzer und Nutzerinnen geführt haben Phishing-Angriffe zu erkennen. Sie setzten ein Eye-Tracking-Gerät ein, um objektive quantitative Daten darüber zu erhalten, welche visuellen Hinweise die Aufmerksamkeit der Nutzer und Nutzerinnen auf sich ziehen, wenn sie die Legitimität von Websites prüften. Obwohl viele Teilnehmer und Teilnehmerinnen meldeten auf die URL geachtet zu haben, ergab die Studie, dass sie entweder versuchten sich an bekannte URLs zu erinnern oder Heuristiken wie die Bewertung der Einfachheit der URL verwendeten. Garera et al. (2007) argumentierten nachdrücklich, dass es oft möglich ist, Phishing-Websites von seriösen Websites zu unterscheiden, indem man sich die URL genau ansieht ohne den Inhalt der entsprechenden Website, Zeichen und Symbole wie Padlock-Symbole zu kennen (Arachchilage, Love and Beznosov, 2016, p. 187).

In Bezug auf Browser-Sicherheitsindikatoren haben Franz et al. (2021) 17 Studien zu Awareness Maßnahmen identifiziert, von denen drei passive Warnungen (d.h. die Warnung erfordert keine Interaktion des Nutzers oder der Nutzerin) und 15 interaktive Warnungen (d.h. die Warnung erfordert eine Interaktion des Nutzers oder der Nutzerin) untersuchten (Franz *et al.*, 2021, p. 344). Passive Phishing-Warnungen weisen den Benutzer oder die Benutzerin auf potenzielle Gefahren hin, ohne die Hauptaufgabe zu unterbrechen, z.B. durch Änderung der Farbe der Symbolleiste, Bereitstellung von Textinformationen und dynamischen Sicherheitsskins oder Hervorhebung der Domänenname in der Adressleiste. Wu et al. (2006) untersuchten drei Anti-Phishing-Symbolleisten, die den Benutzer und Benutzerinnen helfen sollten zu erkennen, wann sie mit betrügerischen Websites interagieren. Die meisten Teilnehmer und Teilnehmerinnen ignorierten die passiven Sicherheitsindikatoren und verließen sich stattdessen

hauptsächlich auf den Inhalt der Website, um deren Vertrauenswürdigkeit zu bestimmen. Die Teilnehmer und Teilnehmerinnen, die die Warnungen bemerkten, gingen davon aus, dass die Warnungen ungültig waren, weil sie die Warnungen nicht verstanden (Yang *et al.*, 2017, p. 2).Mehrere frühere Studien (Egelman et al., 2008, Wu et al., 2006) haben gezeigt, dass passive Maßnahmen wie Sicherheitssymbolleisten in einem Internetbrowser Phishing-Angriffe nicht wirksam verhindern konnten (Franz *et al.*, 2021, p. 344).Akhawe et al. (2012) fanden jedoch heraus, dass solche Meldungen in der Praxis tatsächlich wirksam sein können. Wenn Malware- oder Phishing-Warnungen angezeigt wurden, ignorierte nur ein Viertel der Nutzer und Nutzerinnen die Warnungen und öffnete die Website weiter. Wurde jedoch die Secure Socket Layer (SSL)-Warnseite angezeigt, klickten sich mehr als 70% der Nutzer und Nutzerinnen durch. Die Autoren und Autorinnen kamen zu dem Schluss, dass die Erfahrung eines Nutzers und einer Nutzerin mit einer bestimmten Warnmeldung einen erheblichen Einfluss auf die Klickrate hat. Nach Engelman et al. (2008) müssen solche Warnmeldungen so gestaltet sein (Jampen *et al.*, 2020, pp. 26–27), dass sie die aktive Aufmerksamkeit des Nutzers oder der Nutzerin haben, indem sie sie dazu gezwungen werden sich für eine der Optionen zu entscheiden, die in den Warnhinweisen präsentiert werden (Yang *et al.*, 2017, p. 2). Die Warnhinweise sollten nur dann erscheinen, wenn es notwendig ist und den Benutzer oder die Benutzerin dazu bringen die Nachricht tatsächlich zu lesen. Außerdem sollten die Hinweise klare und verständliche Auswahlmöglichkeiten anzeigen (Jampen *et al.*, 2020, p. 27).

Mehrere Forschungsarbeiten haben sich mit dem Mechanismus der erzwungenen Aufmerksamkeit befasst. Egelman et al. (2008) haben gezeigt, dass interaktive Warnungen, bei denen die Nutzer und Nutzerinnen zwischen Optionen wie „Zurück“ oder „Weiter zur Website“ wählen mussten, im Vergleich zu passiven Warnungen deutlich häufiger beachtet werden. Darüber hinaus haben Petelka et al. (2019) gezeigt, dass auf Links ausgerichtete Warnungen wirksamer sind als allgemeine E-Mail-Bannerwarnungen, um Nutzer und Nutzerinnen vor dem Anklicken bösartiger URLs zu schützen. Des Weiteren wurde festgestellt, dass die erzwungene Aufmerksamkeit diesen Effekt verstärkt (Franz *et al.*, 2021, p. 344). Die meisten Forschungsarbeiten zu Phishing-Warnungen wurden in Form von Rollenspielexperimenten in Laborumgebungen durchgeführt (Downs et al., 2006, Wogalter et al., 1997). Es ist jedoch fraglich inwieweit die Daten, die durch die Vorführung von Phishing-Warnungen im Labor gewonnen wurden, das Verhalten der Benutzer und Benutzerinnen in der Praxis widerspiegeln können (Yang *et al.*, 2017, p. 2).

Cuchta et al. (2019) untersuchten die Ergebnisse von drei Schulungsmethoden zur Awareness. Sie führten ein Experiment mit 4.777 Mitarbeiter und Mitarbeiterinnen, Fakultätsmitglieder und -mitgliederinnen und Studenten und Studentinnen der Fairmont State University durch. Während eines zweimonatigen Zeitraums wurden 90.000 E-Mails an die Teilnehmer und Teilnehmerinnen verschickt, wobei die E-Mails jeden Tag einen anderen Täuschungsansatz enthielten, um die Benutzer und Benutzerinnen zum Anklicken von Phishing-URLs zu verleiten. Folgende Methoden zur Awareness wurden angewandt (Papatsaroucha *et al.*, 2021, p. 30):

- Lange, textbasierte Dokumente, bei denen die Teilnehmer und Teilnehmerinnen ein 28-seitiges Dokument erhielten, das sie über Phishing informiert haben (Papatsaroucha *et al.*, 2021, p. 30).
- Phishing-E-Mail-Beispiele, bei denen die Teilnehmer und Teilnehmerinnen bestimmte verdächtige Schlüsselwörter in Phishing-E-Mails beobachten konnten (Papatsaroucha *et al.*, 2021, p. 30).
- Interaktive Spiele, bei denen die Teilnehmer und Teilnehmerinnen zunächst lernen mussten, wie sie Phishing-URLs erkennen können, und dann durch legitime und bösartige URLs navigieren mussten (Papatsaroucha *et al.*, 2021, p. 30).

Die Ergebnisse von Cuchta et al. (2019) zeigten, dass fast die Hälfte der für dieses Experiment rekrutierten Personen (44,3%) Opfer der simulierten Angriffe wurden. Die zweite Awareness Methode erzielte die besten Ergebnisse. Darüber hinaus erwies sich dieser Ansatz als noch wirksamer, wenn die Beispiele den Teilnehmer und Teilnehmerinnen präsentiert wurden, nachdem sie Opfer eines Phishing-Angriffs waren (Papatsaroucha *et al.*, 2021, p. 30).

#### 2.3.6.3 Design

Franz et al. (2021) haben 20 Publikationen identifiziert, die Designinterventionen untersuchten, um den sicheren Umgang der Nutzer und Nutzerinnen mit E-Mails und Online-Aktivitäten zu unterstützen. Visuelle Elemente spielten in mehreren Forschungsarbeiten eine Rolle (10 Publikationen). Iacono et al. (2004) haben das so genannte "UI-dressing" vorgeschlagen, einen Mechanismus, der auf der Idee individuell gestalteter Webanwendungen beruht (z.B. durch die Verwendung angepasster Bilder), um den Benutzer oder der Benutzerin bei der Erkennung gefälschter Websites zu unterstützen. Bei Farbcodes handelt es sich um einfache visuelle Hinweise (z.B. Ampelfarben), mit denen Benutzer und Benutzerinnen zwischen sicheren und riskanten

Umgebungen unterscheiden können. Diese Designintervention hat sich jedoch bisher als Sicherheitsindikatoren, ob eine Website echt oder gefälscht ist, als wenig erfolgreich erwiesen. Im Gegensatz dazu soll die Hervorhebung einer URL beispielsweise die Aufmerksamkeit der Nutzer und Nutzerinnen auf kritische Elemente richten. So haben sowohl Volkamer et al. (2017) als auch Lin et al. (2011) die Wirksamkeit von Domänen-Hervorhebung untersucht, um Nutzer und Nutzerinnen zu ermöglichen, den relevanten Teil einer URL zu finden. Nicholson et al. (2017) haben die Hervorhebung des Namens und der Adresse des Absenders oder Absenderin einer E-Mail untersucht. Andere gestalterische Maßnahmen zielten darauf ab, das Verhalten der Nutzer und Nutzerinnen umzuleiten, indem beispielsweise die Gewohnheit geschaffen wird, Browser-Lesezeichen anstelle von Hyperlinks zu verwenden. Ronda et al. (2008) haben "iTrustPage" entwickelt, ein Tool, das den Benutzer oder der Benutzerin vor verdächtigen Websites warnt (z.B. einer gefälschten PayPal-Website). Darüber hinaus bietet es Korrekturmaßnahmen in Form von Vorschlägen für alternative Websites an, die auf der Grundlage des Google-Suchindexes als vertrauenswürdig eingestuft werden (z.B. die echte PayPal-Website) (Franz *et al.*, 2021, p. 344).

#### 2.3.6.4 Schulung

Im Vergleich zu Bildung geht die Schulung einen Schritt weiter. Sie beinhalten in der Regel eine Art praktische Übung, bei der die Benutzer und Benutzerinnen Fähigkeiten entwickeln, die sie im Falle einer realen Bedrohung anwenden können. Schulungsansätze sollen dabei helfen Benutzer und Benutzerinnen Phishing-Websites, Phishing-E-Mails oder andere bösartige Angriffe zu erkennen (Franz *et al.*, 2021, p. 342). Zu den Schulungsmethoden gehören virtuelle Labore, Simulationen und Spiele (Mashtalyar *et al.*, 2021, pp. 424–425), in denen die Benutzer und Benutzerinnen das Lesen einer URL, das Analysieren einer E-Mail oder das Erkennen von Social-Engineering-Versuchen erlernen können (Franz *et al.*, 2021, p. 342). Die Forschungsergebnisse von Wright und Marett (2010) zeigten, dass die Erfahrung und die Schulung die wirksamsten Mittel zum Schutz vor Phishing sind (Miller *et al.*, 2020, p. 2). Das Ponemon Institute (2015) fand aus einer Umfrage mit 377 IT-Fachkräften ebenfalls heraus, dass die Wirksamkeit von Benutzer- und Benutzerinnenschulungen zur Erhöhung der Awareness durch einen erheblichen Rückgang von 64% der Klickrate auf bösartige Links belegt wurde (Kwak *et al.*, 2020, pp. 1–2). Drei Studien (Kumaraguru et al., 2009; Nyeste und Mayhorn, 2010; Sheng et al., 2007) fanden heraus, dass Phishing Schulungen die Wahrscheinlichkeit verringerte, dass Nutzer und Nutzerinnen auf Phishing-Attacken hereinfallen. Währenddessen zeigten die Ergebnisse der Studie von Caputo et al. (2013), dass Phishing-

Schulungsprogramme der behandelten Gruppe nicht dabei halfen, die Wahrscheinlichkeit zu verringern auf Phishing-Attacken hereinzufallen. Die Ergebnisse von Back und Guerette (2021) zeigten ebenfalls, dass die Schulung zum Thema Cybersicherheit nicht dazu beigetragen hat, die Teilnehmer und Teilnehmerinnen daran zu hindern, im Phishing Experiment hereinzufallen (Back and Guerette, 2021, pp. 429–442). Caputo et al. (2014) kamen gleichermaßen in ihrer Studie zu dem Ergebnis, dass sich die Phishing-Erkennungsrate von Mitglieder und Mitgliederinnen zweier Gruppen überhaupt nicht verbesserte unabhängig von der angewandten Schulungsmethode (Jampen *et al.*, 2020, p. 13).

Des Weiteren sind die Erkenntnisse der Studien darüber, wie lange die Teilnehmer und Teilnehmerinnen das in der Schulung erworbene Wissen behalten bzw. wie groß die Intervalle bis zu möglichen Nachschulungen sein sollten, unterschiedlich (Jampen *et al.*, 2020, p. 28). Caputo et al. (2014) sind der Meinung, dass die Auswirkungen der Schulungen nur kurzfristig sind (Goel, Williams and Dincelli, 2017, p. 26). In drei Fällen kamen Kumaraguru et al. (2007, 2008, 2010) zu dem Schluss, dass die Nutzer und Nutzerinnen die gelernten Inhalte mindestens eine Woche lang behalten konnten. Kumaraguru et al. (2009) bestätigten, dass das Wissen auch noch nach 28 Tagen erhalten bleibt. In einem ähnlichen Zeitrahmen zeigten Jackson et al. (2017), dass Nutzer das Anti-Phishing-Wissen bis zu 16 Tage nach ihrer ersten Schulung behalten haben (Jampen *et al.*, 2020, p. 28). Reinheimer et al. (2020) fanden eine signifikant verbesserte Leistung bei der korrekten Identifizierung von Phishing- und legitimen E-Mails direkt nach der Einführung des Programms fest und dies war nach vier Monate noch der Fall. Jedoch konnte dies nach sechs Monaten nicht mehr bestätigt werden. Aus diesem Grund wird eine Erinnerung der Nutzer und Nutzerinnen nach einem halben Jahr empfohlen (Reinheimer *et al.*, 2020, p. 259). In ähnlicher Weise stellten Canova et al. (2014) in ihrer Studie nach fünf Monaten einen signifikanten Leistungsabfall bei den Teilnehmer und Teilnehmerinnen fest. Schroeder (2017) rät dazu, dass jeder Nutzer und jede Nutzerin mindestens viermal pro Jahr geschult werden sollte. Anhand der Studien kann festgestellt werden, dass es verschiedene Erkenntnisse (Kumaraguru et al., 2007, 2009, Schroeder, 2017, Caputo et al., 2014) in Bezug auf die Ansicht der Wiederholungen von Schulungen gibt. Jedoch kommen die betrachteten Studien überwiegend zu dem Schluss, dass Schulungen als fortlaufender und integrierter Prozess konzipiert sein sollten. Die Mitarbeiter und Mitarbeiterinnen sollten in der Lage sein, sich auf eine Art und Weise fortzubilden, die sich für sie natürlich anfühlt. Zum Beispiel könnte die Fortbildung in ihre routinemäßigen Arbeitsaktivitäten integriert werden. In Al-Daeef et al., 2017 und

Schroeder, 2017 wurde festgestellt, dass durch kontinuierliches Anti-Phishing-Schulung die Klickraten nach der ersten Schulungseinheit von 58% auf einen einstelligen Prozentsatz reduziert werden konnten (Jampen *et al.*, 2020, pp. 26–29). Heartfield et al. (2016) fanden heraus, dass Nutzer und Nutzerinnen, bei denen die letzte Schulung länger zurückliegt, anfälliger sind auf Phishing-Attacken. Diese Erkenntnis deutet darauf hin wie wichtig es ist, sich über neue sicherheitsrelevante Themen auf dem Laufenden zu halten (Tornblad, Jones, *et al.*, 2021, p. 940). Damit das Lernen tatsächlich stattfindet, schlagen Van Niekerk und Von Solms (2004) ein Modell des organisatorischen Lernens vor. Die Theorien zum organisatorischen Lernen befassen sich mit der Idee, wie Organisationen lernen und das Verhalten anpassen. Das Organisatorische Lernen hat den Ursprung in der Arbeit von Argyris und Schon (1996). Das Organisatorische Lernen findet statt, wenn Einzelpersonen innerhalb einer Organisation eine problematische Situation erleben und sich im Namen der Organisation damit auseinandersetzen. Es gibt verschiedene Anwendungen von Lernprozessen, aber im Allgemeinen können drei Arten des Lernens kategorisiert werden. Diese drei Arten werden von Kennedy (2008) wie folgt zusammengefasst (Kearney and Kruger, 2013, pp. 380–381).

- Single-Loop-Learning: tritt auf, wenn Fehler erkannt und korrigiert werden und Organisationen den gegenwärtigen Status quo beibehalten, ohne die gegenwärtigen Strategien und Ziele zu ändern. Im Wesentlichen geht es beim Single-Loop-Learning um die Verbesserung des Status quo durch kleine inkrementelle Änderungen in der Funktionsweise der Organisation. Ein Beispiel aus dem Bereich der Informationssicherheit wäre der unbefugte Zugriff eines Benutzers oder einer Benutzerin auf privilegierte Daten. Eine Single-Loop-Reaktion würde darin bestehen, diesem Benutzer oder dieser Benutzerin den Zugang in Zukunft einfach zu verweigern. Der Status quo wird beibehalten und die derzeitigen Richtlinien und/oder Ziele werden nicht geändert (Kearney and Kruger, 2013, p. 381).
- Double-Loop-Learning: dabei werden der Status quo und die bestehenden Annahmen und Bedingungen in Frage gestellt und möglicherweise geändert. Das bedeutet, dass die Organisation ihre bestehenden Normen, Richtlinien, Verfahren und Ziele hinterfragt und modifiziert. Es kann dabei zu einem Wandel kommen, der den Status quo radikal verändert. In dem erwähnten Beispiel der Informationssicherheit könnte eine Double-Loop-Learning darin bestehen, die Umstände und Gründe für den unbefugten Zugriff zu untersuchen. Das Double-Loop-Learning kann dann zu einer Entscheidung führen, den Prozess der Vergabe

von Zugriffsrechten zu verbessern (zu ändern), um das Risiko eines unberechtigten Zugriffs in Zukunft zu minimieren (Kearney and Kruger, 2013, p. 381).

- Deutero-Learning: bedeutet, dass sich Fokus auf den Lernprozess selbst bezieht. Diese Art des Lernens zielt darauf ab die Art und Weise zu verbessern, wie Organisationen Single-Loop-Learning und Double-Loop-Learning durchführen. Es kann als "Lernen, wie man lernt" beschrieben werden (Kearney and Kruger, 2013, p. 381).

Aufgrund der Konzentration auf langfristige Ziele und der komplexeren Natur des Double-Loop-Learnings konzentrieren sich die meisten Unternehmen nur auf das Single-Loop-Learning. Nach Van Niekerk und Von Solms (2004) gilt dies auch für den Bereich der Informationssicherheit (Kearney and Kruger, 2013, p. 381).

#### 2.3.6.4.1 Herkömmliche Schulung

Die Wirksamkeit von herkömmlichen Schulungen, wie sie von Ausbilder und Ausbilderinnen mithilfe von Videositzungen und Seminaren durchgeführt werden, hängt in hohem Maße von der Fähigkeit der Ausbilder und Ausbilderinnen ab (CJ *et al.*, 2018, p. 171). Wash und Cooper (2018) haben weiters die Wirksamkeit von zwei Arten von Schulungen verglichen: eine Schulung mit Fakten und Ratschlägen und eine Schulung mit Geschichten von anderen Personen, die auf Phishing-Angriffe hereingefallen sind. Sie untersuchten auch, ob diese Schulungen unterschiedlich wahrgenommen werden, wenn sie von einem Sicherheitsexperten bzw. einer Sicherheitsexpertin oder von einem Kollegen bzw. einer Kollegin durchgeführt werden. Sie fanden heraus, dass Schulungen mit Fakten und Ratschlägen effektiver sind, wenn sie von einem Sicherheitsexperten ausgeübt werden, während Geschichten effektiver sind, wenn sie von Kollegen und Kolleginnen ausgeführt werden (De Bona and Paci, 2020, p. 3; Desolda *et al.*, 2021, p. 16).

Außerdem untersuchten Orunsolu et al. (2017) die Wirksamkeit der Sicherheitstipps, die eine nigerianische Bank den Kunden und Kundinnen als eine Form der Aufklärung zur Verfügung stellte. Die Ergebnisse der Autoren und Autorinnen zeigten, dass die meisten Teilnehmer und Teilnehmerinnen nicht in der Lage waren, eine Phishing-E-Mail zu erkennen, obwohl sie die Sicherheitstipps erhalten haben. Nach diesem Test führten die Autoren und Autorinnen eine kursbasierte Schulung durch und im Folgetest zeigten die Teilnehmer und Teilnehmerinnen eine höhere Erfolgsquote bei der Erkennung von Phishing-Bedrohungen (Jampen *et al.*, 2020, p. 13). Carella et al. (2017) fanden weiters heraus, dass Schulung mithilfe von Dokumenten im Vergleich zu In-Class-Schulungen

oder keiner Schulung am effektivsten ist (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 7). Sheng et al. (2010) untersuchten und testeten mehrere Anti-Phishing-Materialien und kamen jedoch zu dem Ergebnis, dass es keinen signifikanten Unterschied zwischen den Schulungseffekten der Materialien gibt, solange die Nutzer und Nutzerinnen mindestens eines von den Anti-Phishing-Materialien zur Verfügung gestellt bekommen. Ein ähnliches Ergebnis erzielten Jensen et al. (2017), die zu dem Schluss kamen, dass Schulungsmaterialien, die nur aus Text bestehen, ebenso wirksam sind wie die mit Text und Grafiken. Unter anderem fanden Carella et al. (2017) heraus, dass In-Class-Schulungen die stärksten kurzfristigen Auswirkungen haben. Der hohe kurzfristige Schulungseffekt von In-Class-Schulungen wurde auch von Karumbaiah et al. (2016) beobachtet, die zu dem Schluss kamen, dass Nutzer und Nutzerinnen die einem hochwertigen Anti-Phishing-Schulungsvideo ausgesetzt waren, während eines anschließenden 30-minütigen Experiments seltener auf Phishing-Links klickten als Nutzer und Nutzerinnen die anderen Schulungsmethoden ausgesetzt waren (Jampen *et al.*, 2020, pp. 26–27).

Sjouwerman, der Gründer und CEO von KnowBe4 (einer Phishing-Simulationsplattform), sagte jedoch, dass Herkömmliche Schulungen nicht funktionieren. Er meint, dass das erworbene Wissen durch diese Art von Schulung in Vergessenheit gerät, wenn diese nur einmal im Jahr durchgeführt wird. Des Weiteren hat er gesagt, dass die Botschaft innerhalb der Schulung nach einer Woche von jeden Teilnehmer und Teilnehmerinnen vergessen wird. Er ist der Meinung, dass mithilfe einer Schulung eine menschliche Firewall geschaffen werden muss. Das wichtigste Instrument zur Erreichung dieses Ziels ist der simulierte Phishing-Angriff. Es wird mit einem Basistest begonnen und dabei erhalten alle Mitarbeiter und Mitarbeiterinnen einen simulierten Phishing-Angriff und überprüft danach, wie viel Prozent der Mitarbeiter und Mitarbeiterinnen auf einen Link geklickt haben. Wenn der Wert hoch ist, dann müssen die Mitarbeiter und Mitarbeiterinnen diesen Wert erfahren. Danach müssen alle geschult werden und zwar durch interaktive und ansprechende Schulungen. So können die Mitarbeiter und Mitarbeiterinnen verstehen, dass es sehr riskant ist, auf Links zu klicken oder Anhänge von betrügerischen E-Mails zu öffnen. Sjouwerman sagt auch, dass es wichtig ist, laufend Tests durchzuführen. Das Problem der Phishing-Anfälligkeit der Mitarbeiter und Mitarbeiterinnen wird vielleicht nicht verschwinden, aber die Strategie besteht jedoch darin, den Angreifer und Angreiferinnen einen Phishing-Angriff so schwer wie möglich zu machen. Der Wert des simulierten Phishing-Angriff kann anfangs beispielsweise bei 27% liegen. Nach dreimonatiger Schulung sinkt der Anfangswert auf z.B. auf 13%. Nach einem

Jahr sind es in der Regel nur noch 2% der Personen, die bei den Tests durchfallen. Schulungen können dramatische Verbesserungen schaffen, es wird nicht perfekt sein, aber es nicht möglich einfach nichts dagegen zu unternehmen (Mansfield-Devine, 2018, p. 19).

#### 2.3.6.4.2 Eingebettete Schulung

Da die eingebettete Schulung oft effektiver sind als eine Lektüre oder die Teilnahme an einem Seminar, sollten die Ausbilder und Ausbilderinnen Phishing-Attacken simulieren und die Mitarbeiter und Mitarbeiterinnen darin schulen, wie sie Phishing-Attacken erkennen können (Miller *et al.*, 2020, p. 5). Die eingebettete Schulungsmethode (Alabdan, 2020, p. 24) ermöglicht es den Menschen, während der regelmäßigen Nutzung von E-Mails etwas über Phishing-Angriffe zu lernen. Dabei werden Phishing-E-Mails an die Benutzer und Benutzerinnen gesendet. Wenn ein Benutzer oder eine Benutzerin auf einen Phishing Link klickt, werden sofort Rückmeldungen und Anweisungen angezeigt, die es den Personen ermöglichen den Fehler zu erkennen (CJ *et al.*, 2018, p. 171).

Kumaraguru et al. (2009) entwickelten das Schulungssystem PhishGuru (Kirlappos and Sasse, 2012, p. 1). PhishGuru ist ein eingebettetes Schulungssystem, das Benutzer und Benutzerinnen beibringt nicht auf Phishing-Angriffe hereinzufallen, indem es eine Schulungsnachricht liefert, wenn der Benutzer und die Benutzerin auf die URL in einer simulierten Phishing-E-Mail klickt (Kumaraguru *et al.*, 2009, p. 2). Die simulierte Phishing-E-Mail dient nicht nur als Schulungsmechanismus, sondern auch als Test, um festzustellen, ob der Benutzer oder die Benutzerin gelernt hat legitime Nachrichten von Phishing-Nachrichten zu unterscheiden. Auf diese Weise können nur diejenigen Benutzer und Benutzerinnen identifiziert werden die weiterhin auf simulierte Phishing-Angriffe hereinfallen und nur ihnen werden Schulungen angeboten (Jansson and von Solms, 2013, p. 585). Die Ergebnisse von Kumaraguru et al. (2009) zeigten auch, dass Personen, die mit PhishGuru geschult wurden, das Gelernte langfristig behalten und dass mehrere Schulungsinterventionen die Leistung steigerten. Die Ergebnisse zeigten weiters, dass Benutzer und Benutzerinnen für die reale Welt effektiv geschult wurden und dieses Wissen mindestens 28 Tage lang behalten konnten. Die Ergebnisse zeigten auch, dass Personen, die zweimal geschult wurden, bei Tests zwei Tage, eine Woche und zwei Wochen nach der Schulung mit deutlich geringerer Wahrscheinlichkeit Informationen an die simulierten Phishing-Websites weitergaben. Kumaraguru et al. (2009) fanden außerdem heraus, dass die Schulung mit PhishGuru die Wahrscheinlichkeit von falsch-positiven Fehlern (Teilnehmer und Teilnehmerinnen, die legitime E-Mails als Phishing-E-Mails

identifizieren) nicht erhöht (Kumaraguru *et al.*, 2009, pp. 2–3). Für eingebettete Schulungen empfehlen Kumaraguru et al. (2007) und Jensen et al. (2017), dass eine Kombination aus Text und grafischen Hinweisen zu Phishing (Yeoh *et al.*, 2021, p. 6) effektiver ist als eine herkömmliche Sicherheitsmitteilung (Aleroud and Zhou, 2017, p. 171).

Doge et al. (2012) berichteten von Erfolgen beim Einsatz eingebetteter Schulungen. In einem Experiment mit drei Gruppen von jeweils 300 Teilnehmer und Teilnehmerinnen wurde die erste Gruppe einer eingebetteten Schulung unterzogen, die zweite Gruppe erhielt eine Benachrichtigung, nachdem sie Opfer einer Phishing-E-Mail wurden, und die dritte Gruppe war die Kontrollgruppe, die keiner Schulung unterzogen wurde. Die Ergebnisse zeigen, dass es über einen Zeitraum von zehn Tagen keinen signifikanten Unterschied in der Anfälligkeit der drei Gruppen gab. Über einen längeren Zeitraum (63 Tage in diesem Experiment) wurde jedoch festgestellt, dass die eingebettete Schulung zu einer signifikanten Verbesserung des Klickverhaltens der Teilnehmer und Teilnehmerinnen führte (Yeoh *et al.*, 2021, p. 12). Jansson und von Solms (2013) stellten ebenfalls fest, dass ein simulierter Phishing-Angriff zusammen mit einer eingebetteten Schulung dazu beigetragen hat, die Phishing-Resistenz der Nutzer und Nutzerinnen zu verbessern. Diese Ergebnisse scheinen die Annahme zu stützen, dass Simulation und eingebettete Schulungen eine wirksame Schulungsmethode darstellen (Miller *et al.*, 2020, p. 6).

Al-Daeef et al. (2017) beobachteten weiters, dass Nutzer und Nutzerinnen bessere Entscheidungen in Bezug auf Phishing-E-Mails trafen, nachdem sie eine eingebettete Schulung abgeschlossen haben (Jampen *et al.*, 2020, p. 26). Xiong et al. (2019) fanden außerdem heraus, dass es effektiver ist, eine eingebettete Schulung anzubieten, nachdem eine Person angegriffen wurde. Wenn den Einzelpersonen bewusst ist, dass sie Phishing-E-Mails nicht erkennen können, werden sie die anschließende Schulung eher zu schätzen wissen. Greene et al. (2018) untersuchten ferner die langfristige betriebliche Daten, die während einer eingebetteten Schulungen erfasst wurden. Diese Schulungen wurden viereinhalb Jahre lang in einer US-Regierungseinrichtung durchgeführt. Die Ergebnisse zeigten, dass sich die Phishing-Erkennungsrate der Personen verbesserte (Yeoh *et al.*, 2021, pp. 6–12).

#### 2.3.6.4.3 Simulierte Schulung

Frühere Forschungen (Kumaraguru et al., 2007; Zielinska et al., 2014; Singh et al., 2019) stützten sich häufig auf Simulationen und Spiele (Arachchilage und Love, 2013; Hale und Gamble, 2014; Silic und Lowry, 2020) und untersuchten bewährte Verfahren, Zeitpläne und Strategien für die Schulung von Benutzer und Benutzerinnen (Arduin, 2020, p. 12).

McElwee et al. (2018) untersuchten, wie Unternehmen die Anfälligkeit ihrer Mitarbeiter und Mitarbeiterinnen für Phishing-Angriffe verringern könnten. Grundlage dieser Analyse war eine Studie von vier Jahren, die in einer Organisation durchgeführt wurde. Die simulierte Schulung wurde angewandt, um Mitarbeiter und Mitarbeiterinnen in Bezug auf Phishing-Angriffe zu unterrichten. Diese Studie ergab, dass wiederholte und gezielte Übungen tatsächlich eine gute Methode darstellt, um die Anfälligkeit der Mitarbeiter und Mitarbeiterinnen für Phishing-Angriffe zu verringern (Desolda *et al.*, 2021, p. 14). Des Weiteren untersuchten Gordon et al. (2019) die Auswirkungen eines Phishing-Schulungsprogramms auf die Phishing-Klickraten von Mitarbeiter und Mitarbeiterinnen einer US-Gesundheitseinrichtung. Gordon et al. (2019) teilten ihre Teilnehmer und Teilnehmerinnen in zwei Gruppen ein: Täter bzw. Täterinnen und Nicht-Täter bzw. Nicht-Täterinnen. Als Täter bzw. Täterinnen wurden diejenigen definiert, die auf mindestens fünf simulierte Phishing-E-Mails geklickt haben, und als Nicht-Täter bzw. Nicht-Täterinnen diejenigen, die dies nicht getan haben. Insgesamt gab es 5.416 Teilnehmer und Teilnehmerinnen, davon klickten 772 auf mindestens fünf E-Mails und nur 975 (17,9%) klickten auf null Phishing-E-Mails. 3.565 Personen (65,3%) klickten auf mindestens zwei E-Mails. Gordon et al. (2019) weisen darauf hin, dass die Klickraten von Mitarbeiter und Mitarbeiterinnen bei Simulationen durch wiederholte Tests sinken (Gordon *et al.*, 2019, p. 547). Nachin et al. (2019) untersuchten weiters die Erhöhung von Cybersecurity-Awareness mit mehr als 4.500 Mitarbeiter und Mitarbeiterinnen aus 20 Organisationen. Sie stellten auch fest, dass der simulationsbasierte Ansatz zur Erhöhung der Cybersecurity-Awareness beitragen kann und praktischer ist als eine herkömmliche Schulung die von Ausbilder und Ausbilderinnen geleitet werden (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 9). Baillon et al. (2019) testeten in einem großen Feldexperiment mit mehr als 10.000 Mitarbeiter und Mitarbeiterinnen eines niederländischen Ministeriums die Wirkung einer simulierten Schulung und die Bereitstellung von Information. Des Weiteren wurde auch die Wirkung der Kombination der beiden Ansätzen analysiert. Beide Ansätze getrennt verringerten den Anteil der Mitarbeiter und Mitarbeiterinnen, die das Passwort weitergaben. Jedoch hat die

Kombination von beiden Ansätzen keine größere Wirkung gezeigt (Baillon *et al.*, 2019, p. 1).

#### 2.3.6.4.4 Spielbasierte Schulung

Die spielbasierte Anti-Phishing-Schulung ist so konzipiert, dass sie die Aufmerksamkeit der Benutzer und Benutzerinnen weckt, aufrechterhält, herausfordert und weiterbildet. Mit dem spielbasierten Ansatz wird versucht, die herkömmlichen Schulungsmethoden wie PowerPoint, Videos und Vorträge zu umgehen. Bei den herkömmlichen Schulungsmethoden klicken sich meist die Benutzer und Benutzerinnen in der Regel durch die Folien oder spielen die Videos im Hintergrund ab (Brickley, Thakur and Kamruzzaman, 2021, p. 34). Serious Games sind eine Kategorie computergestützter Spiele, die für die Schulung von Nutzer und Nutzerinnen konzipiert sind. Spiele gelten als besonders effektiv, wenn sie auf ein bestimmtes Problem ausgerichtet sind oder eine bestimmte Fähigkeit vermitteln sollen. Spiele helfen dabei, neue Regeln und Ideen zu entdecken, anstatt sie nur auswendig zu lernen. Sie können auch als Übungswerkzeug dienen, um vorhandenes Wissen anzuwenden (CJ *et al.*, 2018, p. 171).

Kumaraguru et al. (2007) stellten eine Studie vor, um Menschen über Phishing-Angriffe aufzuklären. Die Autoren und Autorinnen entwarfen dafür ein Online-Spiel namens "Anti-Phishing Phil". Dieses Spiel lehrte die Benutzer und Benutzerinnen wie sie Hinweise in Domänennamen verstehen können (Ltd, 2018, p. 141). Anti-Phishing Phil bringt zudem Benutzer und Benutzerinnen bei, wie sie Phishing-URLs erkennen können, wo sie nach Hinweisen in Webbrowsern suchen und wie sie Suchmaschinen nutzen können, um legitime Websites zu finden. Kumaraguru et al. (2007) berichteten, dass die Benutzer und Benutzerinnen nach der Schulung besser in der Lage waren, Phishing-Websites zu erkennen. Die Falsch-Positiv-Rate sank von 30% auf 14% und die Falsch-Negativ-Rate von 34% auf 17%. Trotz dieser Rückgänge zeigt die Addition der beiden Prozentsätze, dass 31% der Nutzer und Nutzerinnen noch nicht in der Lage sind, zwischen einer guten und einer schlechten Website zu unterscheiden (Kirlappos and Sasse, 2012, pp. 1–2). Sheng et al. (2007) zeigten außerdem, dass Nutzer und Nutzerinnen die das Spiel spielten, Phishing-Websites unmittelbar nach dem Spiel und eine Woche später besser erkennen konnten (Alsharnouby, Alaca and Chiasson, 2015, p. 71).

Nyeste et al. (2010) erstellten weiters eine Phishing-Schulung in Form eines einfachen Comics und eines komplexen Videospiels und zeigten, dass beide hilfreich waren, um die Phishing-Anfälligkeit zu verringern (Nicholson *et al.*, 2020, pp. 3–4). Mayhorn und Nyeste

(2012) zeigten auch, dass Schulungen durch Comics und Videospiele die Anfälligkeit für Social-Engineering sehr wirksam verringerten (Goel, Williams and Dincelli, 2017, p. 26).

Arachchilage et al. (2016) berichteten über den Entwurf und die Entwicklung eines Prototyps für ein mobiles Spiel, das Nutzer und Nutzerinnen helfen sollte, sich vor Phishing-Angriffen zu schützen. Es wurde eine Studie mit einem Prä- und Posttest durchgeführt, um das Spielkonzept anhand des entwickelten Prototyps zu bewerten. Die Ergebnisse der Studie zeigten eine signifikante Verbesserung des Phishing-Vermeidungsverhaltens der Teilnehmer und Teilnehmerinnen in der Post-Test-Bewertung. Die Teilnehmer und Teilnehmerinnen erreichten 49% im Prätest und 78% im Posttest, wenn es darum ging, Phishing-Websites von legitimen Websites zu unterscheiden. Alle Teilnehmer und Teilnehmerinnen gaben an, dass sie bei der Bewertung der Websites im Prätest nur selten auf die Adressleiste gesehen und Posttest dies geändert haben. Am Anfang haben viele Teilnehmer und Teilnehmerinnen falsche Strategien angewandt, um die Legitimität einer Website zu bestimmen. Eine der häufigsten Strategien bestand darin zu prüfen, ob die Website professionell gestaltet wurde oder nicht. Dies ist jedoch keine sinnvolle Strategie, denn viele Phishing-Websites sind exakte Nachbildungen legitimer Websites (Arachchilage, Love and Beznosov, 2016, pp. 185–191).

Cj et al. (2018) führten ein Experiment mit dem Spiel „Phishy“ durch, einer spielbasierten Phishing Awareness Schulung. Die Ergebnisse deuteten darauf hin, dass Phishy für die Teilnehmer und Teilnehmerinnen, die wenig Wissen über das Thema hatten, effektiver war. Die Ergebnisse der Umfrage nach dem Spiel zeigten einen signifikanten Anstieg des Prozentsatzes der richtigen Antworten im Vergleich zur Umfrage vor dem Spiel. Dies unterstreicht die Tatsache, dass spielbasiertes Lernen einen positiven Beitrag zur Schulung von Benutzer und Benutzerinnen in Unternehmen leistet (CJ *et al.*, 2018, pp. 169–178). Pandit et al. (2018) führten auch einen umfangreichen Test zur Nutzer- und Nutzerinnenschulung mit dem Spiel Phishy durch. Das Spiel führte zu höheren Werten bei der Identifizierung von Phishing-Links unter den Nutzer und Nutzerinnen in Unternehmen (Das *et al.*, 2019, p. 5).

Eine weitere spielbasierte Schulung zu Phishing-Angriffen wurde von Wen et al. (2019) vorgestellt. Das Spiel „What.Hack“ zielt darauf ab, Benutzer und Benutzerinnen in Phishing zu schulen, indem sie in ein Rollenspiel eingebunden werden. Das Rollenspiel simuliert Phishing-Attacken vor dem sich die Spieler und Spielerinnen schützen müssen.

Die Studie hat gezeigt, dass das Rollenspiel effektiver und ansprechender ist als herkömmliche Formen der Schulung (Desolda *et al.*, 2021, p. 16).

Kumaraguru et al. (2010), Ndibwile et al. (2017), Wen at al. (2019) und Sheng et al. (2007) schlagen interaktive, spielbasierte Lösungen vor, um Nutzer und Nutzerinnen zu verschiedenen sicherheitsrelevanten Themen zu schulen. Diese Arbeiten schlagen Ansätze vor, die effektiver sind als herkömmliche Schulungsmethoden, die beispielsweise auf der Verwendung von Videos mit Demonstrationen möglicher Angriffe beruhen, die sich die Nutzer und Nutzerinnen öfters passiv ansehen (Desolda *et al.*, 2021, p. 18). Silic und Lowry (2020) haben beobachtet, dass spielbasierte Sicherheitsschulungssysteme die verschiedenen Levels oder Leaderboards enthalten die intrinsische Motivation der Nutzer und Nutzerinnen erhöhten und zu einem besseren Sicherheitsverhalten führten (Franz *et al.*, 2021, p. 342).

#### 2.3.6.4.5 Verhaltensschulung

Eine weitere Methode zur Verringerung der Erfolgsquote von Phishing-Versuchen ist die Verhaltensänderung. Die Verhaltensänderung kann eine Herausforderung darstellen, weil Verhaltensweisen schwer zu ändern sind (Miller *et al.*, 2020, p. 4). Verhaltensschulungen helfen Mitglieder und Mitgliederinnen eines Unternehmens nicht nur, Phishing-Nachrichten zu erkennen und zu vermeiden, sondern auch neue Angriffe zu erkennen und die automatisierte Anti-Phishing-Techniken zu verfeinern. Sicherheitsforscher und Sicherheitsforscherinnen haben bereits zahlreiche Verhaltensschulungsprogramme entwickelt, mit denen Einzelpersonen lernen können, Phishing-Angriffe zu erkennen. Die meisten dieser Schulungsprogramme verfolgen einen regelbasierten Ansatz. Bei regelbasierten Schulungsansätzen wird die Abwehr von Phishing-Angriffen als eine Identifizierungsaufgabe verstanden. Dabei werden die Teilnehmer und Teilnehmerinnen trainiert auf Hinweise zu achten und zu erkennen und Schutzmaßnahmen zu ergreifen. Dabei müssen bestimmte Regeln befolgt werden wie z.B. nicht auf einen Link in einer E-Mail von einem unbekannten Absender oder einer unbekannten Absenderin klicken oder in der Adressleiste nach HTTPS suchen. Durch die Wiederholung von Schulungen hilft der regelbasierte Ansatz den Personen Verhaltensweisen zu verinnerlichen und in gewohnter Weise anzuwenden. Die Unternehmen schicken daher beispielsweise häufig Erinnerungsschreiben oder verlangen jährliche oder halbjährliche Schulungen (Jensen *et al.*, 2017, p. 599).

Eine Verhaltensschulung kann damit beginnen, Schulungen für alle Mitarbeiter und Mitarbeiterinnen zu priorisieren, aber es sollten auch die Mitarbeiter und Mitarbeiterinnen identifiziert werden, die am anfälligsten auf Phishing-Attacken sind. Unternehmen können eine Reihe von Techniken anwenden, um die anfälligsten Personen zu ermitteln wie z.B. die Verwendung von simulierten Phishing-Attacken. Die Verhaltensschulung kann weiter verbessert werden, wenn Manager und Managerinnen und IT-Mitarbeiter und IT-Mitarbeiterinnen die Gedankengänge der Mitarbeiter und Mitarbeiterinnen zu riskanten Verhaltensweisen erkennen können. Des Weiteren müssen sie den Mitarbeiter und Mitarbeiterinnen beibringen, welche typische Anzeichen es für Phishing-Attacken gibt wie z.B. Rechtschreibfehler, ein hohes Maß an Dringlichkeit, Drohungen, generelle Anreden oder Aufforderungen zur Angabe persönlicher oder arbeitsbezogener Daten (Miller *et al.*, 2020, p. 4). Es ist auch bekannt, dass die Beteiligung der obersten Führungsebene einen starken Einfluss auf die Organisationskultur und die Einstellung der Mitarbeiter und Mitarbeiterinnen zur Einhaltung von Informationssicherheitsrichtlinien hat. Nach Hu et al. (2012) übt die oberste Führungsebene den organisatorischen Einfluss über drei Mechanismen aus: Legitimität, Engagement und wahrgenommene Fairness. Durch die Teilnahme von der obersten Führungsebene an Sicherheitsinitiativen wird den Schulungsprogrammen Legitimität verliehen und ein Gefühl des Engagements für die Sicherheitsrichtlinien vermittelt. Des Weiteren wird den Mitarbeiter und Mitarbeiterinnen die Möglichkeit gegeben selbst Kontrolle auszuüben und das trägt so zur wahrgenommenen Fairness bei (Bansal, 2018, p. 2).

Knapp et al. (2006) stellten eine positive Korrelation zwischen der Unterstützung durch die oberste Führungsebene und der Sicherheitskultur sowie der Durchsetzung der Sicherheitspolitik fest. Bansal (2018) untersuchte die Rolle der Beteiligung des Top-Managements bei der Schaffung von Phishing Awareness in einer Organisation. In dieser Studie wurde ein Feldstudienexperiment mit Phishing-Täuschung durchgeführt. Die Studie wurde in zwei Phasen durchgeführt. In der ersten Phase wurden die teilnehmenden Mitarbeiter und Mitarbeiterinnen einer Universität nach dem Zufallsprinzip mit zwei verschiedenen Phishing-Awareness-Schulungsvideos geschult. Das erste Video beinhaltete eine Person aus dem Top-Management einer Universität und das zweite Video einen neu eingestellten IT-Mitarbeiter bzw. IT-Mitarbeiterin. In der zweiten Phase wurden drei Phishing-Angriffe durchgeführt. Die Ergebnisse zeigen ebenfalls, dass die wahrgenommene Beteiligung des Top-Managements einen signifikant positiven Einfluss auf die Schaffung von Awareness für Phishing und die Verhinderung

von Phishing-Angriffen auf Mitarbeiter und Mitarbeiterinnen hat (Bansal, 2018, p. 1). Wie bereits besprochen wurde, verwenden Unternehmen häufig regelbasierte Schulungen, um die Auswirkungen von Phishing einzudämmen. Jedoch haben Forscher und Forscherinnen vorgeschlagen, den Schwerpunkt auf Verhaltensschulungen zu legen. Denn die Wiederholung von regelbasiertem Schulung führt aus mehreren Gründen möglicherweise nicht zu einer erhöhten Resistenz gegenüber Phishing-Angriffen (Jensen *et al.*, 2017, pp. 597–600).

- Erstens: Es kann eine wiederholte regelbasierte Schulung an Effektivität verlieren, weil es zu einem (echten oder falschen) Gefühl der Beherrschung von Schulungskonzepten führen kann. Eine wirksame Sicherheitsschulung sollte den aktuellen Wissensstand der Person mitberücksichtigen. Mit zunehmender Wiederholung der Schulung entwickelt die Person ein Gefühl der Vertrautheit mit den Schulungskonzepten und glaubt zunehmend das Konzept bereits zu verstehen. Daher kann es die Person als unnötig empfinden sich mit wiederholten Schulungen zu befassen (Jensen *et al.*, 2017, p. 600).
- Zweitens: Es kann eine regelbasierte Schulung dazu führen, dass eine Person sich an vorgegebene Hinweise und Regeln gewöhnt, die jedoch keinen ausreichenden Schutz gegen individuelle oder neuartige Phishing-Angriffe bietet (Jensen *et al.*, 2017, p. 600).
- Drittens: Eine regelbasierte Schulung ignoriert die Grenzen der menschlichen Wahrnehmung und vernachlässigt die Aufmerksamkeit der Personen bei der Erkennung von Phishing-Angriffen. Wenn eine neue Nachricht eintrifft, ist die Feststellung, ob es sich um eine Bedrohung handelt oft eine Nebenaufgabe, die durch operativ wichtigere Aufgaben (z.B. schnelles Reagieren auf eine E-Mail) verdrängt wird (Jensen *et al.*, 2017, p. 600).

Folglich nutzen Phisher und Phisherinnen erfolgreich Ablenkungen oder routinierte, gedankenlose Reaktionen aus, die sich aus einer solchen schlechten Aufmerksamkeit ergeben. Damit die Verhaltensschulung verbessert werden kann, sind Ansätze erforderlich die die Aufmerksamkeit der Einzelpersonen auf Angriffe zu richten. Die regelbasierten Schulungsansätze sind gut geeignet, um ein grundlegendes Verständnis für Phishing zu schaffen. Jedoch bieten diese Theorien und Ansätze oft nicht die dynamische Awareness, welches für die Abwehr von neu entwickelnden und angepassten Phishing-Angriffe erforderlich ist. Fast alle Mitarbeiter und Mitarbeiterinnen erhalten einen ständigen Strom von Nachrichten die über diverse digitale Kanäle (z.B. E-Mail, Chat, Textnachrichten oder soziale Medien) übermittelt werden. Die angestellten

Personen müssen bei der Verarbeitung dieser Nachrichten dabei auf mehrere Ziele achten. Sie müssen den nahezu konstanten Strom von Nachrichten verwalten und angemessen darauf reagieren. Außerdem müssen sie arbeitsbezogene Aufgaben schnell und effizient erledigen. Die Bewältigung von Mehrfachbelastungen (z.B. die schnelle Verarbeitung von Informationen und die Erledigung betrieblicher Aufgaben) kann dazu führen, dass die Arbeitnehmer und Arbeitnehmerinnen nicht in der Lage sind, organisatorischen und individuellen Sicherheitspraktiken Priorität einzuräumen. Aus diesem Grund nutzte Jensen et al. (2017) die Achtsamkeitstheorie, um einen neuartigen Schulungsansatz zu entwickeln. Dieser Schulungsansatz kann durchgeführt werden, nachdem die Teilnehmer und Teilnehmerinnen mit der regelbasierten Schulung vertraut sind. Die Achtsamkeitsschulung lehrt Einzelpersonen ihre Aufmerksamkeit während der Bewertung von Nachrichten dynamisch zu nutzen. Zusätzlich soll diese Art der Schulung die Awareness für den Kontext einer Nachricht erhöhen und die falsche Bewertung verdächtiger Nachrichten verhindern. Um die Wirksamkeit des Ansatzes von Jensen et al. (2017) zu bewerten, verglichen sie in einer Feldstudie an einer US-amerikanischen Universität die regelbasierte Schulung und die Achtsamkeitsschulung mit 355 Studenten und Studentinnen, Dozenten und Dozentinnen und Mitarbeiter und Mitarbeiterinnen, die mit Phishing-Angriffen vertraut waren und bereits regelmäßig regelbasierte Schulungen erhielten. Jensen et al. (2017) fanden heraus, dass die Teilnehmer und Teilnehmerinnen die eine Achtsamkeitsschulung erhielten, besser in der Lage waren Phishing-Angriffe zu vermeiden. Jensen et al. (2017) erläutern im Folgenden, wie Achtsamkeitskonzepte die Phishing-Resistenz verbessern können (Jensen *et al.*, 2017, pp. 598–602).

- Erstens: Um Informationen zu stehlen oder Malware auszuliefern, müssen Phishing-Nachrichten eine ausdrückliche Handlungsaufforderung enthalten (z.B. auf einen Link klicken, einen Anhang herunterladen). Eine Nachricht, die keine solche Aufforderung enthält, ist weniger verdächtig. Aus diesem Grund sind explizite Handlungsaufforderungen der Auslöser für eine aufmerksamere Betrachtung des Kontextes einer empfangenen Nachricht. Im Gegensatz zum regelbasierten Ansatz, der sich auf die Beurteilung der Merkmale einer Nachricht konzentriert (z.B. die E-Mail-Adresse der Absender und Absenderinnen, die Beschaffenheit eines eingebetteten Links), hilft ein Fokus auf explizite Aufforderungen einer Person dabei den Zweck oder das beabsichtigte Ergebnis der Nachricht zu verstehen. Zusammengefasst unterstützt die Achtsamkeitsschulung Einzelpersonen bei der dynamischen Zuweisung von Aufmerksamkeit während der

Bewertung einer Nachricht je nachdem ob diese eine ausdrückliche Handlungsaufforderung enthält oder nicht (Jensen *et al.*, 2017, p. 602).

- Zweitens: Die Achtsamkeitsschulung ermutigt die Personen häufig dazu, innezuhalten und über den Kontext und die Umgebung nachzudenken. Eine solche Reflexion führt zu einer größeren Aufmerksamkeit für die Umgebung, was den Menschen hilft die gedankenlose Verarbeitung eingehender Nachrichten zu vermeiden. Wenn Personen innehalten, um die Nachrichten und den Kontext zu betrachten, erkennen sie mit größerer Wahrscheinlichkeit kritische Details wie die Beziehung zwischen ihnen und dem Absender oder der Absenderin einer Nachricht, die Relevanz von Themen in der Nachricht oder die Angemessenheit einer Anfrage. Damit sind die Personen besser in der Lage Phishing-Nachrichten von legitimen Nachrichten zu unterscheiden. Das Nachdenken erfordert kognitive Ressourcen und Zeit und ist daher nur dann ratsam, wenn eine Nachricht eine ausdrückliche Aufforderung zum Handeln enthält (z.B. auf einen Link klicken, einen Anhang herunterladen). Zusammengefasst unterstützt die Achtsamkeitsschulung bei der Awareness von Personen für den Kontext einer Nachricht und das aktive Hinterfragen dieser Nachricht. (Jensen *et al.*, 2017, p. 602).
- Drittens: Um keine voreiligen Schlüsse zu ziehen, ermutigen Achtsamkeitsschulungen dazu Schlussfolgerungen zu unterlassen. In der Phishing-Schulung bekommt das Vorwegnehmen einer Schlussfolgerung eine neue Bedeutung. Wenn Menschen mit Täuschungen konfrontiert werden, sind sie oft misstrauisch gegenüber betrügerischen Nachrichten, zögern aber die Nachrichten als Täuschung einzustufen, weil sie befürchten, dass sie legitim sein könnten. Wenn eine Person sich über die Rechtmäßigkeit einer Nachricht unsicher ist, könnte die Bestätigung des Verdachts auch ein Anstoß sein den Verdacht mit einer vertrauenswürdigen dritten Partei (z.B. IT-Abteilung) zu überprüfen. Zusammengefasst unterstützt die Achtsamkeitsschulung bei der Vorbeugung von Schlussfolgerungen in Bezug auf verdächtige Nachrichten (Jensen *et al.*, 2017, pp. 602–603).

### 2.3.7 Phishing Anfälligkeitsmerkmale

In den letzten Jahren haben Forscher und Forscherinnen versucht die wichtigsten Faktoren zu ermitteln, die die individuelle Anfälligkeit für Phishing-E-Mails beeinflussen könnten. Diese Faktoren werden nun besprochen und der aktuelle Stand der Forschung wird miteinbezogen.

#### 2.3.7.1 Demografische Merkmale

##### 2.3.7.1.1 Geschlecht

Es haben mehrere Studien (Hambyrger und Ben-Artzi 2000, 2003, Jagatic et al., 2007, Bilge et al., 2009, Sheng et al., 2010, Hong et al., 2013, Tzipora Halevi et al., 2015, Sun et al., 2016, Iuga et al., 2016, Gregory et al., 2017) gezeigt, dass Frauen im Vergleich zu Männern anfälliger für Phishing sind (Benenson, Gassmann and Landwirth, 2017, p. 939; Goel, Williams and Dincelli, 2017, p. 24; Moody, Galletta and Dunn, 2017, p. 313; Broadhurst *et al.*, 2018, p. 7; Rastenis *et al.*, 2020, p. 3; Tornblad, Jones, *et al.*, 2021, p. 565).

Jagatic et al. (2007) z.B. schickten simulierte Phishing-E-Mails an Versuchspersonen und untersuchten, ob das Geschlecht und die Vertrautheit zum scheinbaren Absender oder Absenderin die Anfälligkeit der Empfänger und Empfängerinnen für Phishing-Angriffe veränderten. Zu diesem Zweck sammelten die Forscher und Forscherinnen über ein soziales Netzwerk Informationen zu den Freunden und Freundinnen der Versuchspersonen und schickten dann eine E-Mail mit dem Betreff: „Hey, schau dir das an“ und einem Link. Nachdem die Teilnehmer und Teilnehmerinnen auf den Link geklickt hatten, mussten sie sich auf der Website anmelden. Die Studie ergab, dass nicht nur die Mehrheit der Probanden bereit war, ihre Anmeldedaten auf einer unechten Website einzugeben, sondern auch eher reagierten, wenn die E-Mail von einem bekannten Freund oder einer bekannten Freundin stammt. Des Weiteren wurde festgestellt, dass Männer eher auf eine Nachricht reagierten, die scheinbar von einer Frau stammte. Sie fanden auch heraus, dass Frauen eher auf Links klicken als Männer (Moody, Galletta and Dunn, 2017, p. 566). Halevi et al. (2013) stellten ebenfalls fest, dass Frauen anfälliger für Phishing-Angriffe sind als Männer (53% der Frauen im Vergleich zu 14% der Männer). Halevi et al. (2015) bestätigten, dass Frauen anfälliger für Phishing-Angriffe sind als Männer (40% der Frauen fielen auf ein zweistufiges Phishing-Schema herein, aber nur 27% der Männer) (De Bona and Paci, 2020, p. 2; Tornblad, Jones, *et al.*, 2021, p. 939). Die Studie von Goel et al. (2015) ergab, dass 68,7% der Studenten und Studentinnen, die die E-Mails öffneten, auch auf den Link klickten. Die Frauen öffneten die E-Mails häufiger als Männer, klickten aber genauso häufig auf den Link wie Männer (Papatsaroucha *et al.*, 2021, p. 17). Oliveira et al. (2017) untersuchten den Bedarf an individuelleren Verteidigungsmechanismen gegenüber Phishing-Angriffen, und die Ergebnisse zeigten, dass Frauen anfälliger sind und daher eine gute Verteidigungsstrategie das Geschlecht berücksichtigen sollte (Desolda *et al.*, 2021, p. 16). Sheng et al. (2010) argumentierten,

dass die höhere Anfälligkeit von Frauen für Phishing auf das geringere technische Wissen und ihre Erfahrung zurückzuführen ist. Darwish et al. (2012) stellten fest, dass die Anfälligkeit der Frauen eine Folge ihrer angenehmeren Persönlichkeit sein könnte (Anawar *et al.*, 2019, p. 2868).

In der Studie von Goel et al. (2017) umfasste der Akt auf einen Phishing-Betrug hereinzufallen, zwei Schritte: erstens das Öffnen einer Phishing-E-Mail, und zweitens das Klicken auf den darin enthaltenen bösartigen Link. Die Autoren und Autorinnen fanden heraus, dass Frauen riskante E-Mails eher als Männer öffnen, jedoch seltener auf Links klicken jedoch waren die Unterschiede nicht statistisch signifikant (Broadhurst *et al.*, 2018, p. 7). Andere Studien (Kumaraguru et al., 2009, Zielinska et al., 2014, Gavett et al., 2017, Moody et al., 2017, Butavicius et al., 2017, Oliviera et al., 2017, Parsons et al., 2019) fanden keine geschlechtsspezifischen Unterschiede in der Anfälligkeit von Phishing-Angriffen (Tornblad, Jones, *et al.*, 2021, p. 940).

Mohebzada et al. (2012) jedoch haben darauf hingewiesen, dass Männer mit größerer Wahrscheinlichkeit auf Phishing-Links klicken und persönliche Daten preisgeben als Frauen (Tornblad, Jones, *et al.*, 2021, p. 940). Flores et al. (2014) führten eine Studie durch, die sich auf gezielte Phishing-Angriffe konzentrierte. Sie fanden heraus, dass Frauen weniger anfällig für Phishing-Angriffe sind als Männer (Jampen *et al.*, 2020, p. 16). Die Umfrage des Australian Institute of Criminology ergab ebenfalls, dass Männer deutlich häufiger Opfer eines Identitätsdiebstahls werden als Frauen (Broadhurst *et al.*, 2018, p. 7).

#### 2.3.7.1.2 Alter

Mehrere Studien (Jagatic et al., 2007, Kumaraguru et al., 2009, Sheng et al., 2010, Parsons et al., 2019, Sarno et al., 2019, Li et al., 2020, Back und Guerette 2021) haben ergeben, dass die Anfälligkeit bei Menschen im Alter von 18 bis 25 Jahren am höchsten ist (Benenson, Gassmann and Landwirth, 2017, p. 939; Goel, Williams and Dincelli, 2017, p. 10; Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 25; Tornblad, Jones, *et al.*, 2021, p. 3).

Darwish et al. (2013) untersuchten eine Liste menschlicher Merkmale, die auf die Anfälligkeit für Phishing hinweisen könnten, darunter das Geschlecht des Opfers, Bildungsniveau, Phishing-Schulung, Methode der Phishing-Schulung, Persönlichkeit und Internetnutzung. Die Ergebnisse deuten darauf hin, dass die Person die am anfälligsten für Phishing-Angriffe zwischen 18 und 25 Jahre alt sind, ein geisteswissenschaftliches

Studium absolviert haben, keine Anti-Phishing-Schulungen absolviert haben und im E-Commerce tätig sind (Thomas, 2018, p. 6). Die Ergebnisse von Bandi 2016 zeigten ebenfalls, dass jüngere Menschen im Vergleich zu älteren Altersgruppen ein geringeres Online-Sicherheitsverhalten aufweisen (Anawar *et al.*, 2019, p. 2868). Sarno et al. (2017) untersuchten die Beziehung zwischen Alter (zwischen 18 und 46 Jahren) und Geschlecht bei der Identifizierung einer E-Mail als Spam, authentisch oder gefährlich. Ihre Ergebnisse deuteten darauf hin, dass jüngere Erwachsene stärker durch nicht authentische E-Mails gefährdet sind als Erwachsene mittleren Alters (Abroshan *et al.*, 2021c, p. 44931). Die Umfrage des Australian Institute of Criminology ergab, dass die 25- bis 34-Jährigen deutlich häufiger Opfer eines Identitätsdiebstahls werden als andere Altersgruppen (Goldsmid et al., 2017) (Broadhurst *et al.*, 2018, p. 7).

Andere Studien (Oliveira et al., 2017, Lin et al., 2019, Whitty 2019, Li et al., 2020) hingegen deuten darauf hin, dass ältere Erwachsene möglicherweise tatsächlich anfälliger sind als jüngere Erwachsene (Benenson, Gassmann and Landwirth, 2017, p. 939; Tornblad, Jones, *et al.*, 2021, p. 3). Kim et al. (2019) berichteten ebenso, dass die jüngste Gruppe aus den vier verschiedenen Altersgruppen (19 bis 30 Jahre, 31 bis 40 Jahre, 41 bis 65 Jahre und mehr als 65 Jahre) tendenziell die höchste Awareness für Cybersicherheit hatten, während die älteste Gruppe tendenziell die niedrigste Awareness für Cybersicherheit aufgewiesen haben. Baillon et al. (2019) untersuchten eine sehr große Zahl von Arbeitnehmer und Arbeitnehmerinnen in den Niederlanden und fanden ebenfalls heraus, dass die jüngere Altersgruppe (16-25 Jahre) am wenigsten wahrscheinlich auf Phishing-Links klickten, während die Arbeitnehmer und Arbeitnehmerinnen in der Altersgruppe über 46 Jahre 15% wahrscheinlicher auf den gefälschten Link klicken als die jüngste Gruppe (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 10).

Die Auswirkung des Alters auf die Anfälligkeit für Phishing wurde größtenteils durch frühere Erfahrungen mit Phishing, Erfahrung im Umgang mit dem Internet, Wahrnehmung des finanziellen Risikos und Bildungsjahre erklärt. Ältere Erwachsene sind möglicherweise besonders anfällig für Phishing-Versuche. Ältere Erwachsene scheinen überproportional häufig Ziel vieler Arten von Betrug zu sein, einschließlich finanzieller Ausbeutung aufgrund ihres größeren Vermögenspotenzials, geringeren Vertrautheit, geringeren Komforts und geringeren Selbstwirksamkeit im Umgang mit Computern, geringeren Erfahrung mit dem Surfen im Internet und erhöhten Risikos für altersbedingten kognitiven Abbau. Selbst wenn keine leichte kognitive Beeinträchtigung oder Demenz vorliegt, können ältere Erwachsene Beeinträchtigungen bei der

Entscheidungsfindung aufweisen. Es ist jedoch anzumerken, dass einige Studien (Gavett et al., 2017, Baillon et al., 2019) keine erhöhte Anfälligkeit in der Altersgruppe der 18- bis 25-Jährigen im Vergleich zu älteren Gruppen nachweisen konnten. So fanden Zielinska et al. (2014) beispielsweise keinen Unterschied zwischen jungen Menschen (18-25 Jahre) und anderen Menschen (über 26 Jahre) in Bezug auf die Phishing-Anfälligkeit (Gavett *et al.*, 2017, pp. 2–3).

#### 2.3.7.1.3 Herkunft

Flores et al. (2015) untersuchten kulturelle Unterschiede und persönliche Einstellungen zu Phishing. Sie fanden in ihrer Studie keine signifikante Korrelation zwischen Phishing-Verhalten und Alter oder Geschlecht. Sie fanden hingegen signifikante positive Korrelationen zwischen dem von dem Mitarbeiter und der Mitarbeiterin beobachteten Phishing-Verhalten und Sicherheit Awareness und Schulung. Die Stärke der Korrelationen war jedoch in den verschiedenen Kulturen unterschiedlich (d.h. USA, Indien und Schweden). Die Korrelationen Sicherheit Awareness und dem Phishing-Verhalten waren bei amerikanischen und indischen Personen nicht signifikant, bei schwedischen Personen jedoch schon. Die Korrelation zwischen Schulung und Phishing-Verhalten war bei amerikanischen Personen stärker als bei schwedischen Personen und bei indischen Personen nicht signifikant (Goel, Williams and Dincelli, 2017, p. 25).

#### 2.3.7.1.4 Bildungsstand und Studienrichtung

Das Bildungsniveau hat einen signifikanten Einfluss auf das Misstrauen gegenüber Phishing, so dass Personen mit einem höheren Bildungsniveau misstrauischer sind, was darauf hindeutet, dass sie weniger wahrscheinlich Opfer von Phishing werden. Jagatic et al. (2007) wiesen nach, dass Personen mit naturwissenschaftlichen und technologiebezogenen Studienfächern (z.B. Informatik) weniger anfällig für regelmäßiges Phishing waren als andere Studienfächer. Interessanterweise waren jedoch Nutzer und Nutzerinnen in naturwissenschaftlichen Studiengängen die anfälligste Gruppe für Phishing, wenn die Nachrichten von einem Freund stammten. Parsons et al. (2013) fanden heraus, dass Personen mit einem höheren Bildungsniveau signifikant besser in der Lage waren, mit Phishing-E-Mails umzugehen, allerdings nur, wenn ihnen nicht mitgeteilt wurde, dass es sich um eine Phishing-Studie handelte (Tornblad, Jones, *et al.*, 2021, p. 940).

Die Studie von Goel et al. (2015) ergab hingegen, dass Studenten und Studentinnen des Studiengangs Wirtschaft die E-Mails eher öffneten, aber die Klickrate war die gleiche wie

bei Studenten und Studentinnen des Studiengangs Humanwissenschaften. Die Autoren und Autorinnen schlugen vor, dass diese Ergebnisse darauf hindeuten, dass Personen mit einem hohen Maß an Neugier oder mit Berufs-/Ausbildungsrollen die eine höhere Rate an menschlicher Interaktion durch E-Mails erfordern, eher dazu neigen Phishing-E-Mails zu öffnen. Allerdings werden diese Personen oft nicht Opfer der angewandten Täuschungstechniken (Papatsaroucha *et al.*, 2021, pp. 17–18). Moody et al. (2017) konnten hingegen nicht nachweisen, dass die Bildung die Anfälligkeit vorhersagt (Tornblad, Jones, *et al.*, 2021, p. 940). Die Ergebnisse der Studie von Abroshan et al. (2021) zeigten jedoch, dass Personen mit höherem Bildungsniveau ein größeres Risiko haben, während des COVID-19-Ausbruchs Opfer von Phishing zu werden (Abroshan *et al.*, 2021b, p. 121925).

#### 2.3.7.1.5 Beruf

Der Stil des beruflichen Engagements besteht aus drei Unterskalen, die sich auf die Gründe beziehen, warum sich Menschen für ihre Arbeit engagieren (Tornblad, Jones, *et al.*, 2021, p. 941):

- Normatives Engagement aufgrund von Verpflichtungen (Tornblad, Jones, *et al.*, 2021, p. 941).
- Kontinuierliches Engagement, das auf den wahrgenommenen Vorteilen der Beschäftigung und den Kosten des Ausscheidens beruht; und (Tornblad, Jones, *et al.*, 2021, p. 941).
- Emotionales Engagement, das auf der Identifikation mit der Organisation und der emotionalen Bindung beruht (Tornblad, Jones, *et al.*, 2021, p. 941).

Workman (2008) fand heraus, dass der Stil des beruflichen Engagements die Anfälligkeit für Phishing in Abhängigkeit vom Inhalt des Angriffs vorhersagte wie z.B. das Personen mit hohem kontinuierlichem Engagement anfällig für Angriffe waren, die eskalierende Anfragen beinhalteten und Personen mit hohem emotionalem Engagement anfällig für Angriffe waren, die soziale Erwünschtheit beinhalteten. Vishwanath (2015) fand außerdem heraus, dass normatives und kontinuierliches Engagement signifikante positive Prädiktoren für die Beantwortung einer Freundschaftsanfrage von einem gefälschten Profil auf Facebook sind, aber nicht für die anschließende Beantwortung einer Phishing-Nachricht, die von diesem Profil aus gesendet wurde. Emotionales Engagement hingege trug nicht zur Phishing-Anfälligkeit bei (Tornblad, Jones, *et al.*, 2021, p. 941).

Frühere Untersuchungen haben ergeben, dass die Anfälligkeit für Phishing in Unternehmen nach der demografischen Komponente der Mitarbeiter und

Mitarbeiterinnen variiert. Sebescen und Vitak (2017) z.B. fanden heraus, dass jüngere Mitarbeiter und Mitarbeiterinnen am anfälligsten für Phishing-Bedrohungen sind (Anawar *et al.*, 2019, p. 2868). Kumaraguru et al. (2008) stellten außerdem fest, dass Mitarbeiter und Mitarbeiterinnen in technischen und nichttechnischen Berufen ähnlich anfällig für Phishing sind. Dies wird von Vishwanath et al. (2011) bestätigt, dass selbst geschulte Nutzer und Nutzerinnen Opfer von Phishing werden können (Jampen *et al.*, 2020, p. 20). Die Analyse von Back und Guerette (2021) deutet darauf hin, dass Personen in höheren Positionen und mit längerer Betriebszugehörigkeit eher auf Phishing-Angriffe reinfallen (Back and Guerette, 2021, p. 443). Thomas (2018) zeigte ebenfalls auf, dass Nutzer und Nutzerinnen in hochrangigen Positionen, die mit sensiblen Daten umgehen und mit der Unternehmensführung interagierten, anfälliger für Phishing-Angriffe sind. Thomas (2018) hat außerdem herausgefunden, dass Nutzer und Nutzerinnen die täglich große Mengen an E-Mails verarbeiten, anfälliger für Phishing-Angriffe sind. Die vertraute und gewohnheitsmäßige Nutzung von E-Mails kann Nutzer und Nutzerinnen anfälliger für Phishing-Angriffe machen. Diese Personen sollten auch als eine Kategorie identifiziert werden, die besonders geschult und überwacht werden sollte, um die Anfälligkeit zu verringern (Thomas, 2018, p. 16).

#### 2.3.7.2 Menschliche Anfälligkeiten

Die Angreifer und Angreiferinnen überzeugen gerne ihre Opfer, um diese positiv oder negativ zu beeinflussen. Eine positive Beeinflussung durch Überredung beinhaltet beispielsweise die Täuschung über eine Belohnung, wenn eine bestimmte Handlung ausgeführt wird. Eine negative Beeinflussung erfolgt hingegen durch Drohungen oder autoritäre Einschüchterung (Mashtalyar *et al.*, 2021, p. 420). Cialdini (2007) identifizierte sechs Schlüsselprinzipien der Überzeugung: Reziprozität, Engagement oder Konsistenz, sozialer Beweis oder Konformität, Autorität, Sympathie und Knappheit (Frauenstein and Flowerday, 2020, p. 3). Die Überzeugungsprinzipien von Cialdini werden in der Literatur häufig als Prädiktoren für den Erfolg von Phishing eingesetzt. Diese Prinzipien können genutzt werden, um individuelle Entscheidungen zu beeinflussen (Burda *et al.*, 2020, p. 2).

##### 2.3.7.2.1 Reziprozität

Eine Nachricht wird als hilfreich dargestellt, so dass sich der Nutzer oder die Nutzerin verpflichtet fühlt im Gegenzug etwas zu tun, z.B. eine Nachricht zu teilen in der andere

gewarnt werden, dass die Möglichkeit besteht, dass das Facebook-Konto gehackt wurde (Frauenstein and Flowerday, 2020, p. 3).

#### 2.3.7.2.2 Engagement oder Konsistenz

Der Grundsatz des Engagements bezieht sich auf die Wahrscheinlichkeit, dass sich eine Person einer Sache oder Idee widmet, nachdem ein Versprechen gegeben oder eine Vereinbarung ausgemacht wurde. Wenn Menschen sich einmal für etwas entschieden haben, werden sie in der Regel durch persönlichen und zwischenmenschlichen Druck dazu gebracht sich konsequent an diese Verpflichtung zu halten (Frauenstein and Flowerday, 2020, pp. 3–4).

#### 2.3.7.2.3 Autorität

Das Autoritätsprinzip ist die am häufigsten verwendete Überzeugungstechnik beim Phishing. Nachrichten, die den Anschein erwecken, als kämen sie von autoritären Stellen (z.B. Bank), können Opfer dazu verleiten sich verpflichtet zu fühlen der Aufforderung Folge zu leisten. Dies liegt daran, dass Menschen durch soziales Lernen ermutigt wurden Autoritäten nicht in Frage zu stellen und daher konditioniert sind oder sich verpflichtet fühlen auf Autorität zu reagieren (Frauenstein and Flowerday, 2020, p. 4).

#### 2.3.7.2.4 Sozialer Beweis oder Konformität

Die Tendenz, das Verhalten von Mitglieder und Mitgliederinnen einer Gruppe zu imitieren, wird als sozialer Beweis bezeichnet. Menschen werden einer Aufforderung nachkommen, wenn sie sehen, dass andere dieser Aufforderung ebenfalls nachgekommen sind. Zum Beispiel wird eine Nachricht auf Facebook von Freunden oder Freundinnen des Nutzer oder der Nutzerin geteilt, und er oder sie teilt dann die Nachricht auch (Frauenstein and Flowerday, 2020, p. 4).

#### 2.3.7.2.5 Verknappung

Eine Nachricht die eine Knappheit beinhaltet, kann ein Gefühl der Dringlichkeit erzeugen und den Nutzer oder die Nutzerin unter Druck setzt, zu handeln. Der Nutzer oder die Nutzerin möchte die Gelegenheit das Produkt, die Dienstleistung oder die Information zu erwerben nicht verpassen, insbesondere wenn diese nur begrenzt verfügbar sind. Die Dringlichkeit kann durch Hinzufügen einer Konsequenz oder eines Zeitrahmens weiter verstärkt werden (z.B. spezieller Rabatt oder Preis, der nur für einen bestimmten Zeitraum gültig ist) (Frauenstein and Flowerday, 2020, p. 4).

#### 2.3.7.2.6 Sympathie

Menschen können dazu gebracht werden anderen zu gehorchen, wenn diese Personen bestimmte positive oder vertraute Eigenschaften aufweisen. Ein Facebook-Nutzer oder -Nutzerin kann zum Beispiel eine Freundschaftsanfrage erhalten, aber bevor die Anfrage angenommen wird, können Informationen über den Absender oder der Absenderin eingeholt werden, z.B. über die Anzahl der gemeinsamen Freunde und Freundinnen, Beruf und Wohnort. Wenn es Merkmale gibt, die dem Nutzer oder der Nutzerin gefallen, kann er oder sie beschließen die Einladung anzunehmen. Wenn der Nutzer oder die Nutzerin in einem für sie wichtigen Punkt mit dem Absender oder der Absenderin übereinstimmt, steigt die Wahrscheinlichkeit, dass er oder sie antwortet (Frauenstein and Flowerday, 2020, pp. 4–5).

Kognitive Schwachstellen werden häufig in Phishing-Kampagnen ausgenutzt. Die Ergebnisse zu der Wirksamkeit lieferten jedoch in den verschiedenen Studien sehr unterschiedliche Meinungen. So wurde beispielsweise berichtet, dass sich Sympathie und Sozialer Beweis oder Konformität positiv auf den Phishing-Erfolg auswirken (Wright et al., 2014). Des Weiteren war Autorität laut Butavicius et al. (2016), Hu und Wang (2018), Williams et al. (2018) und Knappheit laut Williams et al. (2018) auch sehr wirksam in Bezug auf Phishing-Angriffen (Burda *et al.*, 2020, p. 2).

Andere Studien finden jedoch umgekehrte Effekte, dass das Vorhandensein bestimmter kognitiver Schwachstellen die Erfolgswahrscheinlichkeit des Angriffs verringert. Zum Beispiel fanden van der Heijden et al. (2019) eine negative Korrelation zwischen Reziprozität und der Anzahl der Nutzer und Nutzerinnen, die auf den Angriff im Bankenbereich hereinfallen. Andere Studien berichteten von ähnlichen negativen Effekten für Autorität (Wright et al., 2014) und Sozialer Beweis oder Konformität (Butavicius et al., 2018). Wright et al., 2014 berichteten keine signifikanten Auswirkungen in beide Richtungen für Engagement oder Konsistenz und Reziprozität (Burda *et al.*, 2020, p. 2).

Diese gegensätzlichen Ergebnisse liefern gemischte Erkenntnisse über die Wirksamkeit und den Einsatz von kognitiven Schwachstellen bei Phishing-Angriffen. Es scheint jedoch dass der Kontext eine Rolle spielt, dass bedeutet das die Art und Weise wie diese kognitiven Angriffe an die Opfer übermittelt werden, Auswirkungen auf die Wirksamkeit hat (Burda *et al.*, 2020, p. 2). Wright et al. (2014) untersuchten die Wirksamkeit verschiedener Beeinflussungstechniken mit Blick auf den Inhalt der E-Mail selbst. Sie

fanden heraus, dass eine Reihe von Techniken eine signifikante Vorhersage der Zustimmung der Nutzer und Nutzerinnen ermöglichte. Dazu gehörten die Sympathie für den Absender oder der Absenderin, Sozialer Beweis oder Konformität, Engagement oder Konsistenz, Autorität und Knappheit (Moody, Galletta and Dunn, 2017, p. 566).

#### 2.3.7.3 Persönlichkeitsmerkmale

Persönlichkeitsmerkmale beschreiben individuelle Unterschiede in Form von charakteristischen Gedanken, Gefühlen und Verhaltensweisen. Persönlichkeitsmerkmale sind bei jedem Menschen einzigartig, da sie in erster Linie durch die Genetik, soziale und umweltbedingte Einflüsse und Erfahrungen bestimmt werden. Persönlichkeitsmerkmale sind ein wesentlicher Bestandteil des menschlichen Denkens und Verhaltens und haben daher einen Einfluss darauf, ob eine Person in böswillige Aktivitäten oder riskantes Verhalten verwickelt wird oder nicht. Das Fünf-Faktoren-Modell (FFM), bestehend aus den "Big Five"-Persönlichkeitsmerkmalen und ist das am weitesten verbreitete und am intensivsten erforschte Modell der Persönlichkeit. Es umfasst die fünf empirisch abgeleiteten Faktoren: Offenheit, Gewissenhaftigkeit, Extrovertiertheit, Sympathie und Neurotizismus und werden üblicherweise mit dem Akronym OCEAN oder CANOE dargestellt (Frauenstein and Flowerday, 2020, p. 6).

##### 2.3.7.3.1 Offenheit

Offenheit für Erfahrungen ist ein Persönlichkeitsmerkmal, das sich auf Menschen bezieht, die aufgeschlossen sind, neue Erfahrungen suchen, eine aktive Vorstellungskraft haben und sich auf intellektuelle Aktivitäten konzentrieren. Sie neigen dazu unabhängig von Urteilen zu sein und haben eine Wertschätzung für Kunst, Natur, andere Ideen und Überzeugungen (Frauenstein and Flowerday, 2020, p. 6). Hong et al. (2013) fanden heraus, dass Nutzer und Nutzerinnen die weniger offen für neue Erfahrungen sind, legitime E-Mails häufiger löschten als solche die offener waren, was auf eine geringere Anfälligkeit für Phishing hinweisen könnte. Alseadon (2014) fand hingegen heraus, dass die Offenheit für Erfahrungen bzw. die Bereitschaft Neues auszuprobieren signifikant positiv korreliert mit der Phishing-Anfälligkeit. Im Gegensatz zu diesen Ergebnissen fanden Pattinson et al. (2012) heraus, dass Nutzer und Nutzerinnen mit hoher Offenheit, die nicht darüber informiert wurden, dass sie an einer Phishing-Studie teilnahmen, besser in der Lage waren mit Phishing-E-Mails richtig umzugehen als Nutzer und Nutzerinnen mit geringer Offenheit (Tornblad, Jones, *et al.*, 2021, pp. 938–939).

#### 2.3.7.3.2 Gewissenhaft

Gewissenhaftigkeit bezieht sich auf Personen, die ehrlich, vertrauenswürdig, ordentlich und fleißig sind. Sie verfügen über Selbstdisziplin, sind zielorientiert, umsichtig und neigen dazu Regeln, Normen und Verfahren zu befolgen (Frauenstein and Flowerday, 2020, p. 6). Gewissenhafte Menschen sind in der Regel ruhig, zurückhaltend, aufgabenorientiert, schüchtern und angenehm (Sumner *et al.*, 2021, p. 3). Halevi et al. (2015) fanden heraus, dass Nutzer und Nutzerinnen die auf Phishing-Betrügereien hereinfallen, ein höheres Maß an Gewissenhaftigkeit aufwiesen als Nutzer und Nutzerinnen die nicht auf Phishing-Betrügereien hereingefallen sind (Tornblad, Jones, *et al.*, 2021, p. 938). Halevi et al. (2019) fanden heraus, dass Gewissenhaftigkeit von Angreifer und Angreiferinnen gezielt eingesetzt werden, um eine höhere Phishing-Antwortrate zu erzielen (Jampen *et al.*, 2020, p. 16). Frauenstein und Flowerday (2020) fanden jedoch heraus, dass Nutzer und Nutzerinnen mit hoher Gewissenhaftigkeit weniger anfällig für Phishing-Angriffe auf Social Networking Sites waren, da sie weniger auf schnelle und heuristische Verarbeitung angewiesen sind (Tornblad, Jones, *et al.*, 2021, p. 938).

#### 2.3.7.3.3 Extrovertiertheit

Extrovertiertheit ist ein Persönlichkeitsmerkmal das Personen zugeschrieben wird, die dazu neigen positive Emotionen wie Aufregung zu erleben. Sie ziehen es vor mit anderen zusammenzuarbeiten und neigen dazu gesellig, energisch, gesprächig, durchsetzungsfähig, impulsiv und dominant zu sein (Frauenstein and Flowerday, 2020, p. 6). Extrovertiertheit, d.h. der Grad der Kontaktfreudigkeit, war ein signifikanter Prädiktor für die Anfälligkeit für Phishing, so dass extrovertierte Nutzer und Nutzerinnen anfälliger waren. Hong et al. (2013) zeigten ebenfalls, dass weniger extrovertierte Nutzer und Nutzerinnen legitime E-Mails häufiger löschten als extrovertierte Nutzer und Nutzerinnen, was das Risiko erhöhen könnte auf einen Phishing-Angriff hereinzufallen. Welk et al. (2015) fanden ebenso heraus, dass Nutzer und Nutzerinnen mit geringer Extrovertiertheit bei einer Phishing-Erkennungsaufgabe eine bessere Leistung zeigten als Nutzer und Nutzerinnen mit hoher Extrovertiertheit. Pattinson et al. (2012) fanden jedoch heraus, dass Nutzer und Nutzerinnen mit hoher Extrovertiertheit die nicht darüber informiert wurden, dass sie an einer Phishing-Studie teilnahmen besser in der Lage waren, Phishing-E-Mails korrekt zu handhaben als Nutzer und Nutzerinnen mit niedriger Extrovertiertheit (Tornblad, Jones, *et al.*, 2021, p. 939).

#### 2.3.7.3.4 Sympathie

Sympathie wird Personen zugeschrieben die tolerant, mitfühlend, bescheiden, höflich, kooperativ und vertrauensvoll gegenüber anderen sind, da sie glauben, dass Menschen mit denen sie zu tun haben im Allgemeinen gute Absichten haben und ehrlich sind. Sie schätzen und respektieren auch die Überzeugungen und Konventionen anderer Menschen (Frauenstein and Flowerday, 2020, p. 6). Alseadon (2014) fand heraus, dass die Sympathie ein signifikanter Prädiktor für die Anfälligkeit für Phishing war, d.h., Personen mit hoher Sympathie sind anfälliger für Phishing (Tornblad, Jones, *et al.*, 2021, p. 938).

#### 2.3.7.3.5 Emotionale Instabilität (Neurotizismus)

Neurotizismus ist das Gegenteil von emotionaler Stabilität und wird Personen zugeschrieben, die zu negativen Gefühlen wie Pessimismus, Verlegenheit und Schuldgefühlen neigen. Solche Menschen sind in der Regel traurig oder nervös, könnten auch zornig sein und haben ein geringes Selbstwertgefühl (Frauenstein and Flowerday, 2020, p. 6). Neurotizismus steht in direktem Zusammenhang mit Faktoren wie Impulsivität und Ängstlichkeit (López-Aguilar and Solanas, 2021, p. 1363). Halevi et al. (2013) fanden heraus, dass die Tendenz negative Gefühle (z.B. Schuldgefühle) zu empfinden eine signifikante positive Korrelation mit der Anfälligkeit für Phishing aufweiste. Alseadon (2014) stellte fest, dass emotionale Stabilität ein signifikanter Prädiktor für die Anfälligkeit für Phishing ist, d.h. Personen mit geringer emotionaler Stabilität waren unabhängig vom Geschlecht anfälliger (Tornblad, Jones, *et al.*, 2021, p. 938). Vishwanath et al. (2015) fanden ebenfalls heraus, dass Studenten und Studentinnen mit geringer emotionaler Stabilität impulsive E-Mail-Gewohnheiten hatten, wie z.B. das reaktive Überprüfen von E-Mails und das Reagieren auf E-Mail-Benachrichtigungen, und dass sie mit größerer Wahrscheinlichkeit auf Phishing-Links in E-Mails klickten (Goel, Williams and Dincelli, 2017, pp. 25–26).

Montanez et al. (2020) lieferten eine Überprüfung bestehender Studien zu verschiedenen Aspekten von Social-Engineering-Angriffen und hoben hervor, dass hoher Neurotizismus mit geringer Selbstwirksamkeit verbunden war, während niedriger Neurotizismus mit hoher Selbstwirksamkeit verbunden war. Neurotiker oder Neurotikerinnen mit hohem Neurotizismus könnten dazu neigen negative Emotionen zu empfinden und daher Opfer von Phishing-Angriffen werden, wenn der Inhalt der E-Mail an die Furcht, Angst und das Gefühl der Dringlichkeit des Opfers appelliert. Van de Weijer und Leukfeldt (2017) wiesen in einer Stichprobe von 3.648 Personen nach, dass Personen mit hoher emotionaler

Stabilität (weniger neurotisch) weniger anfällig für Phishing-Angriffe waren. Darwish et al. (2012) gaben einen Überblick über demografische und Persönlichkeitsmerkmale von Phishing-Opfern. Obwohl die Ergebnisse hervorheben, dass die demografischen Merkmale und die Persönlichkeitsmerkmale der Nutzer und Nutzerinnen wertvolle Faktoren für weitere Social-Engineering-Studien sein könnten, wurde der Neurotizismus nicht hervorgehoben (López-Aguilar and Solanas, 2021, pp. 1365–1366).

#### 2.3.7.4 Psychologische Merkmale

Cyber-Angreifer und -Angreiferinnen nutzen häufig psychologische Techniken für den Phishing-Angriff, um die kognitiven Ressourcen der Opfer zu verringern, so dass die Hinweise in der Phishing-E-Mail nicht genügend Aufmerksamkeit geschenkt wird. Die Auswirkungen von Psychologischen Merkmalen wie z.B. Angst und damit die Anfälligkeit für Phishing wurden von mehreren Forscher und Forscherinnen aufgezeigt (Abroshan *et al.*, 2021b, p. 121917).

##### 2.3.7.4.1 Angst

Studien haben gezeigt, dass Angst die Aufmerksamkeitskontrolle bei der Ausführung von Aufgaben verringern kann. Dies kann erklären warum ein Benutzer oder eine Benutzerin mit einem hohen Maß an Angst, den Phishing-Hinweisen in einer E-Mail weniger Aufmerksamkeit schenkt und infolgedessen z.B. auf den gefährlichen Phishing-Link klickt. Sowohl Angst als auch Furcht wirken wie ein Gefahren- oder Bedrohungssignal, das entsprechende Reaktionen auslösen kann. Viele Wissenschaftler und Wissenschaftlerinnen unterscheiden zwischen Angst und Furcht und sind der Meinung, dass Furcht mit bekannten Bedrohungen zusammenhängt, während Angst als ein unbekanntes Bedrohungssignal wirkt. Die Ergebnisse der Regressionsanalyse von Abroshan et al. (2021) wiesen darauf hin, dass die Angst vor COVID-19 die Wahrscheinlichkeit erhöht, sowohl auf gewöhnliche als auch auf COVID-19 thematisierte Phishing-Angriffe hereinzufallen (Abroshan *et al.*, 2021b, pp. 121924–121925).

##### 2.3.7.4.2 Furcht

Die Furcht etwas Wertvolles zu verlieren, kann Menschen unbewusst zum Handeln veranlassen oder drängen. Furcht entsteht durch die Wahrnehmung einer Bedrohung des eigenen Wohlbefindens und dient als Warnsignal für einen bevorstehenden Schaden. Furcht verstärkt die sofortigen Vorsichtsmaßnahmen, um sich selbst und den Besitz zu schützen. Ein typischer Bankbetrug nutzt Furchtreaktionen aus, indem das Konto eines

Opfers gesperrt wird, wenn die Benutzer und Benutzerinnen nicht ihre Anmeldedaten durch Anklicken eines Weblinks ändern. Die Angst etwas Wertvolles zu verlieren könnte dazu führen, dass die Benutzer und Benutzerinnen ihre Anmeldedaten weitergeben (Goel, Williams and Dincelli, 2017, pp. 23–28).

#### 2.3.7.4.3 Autorität

Autoritätshinweise konzentrieren sich auf die Nachahmung von Organisationen oder Personen die respektiert werden und eine gewisse Autorität gegenüber dem Empfänger oder der Empfängerin haben (Williams, Hinds and Joinson, 2018, p. 3). Butavicius et al. (2015) führten ein Phishing-Experiment durch wie Phishing-Nachrichten die mit drei Social-Engineering-Strategien (Autorität, Knappheit und sozialer Beweis) erstellt wurden, das Urteil der Nutzer und Nutzerinnen darüber beeinflussen, wie sicher ein Link in einer E-Mail ist. Sie fanden heraus, dass Inhalte die auf Autorität basierten die effektivste Strategie waren, um Nutzer und Nutzerinnen davon zu überzeugen, dass der Link sicher war (Goel, Williams and Dincelli, 2017, p. 25).

#### 2.3.7.4.4 Dringlichkeit

Atkins und Huang (2013) sammelten zahlreiche Phishing-E-Mails und stellten fest, dass die beliebteste Technik die Dringlichkeit war, denn 71% der untersuchten Phishing-E-Mails enthielten eine Notfallanweisung (Yeoh *et al.*, 2021, p. 2). De Bona und Paci (2020) untersuchten, ob Autorität oder Dringlichkeit als Überzeugungstechniken effektiver waren, um die Phishing-Anfälligkeit der Mitarbeiter und Mitarbeiterinnen zu erhöhen. Sie fanden heraus, dass die Mitarbeiter und Mitarbeiterinnen anfälliger für Phishing-Angriffe waren, wenn das Dringlichkeitsprinzip ausgenutzt wurde (De Bona and Paci, 2020, p. 1).

#### 2.3.7.4.5 Neugierde

In der psychologischen Forschung wurde Neugier als der Wunsch definiert, neues Wissen zu finden bzw. zu erlangen. Neugier wurde mit Offenheit für Erfahrungen gleichgesetzt und im IT-Kontext weiter definiert als Begeisterung über die Möglichkeiten die eine Technologie bietet (Moody, Galletta and Dunn, 2017, p. 568). Moody et al. (2017) fanden heraus, dass der Wunsch, sich neues Wissen und Erfahrungen anzueignen ein signifikanter Prädiktor für die Anfälligkeit für Phishing war, sodass neugierige Nutzer und Nutzerinnen anfälliger waren (Tornblad, Jones, *et al.*, 2021, p. 939).

#### 2.3.7.4.6 Vertrauen und Misstrauen

Vertrauen wird definiert als ein psychologischer Zustand und umfasst die Grundlage positiver Erwartungen in Bezug auf die Absichten oder das Verhalten einer anderen Person bezüglich einer Gefährdung zu akzeptieren (Jalali *et al.*, 2020, p. 2). Das bedeutet, dass Menschen möglicherweise einer Person vertrauen, wenn sie glauben, dass dieses Vertrauen für sie von Vorteil sein könnte, obwohl sie wissen das sie etwas verlieren könnten. Menschen mit unterschiedlichem kulturellem Hintergrund, Erfahrungen und persönlichem Charakter haben eine unterschiedliche Neigung zu vertrauen (Abroshan *et al.*, 2018, p. 192). Vertrauen ist auch die Bereitschaft, sich einer anderen Person gegenüber verletzlich zu zeigen. Misstrauen hingegen wurde definiert als die mangelnde Bereitschaft sich einer anderen Person gegenüber verletzlich zu zeigen und die Erwartung, dass eine Person versucht einer anderen Person zu schaden (Moody, Galletta and Dunn, 2017, pp. 567–568). Vertrauen wirkt sich nachweislich auf die Unterstützung und das Engagement in der Organisation sowie auf das Verhalten der Mitarbeiter und Mitarbeiterinnen in der Organisation aus. Untersuchungen haben gezeigt, dass sich Mitarbeiter und Mitarbeiterinnen, die dem Management vertrauten, stärker an das Unternehmen gebunden fühlten und eher bereit sind die Unternehmensrichtlinien zu befolgen. Mitarbeiter und Mitarbeiterinnen die das Gefühl haben, dass das Management ihnen vertraut, achteten bei ihrem Verhalten stärker darauf dass das entgegengebrachte Vertrauen nicht verletzt wurde (Jalali *et al.*, 2020, pp. 2–3).

Jagatic et al. (2007) fanden heraus, dass Menschen sich leichter von ähnlichen Personen überzeugen ließen, weil diese als sympathischer angesehen werden, was eine Grundlage für Vertrauen ist (Martin, Lee and Parmar, 2021, p. 40). Wright und Marett (2010) fanden heraus, dass ein höheres Misstrauen gegenüber Menschen mit einer geringeren Anfälligkeit verbunden war (Tornblad, Jones, *et al.*, 2021, p. 939). Flores et al. (2014) berichten, dass das Vertrauensverhalten einer Person während des Phishing-Experiments erheblich beeinflusst (Jampen *et al.*, 2020, p. 16). Moody et al. (2017) fanden in Post-Tests heraus, dass Vertrauen und Misstrauen signifikante Prädiktoren sein könnten und dass diese Signifikanz von den Merkmalen der Botschaft abhängt (Moody, Galletta and Dunn, 2017, p. 564). Sie haben außerdem gezeigt, dass Menschen anfälliger für Angriffe sind, wenn der Absender oder die Absenderin bekannt war. Diese Ergebnisse unterstrichen die Rolle von Vertrautheit bei Phishing-Angriffen und legten nahe, dass das Vertrauen in bekannte Absender und Absenderinnen eine Rolle spielt (Martin, Lee and Parmar, 2021, p. 40).

#### 2.3.7.4.7 Gewinn und Verlust

Ein weiterer Faktor, der sich auf die Anfälligkeit für Phishing auswirkt, ist wenn Empfänger oder Empfängerinnen etwas Wertvolles gewinnen oder verlieren. Menschen sind motiviert Dinge von Wert zu gewinnen und sie können durch die Verlockung von Geld oder materiellen Gütern dazu gebracht werden persönliche Informationen preiszugeben. Kahneman und Tversky (1979) wiesen jedoch darauf hin, dass potenzielle Verluste einen stärkeren Einfluss auf das Urteilsvermögen und die Handlungen der Menschen ausübten als potenzielle Gewinne. Menschen messen Gewinnen und Verlusten einen subjektiven Wert bei, so dass Gewinne mit einem positiven Wert und Verluste mit einem negativen Wert assoziiert werden. Das heißt, der Schmerz 100 Dollar zu verlieren ist größer als die Freude 100 Dollar zu gewinnen. Botschaften die den Verlust von etwas Wertvollem androhen, könnten wirksamer sein als Botschaften die die Möglichkeit eines Gewinns bieten (Goel, Williams and Dincelli, 2017, p. 28). Parsons et al. (2015) kamen zu dem Schluss, dass die Teilnehmer und Teilnehmerinnen mit größerer Wahrscheinlichkeit Opfer von Phishing-E-Mails wurden, wenn deren Inhalt einen potenziellen finanziellen Verlust für den Empfänger oder Empfängerin androhte (Jampen *et al.*, 2020, p. 22). Die Forschungsergebnisse von Goel et al. (2017) zeigten, dass die Angst vor dem Verlust oder die Erwartung etwas Wertvolles zu gewinnen, die Anfälligkeit für Phishing erhöhte (Miller *et al.*, 2020, p. 5). Die Ergebnisse von Tornblad et al. (2021) belegten jedoch, dass die Empfänger und Empfängerinnen von Phishing-E-Mails mit Gewinnversprechen oder hohen Gewinnbeträgen eher misstrauisch gegenüberstehen (Tornblad, Armstrong, *et al.*, 2021, p. 363).

### 2.3.7.5 IT-Kompetenzen

Es hat sich gezeigt, dass eine Reihe von Faktoren die Sicherheit Awareness der Menschen beeinflussen (Aleroud and Zhou, 2017, p. 171). Im Folgenden werden einige IT-Faktoren näher erläutert.

#### 2.3.7.5.1 Sicherheit Awareness

Furnell (2007) und Karakasiliotis et al. (2007) führten eine webbasierte Umfrage durch, um die Anfälligkeit der Nutzer und Nutzerinnen für Phishing-Angriffe zu untersuchen. Den Teilnehmer und Teilnehmerinnen wurden potenzielle Phishing-Nachrichten gezeigt und sie wurden gebeten, die Legitimität der einzelnen Nachrichten zu beurteilen. Die Ergebnisse dieser Studien zeigten, dass die Menschen nicht genau wussten, worauf sie in einer Phishing-Nachricht achten müssen. Die Autoren und Autorinnen kamen zu dem

Schluss, dass es den Benutzer und Benutzerinnen an einem grundlegenden Awareness für Online-Sicherheit mangelte. Bakhshi et al. (2009) führten ein E-Mail-basiertes Experiment durch, bei dem 152 Mitarbeiter und Mitarbeiterinnen eine Nachricht erhielten, in der sie aufgefordert wurden, einem Link zu einer externen Website zu folgen und ein Software-Update zu installieren. Die Ergebnisse zeigten, dass 23% der Empfänger und Empfängerinnen auf den Angriff hereinfielen, was darauf hindeutete, dass vielen Nutzer und Nutzerinnen eine grundlegende Awareness fehlte, das für den Online-Schutz erforderlich ist (Purkait, Kumar De and Suar, 2014, pp. 200–203).

Halevi et al. (2015) fanden hingegen heraus, dass Nutzer und Nutzerinnen, die sich der Cyber-Risiken stärker bewusst waren und eine pessimistische Sicht in Bezug auf Risiken bei der Nutzung des Internets hatten, weniger anfällig für Phishing waren (Tornblad, Jones, *et al.*, 2021, p. 940). Abassi et al. (2016) stützten sich auf eine Stichprobe von 509 Universitätsstudenten und -studentinnen, -mitarbeiter und -mitarbeiterinnen und Mitglieder und Mitgliederinnen der Öffentlichkeit. In der Studie wurden die Personen auf der Grundlage gemeinsamer Online-Erfahrungen in Gruppen eingeteilt und ihre Interaktionen mit gefälschten Phishing-Seiten wurde analysiert. Sie fanden heraus, dass die am besten abgeschnitten Teilnehmer und Teilnehmerinnen diejenigen waren, die sich des Phishings bewusst waren, mit Websites vertraut waren, die Wirksamkeit von Anti-Phishing-Tools positiv einschätzten und die bereits finanzielle Verluste durch Phishing erlitten hatten. Einige dieser Eigenschaften wirkten sich jedoch auch negativ auf die Fähigkeit einer Person aus. Dies lag daran, dass frühere Begegnungen und das Wissen über Phishing offenbar das Selbstvertrauen der Personen in ihre Fähigkeit gestärkt hatten und dass die Vertrautheit mit häufig besuchten Websites zu übermäßigem Vertrauen geführt hatten (Broadhurst *et al.*, 2018, pp. 7–8).

#### 2.3.7.5.2 Phishing-Wissen

Downs et al. (2007) fanden heraus, dass diejenigen die mit der Definition von Phishing vertraut waren, deutlich seltener auf E-Mail- und Website-Phishing hereinfielen. Wang et al. (2012) zeigten ebenfalls, dass mit zunehmendem Wissen über Phishing-Betrügereien die Wahrscheinlichkeit sinkte, dass die Nutzer und Nutzerinnen auf Phishing hereinfielen (Tornblad, Jones, *et al.*, 2021, p. 940). Purkait (2012) simulierte jedoch ein Szenario in einem Computerlabor, bei dem die Teilnehmer und Teilnehmerinnen aufgefordert wurden, E-Mails über das persönliches Gmail-Konto zu versenden. Die Studie ergab, dass die Teilnehmer und Teilnehmerinnen sehr anfällig für den Phishing-Angriff waren, da die meisten Personen die SSL-Anzeige im Browser ignorierten. Es wurde jedoch festgestellt,

dass die Benutzer und Benutzerinnen die in der Vergangenheit bereits Opfer von Phishing waren die gefälschte Gmail-Website gut erkannten (Purkait, Kumar De and Suar, 2014, p. 200). Chen et al. (2020) führten eine Umfrage durch, um zu untersuchen, wie sich frühere Phishing-Begegnungen auf die Phishing-Anfälligkeit auswirken. Die Autoren und Autorinnen rekrutierten Studenten und Studentinnen einer großen öffentlichen Universität und baten sie, über ihre jüngsten Erfahrungen mit einem Phishing-Angriff zu berichten. Die Ergebnisse dieser Umfrage zeigten, dass Schwierigkeiten bei der Erkennung sowie der negative Ausgang eines erlebten Angriffs einen erheblichen Einfluss auf die Anfälligkeit der Benutzer und Benutzerinnen hatten. Teilnehmer und Teilnehmerinnen die einen früheren Phishing-Angriff nicht erkennen konnten, erkannten Täuschungen leichter. Den Autoren und Autorinnen zufolge könnte dies auf das Wissen zurückführen, das durch den negativen Ausgang und das Scheitern in der Vergangenheit gewonnen wurde und das nun zu einer erhöhten Wachsamkeit führte (Papatsaroucha *et al.*, 2021, p. 21). Li et al. (2020) führten jedoch eine simulierte Phishing-Kampagne an einer Universität durch und stellten fest, dass Nutzer und Nutzerinnen die auf einen Link in einer Phishing-E-Mail geklickt haben, mit größerer Wahrscheinlichkeit eine Woche später auf einen anderen Phishing-Link klicken würden (Tornblad, Jones, *et al.*, 2021, p. 940).

#### 2.3.7.5.3 Einstellung zur Sicherheit

Die Angst des Internets spiegelt das allgemeine Gefühl des Unbehagens oder der Besorgnis eines Nutzers oder einer Nutzerin gegenüber der Online-Umgebung wider. Diese Art von Angst führt zu dem starken Wunsch, die Nutzung des Internets zu vermeiden und/oder die eigene Exposition gegenüber dem Internet zu minimieren (Moody, Galletta and Dunn, 2017, p. 569). Vishwanath (2015) fand erstaunlicherweise heraus, dass die Sorge um die Online-Privatsphäre oder die Befürchtung, persönliche Informationen online preiszugeben, ein signifikanter positiver Prädiktor für die Beantwortung einer Freundschaftsanfrage von einem gefälschten Profil auf Facebook war. Hadlington (2017) fand heraus, dass eine negativere Einstellung und ein geringeres Engagement für Cybersicherheitspraktiken das Engagement für riskantes Cybersicherheitsverhalten positiv vorhersagten. Das kann dazu führen, dass ein Nutzer oder eine Nutzerin häufig ein Opfer eines Phishing-Angriff wird (Tornblad, Jones, *et al.*, 2021, p. 940).

#### 2.3.7.5.4 Computer- und Internet-Kenntnisse

Downs et al. (2007) stellten in einer Umfrage fest, dass technisches Wissen über die Web-Umgebung zu einem erhöhten Widerstand gegen Phishing führte (Alsharnouby, Alaca and Chiasson, 2015, p. 71). Sheng et al. (2010) fanden heraus, dass Nutzer und Nutzerinnen mit guten Computerkenntnissen besser in der Lage waren Nachrichten und Hyperlinks auf gefährliche Anomalien zu analysieren (Thomas, 2018, p. 15). Pattinson et al. (2012) haben festgestellt, dass diejenigen die sich gut mit Computern auskannten, besser mit Phishing-E-Mails umgehen konnten. Jedoch war dies bei der Kontrollgruppe nicht der Fall, was darauf hindeutet, dass sich die Personen aktiv über Phishing bewusst sein müssen (Broadhurst *et al.*, 2018, p. 7). Parsons et al. (2013) präsentieren interessante Ergebnisse bezüglich der Auswirkungen des technischen Wissens der Teilnehmer und Teilnehmerinnen. Personen die darüber informiert waren, dass sie an einer Phishing-Studie teilnahmen, zeigten eine signifikant bessere Leistung bei der Identifizierung von Phishing-E-Mails (Jampen *et al.*, 2020, p. 16). Eine empirische Studie von Halevi et al. (2015) legte nahe, dass ein höheres Maß an technischem Sachverstand, z.B. Kenntnisse über Tracking-Informationen wie Cookies, Spyware, Netzwerksicherheit und Virenverbreitung auch zu einer geringeren Phishing-Anfälligkeit führt (Thomas, 2018, p. 6). Albladi und Weir (2018) führten ihre Studie mit 30 Fachleuten und zwölf Experten und Expertinnen durch. Sie fanden heraus, dass Computerkenntnisse, Bildung und Sicherheit Awareness als die wichtigsten Faktoren für den Schutz der Nutzer und Nutzerinnen vor Cyberangriffen angesehen wurden (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 9).

Downs et al. (2007) fanden jedoch heraus, dass das Wissen über allgemeine Computerrisiken und -konzepte (z.B. Cookies, Viren) die Phishing-Anfälligkeit nicht vorhersagt (Tornblad, Jones, *et al.*, 2021, p. 940). Tzipora Halevi et al. (2015) führten Untersuchungen durch, um einige Hypothesen zu überprüfen, was die Anfälligkeit von Personen für Phishing-Angriffe beeinflusste. Die Ergebnisse zeigten zwar, dass Nutzer und Nutzerinnen die sich der Cyber-Risiken bewusster waren, resistenter gegen Phishing-Angriffe waren. Jedoch ergab die Untersuchung, dass die Internetnutzung nicht mit der Anfälligkeit für Phishing-Angriffe korrelierte. Diese Ergebnisse zeigten, dass die Nutzung und das Verständnis von Informationstechnologien nicht ausreichen, um Phishing-Angriffe zu erkennen. Mohamed Alsharnouby et al. (2015) bestätigten, dass die allgemeine technische Kompetenz der Nutzer und Nutzerinnen nicht mit besseren Ergebnissen in Bezug auf Phishing Erkennung korrelierte (Rastenis *et al.*, 2020, p. 313). Albakry et al. (2020) fanden ebenfalls heraus, dass diejenigen die die Technologie regelmäßig nutzen,

nicht wesentlich besser abschneiden. Diese Erkenntnis ist besorgniserregend, denn es zeigt, dass die regelmäßige Nutzung von Technologie nicht zu ausreichenden Sicherheitserfahrungen oder -kenntnissen führt. Die Ergebnisse von Lévesque et al. (2018) zeigten wiederum, dass Nutzer und Nutzerinnen, die ein hohes Maß an Computerkenntnissen hatten, anfälliger für Phishing-Angriffe waren (Desolda *et al.*, 2021, pp. 17–21).

Dhamija et al. (2006) führten eine laborgestützte Studie durch, bei der die Teilnehmer und Teilnehmerinnen die Legitimität einer Reihe von Websites bewerten sollten. Die Teilnehmer und Teilnehmerinnen wurden über den Zweck der Aufgabe aufgeklärt. Trotzdem wurden 42% der Websites von Nutzer und Nutzerinnen falsch eingestuft. Es wurde festgestellt, dass sich 59% der Nutzer und Nutzerinnen ausschließlich auf den Inhalt der Website und die URL konzentrierten, um die Legitimität zu beurteilen und jegliche Sicherheitshinweise des Browsers außer Acht ließen (Alsharnouby, Alaca and Chiasson, 2015, p. 71). Schechter et al. (2007) berichteten, dass 53% ihrer Teilnehmer und Teilnehmerinnen versuchten sich weiterhin bei einer Website anzumelden, nachdem eine Sicherheitswarnung angezeigt wurde (Kirlappos and Sasse, 2012, p. 1). Wu et al. (2006), Schechter et al. (2007) und Herzberg (2009) zeigten, dass die Nutzer und Nutzerinnen ihre Passwörter oft eingegeben haben ohne zu überprüfen, ob Secure Sockets Layer (SSL)/Transport Layer Security (TLS) aktiv oder die URL korrekt war (Purkait, Kumar De and Suar, 2014, p. 201). Die Studie von Williams und Li (2007) zeigte, dass die Nutzer und Nutzerinnen die Rolle des HTTPS-Vorhängeschlosses oft nicht verstanden und so Opfer von Phishing-Websites wurden (Desolda *et al.*, 2021, p. 16). Egelman et al. (2008) fanden heraus, dass 21% der Teilnehmer und Teilnehmerinnen die die aktiven Phishing-Warnungen sahen, diese ignorierten. Erstaunlicherweise ignorierten 99% der Teilnehmer und Teilnehmerinnen passive Warnungen und gaben ihre persönlichen Anmeldedaten auf einer betrügerischen Website ein (Purkait, Kumar De and Suar, 2014, p. 201). Althobaiti et al. (2021) behaupten, dass der durchschnittliche nichttechnische Benutzer bzw. Benutzerin im Vergleich zu Sicherheitsexperten und -expertinnen nicht über das Wissen verfügt, um die Gültigkeit einer URL sicher zu beurteilen. Daher ist es oft der Fall, dass die Nutzer und Nutzerinnen Unstimmigkeiten in URL-Namen nicht hinterfragen oder gar erst bemerken (Desolda *et al.*, 2021, p. 22).

Miyamoto et al. (2014) entwickelten ein Eye-Tracking basierendes System, um die Gewohnheit der Teilnehmer und Teilnehmerinnen zu fördern auf die URL-Adressleiste zu sehen, bevor sensible Informationen eingegeben werden. Das System deaktiviert zunächst die Eingabefelder auf einer Website und ermittelt mithilfe von Eye-Tracking-Daten, ob

der Nutzer oder die Nutzerin die URL der Website angesehen hat. Die Eingabefelder werden aktiviert, nachdem die Aufmerksamkeit des Benutzers oder der Benutzerin auf die URL-Adressleiste gelenkt wurde. Das System zeigte eine gute Lernfähigkeit und verbesserte die Genauigkeit bei der Erkennung von Phishing-Websites (Nicholson *et al.*, 2020, p. 4). Alsharnouby et al. (2015) verwendeten Eye-Tracking, um Daten zu erhalten, welche visuellen Hinweise die Aufmerksamkeit der Nutzer und Nutzerinnen auf die Legitimität von Websites lenkten. Die Ergebnisse zeigten, dass die Nutzer und Nutzerinnen nur 53% der Phishing-Websites erfolgreich erkannten und dass sie im Allgemeinen sehr wenig Zeit damit verbrachten auf Sicherheitsindikatoren zu achten im Vergleich zum Inhalt der Website (Alsharnouby, Alaca and Chiasson, 2015, p. 69).

#### 2.3.7.5.5 Computer- und Internet-Nutzung

Die allgemeine Internetnutzung bezieht sich auf die kumulierte Zeit, die eine Person online mit einer Vielzahl von Aktivitäten verbringt (Moody, Galletta and Dunn, 2017, p. 569). Die Ergebnisse von Iuga et al. (2016) deuteten darauf hin, dass die Anzahl der Jahre an Computernutzungserfahrung einen statistisch signifikanten Einfluss auf die Phishing-Erkennungsrate hatte (Jampen *et al.*, 2020, p. 15). Moody et al. (2017) zeigten, dass die kumulative Zeit, die ein Nutzer oder eine Nutzerin im Internet verbrachte, die Anfälligkeit für Phishing vorhersagte, wobei hier hingegen mehr Zeit mit einer höheren Anfälligkeit verbunden ist. Parsons et al. (2019) fanden ebenfalls heraus, dass der prozentuale Anteil der am Computer verbrachten Zeit ein signifikanter Prädiktor für die Anfälligkeit für Phishing war, d.h. Nutzer und Nutzerinnen die mehr Zeit am Computer verbrachten, waren anfälliger. Kumaraguru et al. (2007) hingegen fanden keinen Zusammenhang zwischen den im Internet verbrachten Stunden und der Anfälligkeit für Phishing. Andere Studien (Wright et al., 2009, Wright und Marett 2010) haben den gegenteiligen Zusammenhang festgestellt, wonach mehr Interneterfahrung tatsächlich mit einer geringeren Anfälligkeit und einer besseren Fähigkeit zur Erkennung von Phishing verbunden war (Tornblad, Jones, *et al.*, 2021, p. 940).

#### 2.3.7.5.6 E-Mail-Wissen

Parsons et al. (2015) versuchten herauszufinden welche Anhaltspunkte am besten geeignet sind, um Phishing-E-Mails zu erkennen und ob die Nutzer und Nutzerinnen diese Anhaltspunkte tatsächlich nutzten. Die Autoren und Autorinnen untersuchten Studien zu dieser Frage und stellten eine Liste der darin identifizierten Anhaltspunkte zusammen. Sie identifizierten inhaltliche Konsistenz, Link-Legitimität, E-Mail-

Personalisierung und Rechtschreibung als die besten Indikatoren. Ihre Ergebnisse deuteten jedoch darauf hin, dass die Benutzer und Benutzerinnen ihre Entscheidungen häufig auf der Grundlage schlechter Indikatoren treffen. So ließen sich die Teilnehmer und Teilnehmerinnen von der visuellen Präsentation der E-Mail beeinflussen z.B. die Phishing-E-Mail war optisch ansprechend aufgrund eines professionell aussehenden Logos. Andrić et al. (2016) fanden eine erhöhte Phishing-Erfolgsrate, wenn E-Mails verwendet wurden, die dem Original ähnlich aussahen. Außerdem fielen mehr Nutzer und Nutzerinnen dem Phishing zum Opfer, wenn die verlinkte Seite ein identischer Klon der erwarteten Original-Website war (Jampen *et al.*, 2020, p. 23). Benenson et al. (2017) berichteten über die Ergebnisse eines Feldexperiments, bei dem sie über 1.200 Universitätsstudenten und -studentinnen eine E-Mail oder eine Facebook-Nachricht mit einem Link von nichtexistierenden Partybildern von einer nichtexistierenden Person schickten. Später fragten sie nach den Gründen für des Klickverhaltens. Benenson et al. (2017) registrierten einen signifikanten Unterschied in den Klickraten: 20% der E-Mail-Empfänger und Empfängerinnen klickten auf den Link gegenüber 42,5% der Facebook-Empfänger und Empfängerinnen. Der am häufigsten genannte Grund für den Klick eines Links war Neugier (34%), gefolgt von der Erklärung, dass die Nachricht den Erwartungen der Empfänger und Empfängerinnen entsprach (27%). Außerdem dachten 16%, dass sie den Absender oder die Absenderin kennen könnten (Benenson, Gassmann and Landwirth, 2017, p. 1).

#### 2.3.7.5.7 E-Mail-Nutzung

Vishwanath et al. (2011) fanden heraus, dass die Anzahl der an einem Tag erhaltenen E-Mails und das Ausmaß der Relevanz für Empfänger und Empfängerinnen die Wahrscheinlichkeit erhöhte, dass eine Person auf eine Phishing-E-Mail antwortete (Moody, Galletta and Dunn, 2017, p. 565). Vishwanath et al. (2011) zeigten ebenfalls, dass die gewohnheitsmäßige Nutzung von E-Mails erheblich zur Anfälligkeit für Phishing-E-Mails beigetragen hatte. Musuva et al. (2019) fanden jedoch heraus, dass diejenigen die viele E-Mails erhielten, weniger anfällig für Phishing waren. Welk et al. (2015) fanden heraus, dass Nutzer und Nutzerinnen die E-Mails vollständig gelesen haben, Phishing-E-Mails signifikant besser erkennen konnten als Nutzer und Nutzerinnen die den Inhalt der E-Mail nur flüchtig oder nicht vollständig gelesen haben (Tornblad, Jones, *et al.*, 2021, p. 941).

#### 2.3.7.5.8 Plattform-Wissen

Downs et al. (2007) fanden heraus, dass Nutzer und Nutzerinnen von PayPal und eBay seltener auf E-Mail- und webbasierte Phishing-Angriffe hereinfallen, die diese Websites vortäuschen. Alseadon et al. (2012) fanden heraus, dass das Wissen darüber, was für eine Plattform normal und abnormal ist, die Anfälligkeit für Phishing-Angriffe über diese Plattform beeinflussen kann. Heartfield et al. (2016) fanden jedoch heraus, dass die Vertrautheit mit der Plattform eines bestimmten Anbieters oder einer bestimmten Anbieterin nicht die Anfälligkeit vorhersagte (Tornblad, Jones, *et al.*, 2021, pp. 940–941). Aburrous et al. (2010) erstellten eine exakte Nachbildung der Original-Website der „Jordan Ahli Bank" und schickten betrügerische Phishing-E-Mails an 120 Mitarbeiter und Mitarbeiterinnen der Bank. Sie fanden heraus, dass die meisten Mitarbeiter und Mitarbeiterinnen das Zertifikat, das während der Studie in ihrem Browser angezeigt wurde, nicht überprüften, weil sie nicht wussten, was es bedeutete oder sich nicht die Mühe machten es zu überprüfen. Einige Mitarbeiter und Mitarbeiterinnen wiesen darauf hin, dass die inhaltlichen Details der Website und das ausgefallene Design und Stil einer der Hauptgründe für die Legitimität der Website waren. Sie gingen davon aus, dass die Website seriös ist, wenn sie hochwertige Bilder und viele Animationen enthält (Purkait, Kumar De and Suar, 2014, p. 201). Kirlappos und Sasse (2012) bewerteten ein Anti-Phishing-Tool in einem realistischen Umfeld. Die Teilnehmer und Teilnehmerinnen mussten unter Zeitdruck Tickets kaufen und verloren Geld, wenn sie dies auf bösartigen Websites kauften. Während keiner der Teilnehmer und Teilnehmerinnen von Seiten kaufte, die das Tool eindeutig als bösartig identifizierte, riskierten 40% der Teilnehmer und Teilnehmerinnen Geld bei Seiten die als potenziell riskant gekennzeichnet waren, jedoch die Tickets günstiger anboten. Die Analyse der Interviews mit den Teilnehmer und Teilnehmerinnen ergaben, dass sie sich nicht auf die Warnhinweise konzentrierten, wenn sie ein gutes Angebot sahen. Vielmehr suchten sie nach Anzeichen die ihrer Meinung nach die Vertrauenswürdigkeit einer Website bestätigen: vertrautes Design oder Marken, Vertrauenssiegel, Anzeigen, Verweise auf soziale Netzwerke und ein professionell wirkendes Design wurden als zuverlässige Indikatoren für eine seriöse Website genannt (Kirlappos and Sasse, 2012, p. 1).

#### 2.3.7.5.9 Plattform-Nutzung

Heartfield et al. (2016) fanden heraus, dass Nutzer und Nutzerinnen die häufiger auf eine Plattform zugreiften, weniger anfällig waren. Die Interaktion mit einer bestimmten Plattform kann die Awareness für plattformspezifisches Phishing erhöhen, und diejenigen

die länger auf eine Plattform zugreiften, waren auch weniger anfällig für Phishing. Vishwanath (2015) fand heraus, dass die gewohnheitsmäßige Facebook-Nutzung der größte Prädiktor für die Anfälligkeit durch einen Social Media Angriff war, was darauf hindeutete, dass die Anfälligkeit speziell mit der gewohnheitsmäßigen Nutzung einer bestimmten Plattform zusammenhängen könnte (Tornblad, Jones, *et al.*, 2021, p. 941). Leukfeldt et al. (2014) zeigen jedoch, dass die häufige Teilnahme an Online-Aktivitäten wie z.B. Chatrooms, Spielen, Nutzung von Foren oder sozialen Netzwerken nicht mit der Anfälligkeit einer Person für Phishing korrelierte (Jampen *et al.*, 2020, p. 20).

#### 2.3.7.6 Risikobereitschaft

Die Risikobereitschaft bezieht sich auf die Bereitschaft des Einzelnen, die Ungewissheit in verschiedenen Aspekten des Lebens zu akzeptieren und sich auf potenziell riskante Verhaltensweisen einzulassen (Moody, Galletta and Dunn, 2017, p. 569). Es gibt zwei Arten der Risikobereitschaft, nämlich die aktive und die passive Risikobereitschaft (Papatsaroucha *et al.*, 2021, p. 11).

- Die passive Risikobereitschaft ist definiert als die Entscheidung eine möglicherweise vorteilhafte Handlung nicht vorzunehmen, und ist ein starker Prädiktor für die Untersuchung der Absichten eines Nutzers oder einer Nutzerin in Bezug auf die Cybersicherheit (z.B. ein schwaches Passwort nicht zu verstärken) (Papatsaroucha *et al.*, 2021, p. 11).
- Aktive Risikobereitschaft bezieht sich auf risikoreiche Handlungen die eine Person vornehmen könnte (z.B. das Herunterladen einer Datei von einer nicht vertrauenswürdigen Website) (Papatsaroucha *et al.*, 2021, p. 11).

Die Risikobereitschaft wird im Allgemeinen als eine der Hauptursachen für einen erfolgreichen Phishing-Angriff genannt (Abroshan *et al.*, 2021c, p. 44930). Es zeigte sich, dass die Neigung, in verschiedenen Lebensbereichen Risiken einzugehen, die Anfälligkeit für Phishing signifikant vorhersagt, so dass Personen mit höherer Risikoneigung anfälliger waren, allerdings nur wenn die Phishing-E-Mail von einer bekannten Quelle stammte und der darin enthaltene Link eher ein Text als eine Zahl war (Tornblad, Jones, *et al.*, 2021, p. 939). Sheng et al. (2010) haben das Risikoverhalten von Nutzer und Nutzerinnen bei Finanzinvestitionen gemessen und haben festgestellt, dass die Wahrscheinlichkeit auf einen Phishing-Betrug hereinzufallen, umso geringer ist, je risikoscheuer die Personen waren (Abroshan *et al.*, 2021c, p. 44930).

#### 2.3.7.7 Informationsverarbeitung

Informationsverarbeitung bezieht sich auf die Art und Weise wie Menschen die Glaubwürdigkeit von Informationen verarbeiten und beurteilen. Es gibt zwei Hauptwege, die eine Person bei der Informationsverarbeitung beschreiten kann den heuristischen Weg und den systematischen Weg. Der heuristische Weg ist oberflächlicher und erfordert weniger kognitive Ressourcen für die Informationsbewertung. Menschen, die dieser Denkweise folgen, verlassen sich weniger auf den Kontext und die Bedeutung einer empfangenen Nachricht (Papatsaroucha *et al.*, 2021, pp. 10–11). Die heuristische Verarbeitung konzentriert sich auf einfache Entscheidungsaufforderungen, die oft als Faustregeln bezeichnet werden, und erfolgt wenn es den Menschen an Motivation oder kognitiven Ressourcen mangelt (Frauenstein and Flowerday, 2020, p. 7). Auf der anderen Seite ist der systematische Weg ein tiefgründiger Weg der Informationsverarbeitung und höheren kognitiven Aufwand erfordert. Dabei würden die Menschen es vorziehen Informationen zu analysieren und in der Regel neigen sie dazu einige Nachforschungen anzustellen, um die Glaubwürdigkeit der erhaltenen Nachrichten zu beurteilen (Papatsaroucha *et al.*, 2021, p. 11).

Luo et al. (2013) stellten fest, dass die systematische Verarbeitung nicht nur von der eigenen Fähigkeit zum kritischen Denken abhängt, sondern auch von anderen Faktoren wie dem vorhandenen Wissen, der Selbstwirksamkeit bei der Beschaffung relevanter Informationen und der wahrgenommenen Nützlichkeit und Glaubwürdigkeit der verfügbaren Informationen. Im Idealfall würde es weniger Phishing-Opfer geben, wenn die Nutzer und Nutzerinnen die Informationen die sie erhalten, systematisch verarbeiten, sie auf Gültigkeit prüfen und auf visuelle Hinweise achten würden (Frauenstein and Flowerday, 2020, p. 7). Denn Angreifer und Angreiferinnen versuchen bei Phishing-Angriffen die Opfer dazu zu bringen eine schnelle, emotionale Reaktion unter Verwendung von Heuristiken zu nutzen, anstatt eine logische und durchdachte Reaktion auszuführen. Indem der Nutzer oder die Nutzerin jedoch aufgefordert wird eine Pause einzulegen, kann der Gedankenstrom der Nutzer und Nutzerinnen unterbrochen werden und auf ein logisches Denken umgestellt werden. Jensen et al. (2017) haben vorgeschlagen, dass die Aufforderung zum Innehalten den Nutzer oder die Nutzerin dazu anregt über den Inhalt einer E-Mail-Nachricht nachzudenken. Es ist somit vielversprechend den E-Mail-Benutzer oder -Benutzerin zum logischen Denkprozess anzuregen. Es wurde nämlich festgestellt, dass es zu Fehleinschätzungen kommt, wenn Menschen Heuristiken verwenden. (Antonucci *et al.*, 2020, pp. 1–8). Yan et al. (2018) stellte jedoch fest, dass es keinen signifikanten Unterschied zwischen heuristischer und

systematischer Informationsverarbeitung gibt. Nach Ansichten der Autoren und Autorinnen könnte dieses Ergebnis aufgetreten sein, aufgrund des mangelnden Wissens der Studenten und Studentinnen über Cybersicherheit. Diese Beobachtung legte daher nahe, dass eine heuristische und systematische Bewertung der Informationsverarbeitung mehr Erkenntnisse liefern kann, wenn sich eine Studie auf Nutzer und Nutzerinnen konzentriert, die bereits über ein gewisses Maß an Vertrautheit mit Cybersicherheit verfügen (Papatsaroucha *et al.*, 2021, p. 18).

# 3 Empirischer Teil

## 3.1 Vorgehensweise

In dieser Masterarbeit wurde eine quantitative Untersuchung mit Hilfe eines Online-Fragebogens mit fünf Teilen durchgeführt. Im Folgenden wird auf die einzelnen Teile genauer eingegangen. Der Online-Fragebogen wurde mithilfe des Online Tools von SoSci Survey GmbH erstellt. Das Unternehmen bietet die kostenlose Durchführung der Umfrage für nicht-kommerzielle Forschung an. Aus diesem Grund wurde dieses Online-Tool ausgewählt und es wurde die Programm-Version 3.3.13 verwendet (*SoSciSurvey*, 2022). Für die statistische Analyse und Auswertung des Fragebogens wurde die Software „SPSS“ von IBM (Version 28.0.) genutzt. Die Lizenz hierfür wurde im Shop der Ferdinand Porsche FernFH erworben (*SPSS für Studierende*, 2022).

Bevor die einzelnen Teile des Fragebogens näher erläutert werden, ist es wichtig zu erwähnen, dass aufgrund der Forschungsfrage eine Ausschlussfrage für den Fragebogen erstellt wurde. Die Forschungsfrage bezieht sich auf die Großunternehmen in Österreich und die Wirtschaftskammer Wien definiert Großunternehmen wie folgt: Ein Unternehmen wird als Großunternehmen definiert, wenn die Mitarbeiter- und Mitarbeiterinnenanzahl bei größer gleich 250 Personen liegt. Des Weiteren muss der Umsatz größer als 50 Mio. Euro und die Bilanzsumme größer als 43 Mio. Euro betragen. Jedoch erläutert die Wirtschaftskammer Wien auch, dass für statistische Zwecke nur die Anzahl der Mitarbeiter und Mitarbeiterinnen für die Abgrenzung der Unternehmen in Kleinst,- Klein-, Mittlere- und Großunternehmen ausschlaggebend ist (Bildungspolitik, 2022). Aus diesem Grund lautet die Ausschlussfrage wie folgt: Haben Sie jemals in einem Unternehmen in Österreich mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet? Für diese Fragestellung gab es drei Antwortmöglichkeiten (siehe Abbildung 45 im Anhang A). Wenn die dritte Antwortmöglichkeit ausgewählt wird, wird der Fragebogen für diese Teilnehmer und Teilnehmerinnen beendet. Sie erhalten im Zuge

dessen eine Information, wieso der Fragebogen für sie beendet wurde (siehe Abbildung 44 im 0). Der gesamte Fragebogen kann im Anhang A eingesehen werden.

### 3.1.1 Teil 1

Der erste Teil des Fragebogens beschäftigt sich mit folgenden Faktoren: Phishing Vertrautheit, Phishing Awareness und Sicherheitsgewohnheiten. Zu den Faktoren wurden jeweils zwölf Fragen gestellt. Für die Formulierung der Fragen in dieser Befragung wurden Fragen von bereits durchgeführten Studien angepasst und abgewandelt. Bis auf die Definitionsfrage für Phishing Vertrautheit, wurden die restlichen Fragen anhand der fünfstufigen Likert Skala („stimme überhaupt nicht zu", „stimme nicht zu", „stimme weder zu noch stimme zu", „stimme zu" und „stimme voll und ganz zu") beantwortet. Im Folgenden wird auf die einzelnen Aussagen der Faktoren näher eingegangen.

Die Phishing Vertrautheit der Teilnehmer und Teilnehmerinnen des Fragebogens wurde zunächst mit einer Definitionsfrage festgestellt (siehe Abbildung 46). Diese Fragestellung stammte von Esmat et al. (2021) (Esmat, Alharbi and Karrar, 2021, p. 793). Des Weiteren wurde der Faktor Phishing Vertrautheit mit elf Aussagen bestimmt. Diese Aussagen werden anhand der Likert Skala gemessen und sind in der Abbildung 46 ersichtlich. Die ersten zwei Aussagen stammten von Jensen et al. (2017) (Jensen *et al.*, 2017, p. 606). Die dritte Aussage wurde aus folgender der Studie von Akpon-Ebiyonare und Konyeha (2019) bezogen (Akpon-Ebiyonare, 2019, p. 91). Die Aussagen vier bis sieben wurden von Sumner et al. (2021) abgeleitet (Sumner *et al.*, 2021, p. 20). Die letzten vier Aussagen stammen wie auch die Definitionsfrage von Esmat et al. (2021) (Esmat, Alharbi and Karrar, 2021, pp. 794–795).

Der Faktor Phishing Awareness wurde mit zwölf Aussagen definiert (siehe Abbildung 47), die auch mit der Likert Skala von den Teilnehmer und Teilnehmerinnen des Fragebogens beantwortet werden. Die erste, sechste und siebte Aussage des Faktors Phishing Awareness stammte von der Studie Sumner et al. (2021) (Sumner *et al.*, 2021, p. 20). Die Aussagen zwei bis fünf und die letzte Aussage stammte von Akpon-Ebiyonare und Konyeha (2019) (Akpon-Ebiyonare, 2019, p. 91). Die Aussagen acht und neun sind von Esmat et al. (2021) abgeleitet worden (Esmat, Alharbi and Karrar, 2021, p. 794). Die zehnte und elfte Aussage stammte von der Autorin Kim (B. Kim, 2014, p. 119).

Die Sicherheitsgewohnheiten stellen den letzten Faktor im ersten Teil des Fragebogens dar und wurde auch mithilfe von zwölf Aussagen definiert (Abbildung 48). Dieser Faktor

wird auch mit der Likert Skala beantwortet. Die Aussagen eins und vier wurde von der Autorin Kim abgeleitet (B. Kim, 2014, p. 119). Die restlichen Aussagen stammen von Akpon-Ebiyonare und Konyeha (2019) (Akpon-Ebiyonare, 2019, p. 91).

### 3.1.2 Teil 2

Die abhängige Variable Phishing-Anfälligkeit stellt die Fähigkeit der E-Mail-Nutzer und E-Mail-Nutzerinnen dar, eine Phishing-Angriff korrekt zu erkennen. Es gibt zwei Methoden, um die tatsächlichen Fähigkeiten der Teilnehmer und Teilnehmerinnen in Bezug auf die Unterscheidung zwischen Phishing-E-Mails und legitimen E-Mails zu bewerten (Reinheimer *et al.*, 2020, p. 264):

- Phishing-E-Mails mit oder ohne Ankündigung zu senden und die anschließende Aufforderung die Phishing-E-Mails zu melden (Reinheimer *et al.*, 2020, p. 264).
- Eine Reihe von E-Mails im Stil einer Umfrage gestalten und die Aufforderung zu entscheiden, welche E-Mails legitim und welche bösartig sind (Reinheimer *et al.*, 2020, p. 264).

Für die Masterarbeit wurde die zweite Methode ausgewählt. Die Variable Phishing Anfälligkeit wird durch die Befragung der Teilnehmer und Teilnehmerinnen gemessen, indem sie eine Reihe von E-Mail als legitim oder als Phishing identifizieren. In dem Fragebogen werden zehn Screenshots von verschiedenen E-Mails gezeigt. Von diesen zehn Screenshots sind sechs Phishing-E-Mails und vier davon sind legitime E-Mails. Damit die Teilnehmer und Teilnehmerinnen nicht anfangen zu raten, wird auch die Option „Ich weiß es nicht“ zur Verfügung gestellt. Die korrekte Identifizierung einer E-Mail wird mit "1" bewertet, während die falsche Identifizierung oder die Auswahl „Ich weiß es nicht“ mit „0“ bewertet wird. Eine höhere Punktzahl entspricht einem höheren Niveau der Fähigkeit eine Phishing-E-Mail richtig zu identifizieren bzw. ist die Phishing Anfälligkeit niedriger.

Die Phishing-E-Mails wurden aus verschiedenen Online-Quellen entnommen. Die legitimen E-Mails stammen vom Autor selbst und wurden aus dem persönlichen Posteingang des Autors entnommen. Die E-Mails wurden so angepasst, dass sie das gleiche Format haben, dabei wurden unter anderem etwaige persönliche Daten wegretuschiert. Zudem wurde darauf geachtet, dass die Beispiele alle in deutscher Sprache geschrieben sind. Im Folgenden wird auf die Auswahl der Phishing-E-Mails näher eingegangen. Bei der Auswahl der Phishing-E-Mails wurde darauf geachtet, dass keine Spam E-Mails oder leicht erkennbare Phishing-E-Mails ausgewählt wurden. Des

Weiteren wurde die Auswahl der Phishing-E-Mails anhand von Statistiken von Statista ausgewählt.

Die Abbildung 49 stellt eine Phishing-E-Mail dar, die von der UniCredit Bank Austria stammen sollte (*Bank Austria - Phishing*, 2021). Die UniCredit Bank Austria war in 2021 laut Statista einer der Top drei Banken (gemessen anhand der durchschnittlichen Bilanzsumme der österreichischen Banken) in Österreich und aus diesem Grund wurde ein Phishing Beispiel zu dieser Bank ausgewählt (*Statista - Durchschnittliche Bilanzsumme Banken 2021*, 2021). Die Abbildung 51 stellt ein Phishing Beispiel zu Media Markt (Redaktionsteam, 2020a) und Abbildung 52 ein Phishing Beispiel zu Amazon dar (*Amazon - Phishing*, 2019). Diese Anbieter und Anbieterinnen waren 2020 laut Statista in den Top drei der Online-Shops (gemessen an den erwirtschafteten Umsätzen) in Österreich vertreten (*Statista - Top 10 der Online-Shops*, 2020). Aus diesem Grund wurden diese zwei Beispiele in den Fragebogen miteinbezogen. Des Weiteren wurden ein Phishing Beispiel von Netflix (siehe Abbildung 54) ausgewählt (Redaktionsteam, 2019), weil bei einer Umfrage zur Nutzung von Videoportalen in Österreich, Netflix den dritten Platz (gemessen an der Anzahl der Nutzer und Nutzerinnen innerhalb der letzten vier Wochen) erreicht hat (*Statista - Nutzung von Videoportalen 2022*, 2022). Die Abbildung 57 zeigt ein Phishing Beispiel zu Paypal (Redaktionsteam, 2020b). Dieses Beispiel wurde ausgewählt, weil dies einer der bevorzugtesten Zahlungsmethoden bei Käufen über das Handy in Österreich in 2019 und 2020 darstellte (*Statista - Zahlungsmethoden am Handy 2020*, 2020). Das letzte Phishing Beispiel (siehe Abbildung 58) ist von der österreichischen Post. Die Österreichische Post AG ist eines der führenden Logistik- und Postunternehmen in Österreich und hat im Jahr 2021 rund 184 Millionen Pakete befördert (*Statista - Paketsendungen 2021*, 2021). Aus diesen zwei Gründen wurde dieses Phishing Beispiel in den Fragebogen miteinbezogen. Die restlichen Abbildungen (Abbildung 50, Abbildung 53, Abbildung 55 und Abbildung 56) sind legitime E-Mails und wurden vom Autor persönlich ausgewählt.

Die Phishing Anfälligkeit wird auch anhand der Erkennung von URLs (siehe Abbildung 59) gemessen, denn einige E-Mails beinhalten keine Links oder enthalten Buttons und somit könnten die Teilnehmer und Teilnehmerinnen nicht in der Lage eine Phishing-E-Mail anhand eines Links zu erkennen. Aus diesen Gründen werden zehn URLs (siehe Abbildung 59) zur Identifikation den Teilnehmer und Teilnehmerinnen des Fragebogens dargestellt. Fünf der URLs sind legitim und die anderen fünf stellen bösartige URLs dar. Drei der Phishing URLs (https://147.46.236.55/PayPal/login.html, https://www.msn-verify.com/, https://www.ebay-security.com,) wurde von Arachchilage et al. (2016)

entnommen (Arachchilage, Love and Beznosov, 2016, p. 188). Die restlichen URLs sind vom Autor selbst erstellte Beispiele auf Basis der Literaturrecherche. Die URL wurden so umgestaltet, dass sie das gleiche Format haben und alle URLS beginnen mit https://. Wie auch bei der Identifikation von den E-Mails wird hier auch die Möglichkeit mit „Ich weiß es nicht“ angeboten, um das Raten zu vermeiden. Die korrekte Identifizierung einer URL wird mit "1" bewertet, während die falsche Identifikation oder die Option „Ich weiß es nicht“ mit "0" bewertet wird. Eine höhere Punktzahl entspricht einem höheren Niveau der Fähigkeit, eine Phishing-URL richtig zu identifizieren, bzw. ist die Phishing Anfälligkeit niedriger.

### 3.1.3 Teil 3

Der dritte Teil des Fragebogens beschäftigt sich mit Fragen zu Teilnahme einer Phishing Schulung (siehe Abbildung 59), zu durchgeführten Schulungsmethoden (siehe Abbildung 60) und wann Teilnehmer und Teilnehmerinnen ihre letzte Schulung hatten (siehe Abbildung 60). Hierbei wurden drei Fragen gestellt und diese drei Fragen beziehen sich auf das Großunternehmen, in denen die Teilnehmer und Teilnehmerinnen derzeit arbeiten oder bereits gearbeitet haben. Es wurde hier eine kurze Information zur Erinnerung der Teilnehmer und Teilnehmerinnen hinzugefügt: „Beachten Sie bei der Beantwortung der nachfolgenden Fragen, dass diese sich auf das Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen bezieht.“. Mit dieser Erinnerung wird sichergestellt, dass sich diese Fragen auf das Großunternehmen beziehen und somit die Forschungsfrage beantwortet werden kann.

Die erste Frage lautet wie folgt: „Haben Sie schon einmal an einer Phishing Schulung teilgenommen?“. Wenn hier die zweite Antwort („Nein, ich habe an keiner Schulung teilgenommen, die das Thema Phishing behandelt hat.“) ausgewählt wird, erhalten die Teilnehmer und Teilnehmerinnen des Fragebogens die restlichen zwei Fragen nicht mehr (siehe Abbildung 61) und werden zu dem vierten Teil des Fragebogens weitergeleitet (siehe Abbildung 62). Wenn hier die erste Antwort („Ja, ich habe an einer Schulung teilgenommen, die das Thema Phishing behandelt hat.“) oder die Option „Ich weiß es nicht“ ausgewählt wird, kommt die folgende Frage: „Welche Art von Schulung haben Sie erhalten?“ hatten (siehe Abbildung 60). Die vorgeschlagenen Schulungsmethoden sind von dem theoretischen Teil der Masterarbeit abgeleitet. Es gibt die folgenden Antwortmöglichkeiten: „Herkömmliche Schulung“, „Eingebettete Schulung“, „Simulierte Schulung“, „Spielbasierte Schulung“, „Achtsamkeitsschulung“ oder „Keine dieser genannten Schulung habe ich erhalten. Neben den jeweiligen Antwortmöglichkeiten steht

auch eine kurze Information zu den jeweiligen Schulungsmethoden, die sich die Teilnehmer und Teilnehmerinnen durchlesen konnten, um informiert, das Richtige auszuwählen. Die letzte Fragestellung in diesem Teil des Fragebogens beschäftigt sich mit der folgenden Frage: „Wann haben Sie ihre letzte Phishing Schulung absolviert?“ hatten (siehe Abbildung 60). Diese Frage wurde in Monaten gemessen und es gab hierzu fünf Antwortmöglichkeiten („Weniger als 1 Monat“, „1-3 Monate“, „3-5 Monate“, „Mehr als 5 Monate“) und die Option „Ich weiß es nicht“.

### 3.1.4 Teil 4

Der vierte Teil des Fragebogens beschäftigt sich mit den in der Literatur besprochenen Schulungsmethoden (siehe Abbildung 62 und Abbildung 63). Hier werden für alle Teilnehmer und Teilnehmerinnen nochmal die Schulungsmethoden vorgestellt, auch für die Teilnehmer und Teilnehmerinnen, die im dritten Teil des Fragebogens die Frage („Haben Sie schon einmal an einer Phishing Schulung teilgenommen?“) mit: „Nein, ich habe an keiner Schulung teilgenommen, die das Thema Phishing behandelt hat.“, ausgewählt haben (siehe Abbildung 59). Die Teilnehmer und Teilnehmerinnen erhalten zu den Schulungsmethoden jeweils vier Aussagen wie zum Beispiel im Fall der Herkömmlichen Schulungsmethode: „Die Herkömmliche Schulung wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen.“, „Die Herkömmliche Schulung wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann.“, „Die Herkömmliche Schulung ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können.“ und „Die Herkömmliche Schulung ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können.“. Diese Aussagen werden dann mithilfe der Likert Skala („stimme überhaupt nicht zu“, „stimme nicht zu“, „stimme weder zu noch stimme zu“, „stimme zu“ und „stimme voll und ganz zu“) beantwortet.

### 3.1.5 Teil 5

Der letzte Teil des Fragebogens erhebt demografische Daten zu den Teilnehmer und Teilnehmerinnen des Fragebogens, dazu zählen unter anderem das Geschlecht (siehe Abbildung 63), die höchste abgeschlossene Ausbildung (siehe Abbildung 64), der Arbeitsbereich (siehe Abbildung 64), die Arbeitsjahre (siehe Abbildung 65) und die Wochenstundenanzahl (siehe Abbildung 65). Die Fragen zum Beruf beziehen sich wieder auf das Großunternehmen und auch hier wurde eine kleine Erinnerung diesbezüglich hinzugefügt.

## 3.2 Ergebnisse

Der Fragebogen wurde am 06.08.2022 online gestellt und war bis zum 13.08.2022 über den folgenden Link verfügbar: https://www.soscisurvey.de/phishingschulungsmethoden/. Dieser Link wurde an Verwandte, Bekannte, Freunde, Arbeitskollegen und Arbeitskolleginnen über den Instant-Messaging Dienst Whatsapp als auch über soziale Medien wie beispielsweise Facebook und Instagram weitergeleitet. Des Weiteren wurde das Umfrageforum für Seminar-, Bachelor-, und Masterarbeiten der Ferdinand Porsche FernFH genutzt. Der Fragebogen wurde innerhalb einer Woche 279-mal aufgerufen, jedoch haben nur 178 Personen teilgenommen. Von diesen 178 Personen haben 135 den Fragebogen vollständig ausgefüllt. Von den 135 vollständigen Datensätzen haben 14 Personen noch nicht in einem Großunternehmen in Österreich gearbeitet. Dies führte zum Ausschluss dieser Datensätze, da sich die Forschungsfrage dieser Masterarbeit auf Großunternehmen in Österreich bezieht. Die gültige Anzahl der Datensätze betrug somit 121. Die Rücklaufstatistik (siehe Abbildung 43) ist im Anhang A zu finden. Im Folgenden wird auf die einzelnen Ergebnisse des Fragebogens näher eingegangen und die gesamten Fragestellungen befinden sich im 0.

### 3.2.1 Demografische Merkmale

Es haben 52 weibliche Teilnehmerinnen (43%) und 64 männliche Teilnehmer (52,9%) den Fragebogen ausgefüllt. Des Weiteren gab es fünf Personen (4,1%) die die Option: „Ohne Angabe“ gewählt haben (siehe Abbildung 1). Somit gab es für die weitere Analyse und Auswertung 121 gültige Datensätze.

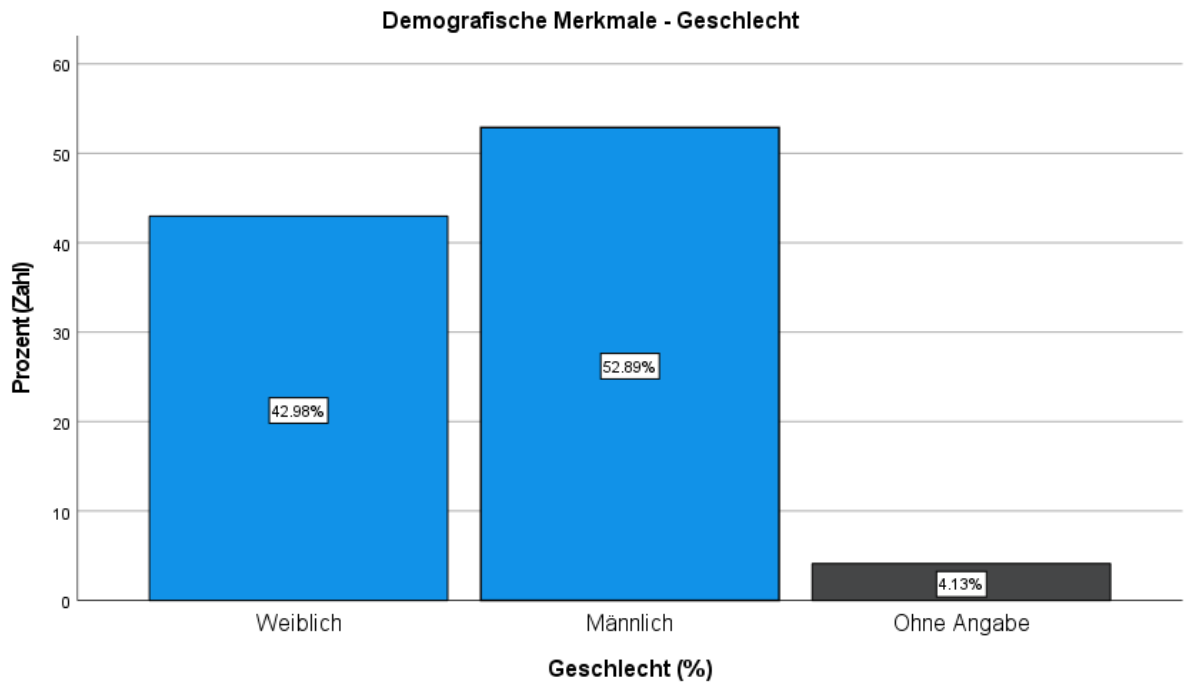



*Abbildung 1: Ergebnis - Geschlecht*

Anhand der Abbildung 2 ist es erkennbar, dass die meisten Teilnehmer und Teilnehmerinnen in diesem Fall 53 Personen (43,8%) bereits ein Bachelorstudium und 28 Personen (23,1%) ein Masterstudium abgeschlossen haben. Eine Person (0,83%) in dem Fragebogen hat bereits einen PhD- oder Doktor-Titel. Die nächsten zwei größten Gruppen sind die Allgemeinbildende (17 Personen – 14,05%) und Berufsbildende (15 Personen – 12,40%) höhere Schulen. Jeweils zwei Personen (1,65%) haben entweder die Berufsschule und Lehre, die Akademie oder die tertiäre Kurzausbildung abgeschlossen. Eine Person (0,83%) hat die Berufsbildende mittlere Schule als höchste abgeschlossene Ausbildung gewählt.

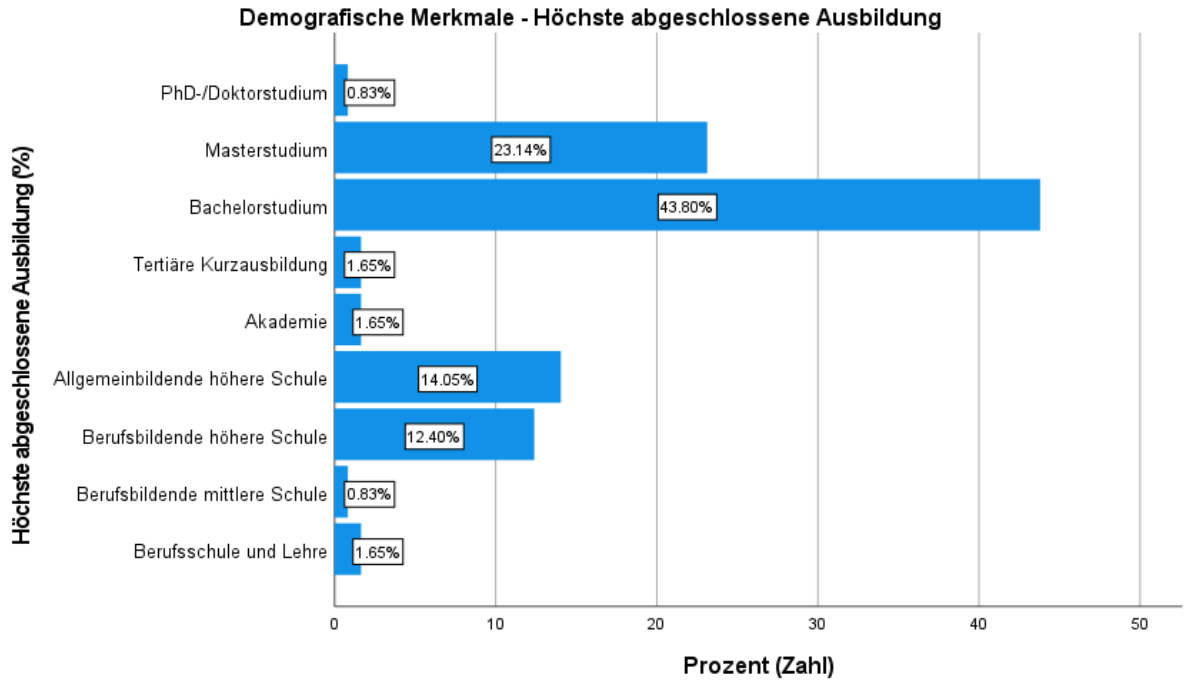



*Abbildung 2: Ergebnis - Höchste abgeschlossene Ausbildung*

Die Abbildung 3 zeigt, dass die meisten Teilnehmer und Teilnehmerinnen (32 Personen – 26,4%) im Bereich Büro, Marketing, Finanz, Recht und Sicherheit arbeiten. Mit 26 Personen (21,5%) ist der Arbeitsbereich – Elektrotechnik, Elektronik, Telekommunikation und IT – die zweitgrößte Gruppe. Danach folgt der Bereich Soziales, Gesundheit und Schönheitspflege mit 19 Personen (15,7%). Die nächsten zwei größten Gruppen sind: Chemie, Biotechnologie, Lebensmittel und Kunststoffe (12 Personen – 9,9%); und Handel, Logistik und Verkehr (9 Personen – 7,4%). In dem Bereich für Maschinenbau, Kfz und Metall arbeiten fünf Personen (4,1%) und jeweils vier Personen (3,3%) arbeiten im Bereich Medien, Grafik, Design, Druck, Kunst und Kunsthandwerk; und Bau, Baunebengewerbe, Holz und Gebäudetechnik. Des Weiteren arbeiten jeweils drei Personen (2,5%) in Wissenschaft, Bildung, Forschung und Entwicklung; und Tourismus, Gastgewerbe und Freizeit. Weitere drei Personen (2,5%) haben die Option: „Andere“ ausgewählt. Eine Person (0,8%) arbeitet im Bereich Textil und Bekleidung, Mode und Leder. Wichtig zu erwähnen ist, dass sich diese Statistik auf Großunternehmen in Österreich bezieht, in welche die Teilnehmer und Teilnehmerinnen derzeit arbeiten oder gearbeitet haben.

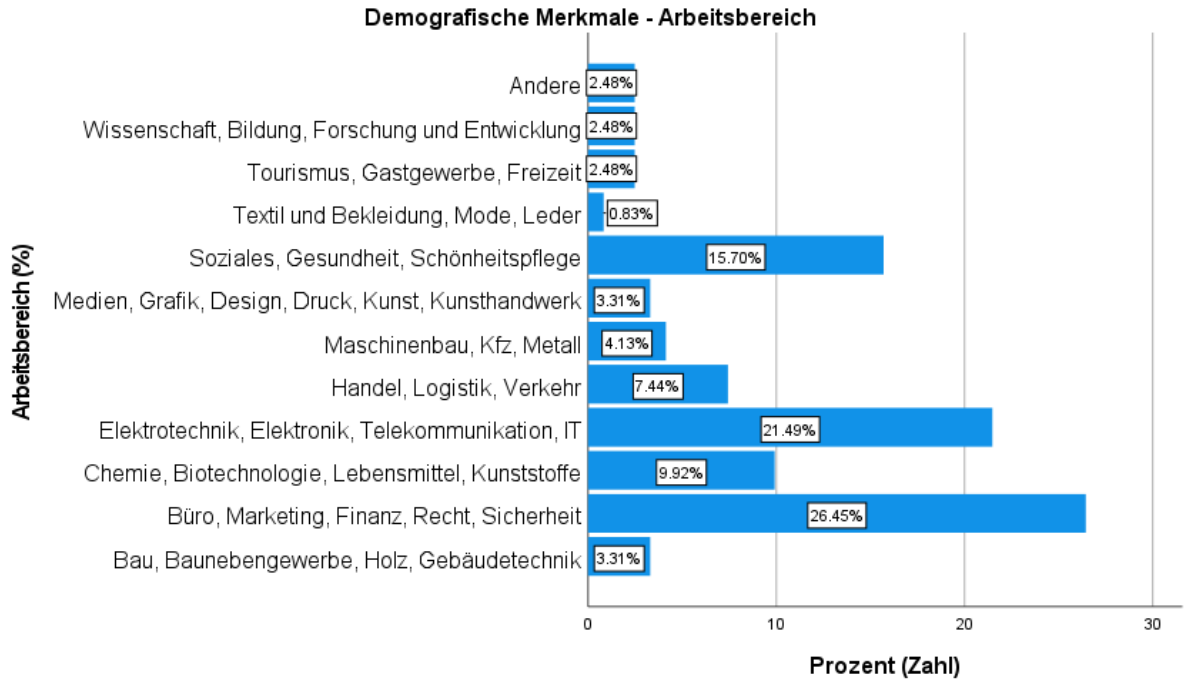



*Abbildung 3: Ergebnis - Arbeitsbereich*

In der Abbildung 4 ist zu erkennen, dass 31 Personen (25,6%) weniger als ein Jahr in einem Großunternehmen in Österreich gearbeitet haben oder derzeit arbeiten. 40 Personen (33,1%) haben 1-3 Jahre gewählt, 27 Personen (22,3%) hingegen 3-6 Jahre und neun Personen (7,4%) haben 6-9 Jahre ausgewählt. 14 Personen (11,6%) haben schon über neun Jahre in einem Großunternehmen in Österreich gearbeitet oder arbeiten derzeit noch dort.

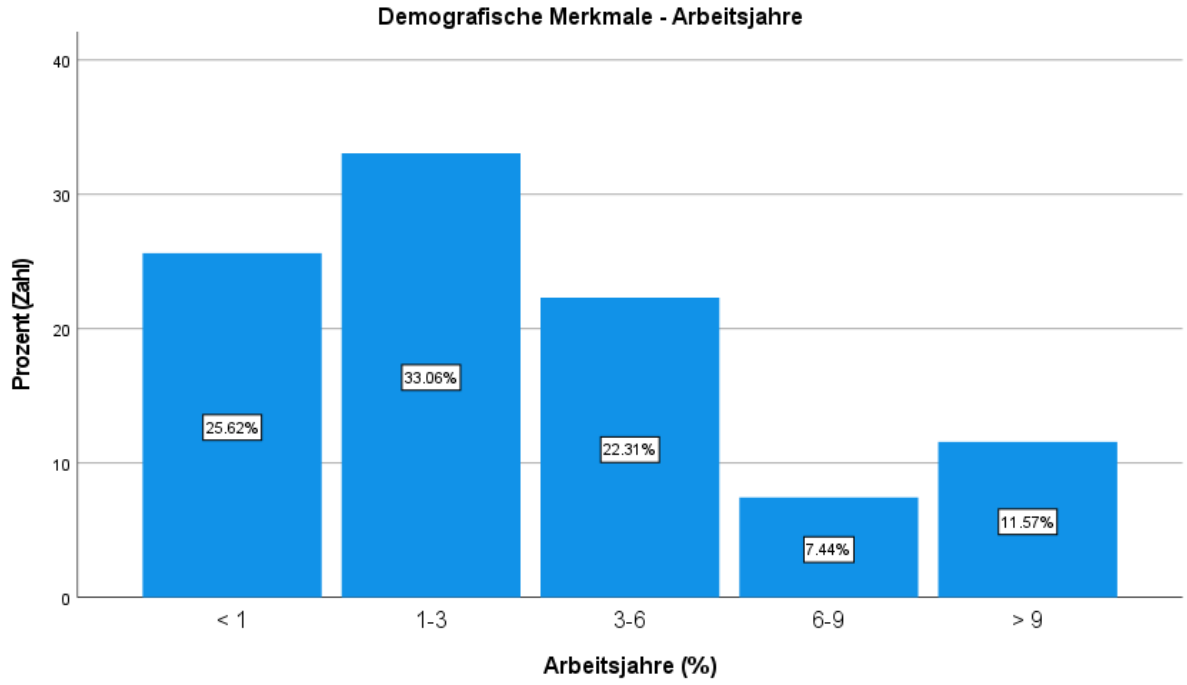



*Abbildung 4: Ergebnis - Arbeitsjahre*

Die Abbildung 5 zeigt, dass die meisten Teilnehmer und Teilnehmerinnen (53 Personen – 43,8%) 31-40 Stunden in der Woche in einem Großunternehmen in Österreich derzeit arbeiten oder gearbeitet haben. 29 Personen (24%) arbeiten sogar über 40 Stunden in der Woche. 18 Personen (14,9%) arbeiten 21-30 Wochenstunden, 15 Personen (12,4%) hingegen nur 11-20 Wochenstunden. Sechs Personen (4,96%) haben die Option „1-10 Wochenstunden“ ausgewählt.

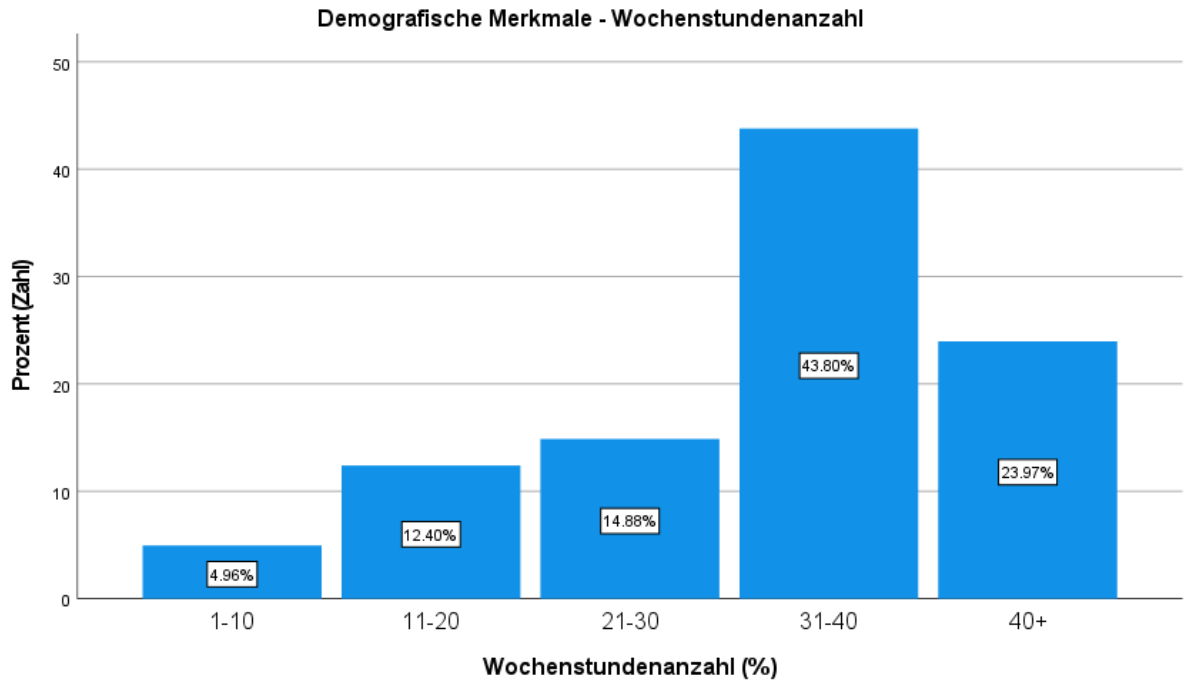



*Abbildung 5: Ergebnis – Wochenstundenanzahl*

### 3.2.2 Vertrautheit, Awareness und Sicherheitsgewohnheiten

Dieser Teil beschäftigt sich mit den folgenden drei Faktoren: „Phishing Vertrautheit“, „Phishing Awareness“ und „Sicherheitsgewohnheiten“. Wie bereits im Kapitel Vorgehensweise (siehe Teil 1) besprochen wurde, wird jeder einzelne Faktor mit einer bestimmten Anzahl von Fragen gemessen. Diese Fragen wurden in SPSS für jeden einzelnen Teilnehmer und jede einzelne Teilnehmerin zusammengefasst und danach wurde der Mittelwert berechnet. Die zusammengefassten Mittelwerte für die einzelnen Personen wurden wie im Artikel von Sözen und Güven (2019) wieder in eine fünfstufige Likert Skala umgewandelt. Die Tabelle 1 ist eine angepasste Version von Sözen und Güven (2019), dabei wurden jedoch die Werte beibehalten (Sözen and Güven, 2019, p. 3). Die beschriebenen Schritte wurden für jeden einzelnen Faktor durchgeführt.

| Bewertungsbereich der Likert Skala | | |
|---|---|---|
| | Wert | Bereich |
| stimme überhaupt nicht zu | 1 | 1,00-1,80 |
| stimme nicht zu | 2 | 1,81-2,60 |
| stimme weder zu noch stimme zu | 3 | 2,61-3,40 |
| stimme zu | 4 | 3,41-4,20 |
| stimme voll und ganz zu | 5 | 4,21-5,00 |

*Tabelle 1: Bewertungsbereich Likert Skala*

Die Abbildung 6 zeigt, dass 72 Personen (59,5%) zustimmen würden, dass sie sich mit dem Thema „Phishing" auskennen („stimme zu" und „stimme voll und ganz zu"). Jedoch haben 41 Personen (33,9%) dafür gestimmt, dass sie weder noch mit dem Thema „Phishing" vertraut sind. Acht Personen (6,7%) sind der Meinung, dass sie sich in diesem Themenbereich nicht auskennen („stimme nicht zu" und „stimme überhaupt nicht zu").

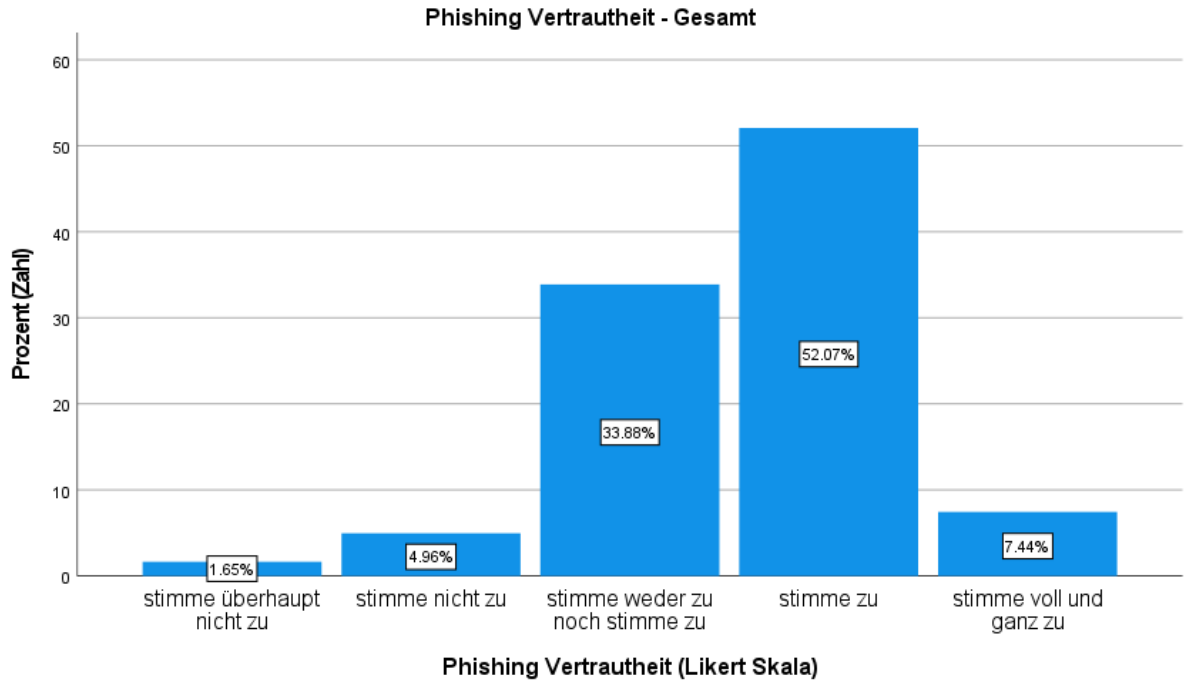



*Abbildung 6: Ergebnis - Phishing Vertrautheit (Gesamt)*

In der Abbildung 7 für Phishing Awareness ist erkennbar, dass 76 Personen (62,8%) eine gewisse Awareness für das Themengebiet „Phishing" haben („stimme zu" und „stimme voll und ganz zu"). 38 Personen (31,4%) wählten hinsichtlich Awareness für Phishing „stimme weder noch zu noch stimme zu" aus. Nur sieben Personen (5,8%) Personen fallen in die Kategorie „stimme nicht zu".

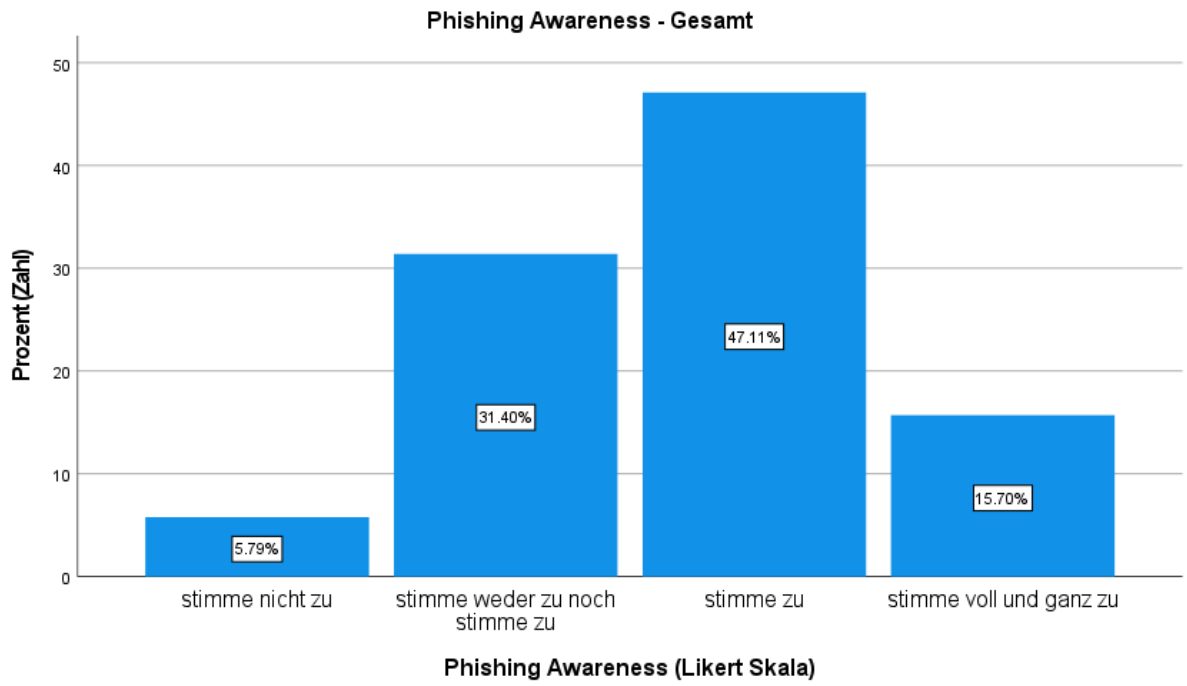



*Abbildung 7: Ergebnis - Phishing Awareness (Gesamt)*

Bei den Sicherheitsgewohnheiten (siehe Abbildung 8) sieht es aber anders aus, denn hier liegt der Wert für „stimme weder zu noch stimme zu“ bei 57 Personen (47,1%). Bei 47 Personen (38,9%) ist eine gewisse Sicherheitsgewohnheit vorhanden („stimme zu“ und „stimme voll und ganz zu“) und bei 17 Personen (14%) ist dies nicht der Fall.

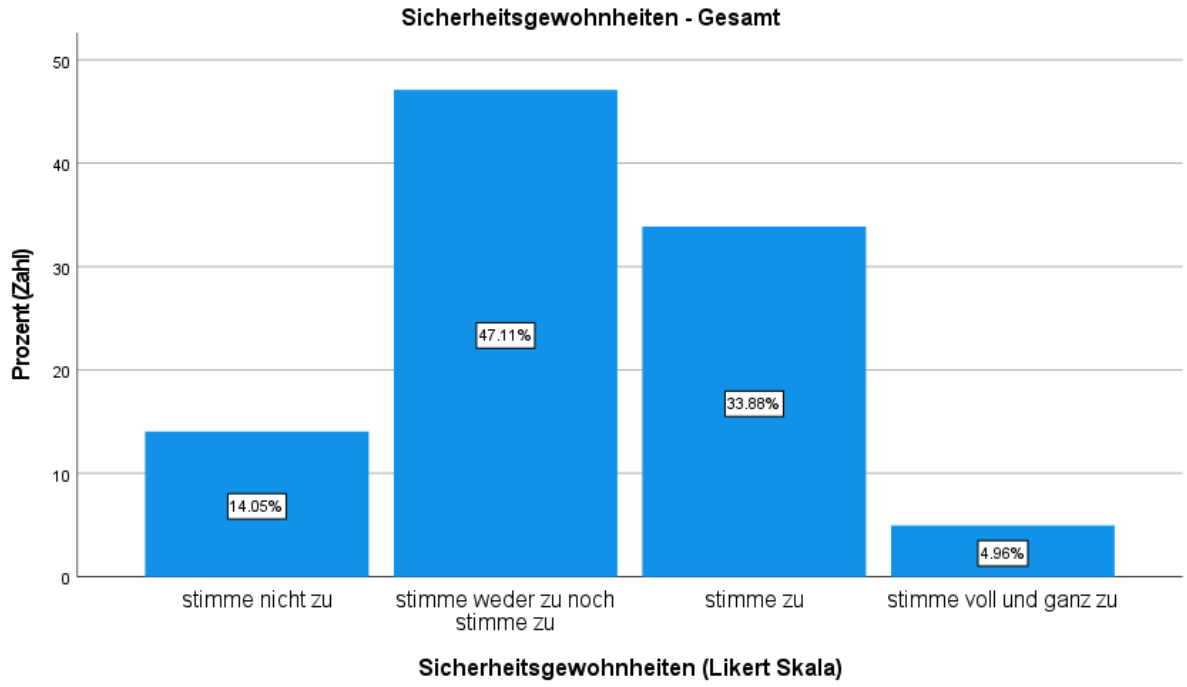



*Abbildung 8: Ergebnis - Sicherheitsgewohnheiten (Gesamt)*

### 3.2.3 Phishing Definition

| Phishing Vertrautheit - Phishing Definition | | | | |
|---|---|---|---|---|
| | Frequency | Percent | Valid Percent | Cumulative Percent |
| Eine Art von Social-Engineering-Angriff. | 115 | 95.0 | 95.0 | 95.0 |
| Eine Art bösartiges Programm. | 3 | 2.5 | 2.5 | 97.5 |
| Ein Virus. | 3 | 2.5 | 2.5 | 100.0 |
| Total | 121 | 100.0 | 100.0 | |

*Tabelle 2: Ergebnis - Phishing Definition*

Anhand der Tabelle 2 ist zu erkennen, dass 115 (95%) von 121 Teilnehmer und Teilnehmerinnen bei der Definitionsfrage (siehe Abbildung 46) die richtige Auswahl getroffen: „Eine Art von Social-Engineering-Angriff". Nur sechs Personen (5%) haben das Falsche angekreuzt: „Eine Art bösartiges Programm" bzw. „Ein Virus". In der Studie von Esmat et al. (2021) wurde die Definitionsfrage von 80,1% der Teilnehmer und Teilnehmerinnen (insgesamt 271 Personen) richtig beantwortet (Esmat, Alharbi and Karrar, 2021, p. 793). In der Studie von Manoharan et al. (2021) haben hingegen nur 20,2% der Teilnehmer und Teilnehmerinnen (insgesamt 368 Personen) diese Frage richtig beantworten können (Manoharan *et al.*, 2021, p. 15). Es ist somit zu erkennen, dass die meisten Teilnehmer und Teilnehmerinnen der Umfrage, die in einem österreichischen Großunternehmen arbeiten oder gearbeitet haben, mit dem Begriff „Phishing" vertraut sind. Im Folgenden werden auf die Ergebnisse der Phishing Anfälligkeit in Bezug auf die richtige Erkennung von E-Mails näher eingegangen.

### 3.2.4 Phishing Anfälligkeit – E-Mail

Das erste Beispiel (siehe Abbildung 49) stellt eine Phishing-E-Mail der „Unicredit Bank Austria AG" dar. In dieser E-Mail kann anhand des Absenders oder der Absenderin erkannt werden, dass diese E-Mail ein Phishing-E-Mail darstellt. Denn die Adresse („results@kenmbarnes") kann nicht von der „Unicredit Bank Austria AG" stammen. Des Weiteren sind einige Rechtschreibfehler in dieser E-Mail enthalten. Zusätzlich hat der Angreifer oder die Angreiferin versucht mit den psychologischen Merkmalen: „Furcht und „Autorität" die Empfänger und Empfängerinnen zu beeinflussen, damit sie auf den Link („Öffne die App jetzt") klicken. Die Teilnehmer und Teilnehmerinnen des Fragebogens haben bei diesem Beispiel erkannt, dass es sich um eine Phishing-E-Mail handelt, denn es haben 115 Personen (95%) diese Frage richtig beantwortet (siehe Abbildung 9). Fünf Personen (4,1%) jedoch haben die Option: „Ich weiß es nicht." ausgewählt und eine Person (0,8%) hat diese E-Mail als legitim eingestuft.

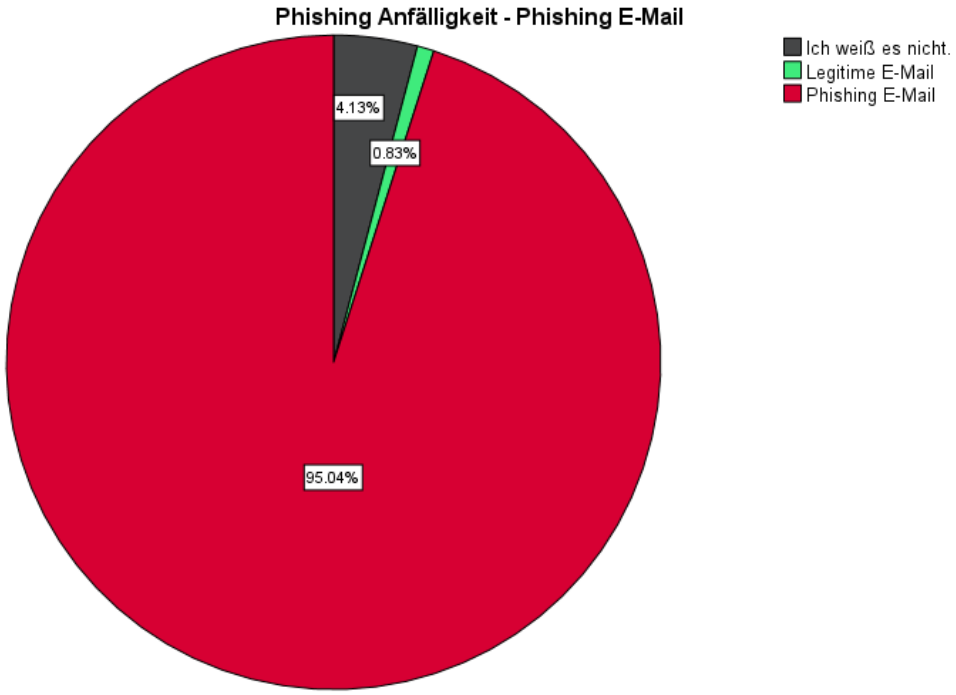



*Abbildung 9: Ergebnis - UniCredit Bank Austria AG (Phishing-E-Mail)*

Das zweite Beispiel (siehe Abbildung 50) stellt tatsächlich eine legitime E-Mail der „Austrian Airlines AG" dar. Jedoch ist die Absender. bzw. Absenderinnenadresse irreführend, weil diese von der „Lufthansa Group" stammt und nicht von der „Austrian Airlines AG". Ohne Hintergrundwissen ist dieses Beispiel schwer zu erkennen, denn die Lufthansa Group beinhaltet folgende Unternehmen: „Deutsche Lufthansa AG", „Austrian Airlines AG" und „Swiss International Air Lines AG" (*Lufthansa Group*, 2022). Des Weiteren war es nicht möglich sich den Link hinter dem Button „Passwort ändern" genauer anzusehen und somit fällt eine Möglichkeit zur Erkennung der E-Mail weg. Tatsächlich haben 45 Personen (37,2%) bei dieser E-Mail die Option „Legitime E-Mail" gewählt und somit richtig beantwortet (siehe Abbildung 10). 55 Personen (45,5%) hingegeben haben diese E-Mail als eine Phishing-E-Mail wahrgenommen und 21 Personen (17,4%) haben die Auswahl „Ich weiß es nicht." gewählt.

Das nächste Beispiel (Abbildung 51) stellt eine klassische Phishing-E-Mail dar. Es werden den Empfänger und Empfängerinnen Gewinne versprochen und die Absender- bzw. Absenderinnenadresse stammt eindeutig nicht von „Media Markt". 113 Teilnehmer und Teilnehmerinnen (93,4%) haben diese E-Mail als Phishing-E-Mail erkannt (siehe Abbildung 11). Jedoch haben fünf Personen (4,1%) diese E-Mail als legitim eingestuft und drei Personen (2,5%) haben die Option „Ich weiß es nicht." ausgewählt und liegen somit falsch in ihrer Aussage. Dennoch kann wie in der Studie von Tornblad et al. (2021) bestätigt werden, dass die Empfänger und Empfängerinnen von Phishing-E-Mails mit

Gewinnversprechen oder hohen Gewinnbeträgen eher misstrauisch gegenüberstehen (Tornblad, Armstrong, *et al.*, 2021, p. 363).

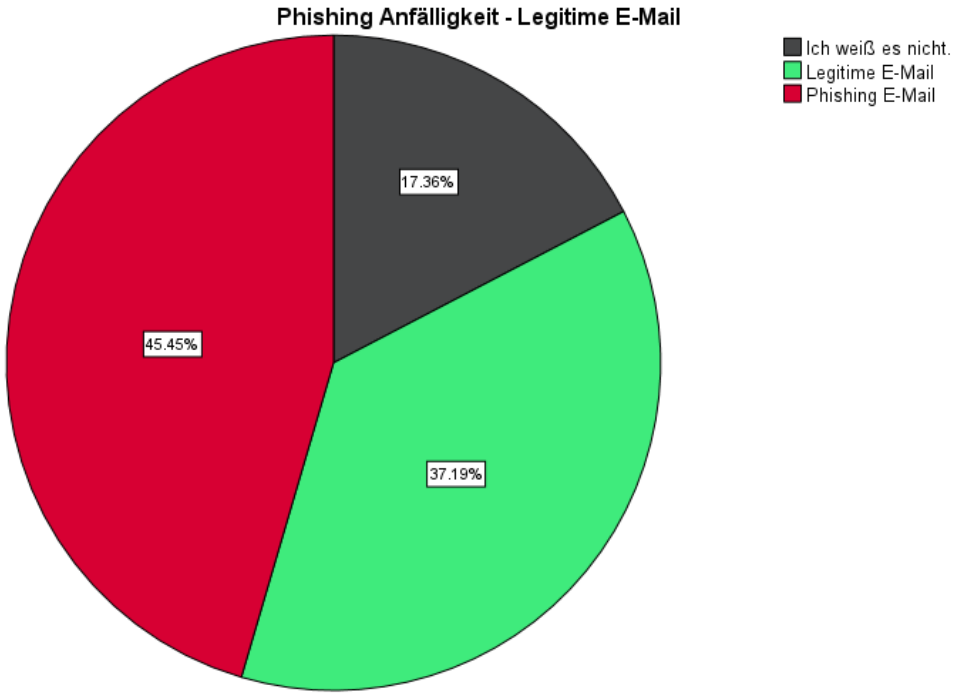



*Abbildung 10: Ergebnis - Austrian Airlines AG (Legitime E-Mail)*

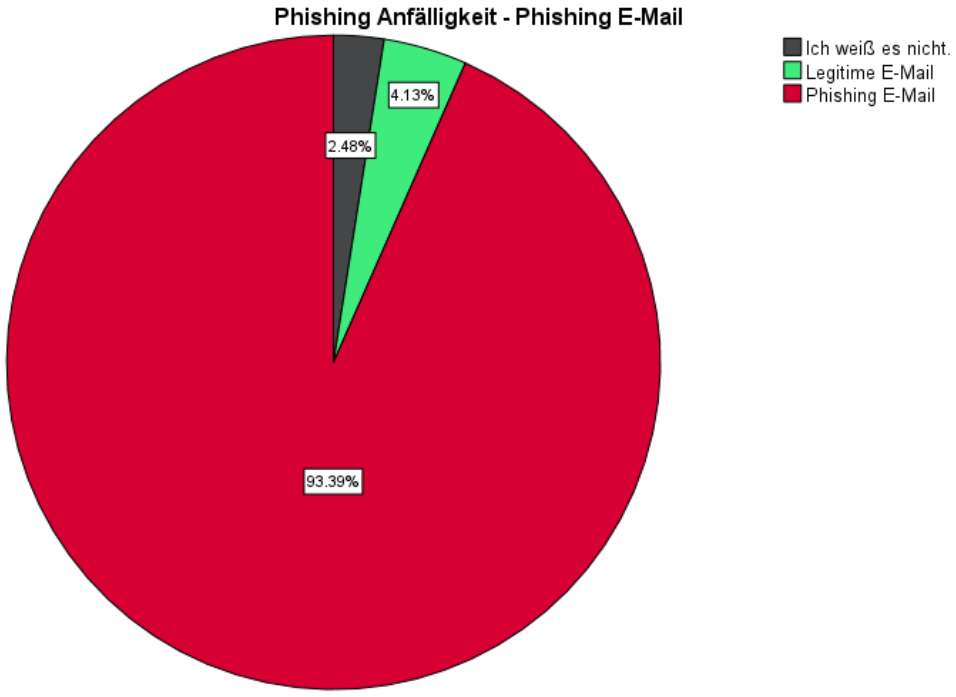



*Abbildung 11: Ergebnis - Media Markt (Phishing-E-Mail)*

Das Beispiel (siehe Abbildung 52) von „Amazon“ stellt eine Phishing-E-Mail dar. Jedoch ist diese anhand der Absender- bzw. Absenderinnenadresse schwer zu erkennen. Wie bereits im Beispiel von Austrian Airlines AG ist auch hier nicht möglich den Link hinter dem Text „können Sie dies einfach hier“ zu erkennen. Wenn eine Person nicht mit der

Versandbestätigung von Amazon vertraut ist, ist es tatsächlich schwer diese E-Mail als eine Phishing-E-Mail zu identifizieren. Diese E-Mail stellt eine fast identische Kopie einer legitimen Versandbestätigung von Amazon dar. Die legitime Version beinhaltet jedoch die Versandadresse des Kunden oder der Kundin und eine Artikelbeschreibung (*Amazon - Phishing*, 2019). Diese Punkte fehlen in dieser Phishing-E-Mail. Des Weiteren ist ein kleiner Rechtschreibfehler in dieser E-Mail enthalten und ist nur erkennbar, wenn die E-Mail aufmerksam gelesen wird. Denn es steht Folgendes geschrieben: „Möchten Sie einen ansehen Ihrer Bestellung, können Sie dies einfach hier". Es haben nur neun Personen (7,4%) diese E-Mail als einen Phishing-Angriff erkannt (siehe Abbildung 12). 104 Teilnehmer und Teilnehmerinnen (86%) haben dieses Beispiel als legitim wahrgenommen und acht Personen (6,6%) haben die Auswahl „Ich weiß es nicht." genutzt.

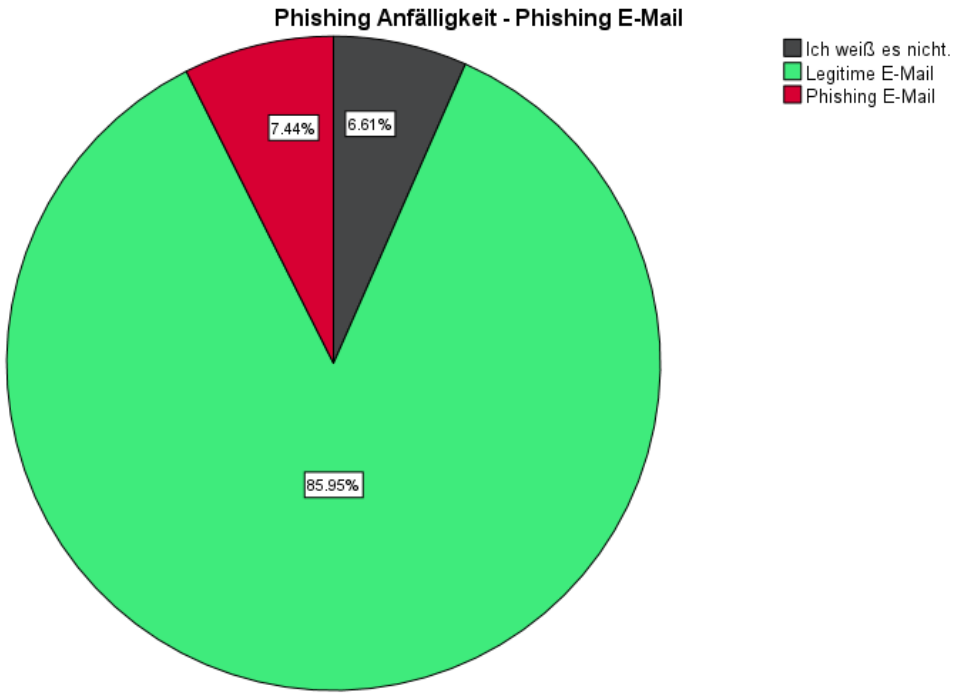



*Abbildung 12: Ergebnis - Amazon (Phishing-E-Mail)*

Die nächste E-Mail stellt ein legitimes Beispiel von „Wiener Linien" dar (siehe Abbildung 53), denn die Absender- bzw. Absenderinnenadresse stimmt mit „Wiener Linien" überein und es sind keine psychologischen Merkmale wie z.B. Furcht, Autorität oder Dringlichkeit, vorhanden. 108 Personen (89,3%) haben dieses Beispiel als eine legitime E-Mail erkannt (siehe Abbildung 13). Sechs Personen (5%) haben bei diesem Beispiel die Auswahl: „Phishing-E-Mail" gewählt und sieben Personen (5,8%) haben auf „Ich weiß es nicht." geklickt.

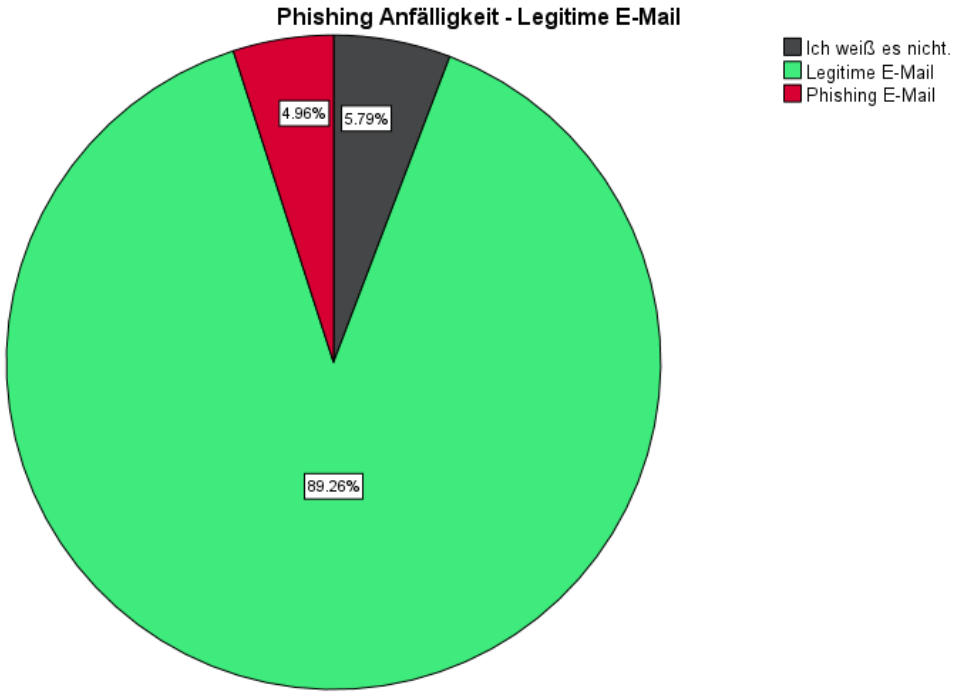



*Abbildung 13: Ergebnis - Wiener Linien (Legitime E-Mail)*

Das nächste Beispiel (siehe Abbildung 54) ist eine E-Mail von „Netflix“ und stellt einen Phishing-Angriff dar. Jedoch ist auch hier schwer zu erkennen, ob es sich um eine legitime oder bösartige E-Mail handelt, denn die E-Mail-Adresse könnte womöglich von „Netflix“ stammen. Dennoch ist die Absender- bzw. Absenderinnenadresse nicht bei „Netflix“ hinterlegt. Diese E-Mail wurde auch nicht korrekt verfasst, denn es wurde Folgendes geschrieben: „Besuche den Hilfecenter …“, dabei handelt es sich um einen kleinen Rechtschreibfehler. Dieser ist nur erkennbar, wenn die E-Mail aufmerksam gelesen wird. Es war auch in diesem Beispiel nicht möglich den Link hinter dem Button „Jetzt Konto aktualisieren“ anzuklicken, um zu sehen wohin dieser Link tatsächlich führt. Jedoch haben 50 Teilnehmer und Teilnehmerinnen (41,3%) diese E-Mail korrekt als eine Phishing-E-Mail identifiziert (siehe Abbildung 14). 46 Personen (38%) haben dieses Beispiel als legitim gekennzeichnet und 25 Personen (20,7%) haben die Wahl „Ich weiß es nicht.“ getroffen.

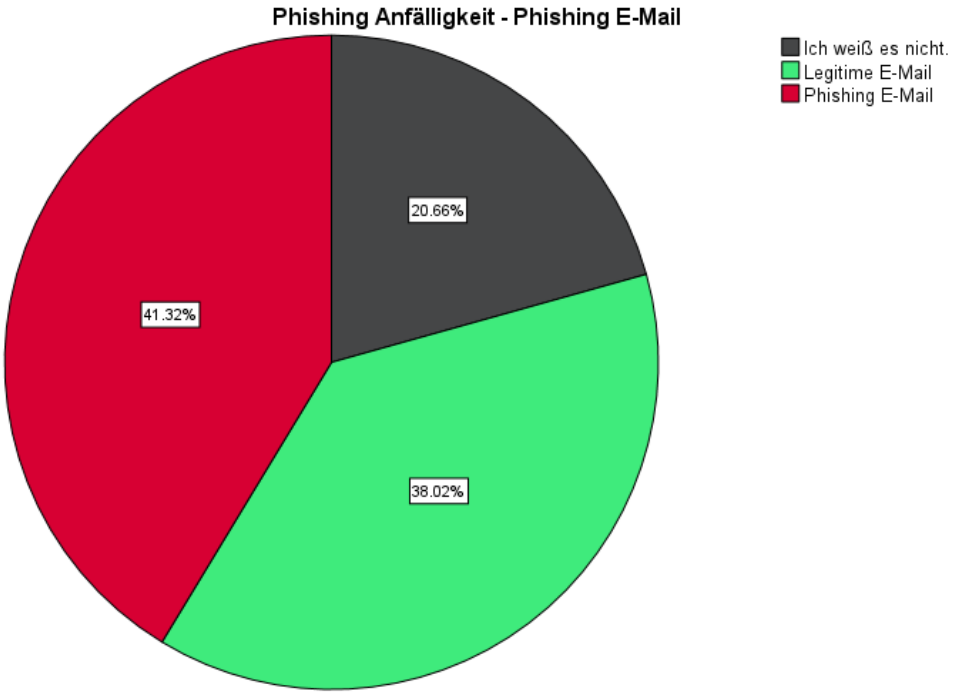



*Abbildung 14: Ergebnis - Netflix (Phishing-E-Mail)*

Bei den nächsten zwei Beispielen (siehe Abbildung 55 und Abbildung 56) handelt es sich um legitime Beispiele. Die Abbildung 55 stellt eine E-Mail von „Lieferando“ dar. Jedoch ist die genaue Absender- bzw. Absenderinnenadresse nicht erkennbar und die Adresse für die „Antwort an“ stellt eine dubiose E-Mail-Adresse dar. Es ist hier ebenfalls nicht möglich gewesen, den genauen Link hinter dem Button „Hol dir deinen Gutschein“ einzusehen. Diese Umstände haben sich auch in den Ergebnissen bemerkbar gemacht (siehe Abbildung 15), denn 40 Personen (33,1%) haben dieses Beispiel als eine Phishing-E-Mail wahrgenommen. 28 Personen (23,1%) haben die Option „Ich weiß es nicht.“ gewählt. 53 Personen (43,8%) haben die richtige Option gewählt.

Die Abbildung 56 stellt eine legitime E-Mail von „FinanzOnline“ dar. Hier konnten Teilnehmer und Teilnehmerinnen des Fragebogens erkennen, dass es sich bei der Absender- bzw. Absenderinnenadresse um eine korrekte E-Mail-Adresse handelt, denn diese stimmt mit „FinanzOnline“ überein. Die Ergebnisse zeigen, dass der größte Teil der Teilnehmer und Teilnehmerinnen (96 Personen – 79,3%) dieses Beispiel korrekt als eine legitime E-Mail identifizieren konnten (siehe Abbildung 16). 15 Personen (12,4%) haben die falsche Wahl getroffen und zehn Personen (8,3%) haben die Option „Ich weiß es nicht.“ ausgewählt.

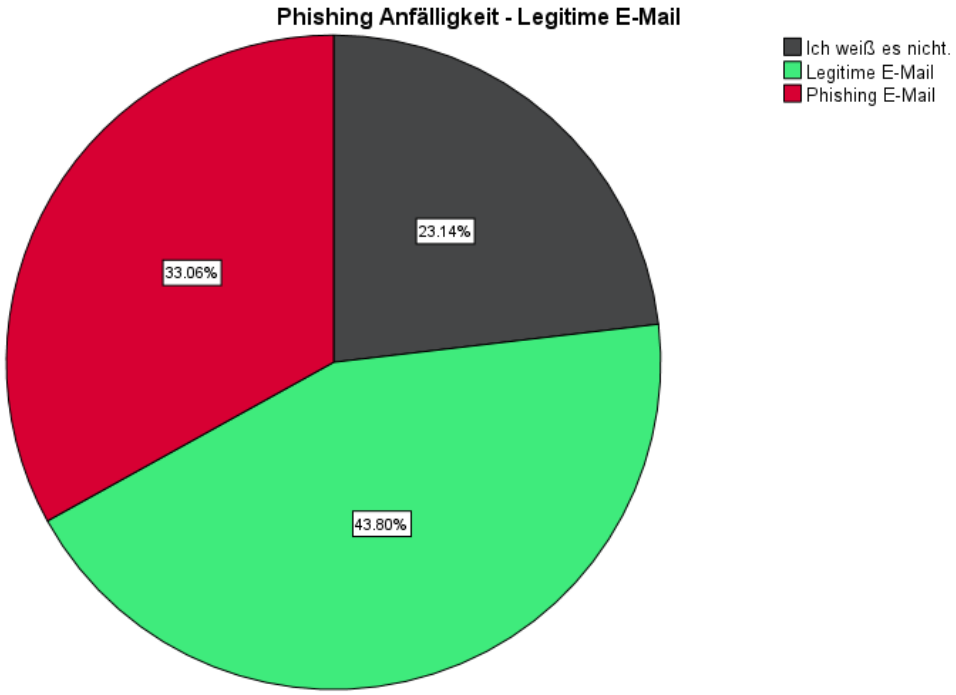



*Abbildung 15: Ergebnis - Lieferando (Legitime E-Mail)*

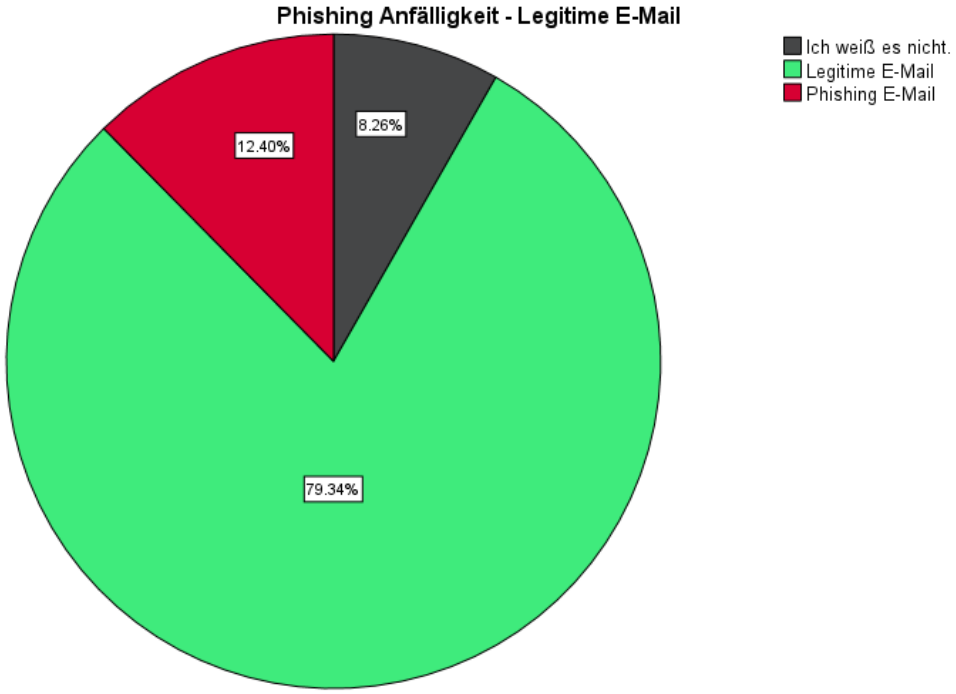



*Abbildung 16: Ergebnis - FinanzOnline (Legitime E-Mail)*

Die Abbildung 57 bildet eine Phishing-E-Mail zu „Paypal“ ab. Anhand der Absender- bzw. Absenderinnenadresse ist diese E-Mail schwer als Phishing zu identifizieren, denn sie ähnelt der richtigen E-Mail-Adresse: „service@intl.paypal.com“ und nur erfahrene Nutzer und Nutzerinnen sind in der Lage dies zu erkennen (*PayPal - Phishing*, 2020). Des Weiteren wurde keine persönliche Anrede angeführt und es ist eine Unstimmigkeit vorhanden, denn der Button („Responsive PayPal-Konto“) ist in englischer Sprache

angeführt. Die E-Mail wurde auch nicht korrekt übersetzt, denn weiter unten steht „Hilfe“, „Kontakt“ und „Gebühren“ auf Deutsch und „Application“ und „Security“ auf Englisch (Redaktionsteam, 2020b). Diese Merkmale fallen Leser und Leserinnen jedoch nur auf, wenn die E-Mail genauer durchgelesen wird. Diese Erkenntnis hat sich auch in dem Ergebnis widergespiegelt (siehe Abbildung 17). Es haben 43 Personen (35,5%) dieses Beispiel korrekt als eine Phishing-E-Mail erkennen können. 42 Personen (34,7%) hingegen haben diese E-Mail als legitim eingestuft. 36 Personen (29,8%) waren sich nicht sicher und haben die Option „Ich weiß es nicht.“ gewählt.

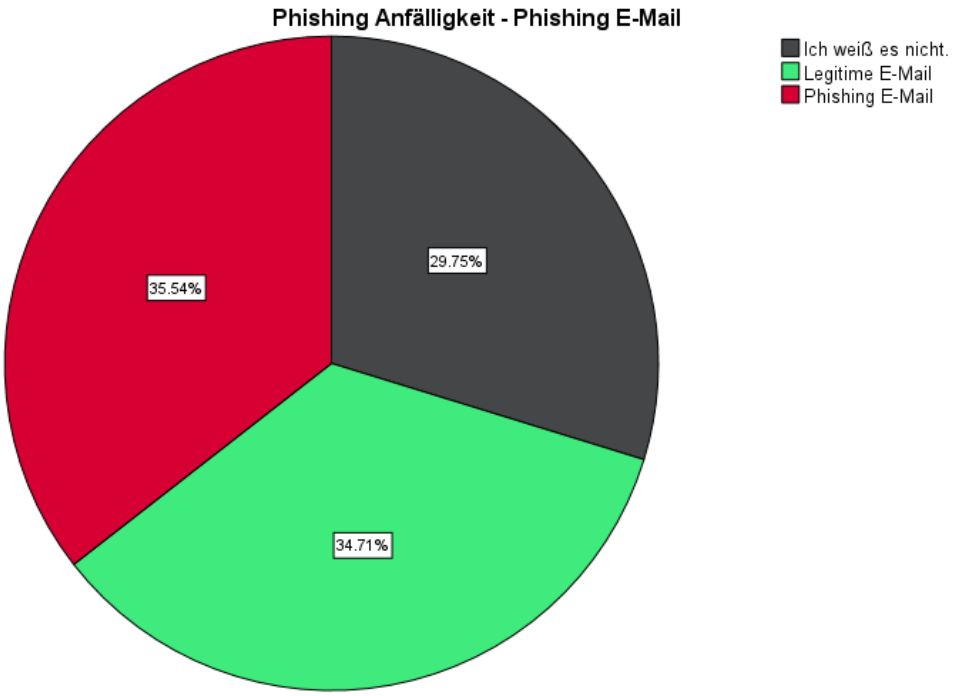



*Abbildung 17: Ergebnis - PayPal (Phishing-E-Mail)*

Das letzte Beispiel stellt auch eine Phishing-E-Mail von der „Österreichischen Post AG“ dar (siehe Abbildung 58). Dieses Beispiel war auch schwer als eine Phishing-E-Mail zu identifizieren, weil die Absender- bzw. Absenderinnenadresse legitim aussieht. Es war auch hier nicht möglich den Link genauer zu betrachten, denn hinter diesem Link ist eine französische URL hinterlegt. In dieser E-Mail wurde von den Angreifer und Angreiferinnen der Dringlichkeitshinweis (Bitte zahlen Sie die Versandkosten für die Lieferung morgen) verwendet, damit Empfänger und Empfängerinnen auf den Link klicken. Es haben 53 Personen (43,8%) dieses Beispiel korrekt als Phishing-E-Mail identifizieren können (siehe Abbildung 18). 48 Personen (39,7%) haben dieses Beispiel als legitim wahrgenommen und 20 Personen (16,5%) haben die Option „Ich weiß es nicht.“ gewählt.

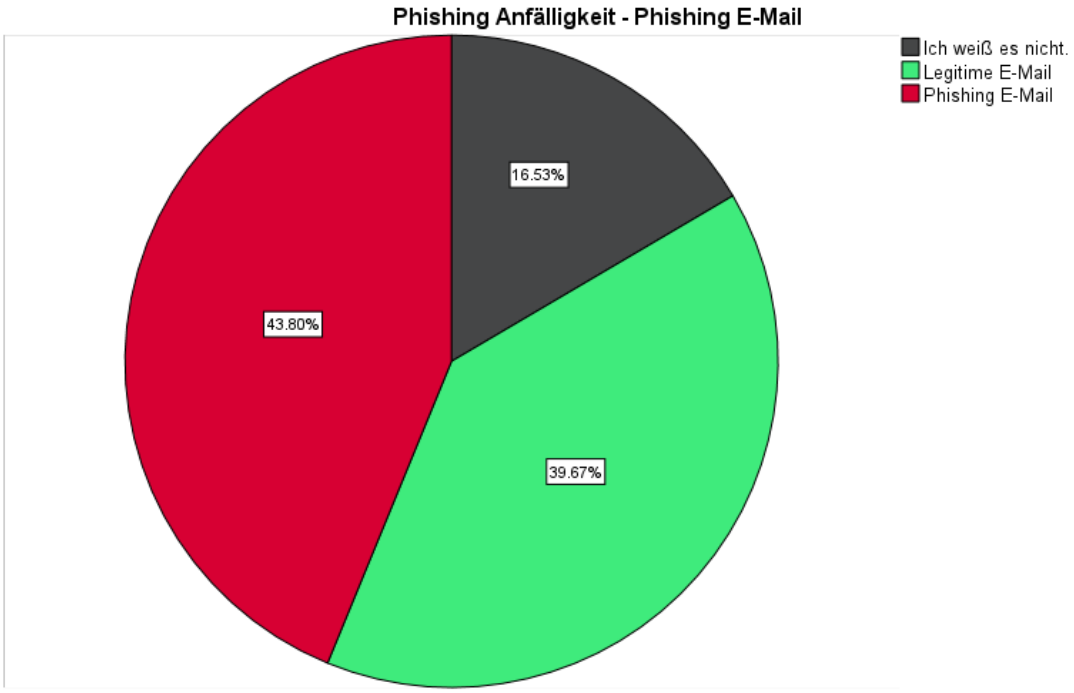



*Abbildung 18: Ergebnis - Österreichische Post AG (Phishing-E-Mail)*

Die Abbildung 19 stellt die Phishing Anfälligkeit in Bezug auf die Phishing Anfälligkeit anhand des Geschlechts dar. Es bestand die Möglichkeit insgesamt zehn Punkte zu erhalten, wenn die zehn vorgestellten E-Mails richtig erkannt wurden. In dieser Grafik ist zu erkennen, dass die Frauen bei der Erkennung von E-Mails ein wenig besser abgeschnitten haben als die Männer. Denn zwei Frauen haben jeweils neun bzw. zehn Punkte von den insgesamten zehn Punkten erreicht.

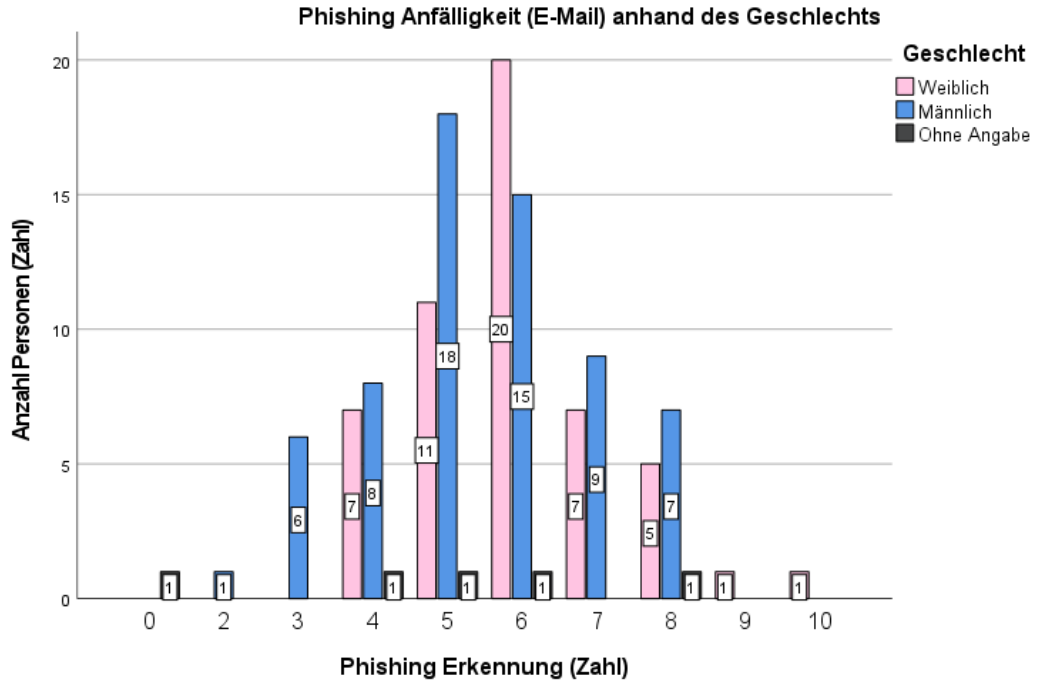



*Abbildung 19: Ergebnis - Phishing Anfälligkeit (E-Mail) anhand des Geschlechts*

Die Abbildung 20 zeigt die Phishing Anfälligkeit von E-Mails in Bezug auf eine Teilnahme einer Phishing Schulung. Eine Person, die eine Phishing Schulung erhalten hat, hat zehn von den möglichen zehn Punkten erhalten. Jedoch hat eine Person, die keine Phishing Schulung erhalten hat, neun Punkte erreicht bzw. neun E-Mails richtig erkannt. Deswegen ist aus der Grafik nicht ersichtlich, ob eine Teilnahme der Phishing Schulung tatsächlich dabei geholfen hat, mehr E-Mails richtig zu identifizieren.

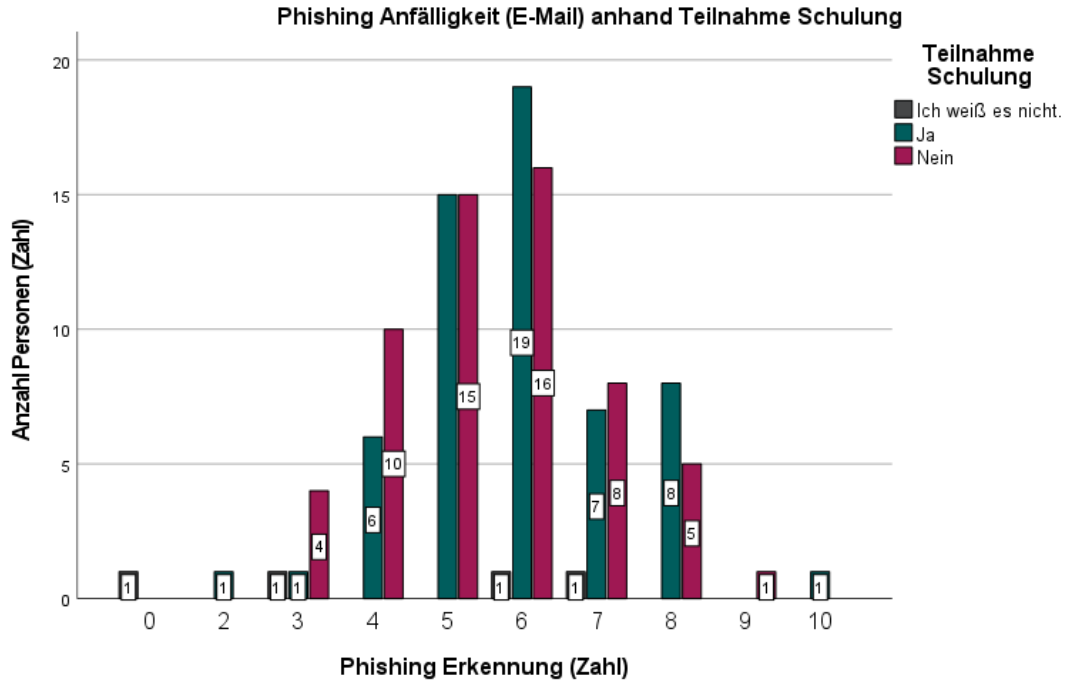



*Abbildung 20: Ergebnis - Phishing Anfälligkeit (E-Mail) anhand Teilnahme Schulung*

Beide Ergebnisse werden im Kapitel 3.3.2 näher analysiert. Im Folgenden werden auf die Ergebnisse der Phishing Anfälligkeit in Bezug auf die richtige Erkennung von URLs näher eingegangen.

### 3.2.5 Phishing Anfälligkeit – URL

Die zwei URLs „https://suppoort.apple.com/“ und „https://www.disney_plus.com/de-de/sign-up?type=standard“ sind klassische Fälle von falsch geschriebenen Domänenamen. Es ist nämlich sehr einfach, einen oder mehrere Buchstaben einer legitimen URL zu verfälschen (Purkait, Kumar De and Suar, 2014, p. 204). In diesen Beispielen wurde bei der ersten URL ein „o“ zu viel hinzugefügt und bei der zweiten URL wurde folgendes Symbol „_“ hinzugefügt. Anhand der Abbildung 21 ist zu erkennen, dass 62 Personen (51,2%) nicht aufgefallen ist, dass ein Buchstabe mehr hinzugefügt wurde. 44 Personen (36,4%) haben erkannt, dass es sich dabei um eine Phishing URL handelt. 15 Personen (12,4%) haben die Auswahl „Ich weiß es nicht.“ genutzt.

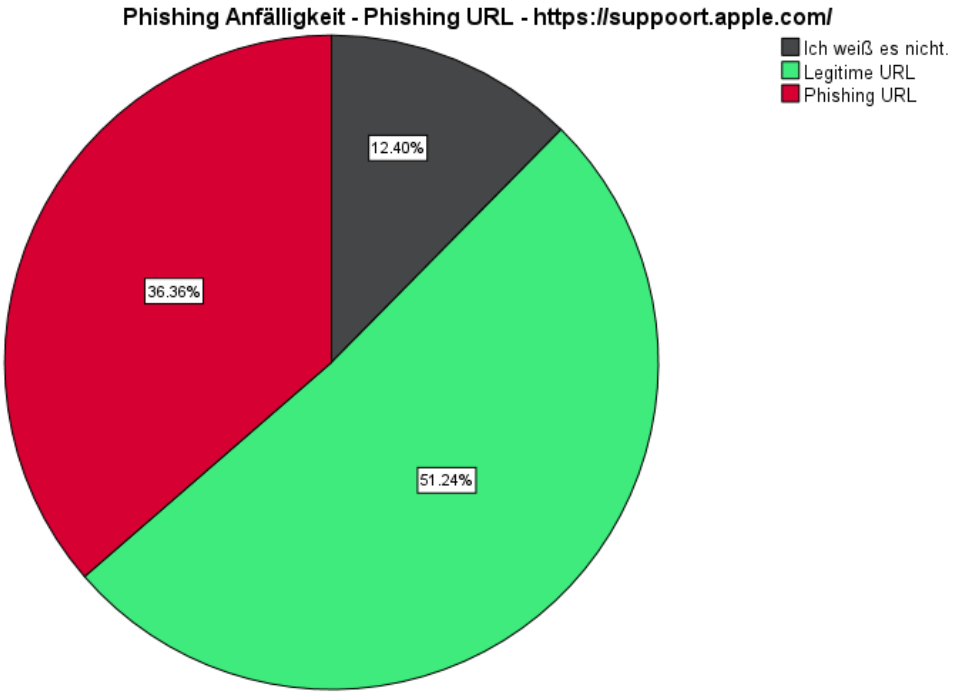



*Abbildung 21: Ergebnis - Phishing URL 1*

Bei der Abbildung 22 haben 41 Personen (33,9%) erkannt, dass es sich dabei um eine Phishing URL handelt. Jedoch haben jeweils 40 Personen (33,1%) dies entweder nicht erkannt oder die Option „Ich weiß es nicht." gewählt.

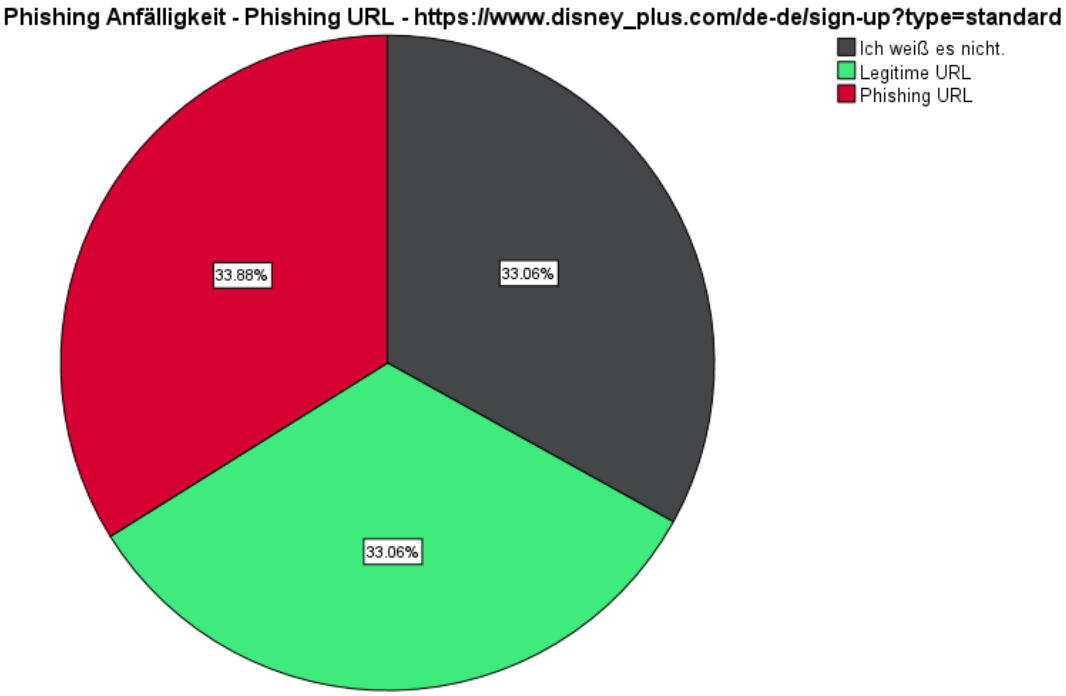



*Abbildung 22: Ergebnis - Phishing URL 2*

Wenn eine URL eine IP-Adresse nutzt wie in diesem Beispiel: „https://147.46.236.55/PayPal/login.html", ist davon auszugehen, dass es sich dabei um eine Phishing URL handelt (Arachchilage, Love and Beznosov, 2016, p. 188). Mehr als die

Hälfte der Teilnehmer und Teilnehmerinnen des Fragebogens haben dies erkannt (siehe Abbildung 23). 81 Personen (66,9%) haben somit die richtige Wahl getroffen. Sieben Personen (5,8%) hingegen haben dies nicht erkannt und haben diese URL als legitim eingestuft. 33 Personen (27,3%) konnten es auch nicht erkennen oder hatten dieses Wissen nicht, denn sie haben die Option „Ich weiß es nicht." genutzt.

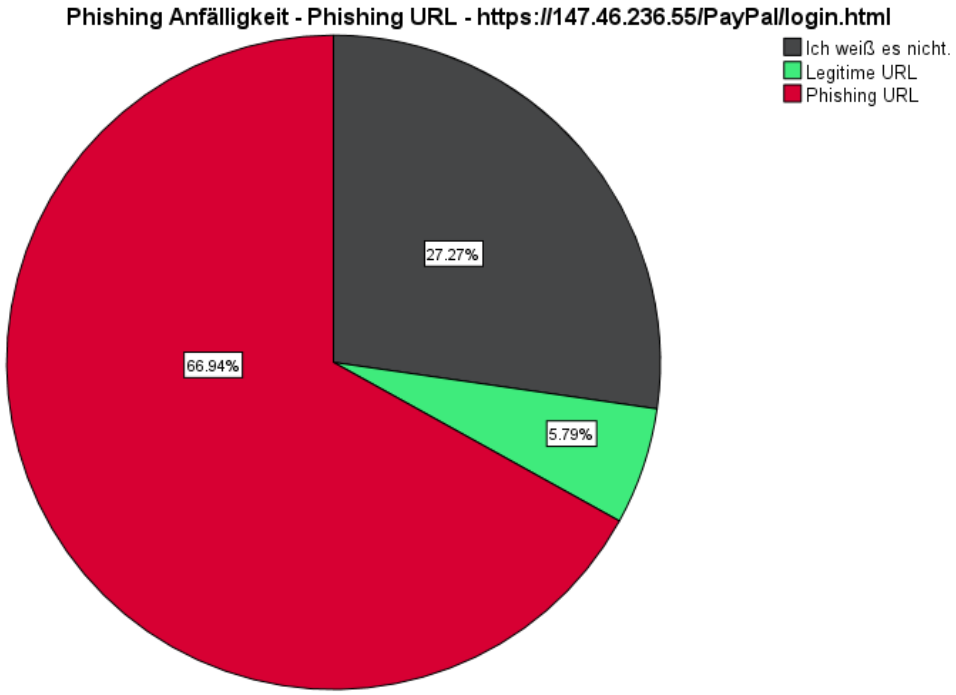



*Abbildung 23: Ergebnis - Phishing URL 3*

Die nächsten zwei URLs wurden aus dem Artikel von Arachchilage et al. (2015) entnommen und stellen Phishing URLs dar. Bei der ersten URL: „https://www.msn-verify.com/", haben die Autoren und Autorinnen erwähnt, dass eine URL mit Firmennamen gefolgt von einem Bindestrich sich in der Regel um eine Phishing URL handelt. Bei der zweiten URL: „https://www.ebay-security.com", ist von den Autoren und Autorinnen zu entnehmen, dass Unternehmen keine sicherheitsrelevanten Schlüsselwörter in den Domänen verwenden (Arachchilage, Love and Beznosov, 2016, p. 188). In der Abbildung 24 ist zu erkennen, dass nur 23 Personen (19%) die Phishing URL: „https://www.msn-verify.com/" richtig erkannt haben. 53 Personen (43,8%) haben diese URL als legitim wahrgenommen und 45 Personen (37,2%) haben die Option „Ich weiß es nicht." genutzt. In der Abbildung 25 haben 24 Personen (19,8%) die Phishing URL: „https://www.ebay-security.com" erkennen können. 58 Personen (47,9%) haben hingegen die ULR als legitim eingestuft und 39 Personen (32.2%) haben die Option „Ich weiß es nicht." gewählt.

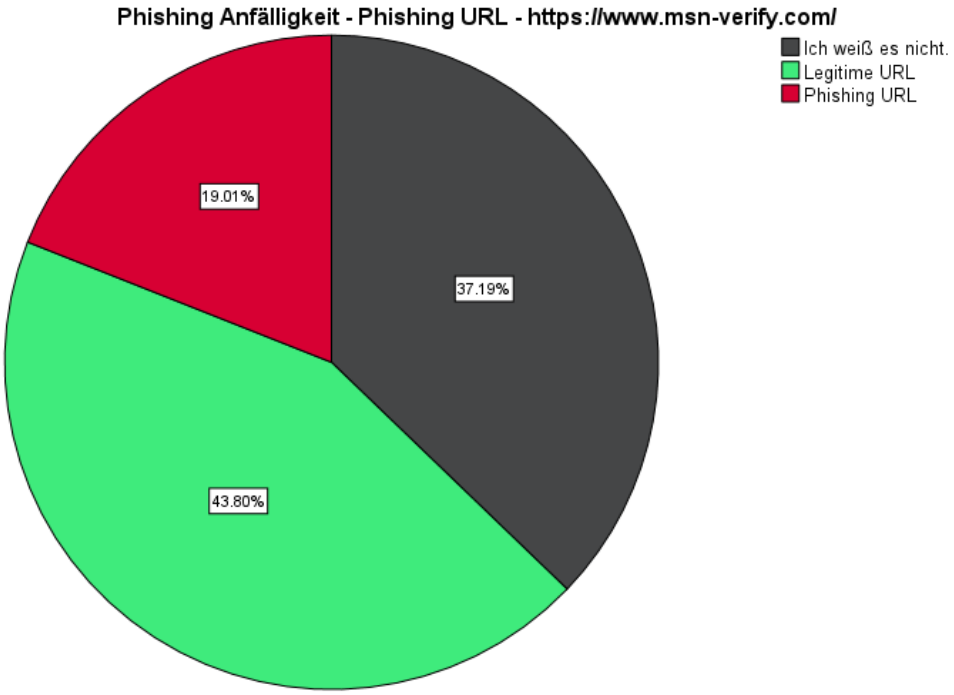



*Abbildung 24: Ergebnis - Phishing URL 4*

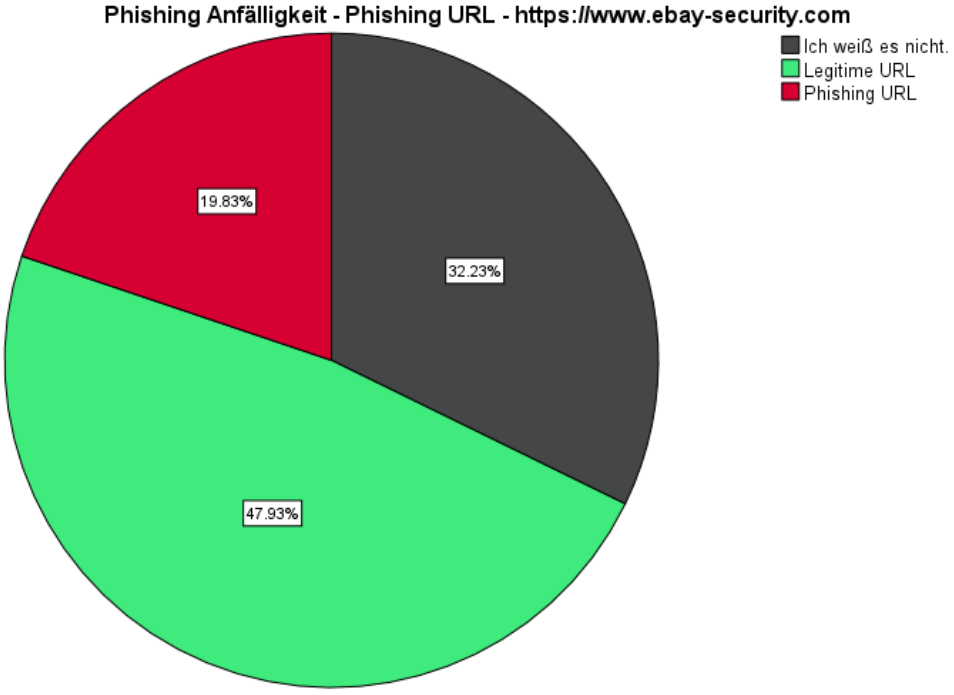



*Abbildung 25: Ergebnis - Phishing URL 5*

Bei den nächsten fünf URLs handelt es sich um legitime URLs und es ist anhand der Grafiken sichtbar, dass mehr als die Hälfte der Teilnehmer und Teilnehmerinnen die richtige Wahl getroffen haben, indem sie die URLs als legitim identifizieren konnten.

Die Abbildung 26 zeigt, dass 98 Personen (81%) die URL von „YouTube“: „https://www.youtube.com/results?search_query=orf“, als legitim erkennen konnten.

Sechs Personen (5%) hingegen haben die URL als Phishing URL wahrgenommen. 17 Personen (14%) haben die Option „Ich weiß es nicht." genutzt.

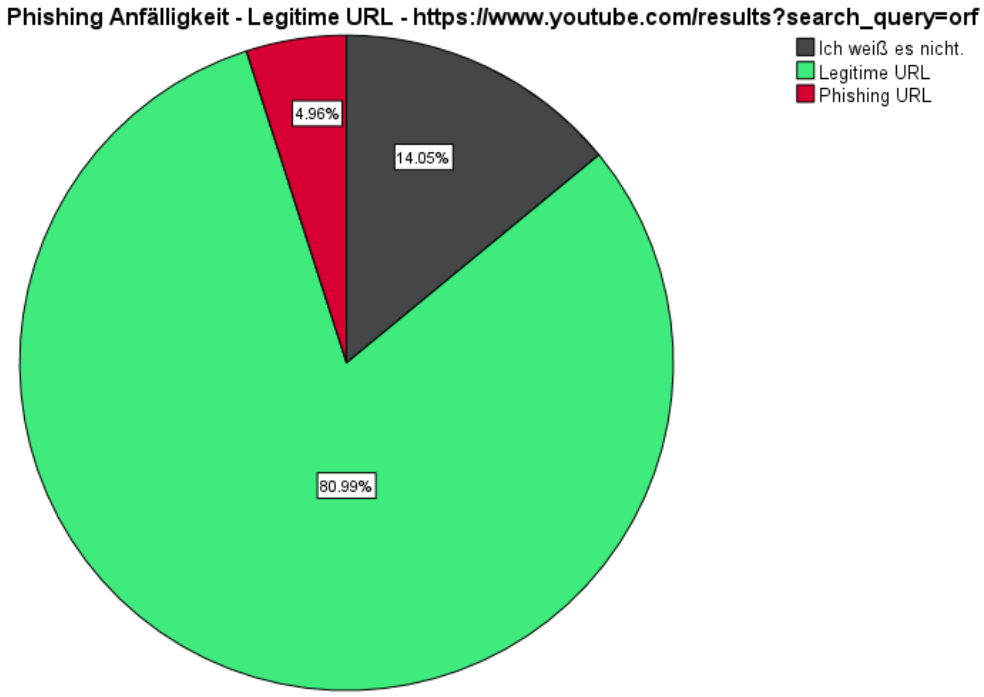



*Abbildung 26: Ergebnis - Legitime URL 1*

Die Abbildung 27 bildet eine URL von „Amazon" ab: „https://www.amazon.de/gp/help/customer/display.html?nodeId=508510&ref_=nav_cs_help". Hier haben 79 Personen (65,3%) richtig geantwortet mit: „Legitime URL". Zehn Personen (8,3%) haben jedoch die falsche Antwortmöglichkeit gewählt: „Phishing URL" und 32 Personen (26,4%) haben die Wahl „Ich weiß es nicht." getroffen.

Bei der Abbildung 28 handelt es sich um eine legitime URL von „Google": „https://www.google.at/?gws_rd=ssl" und dies wurde von 68 Teilnehmer und Teilnehmerinnen (56,2%) des Fragebogens erkannt. Zwölf Teilnehmer und Teilnehmerinnen (9,9%) haben diese URL als Phishing eingestuft und 41 Personen (33,9%) haben die Option „Ich weiß es nicht." gewählt.

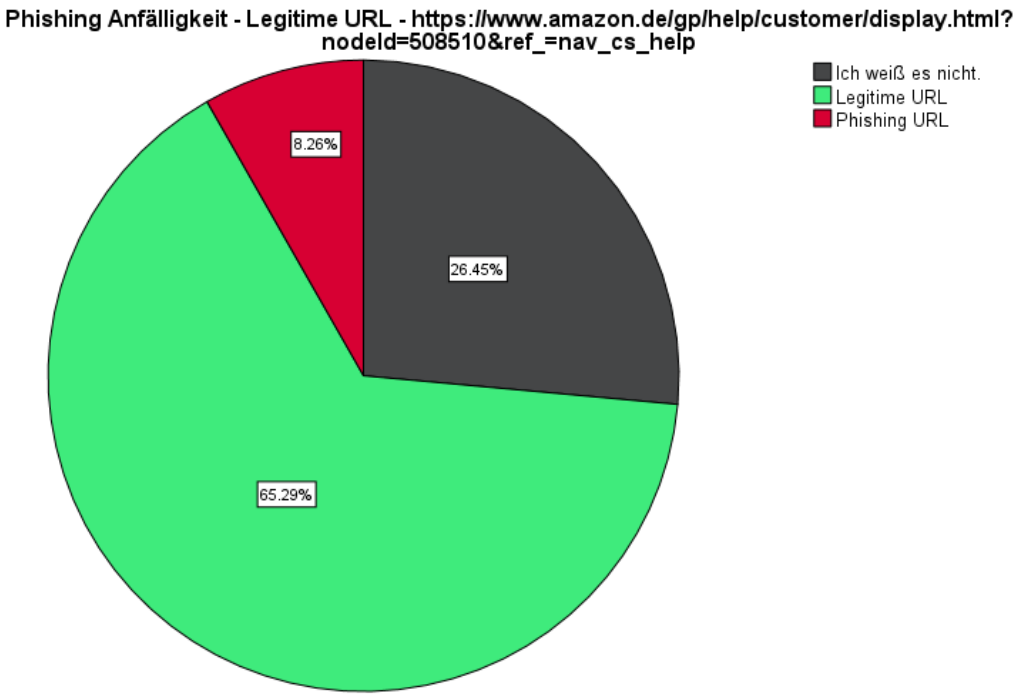



*Abbildung 27: Ergebnis - Legitime URL 2*

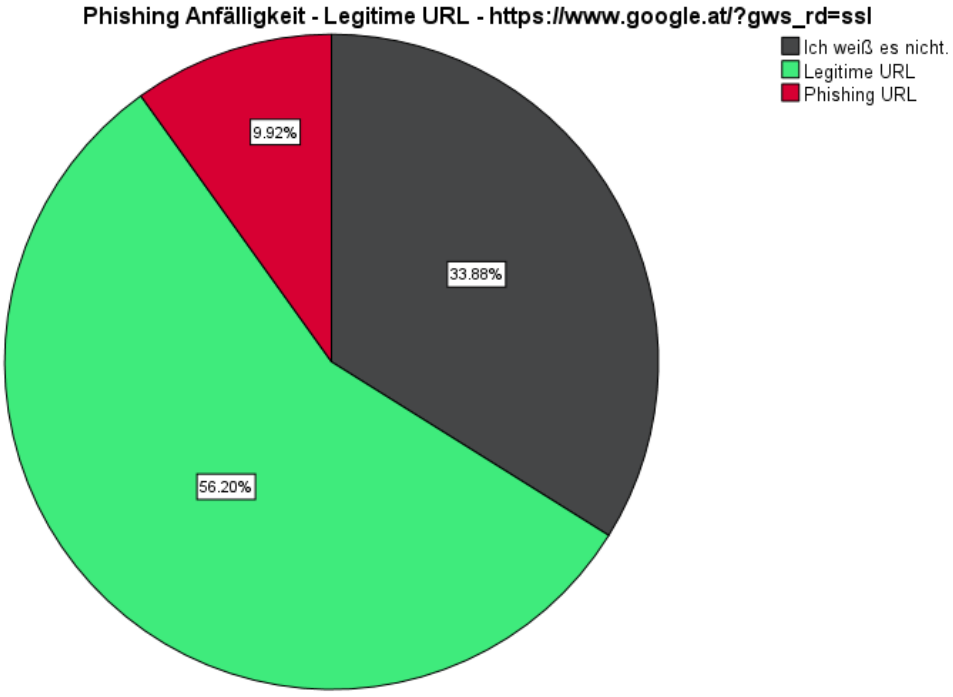



*Abbildung 28: Ergebnis - Legitime URL 3*

Die Abbildung 29 zeigt eine legitime URL von „Facebook“: „https://www.facebook.com/help/1434403039959381/?helpref=hc_fnav“. Es haben 67 Teilnehmer (55,4%) und Teilnehmerinnen diese URL legitim eingestuft und lagen somit richtig in ihrer Wahl. 16 Personen (13,2%) hingegen haben diese URL als Phishing eingestuft und 38 Personen (31,4%) haben die Option „Ich weiß es nicht.“ ausgewählt.

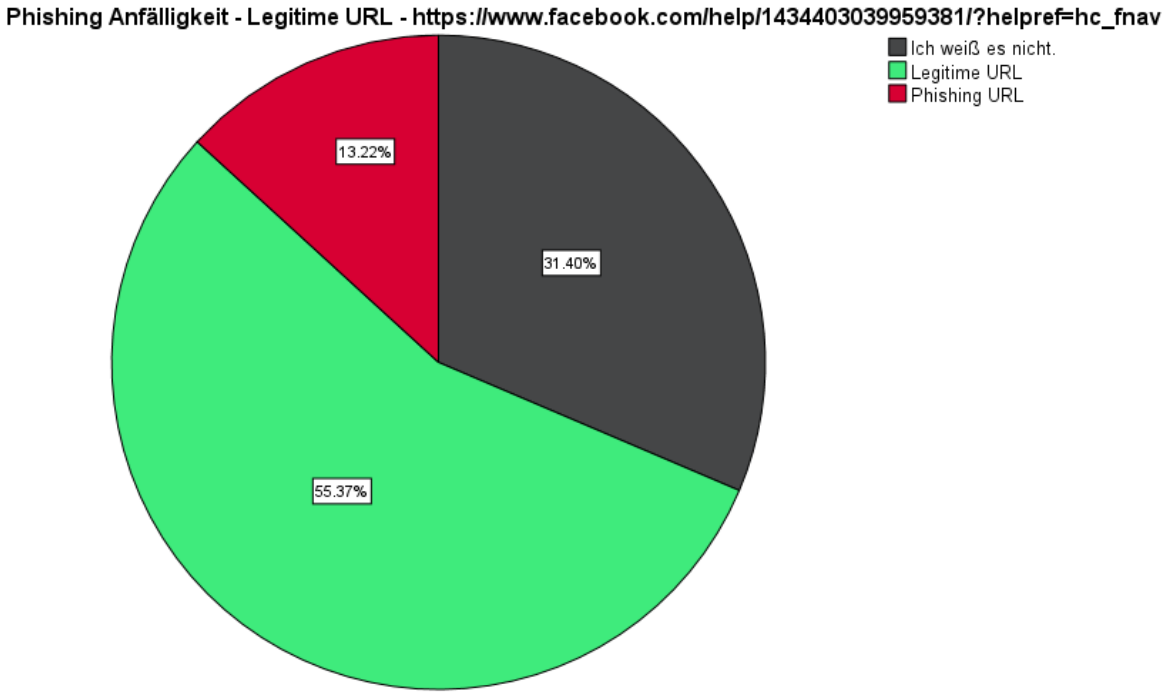



*Abbildung 29: Ergebnis - Legitime URL 4*

Die Abbildung 30 zeigt das letzte URL-Beispiel, welches von „Netflix“ stammt: „https://www.netflix.com/at/browse/genre/3652“. Hier haben 89 Personen (73,6%) erkannt, dass es sich hierbei um eine legitime URL handelt. Neun Personen (7,4%) jedoch haben die URL als Phishing URL wahrgenommen. 23 Personen (19%) haben die Option mit „Ich weiß es nicht.“ gewählt.

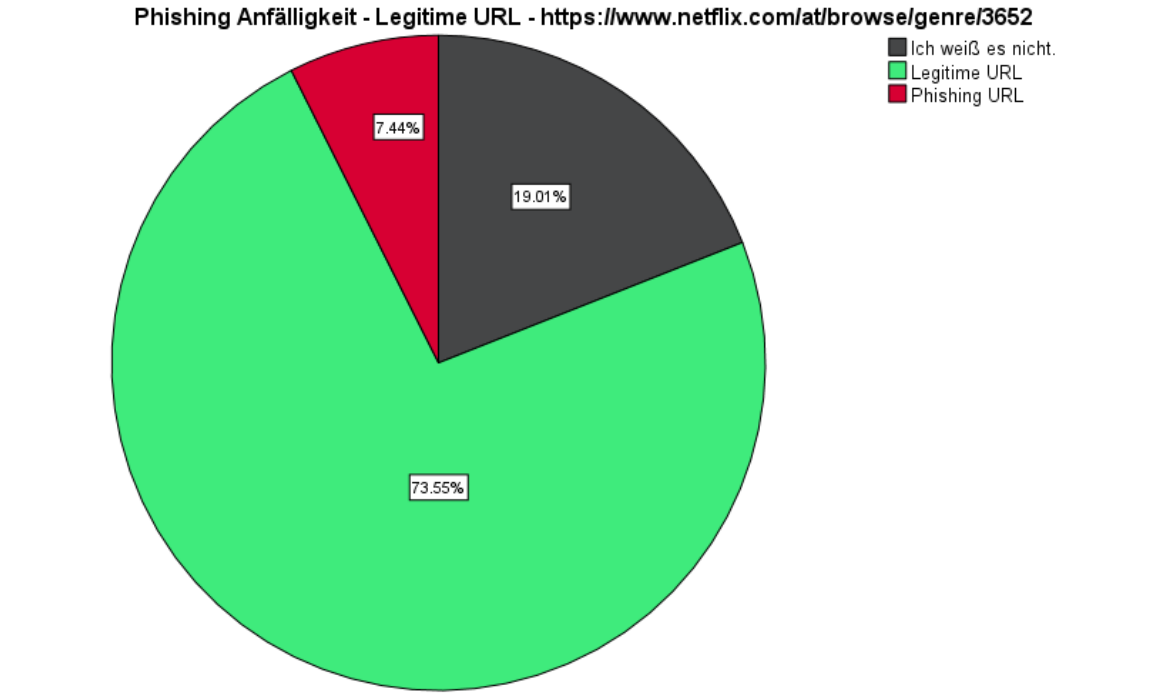



*Abbildung 30: Ergebnis - Legitime URL 5*

Die Abbildung 31 stellt die Phishing Anfälligkeit in Bezug auf die erkannten URLs anhand des Geschlechts dar. Wie bereits erwähnt bestand auch hier die Möglichkeit insgesamt zehn Punkte zu erhalten, wenn die zehn vorgestellten URLs richtig identifiziert wurden. Bei der Erkennung von E-Mails haben die Frauen besser abgeschnitten als die Männer. Jedoch ist zu erkennen, dass die Männer bei der Erkennung von URLs ein wenig besser abgeschnitten haben als die Frauen. Denn drei Männer haben zehn Punkte von den insgesamten zehn Punkten erhalten und fünf Männer haben neun Punkte erzielt. Jedoch ist zu erwähnen, dass auch zwei Frauen zehn Punkte erreicht haben.

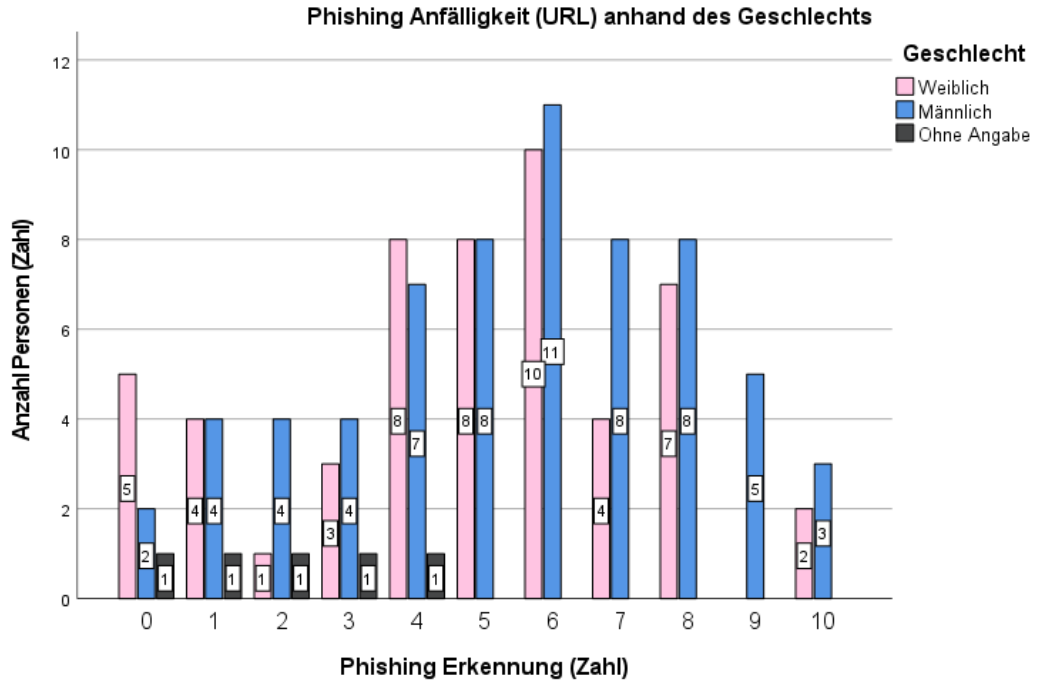



*Abbildung 31: Ergebnis - Phishing Anfälligkeit (URL) anhand des Geschlechts*

Die Abbildung 32 zeigt die Phishing Anfälligkeit bei URLs in Bezug auf eine Teilnahme einer Phishing Schulung. Hier ist es ersichtlich, dass eine Phishing Schulung dazu beitragen kann, besser bei der Erkennung von Phishing URLs abzuschneiden als bei keiner Teilnahme einer Phishing Schulung. Denn es haben jeweils vier Personen, die eine Phishing Schulung erhalten haben, zehn und neun Punkte erzielen können. Jedoch ist auch hier nennenswert, dass jeweils eine Person ohne Phishing Schulung zehn Punkte bzw. neun Punkte erzielen konnte.

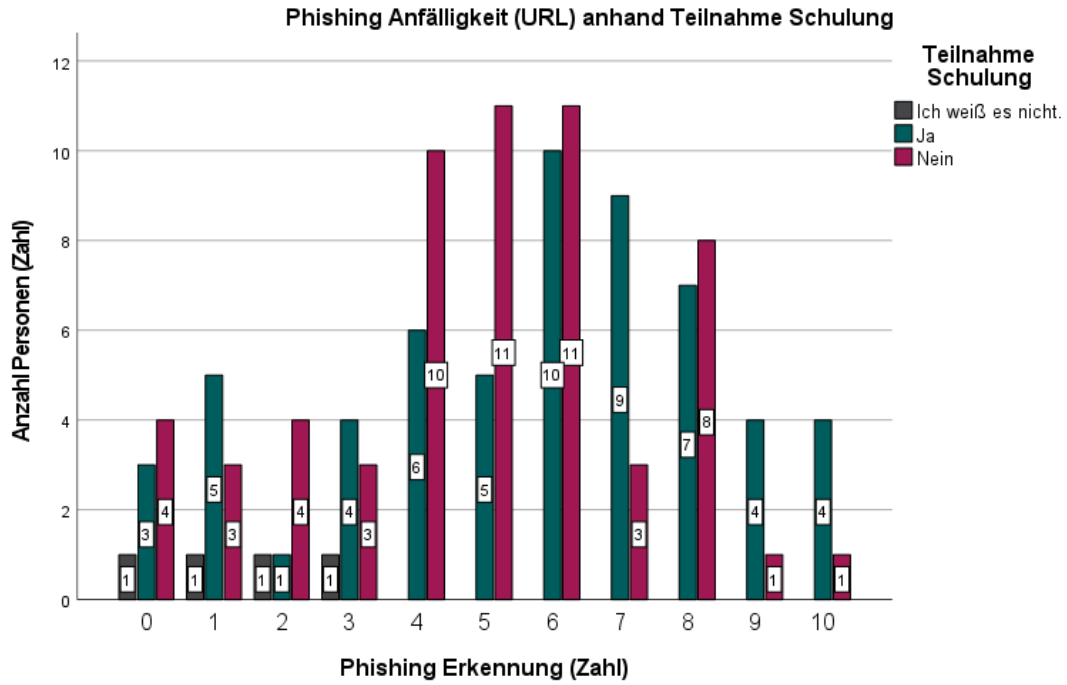



*Abbildung 32: Ergebnis - Phishing Anfälligkeit (URL) anhand Teilnahme Schulung*

Beide Ergebnisse werden im Kapitel 3.3.2 näher analysiert. Im Folgenden werden die Ergebnisse der Phishing Anfälligkeit von E-Mail und URL zusammengefasst betrachtet.

### 3.2.6 Phishing Anfälligkeit – Gesamt

Die erste Grafik zeigt die Phishing Erkennung von E-Mail und URL anhand des Geschlechts (siehe Abbildung 33). In dieser Grafik ist es erkennbar, dass die Männer leicht besser abschneiden als die Frauen, denn fünf Männer haben 17 von 20 Punkten erzielt. Wohingegen nur eine Frau dies geschafft hat. Keine der Teilnehmer und Teilnehmerinnen des Fragebogens hat 20 von 20 Punkten erzielen können.

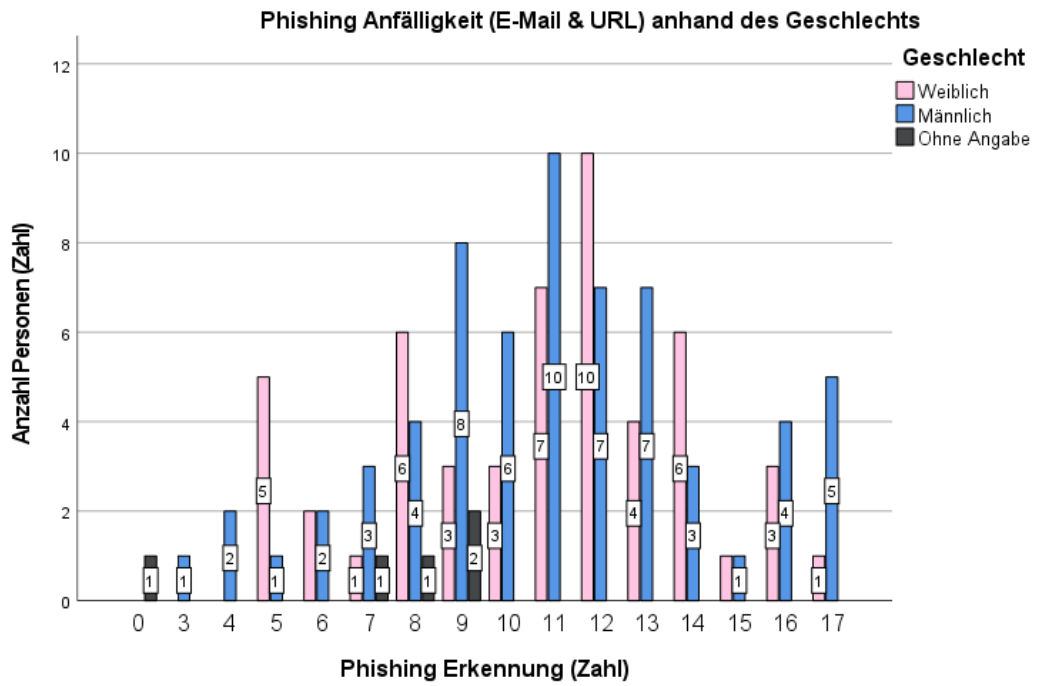



*Abbildung 33: Ergebnis - Phishing Anfälligkeit (E-Mail und URL) anhand des Geschlechts*

Die zweite Grafik zeigt die Phishing Erkennung anhand der Teilnahme einer Phishing Schulung (siehe Abbildung 34). In dieser Grafik ist auch zu erkennen, dass eine Teilnahme an einer Phishing Schulung dazu beitragen kann, die Erkennung von E-Mail und URLs zu erhöhen. Denn es haben fünf Personen 17 von 20 Punkten erreicht, wohingegen nur eine Person ohne einer Phishing Schulung dieses Ergebnis erreichen konnte. Beide Ergebnisse werden im Kapitel 3.3.2 näher analysiert.

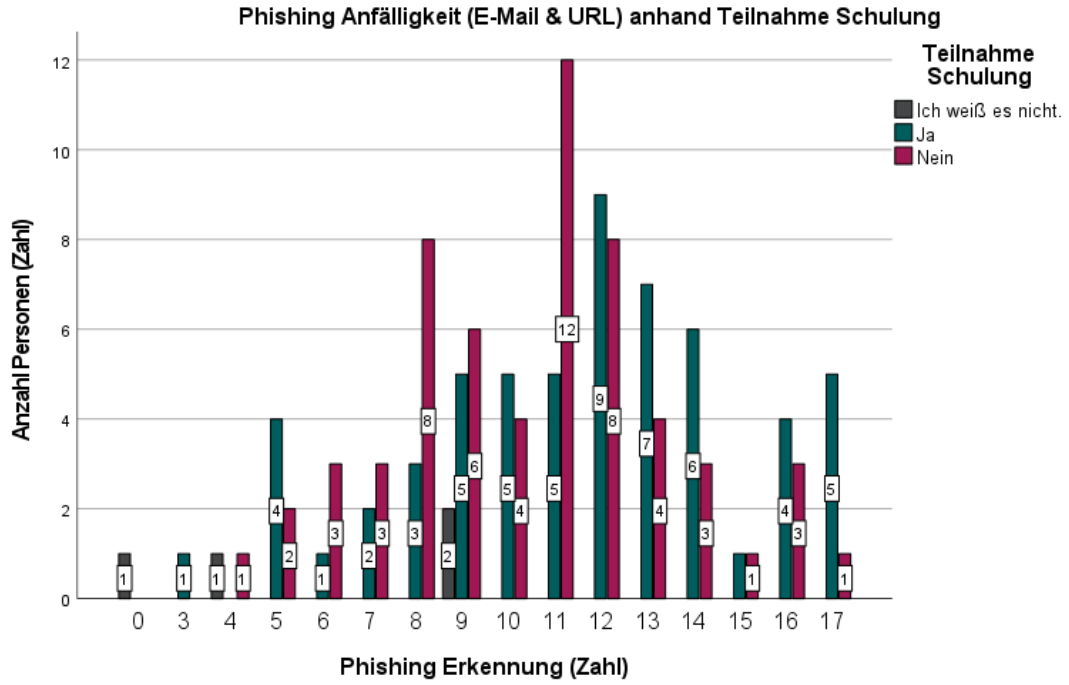



*Abbildung 34: Ergebnis - Phishing Anfälligkeit (E-Mail und URL) anhand Teilnahme Schulung*

### 3.2.7 Durchgeführte Phishing Schulungen und Methoden

In diesem Kapitel wird auf die durchgeführten Schulungen, die Methoden und die Zeitdauer der letzten durchgeführten Schulung näher eingegangen. Die erste Frage (siehe Abbildung 59) beschäftigt sich mit der Teilnahme einer Phishing Schulung. Anhand der Abbildung 35 ist zu erkennen, dass fast die Hälfte der Teilnehmer keine Phishing Schulung erhalten haben, um genau zu sein haben 59 Personen (48,8%) keine Schulung in Bezug auf Phishing erhalten. 58 Personen (47,9%) haben eine Phishing Schulung erhalten und vier Personen (3,3%) haben die Option „Ich weiß es nicht." gewählt.

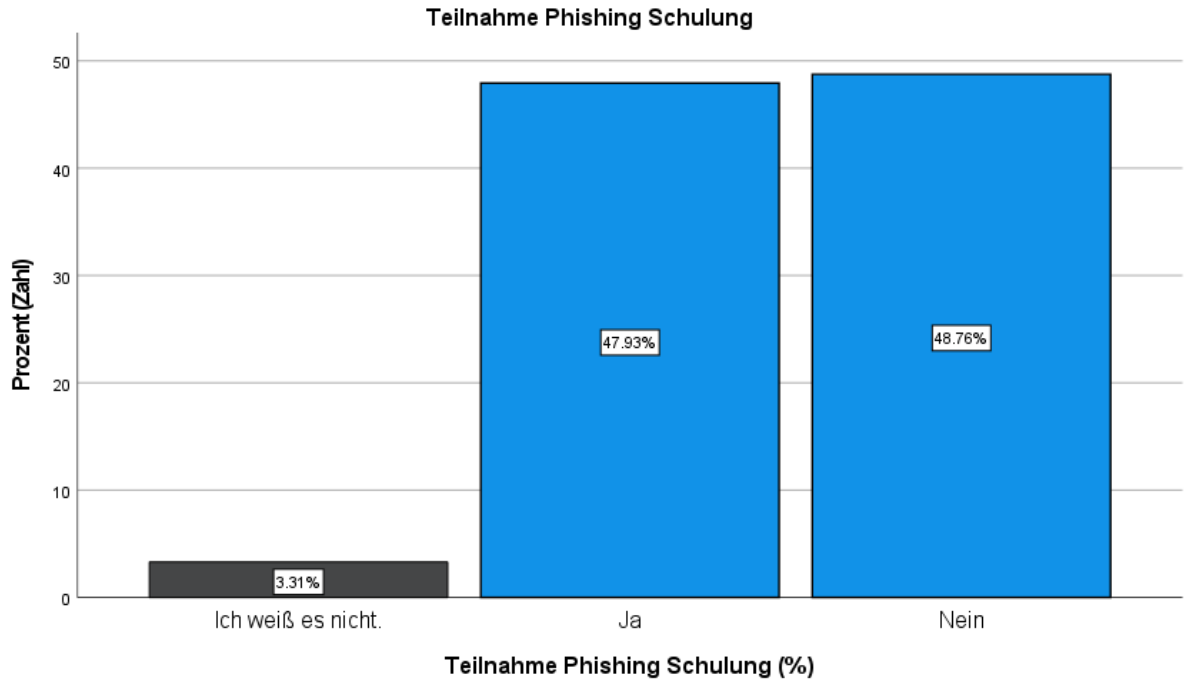



*Abbildung 35: Ergebnis - Teilnahme Schulung*

Dieses Umfrageergebnis war nicht erwartet und deswegen wurde im nächsten Schritt die dritte Aussage für den Faktor Phishing Vertrautheit genauer betrachtet. Die dritte Aussage lautet: Ich habe eine Schulung zum Thema Computer-/Informationssicherheit erhalten. Diese Aussage wurde anhand der fünfstufigen Likert Skala gemessen. Anhand der Abbildung 36 ist zu erkennen, dass wenn die Werte von „stimme überhaupt nicht zu", „stimme nicht zu" und „stimme weder zu noch stimme zu" zusammengefasst werden, 41 Personen (33,9%) tatsächlich noch keine Schulung zum Thema Computer-/Informationssicherheit erhalten haben. Wohingegen 80 Personen (66,1%) eine Schulung bezüglich dieser Thematik absolviert haben („stimme zu" und „stimme voll und ganz zu").

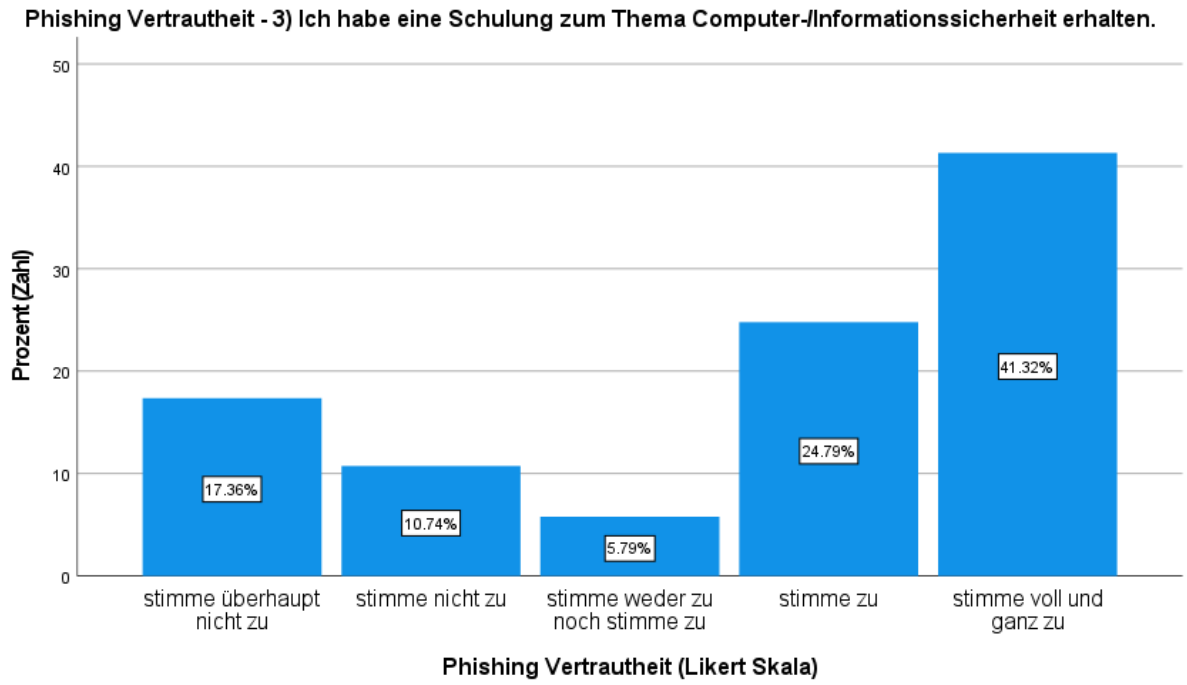



*Abbildung 36: Ergebnis - Phishing Vertrautheit (3. Aussage)*

Die zweite Frage (siehe Abbildung 60) beschäftigt sich mit den 58 Personen, die an einer Phishing Schulung teilgenommen haben und den vier Personen die in der vorigen Fragestellung die Option „Ich weiß es nicht." gewählt haben. Diese Personen wurden gefragt, welche Schulungsmethode sie erhalten haben. Die Abbildung 37 hebt hervor, dass die meisten Teilnehmer und Teilnehmerinnen eine herkömmliche Schulung erhalten haben. Somit haben 32 Personen (51,6%) an einer herkömmlichen Schulung teilgenommen. Die zweit höchste Kategorie ist die eingebettete Schulung mit 13 Personen (21,0%). Danach kommt die Achtsamkeitsschulung mit neun Personen (14,5%). Die drei niedrigsten Kategorien bilden die simulierte Schulung mit vier Personen (6,5%), die spielbasierte Schulung mit drei Personen (4,8%) und eine Person (1,6%) hat die Option „Keine dieser genannten Schulung" gewählt.

Die letzte Frage (siehe Abbildung 60) in diesem Kapitel beschäftigt sich mit der letzten durchgeführten Schulung. In dieser Frage haben insgesamt 61 Personen teilgenommen, die eine Person die in der vorigen Frage die Option „Keine dieser genannten Schulung" gewählt hat, wurde aus dieser Frage ausgeschlossen. Für diese Fragestellung gab es fünf Antwortmöglichkeiten: „Ich weiß es nicht.", „<1 Monat", „1-3 Monate", „3-5 Monate", und „>5 Monate". Drei Personen (4,9%) haben die erste Antwortmöglichkeit mit „Ich weiß es nicht." Ausgewählt (siehe Abbildung 38). Bei vier Personen (6,6%) war die letzte Schulung weniger als ein Monat her, gemessen ab dem Zeitpunkt vom Ausfüllen des Fragebogens (Anfang August). Bei 15 Personen (24,6%) liegt die letzte Schulung schon ein bis drei Monate zurück. Zehn Personen (16,4%) hatten ihre letzte Schulung zwischen drei bis fünf

Monaten und bei 29 Personen (47,5%) liegt die Schulung schon mehr als fünf Monate zurück.

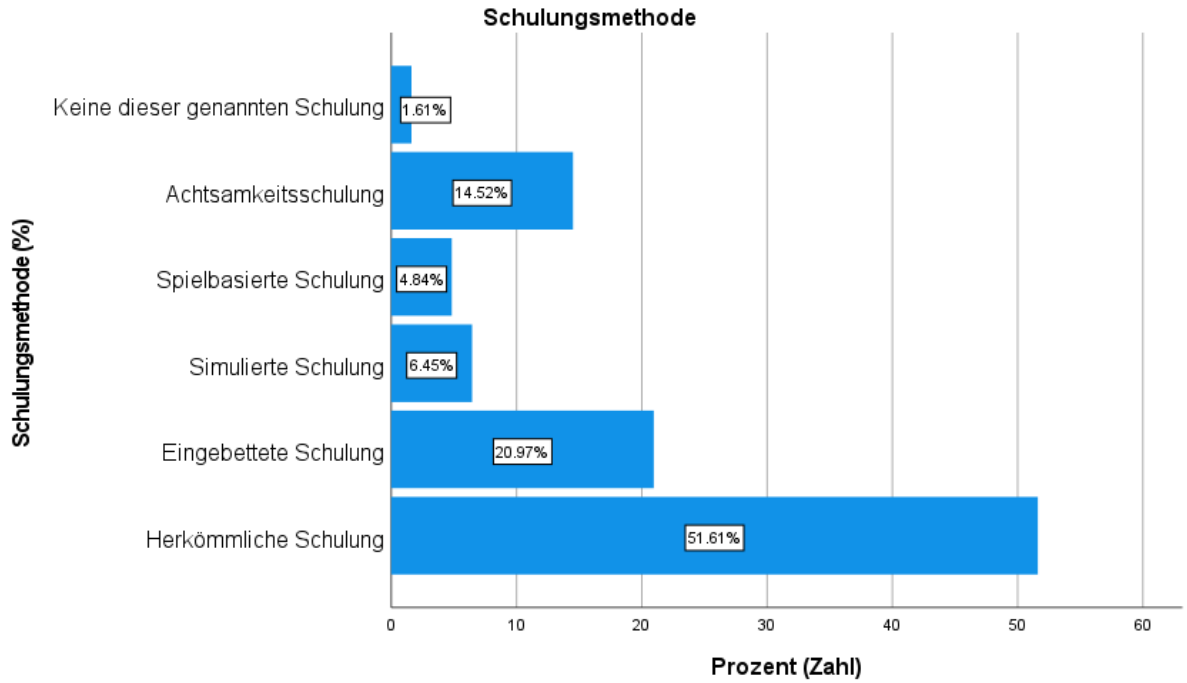



*Abbildung 37: Ergebnis - Schulungsmethode*

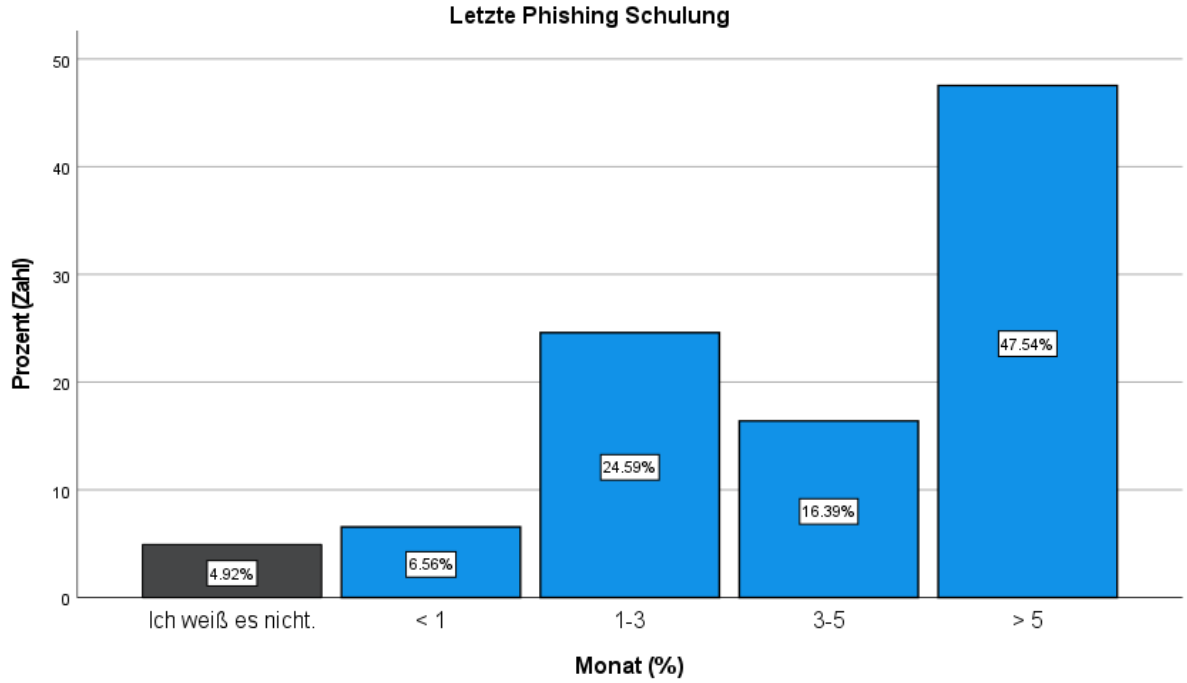



*Abbildung 38: Ergebnis - Letzte Phishing Schulung*

### 3.2.8 Bevorzugte Phishing Schulungsmethoden

In diesem Kapitel werden die bevorzugten Schulungsmethoden der Teilnehmer und Teilnehmerinnen des Fragebogens näher betrachtet. Wie bereits im Kapitel 3.1 (Teil 4) besprochen wurde, wurde für jede Schulungsmethode vier Aussagen definiert und diese

Aussagen wurden anhand der fünfstufigen Likert Skala von den Teilnehmer und Teilnehmerinnen des Fragebogens beantwortet. Die Werte wurden wie bei den Faktoren „Phishing Vertrautheit“, „Phishing Awareness“ und „Sicherheitsgewohnheiten“ zusammengefasst und anschließend wurde der Mittelwert errechnet. Die Mittelwerte wurden wie im Artikel von Sözen und Güven (2019) wieder in eine fünfstufige Likert Skala anhand der Tabelle 1 umgewandelt (Sözen and Güven, 2019, p. 3). Die besprochenen Schritte wurden für jede einzelne Schulungsmethode durchgeführt und schlussendlich ist die Tabelle 3 entstanden. Anhand dieser Tabelle ist zu sehen, dass die Mittelwerte sehr nah beieinander liegen. Diese Werte signalisieren, dass die Teilnehmer und Teilnehmerinnen indifferent sind bezüglich der Entscheidung für die bevorzugte Phishing Schulungsmethode. Angenommen es müsste trotzdem anhand dieser Werten eine Entscheidung getroffen werden, würde die Achtsamkeitsschulung und die eingebettete Schulung ausgewählt werden.

| **Bevorzugte Phishing Schulungsmethode** | | | | | |
|---|---|---|---|---|---|
| | N | Minimum | Maximum | Mean | Std. Deviation |
| Herkömmlich | 121 | 2 | 5 | 3.68 | .777 |
| Eingebettet | 121 | 1 | 5 | 3.83 | .960 |
| Simuliert | 121 | 1 | 5 | 3.72 | .887 |
| Spielbasiert | 121 | 1 | 5 | 3.78 | .871 |
| Achtsamkeit | 121 | 1 | 5 | 3.88 | .818 |

*Tabelle 3: Ergebnis - Bevorzugte Phishing Schulungsmethode*

Es wurde auch versucht anhand des Geschlechts und der Teilnahme einer Phishing Schulung zu ermitteln, welche Phishing Schulungsmethode bevorzugt wird. Die Grafiken im Anhang A (siehe Abbildung 66, Abbildung 67, Abbildung 68, Abbildung 69 und Abbildung 70) zeigen diese Auswertungen grafisch dar. Jedoch ist auch hier schwer zu erkennen, welche Schulungsmethode welches Geschlecht bevorzugen würde. Unter der Voraussetzung, dass nur der höchste zusammengesetzte Wert („stimme zu“ und „stimme voll und ganz zu“) je Geschlecht in Betracht gezogen wird, würden männliche Teilnehmer sich für die Achtsamkeitsschulung entscheiden mit 48 Stimmen. Bei den Frauen mit 38 Stimmen wäre die eingebettete Schulung die bevorzugtere Phishing Schulungsmethode. Bei der Teilnahme einer Phishing Schulung sind die Ergebnisse (siehe Abbildung 71, Abbildung 72, Abbildung 73, Abbildung 74 und Abbildung 75) nah aneinander liegend wie bei den Ergebnissen anhand des Geschlechts. Personen, die bei einer Phishing Schulung teilgenommen haben, würden mit 47 Stimmen die Achtsamkeitsschulung bevorzugen. Personen ohne eine Teilnahme einer Phishing Schulung tendieren mit 40 Stimmen zu einer eingebetteten Schulungsmethode. Jedoch muss auch hier erwähnt werden, dass

diese Werte bei beiden Varianten (Geschlecht und Teilnahme Phishing Schulung) sehr nahe beieinander liegen.

## 3.3 Auswertung

In diesem Kapitel werden verschiedene Auswertungen durchgeführt, um die Alternativhypothesen aus dem Kapitel 1.5 anzunehmen oder zu widerlegen. Bei allen Auswertungen wird bei einem p-Wert < 0,05 das Ergebnis als statistisch signifikant angesehen.

### 3.3.1 Cronbach´s Alpha

Ein in der Forschungsliteratur sehr gebräuchliches Maß für die Zuverlässigkeit ist Cronbachs Alpha und wird in der Forschungsliteratur oft verwendet, um die Zuverlässigkeit der internen Konsistenz mehrerer Items oder Werte zu bewerten, die der Forscher oder die Forscherin zusammenfassen oder summieren möchte, um einen Skalenwert zu erhalten. Der Alpha Wert sollte positiv und in der Regel größer als 0,70 sein, um die interne Konsistenzzuverlässigkeit gut zu unterstützen (Morgan, 2010, p. 122). Cronbach Alpha wurde für „Phishing Vertrautheit“, „Phishing Awareness“, „Sicherheitsgewohnheiten“, „Phishing Anfälligkeit Gesamt“, „Phishing Anfälligkeit E-Mail“ und „Phishing Anfälligkeit URL durchgeführt. Die Werte sind für alle Faktoren über 0,70 bis auf den Faktor „Phishing Anfälligkeit E-Mail“. Aus diesem Grund wird bei der weiteren Auswertung nur der Faktor „Phishing Anfälligkeit Gesamt“ in Betracht gezogen.

Bei Phishing Vertrautheit mit elf Aussagen beträgt der Alpha Wert: 0,708 und ist somit leicht größer als 0,70 (siehe Tabelle 4).

| **Reliability Statistics** | |
|---|---|
| Cronbach's Alpha | N of Items |
| .708 | 11 |

*Tabelle 4: Auswertung - Cronbach´s Alpha (Phishing Vertrautheit)*

Bei Phishing Awareness mit zwölf Aussagen beträgt der Alpha Wert: 0,792 und ist somit größer als 0,70 (siehe Tabelle 5).

| **Reliability Statistics** | |
|---|---|
| Cronbach's Alpha | N of Items |
| .792 | 12 |

*Tabelle 5: Auswertung - Cronbach´s Alpha (Phishing Awareness)*

Bei Sicherheitsgewohnheiten mit zwölf Aussagen beträgt der Alpha Wert: 0,728 und ist somit größer als 0,70 (siehe Tabelle 6).

| Reliability Statistics | |
|---|---|
| Cronbach's Alpha | N of Items |
| .728 | 12 |

*Tabelle 6: Auswertung - Cronbach´s Alpha (Sicherheitsgewohnheiten)*

Bei Phishing Anfälligkeit Gesamt mit 20 Beispielen beträgt der Alpha Wert: 0,810 und ist somit größer als 0,70 (siehe Tabelle 7).

| Reliability Statistics | |
|---|---|
| Cronbach's Alpha | N of Items |
| .810 | 20 |

*Tabelle 7: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit Gesamt)*

Bei Phishing Anfälligkeit E-Mail mit zehn Beispielen beträgt der Alpha Wert: 0,660 und ist somit kleiner als 0,70 (siehe Tabelle 8).

| Reliability Statistics | |
|---|---|
| Cronbach's Alpha | N of Items |
| .660 | 10 |

*Tabelle 8: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit E-Mail)*

Bei Phishing Anfälligkeit URL mit zehn Beispielen beträgt der Alpha Wert: 0,816 und ist somit größer als 0,70 (siehe Tabelle 9).

| Reliability Statistics | |
|---|---|
| Cronbach's Alpha | N of Items |
| .816 | 10 |

*Tabelle 9: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit URL)*

### 3.3.2 Mann-Whitney-U-Test

Für die Auswertung, ob es signifikante Unterschiede zwischen der Phishing Anfälligkeit und dem Geschlecht bzw. der Teilnahme einer Phishing Schulung gibt, wurde hier der Mann-Whitney-U-Test verwendet. Der Mann-Whitney-U-Test untersucht die Unterschiede zwischen zwei verschiedenen Gruppen (Davis, 2013, p. 170). Dieser Test wurde ausgewählt, weil der T-Test nicht möglich war, denn die abhängige Variable „Phishing Anfälligkeit Gesamt“ ist nicht normal verteilt (Back and Guerette, 2021, p. 436) und dies stellt eine der Annahmen des T-Test dar. Die Überprüfung dieser Annahme wurde mithilfe eines Tests für die Normalverteilung festgestellt (siehe Tabelle 10). Für Datensätze mit weniger als 2000 Daten wird der Signifikanz Test des Shapiro-Wilk-Tests

verwendet, ansonsten müsste der Signifikanz Wert des Kolmogorov-Smirnov-Tests betrachtet werden. Der Datensatz für die Auswertung beträgt weniger als 2000 Daten und daher wird der Wert des Shapiro-Wilk-Test angesehen. Im Falle von „Phishing Anfälligkeit Gesamt“ ist der p-Wert von 0,048 kleiner als p<0,05 und daher muss die Alternativhypothese angenommen werden (siehe Tabelle 10). Dementsprechend sind die Daten der Phishing Anfälligkeit nicht normalverteilt (Ifham, 2020) und infolgedessen wurde der Mann-Whitney-U-Test ausgewählt.

| Tests of Normality | | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Statistic | df | Sig. | Statistic | df | Sig. |
| PK Ges | .101 | 121 | .004 | .978 | 121 | .048 |
| a. Lilliefors Significance Correction | | | | | | |

*Tabelle 10: Auswertung - Test für Normalverteilung PK Ges*

Es gibt jedoch zwei Annahmen für den Mann-Whitney-Test die vor der Durchführung des Test beachtet werden müssen (Morgan, 2010, p. 141):

1. Bei diesem Test wird nämlich angenommen, dass die abhängige Variable kontinuierlich ist. Es wird davon ausgegangen, dass der abhängigen Variable eine Kontinuität zugrunde liegt, auch wenn die tatsächlichen Daten diskrete Zahlen wie bei einer Likert-Skala sind (Morgan, 2010, p. 141).
2. Die Daten sind unabhängig (die Ergebnisse eines Teilnehmers oder einer Teilnehmerin sind nicht abhängig von den Ergebnissen der anderen Teilnehmer und Teilnehmerinnen) (Morgan, 2010, p. 141).

Beide dieser Annahmen treffen auf die abhängige Variable „Phishing Anfälligkeit Gesamt“ zu. Im Anschluss wird der Mann-Whitney-Test jeweils für das Geschlecht und für die Teilnahme einer Phishing Schulung durchgeführt. Jedoch wird bei dem Datensatz „Geschlecht“ die Wahl mit „Ohne Angabe“ ausgeschlossen und bei dem Datensatz „Teilnahme Phishing Schulung“ wird die Option mit „Ich weiß es nicht.“ nicht berücksichtigt.

Die Tabelle 11 zeigt, dass es keinen signifikanten Unterschied zwischen der „Phishing Anfälligkeit Gesamt (p=0,916)“ und dem Geschlecht gibt, weil der p-Wert (Asymp. Sig.) größer ist als p < 0,05. Aus diesem Grund wird bei der ersten Hypothese die Nullhypothese angenommen und die Alternativhypothese verworfen (siehe Kapitel 1.5). Die Nullhypothese lautet wie folgt: Es gibt keine signifikanten Unterschiede zwischen der Phishing Anfälligkeit und dem Geschlecht.

| Mann-Whitney U - Test Statistics[a] | |
|---|---|
| | PK Ges |
| Mann-Whitney U | 1645.000 |
| Wilcoxon W | 3023.000 |
| Z | -.106 |
| Asymp. Sig. (2-tailed) | .916 |
| a. Grouping Variable: Geschlecht | |

*Tabelle 11: Auswertung - Mann-Whitney U Test (PKGes & Geschlecht)*

Die Tabelle 12 zeigt, dass es einen signifikanten Unterschied zwischen der „Phishing Anfälligkeit Gesamt“ (p=0,046) und einer Teilnahme einer Phishing Schulung gibt, weil der p-Wert (Asymp. Sig.) kleiner ist als $p < 0,05$. Daher wird bei der zweiten Hypothese die Nullhypothese verworfen und die Alternativhypothese angenommen. Die Alternativhypothese lautet wie folgt: Es gibt signifikante Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme einer Phishing Schulung.

| Mann-Whitney U - Test Statistics[a] | |
|---|---|
| | PK Ges |
| Mann-Whitney U | 1347.500 |
| Wilcoxon W | 3117.500 |
| Z | -1.992 |
| Asymp. Sig. (2-tailed) | .046 |
| a. Grouping Variable: Teilnahme Schulung | |

*Tabelle 12: Auswertung - Mann-Whitney U Test (PKGes & Teilnahme Phishing Schulung)*

### 3.3.3 Korrelation

Mithilfe der Korrelation kann identifiziert werden, ob sich zwei oder mehr Variablen gemeinsam verändern. Die Korrelation misst die Richtung und das Ausmaß bzw. die Stärke der Beziehung zwischen jedem Paar von Variablen. Mit anderen Worten kann die Korrelation den Zusammenhang oder die Assoziation prüfen, ob eine Beziehung zwischen zwei Variablen besteht. Eine positive Korrelation zeigt an, dass sich diese Variablen in die gleiche Richtung bewegen, also gemeinsam steigen oder sinken, während eine negative Korrelation bedeutet, dass sich diese Variablen in die entgegengesetzte Richtung bewegen, also eine Variable steigt und die andere sinkt. Die Korrelationsanalyse ist einfach und offensichtlich, jedoch sollte zwischen der Korrelation, wie oben erwähnt, und der Kausalität unterschieden werden. Kausalität hat zwei Komponenten: eine Ursache und eine Auswirkung. Kausalität kann als Beziehung zwischen zwei Ereignissen erklärt werden und die Korrelation impliziert diese Art von Beziehung nicht. Mit anderen Worten: Zwei Variablen können miteinander korrelieren, aber keine von ihnen verursacht eine andere (Verma and Abdel-Salam, 2019, p. 118).

Die Beziehung zwischen einer Variablen und einer anderen wird im Allgemeinen durch den Korrelationskoeffizienten dargestellt, ein statistischer Wert mit den Grenzen +1 (eine perfekte positive Korrelation) und -1 (eine perfekte negative Beziehung). Liegt ein Ergebnis in der Nähe des Mittelwerts, also bei 0, dann sind die Ergebnisse wahrscheinlich zufällig und deswegen besteht kein feststellbarer Zusammenhang zwischen den Variablen (Davis, 2013, p. 136). Es gibt mehrere Korrelationskoeffizienten für die Forschung, aber der am häufigsten verwendete ist die Pearson-Produkt-Moment-Korrelation, die gewöhnlich als Pearson-Korrelation oder einfach als Pearson r bezeichnet wird. Das Pearson r wurde von Karl Pearson (1896) auf der Grundlage der ersten Entwicklung der Idee durch Sir Francis Galton (1886, 1888) entwickelt. Pearson r bewertet das Ausmaß, in dem zwei Variablen linear miteinander verbunden sind. Das Pearson $r^2$ gibt die Stärke der Beziehung an, d.h. den Anteil der Varianz zwischen den beiden Variablen. Pearson r setzt jedoch voraus, dass die Variablen annähernd Intervallmessungen darstellen und normalverteilt sind. Denn Ausreißer können den Wert der Korrelation erheblich verzerren und sollten daher vor der Datenanalyse entsprechend behandelt werden (Meyers, 2013, p. 159). Es wurde bereits im Kapitel 3.3.1 festgestellt, dass die Phishing Anfälligkeit Gesamt nicht normalverteilt ist und aus diesem Grund muss ein alternativer nichtparametrischer Test wie z.B. der Spearman Korrelationskoeffizient, durchgeführt werden (Verma and Abdel-Salam, 2019, p. 119).

Die Spearman-rho-Korrelation wurde von Sir Charles Spearman (1904b) unter anderem eingeführt, um den nachteiligen Einfluss von Ausreißern bei der Berechnung des Pearson-r zu minimieren. Bei der Berechnung des Spearman rho wird die Differenz zwischen den Rängen der einzelnen Datenpaare ermittelt. Werte von rho die näher bei ± 1 liegen, zeigen an, dass die Ränge von X und Y einander ähnlich sind. Werte von rho die näher bei 0 liegen, zeigen an, dass die Ränge von X und Y unabhängig voneinander sind (Meyers, 2013, p. 166). Es gibt Annahmen und Bedingungen für Spearman Rho ($r_s$) die beachtet werden müssen (Morgan, 2010, p. 111):

1. Die Daten für beide Variablen sind mindestens ordinal (Morgan, 2010, p. 111).
2. Die Werte der einen Variablen sind monoton mit der anderen Variablen verbunden. Das bedeutet, dass bei einem Anstieg der Werte der einen Variablen auch die andere Variable ansteigen sollte, aber nicht unbedingt linear. Die Kurve kann sich abflachen, aber sie kann nicht sowohl nach oben als auch nach unten verlaufen (Morgan, 2010, p. 111).

Die erste Annahme ist für die untersuchenden Variablen „Phishing Anfälligkeit Gesamt“, „Phishing Vertrautheit“, „Phishing Awareness“ und Sicherheitsgewohnheiten gegeben. Die zweite Annahme wurde mithilfe eines Streudiagrammes überprüft (siehe Abbildung 76, Abbildung 77 und Abbildung 78). Ein Streudiagramm ist ein Diagramm oder eine Grafik von zwei Variablen, die anzeigt, wie die Punktzahl einer Person bei einer Variable mit ihrer Punktzahl bei der anderen Variable zusammenhängt. Wenn die Korrelation hoch positiv ist, liegen die aufgezeichneten Punkte nahe an einer geraden Linie (der linearen Regressionslinie), die von der linken unteren Ecke des Diagramms nach rechts oben verläuft. Die lineare Regressionslinie fällt von links oben nach rechts unten ab, wenn die Korrelation stark negativ ist. Bei Korrelationen nahe Null ist die Regressionslinie flach und viele Punkte liegen weit von der Linie entfernt. Anhand des Diagramms kann auch erkannt werden, ob es extreme Ausreißer gibt (weit von der Regressionslinie entfernt), und es kann zeigen, dass eine Kurve anstelle einer Geraden eine bessere Anpassungslinie wäre. In diesem Fall ist die Annahme einer linearen Beziehung verletzt und eine Pearson-Korrelation wäre nicht die beste Wahl (Morgan, 2010, p. 112). Die Tabelle 13 zeigt die Auswertung der Spearman Korrelation.

**Spearman Rank-Order Correlations zwischen Phishing Anfälligkeit Gesamt, Phishing Vertrautheit (PV), Phishing Awareness (PA) und Sicherheitsgewohnheiten (SG)**

| | | | PK Ges | PV | PA | SG |
|---|---|---|---|---|---|---|
| Spearman's rho | PK Ges | Correlation Coefficient | 1.000 | | | |
| | | Sig. (2-tailed) | . | | | |
| | PV | Correlation Coefficient | .312** | 1.000 | | |
| | | Sig. (2-tailed) | <.001 | . | | |
| | PA | Correlation Coefficient | .152 | .446** | 1.000 | |
| | | Sig. (2-tailed) | .096 | <.001 | . | |
| | SG | Correlation Coefficient | .093 | .308** | .517** | 1.000 |
| | | Sig. (2-tailed) | .312 | <.001 | <.001 | . |

**. Correlation is significant at the 0.01 level (2-tailed).

*Tabelle 13: Auswertung - Spearman Korrelation (PK Ges, PV, PA und SG)*

Die Spearman Korrelation wurde zur Untersuchung des Zusammenhangs zwischen „Phishing Anfälligkeit Gesamt“ und „Phishing Vertrautheit“, „Phishing Awareness“ bzw. „Sicherheitsgewohnheiten“ durchgeführt. Dabei wurden festgestellt, dass nur zwischen „Phishing Anfälligkeit Gesamt“ und „Phishing Vertrautheit“ positive und signifikante (Sig.) Korrelationen bestehen, weil $p < 0{,}001$ beträgt. Zwischen „Phishing Anfälligkeit Gesamt“ und „Phishing Awareness“ und „Phishing Anfälligkeit Gesamt“ und „Sicherheitsgewohnheiten“ bestehen zwar positive Korrelationen jedoch sind diese nicht

signifikant, weil die p-Werte nicht kleiner als 0,05 sind. Jedoch konnten weitere positive und signifikante Korrelationen zwischen folgenden Variablen festgestellt werden: „Phishing Vertrautheit“ und „Phishing Awareness“, „Phishing Vertrautheit“ und „Sicherheitsgewohnheiten“ und „Phishing Awareness“ und „Sicherheitsgewohnheiten“. Aufgrund der Spearman Korrelation kann nur bei der dritten Hypothese die Alternativhypothese angenommen werden (siehe Kapitel 1.5). Die Alternativhypothese der dritten Hypothese lautet wie folgt: Es gibt signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit. Bei der vierten und fünften Hypothese wird die Nullhypothese angenommen und die Alternativhypothese verworfen (siehe Kapitel 1.5). Die Nullhypothese für die vierte Hypothese lautet folgendermaßen: Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Awareness. Die Nullhypothese der fünften Hypothese wurde auf folgende Weise beschrieben: Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Sicherheitsgewohnheit. Aufgrund der positiven Korrelation zwischen „Phishing Anfälligkeit Gesamt“ und „Phishing Vertrautheit“ kann festgestellt werden, dass ein höherer Wert bei der Phishing Erkennung von E-Mails und URLS mit einer hohen Phishing Vertrautheit zusammenliegt und umgekehrt.

## 3.4 Diskussion

In diesem Teil werden die Erkenntnisse des theoretischen Teils mit den Ergebnissen und Auswertungen des empirischen Teils miteinander verglichen und zusammengefasst. Bei den Ergebnissen und Auswertungen des empirischen Teils werden die wichtigsten Erkenntnisse die für die Beantwortung der Forschungsfrage hervorgehoben. Infolgedessen beschäftigt sich dieses Kapitel mit der Beantwortung der folgenden Forschungsfrage: „Wie stellt sich derzeit die Phishing Schulung der Arbeitnehmer und Arbeitnehmerinnen in österreichischen Großunternehmen dar?“. Des Weiteren werden interessante Ergebnisse einzelner Aussagen zu den Faktoren „Phishing Vertrautheit“, „Phishing Awareness“ und „Sicherheitsgewohnheiten“ näher betrachtet. Im Anschluss werden die Hypothesen mit vergangenen Studien miteinander verglichen, um etwaige ähnliche oder sogar unterschiedliche Ergebnisse festzustellen.

Anhand der Abbildung 1 ist zu erkennen, dass die Teilnehmer und Teilnehmerinnen fast zur Hälfte männliche und weibliche Personen waren. Des Weiteren kann anhand der Abbildung 2 festgestellt werden, dass die meisten Teilnehmer und Teilnehmerinnen bereits ein Studium abgeschlossen haben. Die Abbildung 3 zeigt auch, dass die Teilnehmer und Teilnehmerinnen des Fragebogens in unterschiedlichen Arbeitsbereichen gearbeitet

haben oder derzeit arbeiten. Die meisten Teilnehmer und Teilnehmerinnen waren ein bis sechs Jahre in einem Großunternehmen in Österreich angestellt oder sind dort noch angestellt (siehe Abbildung 4). Der größte Teil der befragten Personen arbeiten 31-40 Wochenstunden (siehe Abbildung 5). Leider ist aufgrund eines Fehlers des Autors das Alter der Teilnehmer und Teilnehmerinnen nicht erhoben worden. Dennoch wurden die wichtigsten demografischen Daten zu den befragten Personen erhoben, um die Forschungsfrage beantworten zu können. Im nächsten Abschnitt werden die Faktoren „Phishing Vertrautheit", „Phishing Awareness" und „Sicherheitsgewohnheiten" und einzelne interessante Aussagen näher betrachtet.

Die Abbildung 6 zeigt, dass mehr als die Hälfte der Teilnehmer und Teilnehmer des Fragebogens eine gewisse Vertrautheit mit dem Thema Phishing haben. Die Vertrautheit der Teilnehmer und Teilnehmerinnen ist auch anhand des Ergebnisses der Phishing Definition zu erkennen, denn 95% der Personen haben diese Frage richtig beantwortet (siehe Tabelle 2). Downs et al. (2007) fanden heraus, dass diejenigen die mit der Definition von Phishing vertraut sind, deutlich seltener auf E-Mail- und Website-Phishing hereinfallen (Tornblad, Jones, *et al.*, 2021, p. 940). Dies konnte in dieser Befragung jedoch nicht bestätigt werden, denn obwohl 95% der Personen die Definitionsfrage richtig beantwortet haben, haben nur ein wenig mehr als 50% der Teilnehmer und Teilnehmerinnen mehr als 50% der vorgestellten Beispiele richtig identifizieren können.

Des Weiteren wurden zwei Aussagen des Faktors „Phishing Vertrautheit" näher betrachtet und es ist anhand der Tabelle 14 zu erkennen, dass die Aussagen: „Ich weiß, wie man einen Phishing-Angriff verhindern kann." und „Wenn ich meine E-Mail benutze, kann ich eine Phishing-E-Mail erkennen." einen signifikanten positiven Zusammenhang mit der „Phishing Anfälligkeit Gesamt" hat.

**Spearman Rank-Order Correlations zwischen Phishing Anfälligkeit Gesamt und Phishing Vertrautheit (5. und 7. Aussage)**

| | | | PK Ges | PV – 5. Aussage | PV – 7. Aussage |
|---|---|---|---|---|---|
| Spearman's rho | PK Ges | Correlation Coefficient | 1.000 | | |
| | | Sig. (2-tailed) | . | | |
| | PV – 5. Aussage | Correlation Coefficient | .210* | 1.000 | |
| | | Sig. (2-tailed) | .021 | . | |
| | PV – 7. Aussage | Correlation Coefficient | .196* | .506** | 1.000 |
| | | Sig. (2-tailed) | .031 | <.001 | . |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | | |

*Tabelle 14: Diskussion - Spearman Korrelation (PK Ges und PV - 1. & 5. Aussage)*

Des Weiteren ist anhand der Abbildung 39 zu erkennen, dass mehr als die Hälfte der teilgenommenen Personen des Fragebogens noch nicht auf eine Phishing-Attacke hereingefallen sind.

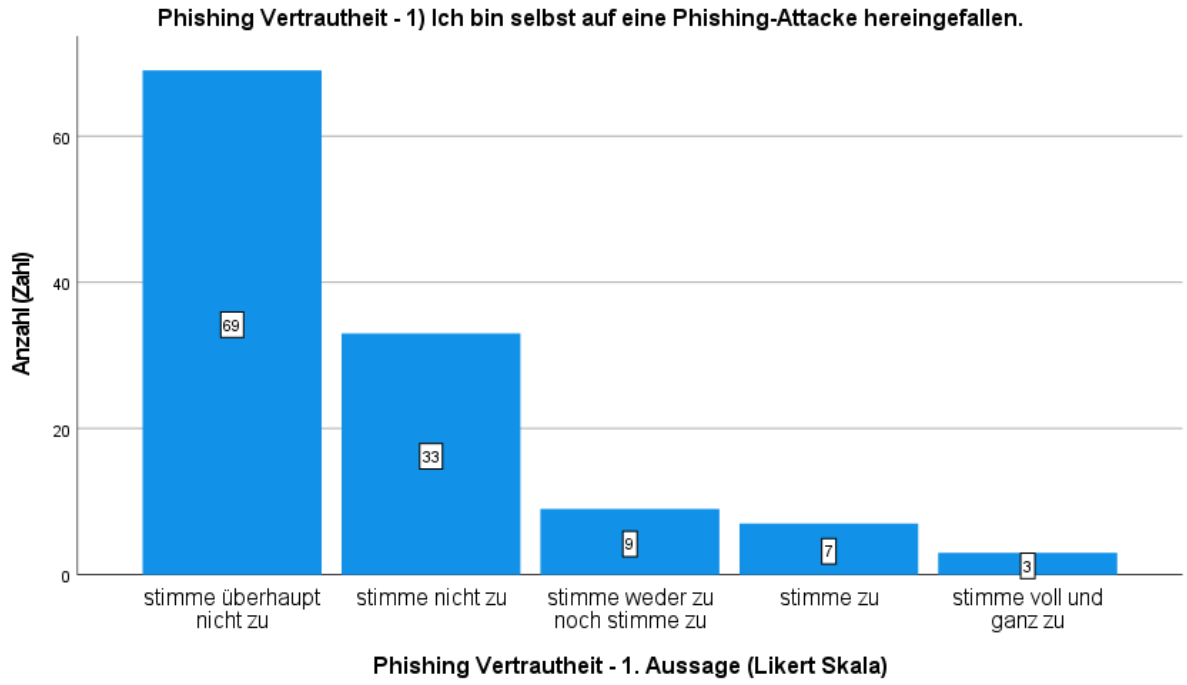



*Abbildung 39: Diskussion - PV (1. Aussage)*

Das Ergebnis der Abbildung 39 könnte auch damit zusammenliegen, dass mehr als 75% der Teilnehmer und Teilnehmerinnen des Fragebogens bereits wissen, dass Phishing-Angriffe nicht nur über Phishing-E-Mails, sondern auch über Telefonanrufe, SMS und über soziale Medien durchgeführt werden können (siehe Tabelle 15, Tabelle 16 und Tabelle 17).

| **Phishing Vertrautheit - 8) Ein Phishing-Angriff kann durch Telefonanrufe erfolgen.** | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 5 | 4.1 | 4.1 | 4.1 |
| | stimme nicht zu | 6 | 5.0 | 5.0 | 9.1 |
| | stimme weder zu noch stimme zu | 17 | 14.0 | 14.0 | 23.1 |
| | stimme zu | 55 | 45.5 | 45.5 | 68.6 |
| | stimme voll und ganz zu | 38 | 31.4 | 31.4 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 15: Diskussion - PV (8. Aussage)*

| Phishing Vertrautheit - 9) Ein Phishing-Angriff kann über SMS erfolgen. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 1 | .8 | .8 | .8 |
| | stimme nicht zu | 6 | 5.0 | 5.0 | 5.8 |
| | stimme weder zu noch stimme zu | 16 | 13.2 | 13.2 | 19.0 |
| | stimme zu | 54 | 44.6 | 44.6 | 63.6 |
| | stimme voll und ganz zu | 44 | 36.4 | 36.4 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 16: Diskussion - PV (9. Aussage)*

| Phishing Vertrautheit - 10) Ein Phishing-Angriff kann über Soziale Medien erfolgen. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 1 | .8 | .8 | .8 |
| | stimme nicht zu | 1 | .8 | .8 | 1.7 |
| | stimme weder zu noch stimme zu | 8 | 6.6 | 6.6 | 8.3 |
| | stimme zu | 64 | 52.9 | 52.9 | 61.2 |
| | stimme voll und ganz zu | 47 | 38.8 | 38.8 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 17: Diskussion - PV (10. Aussage)*

Anhand dieser Ergebnisse kann festgestellt werden, dass die Teilnehmer und Teilnehmerinnen des Fragebogens sehr vertraut sind mit dem Thema „Phishing“. Als nächstes wird die Phishing Awareness näher betrachtet. Die Abbildung 7 zeigt zwar, dass mehr als die Hälfte der befragten Personen bereits eine gewisse Awareness haben. Jedoch ist anhand der Tabelle 18 zu erkennen, dass ein Drittel der Personen den Unterschied zwischen „http://“ und „https://“ nicht kennen.

| Phishing Awareness - 2) Ich kenne den Unterschied zwischen Website-Adressen, die mit "http://" und "https://" beginnen. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 12 | 9.9 | 9.9 | 9.9 |
| | stimme nicht zu | 29 | 24.0 | 24.0 | 33.9 |
| | stimme weder zu noch stimme zu | 6 | 5.0 | 5.0 | 38.8 |
| | stimme zu | 34 | 28.1 | 28.1 | 66.9 |
| | stimme voll und ganz zu | 40 | 33.1 | 33.1 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 18. Diskussion - PA (2. Aussage)*

Bei den Aussagen: „Ich habe meinen Benutzernamen und mein Passwort noch nie auf einer Website eingegeben, deren Adresse mit "http://" beginnt.“ und „Ich habe meine Bankomat-/Kreditkartendaten noch nie auf einer Website eingegeben, deren Adresse mit

"http://" beginnt.“ haben ein Drittel der Personen nicht zugestimmt. 30-40% der Personen haben bei diesen beiden Aussagen die Wahl „stimme weder zu noch stimme zu“ gewählt (siehe Tabelle 19 und Tabelle 20). Infolgedessen könnten diese Personen unsichere Websites besucht haben und dort ihre Anmeldedaten bzw. Bankomat-/Kreditkartendaten eingegeben haben. Denn HTTPs ist ein wichtiger Protokoll, der zum Schutz der Opfer vor Phishing-Angriffen verwendet wird (Adil, Khan and Nawaz Ul Ghani, 2020, p. 6) und in der Regel eine sichere Website darstellt (Desolda *et al.*, 2021, p. 16). Jedoch sind Phisher und Phisherinnen in der Lage das „https“ Symbol zu fälschen und eine Phishing-Website als eine sichere Website erscheinen zu lassen (Chiew, Yong and Tan, 2018, p. 9). Dennoch ist diese Erkenntnis der drei Aussagen sehr wichtig für die Beantwortung der Forschungsfrage und wird im Leitfaden für Phishing Schulungen berücksichtigt.

| **Phishing Awareness - 3) Ich habe meinen Benutzernamen und mein Passwort noch nie auf einer Website eingegeben, deren Adresse mit "http://" beginnt.** | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 12 | 9.9 | 9.9 | 9.9 |
| | stimme nicht zu | 36 | 29.8 | 29.8 | 39.7 |
| | stimme weder zu noch stimme zu | 51 | 42.1 | 42.1 | 81.8 |
| | stimme zu | 13 | 10.7 | 10.7 | 92.6 |
| | stimme voll und ganz zu | 9 | 7.4 | 7.4 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 19: Diskussion - PA (3. Aussage)*

| **Phishing Awareness - 4) Ich habe meine Bankomat-/Kreditkartendaten noch nie auf einer Website eingegeben, deren Adresse mit "http://" beginnt.** | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 8 | 6.6 | 6.6 | 6.6 |
| | stimme nicht zu | 19 | 15.7 | 15.7 | 22.3 |
| | stimme weder zu noch stimme zu | 41 | 33.9 | 33.9 | 56.2 |
| | stimme zu | 24 | 19.8 | 19.8 | 76.0 |
| | stimme voll und ganz zu | 29 | 24.0 | 24.0 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 20: Diskussion - PA (4. Aussage)*

Als nächstes wird die siebte Aussage der Phishing Awareness betrachtet. Die Ergebnisse zeigen, dass zwei Drittel der Personen die E-Mail von bekannten Absender und Absenderinnen auf verdächtige Links oder Anhänge (siehe Abbildung 40) überprüfen. Jedoch ein Drittel der Personen achten nicht auf diese Überprüfung und könnten demnach

anfälliger auf Phishing-Angriffe sein, denn Phisher und Phisherinnen können sich als bekannte Personen des Opfers ausgeben.

Die Tabelle 21 und Tabelle 22 zeigen jedoch, dass 90% der teilgenommenen Personen des Fragebogens sich dessen bewusst sind, dass es Risiken gibt, wenn auf einen Link in der E-Mail geklickt wird oder E-Mail-Anhängen geöffnet und/oder heruntergeladen wird. Aus diesem Grund kann festgelegt werden, dass ein Großteil der befragten Personen eine gewisse Phishing Awareness haben, wenn auch die Unterscheidung zwischen „http://“ und „https://“ nicht für jeden klar ist.

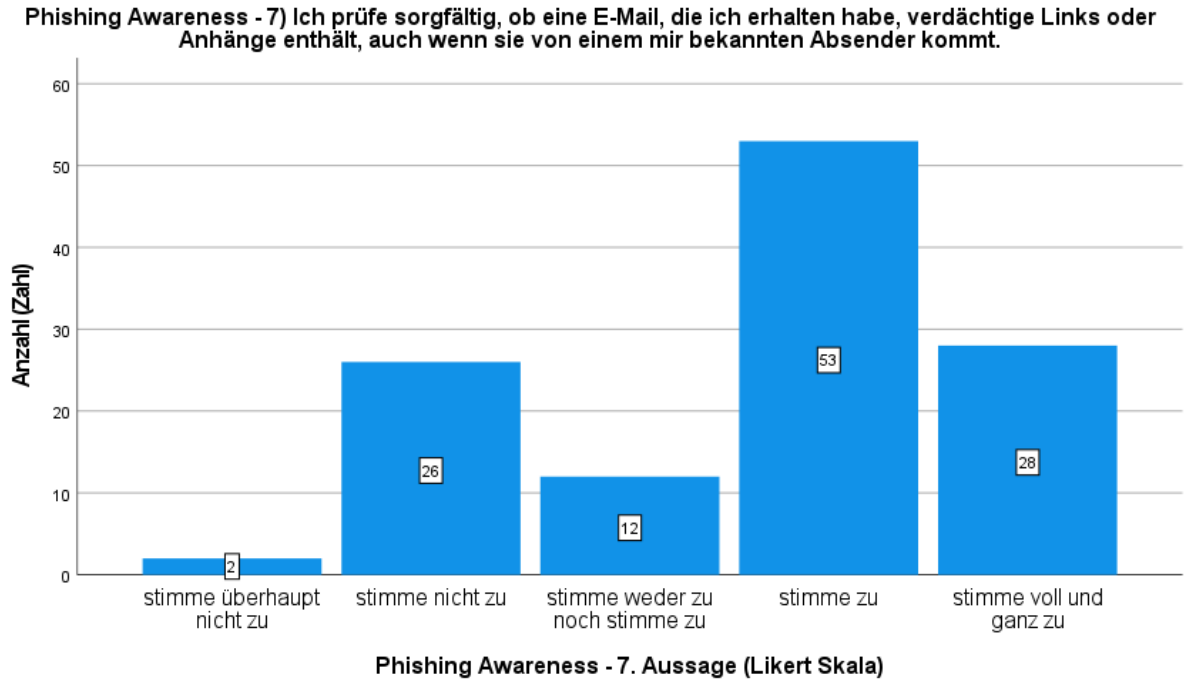



*Abbildung 40: Diskussion - PA (7. Aussage)*

| Phishing Awareness - 10) Ich bin mir des Risikos bewusst, das mit dem Anklicken von E-Mail-Links verbunden ist. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 1 | .8 | .8 | .8 |
| | stimme nicht zu | 8 | 6.6 | 6.6 | 7.4 |
| | stimme weder zu noch stimme zu | 6 | 5.0 | 5.0 | 12.4 |
| | stimme zu | 55 | 45.5 | 45.5 | 57.9 |
| | stimme voll und ganz zu | 51 | 42.1 | 42.1 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 21: Diskussion - PA (10. Aussage)*

| Phishing Awareness - 11) Ich bin mir des Risikos bewusst, das mit dem Öffnen und/oder Herunterladen von E-Mail-Anhängen verbunden ist. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 1 | .8 | .8 | .8 |
| | stimme nicht zu | 6 | 5.0 | 5.0 | 5.8 |
| | stimme weder zu noch stimme zu | 5 | 4.1 | 4.1 | 9.9 |
| | stimme zu | 62 | 51.2 | 51.2 | 61.2 |
| | stimme voll und ganz zu | 47 | 38.8 | 38.8 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 22: Diskussion - PA (11. Aussage)*

Anhand der nächsten Tabelle (siehe Tabelle 23) kann erkannt werden, dass 75% der Personen die Maus über einen Link in einer E-Mail bewegen und sich diese Adresse genau ansehen. Dieses Ergebnis zeigt auch, dass einige Teilnehmer und Teilnehmer eine gewisse Awareness bereits haben. Jedoch machen 25% Personen dies nicht, weil sie entweder dieses Wissen nicht haben oder es tatsächlich nicht ausführen. Erfahrungsgemäß zeigt diese Art der Überprüfung, wohin der Link in einer E-Mail eine Person weiterleitet, wenn dieser angeklickt wird (Patayo, 2021, p. 15).

| Phishing Awareness - 9) Ich scrolle über einen Link in der E-Mail und sehe mir die Adresse genau an, bevor ich auf den Link klicke. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 5 | 4.1 | 4.1 | 4.1 |
| | stimme nicht zu | 8 | 6.6 | 6.6 | 10.7 |
| | stimme weder zu noch stimme zu | 16 | 13.2 | 13.2 | 24.0 |
| | stimme zu | 50 | 41.3 | 41.3 | 65.3 |
| | stimme voll und ganz zu | 42 | 34.7 | 34.7 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 23: Diskussion - PA (9. Aussage)*

Als nächstes werden die Sicherheitsgewohnheiten der Teilnehmer und Teilnehmerinnen des Fragebogens näher betrachtet. Im Vergleich zu „Phishing Vertrautheit“ und „Phishing Awareness“ sind die „Sicherheitsgewohnheiten“ ein wenig schlechter ausgefallen. Denn die Abbildung 8 zeigt die zusammengefassten Ergebnisse der zwölf Aussagen und es kann festgestellt werden, dass der größte Teil der befragten Teilnehmer und Teilnehmerinnen die Wahl: „stimme weder zu noch stimme zu“ ausgewählt haben. Infolgedessen werden die einzelnen Aussagen genauer angesehen.

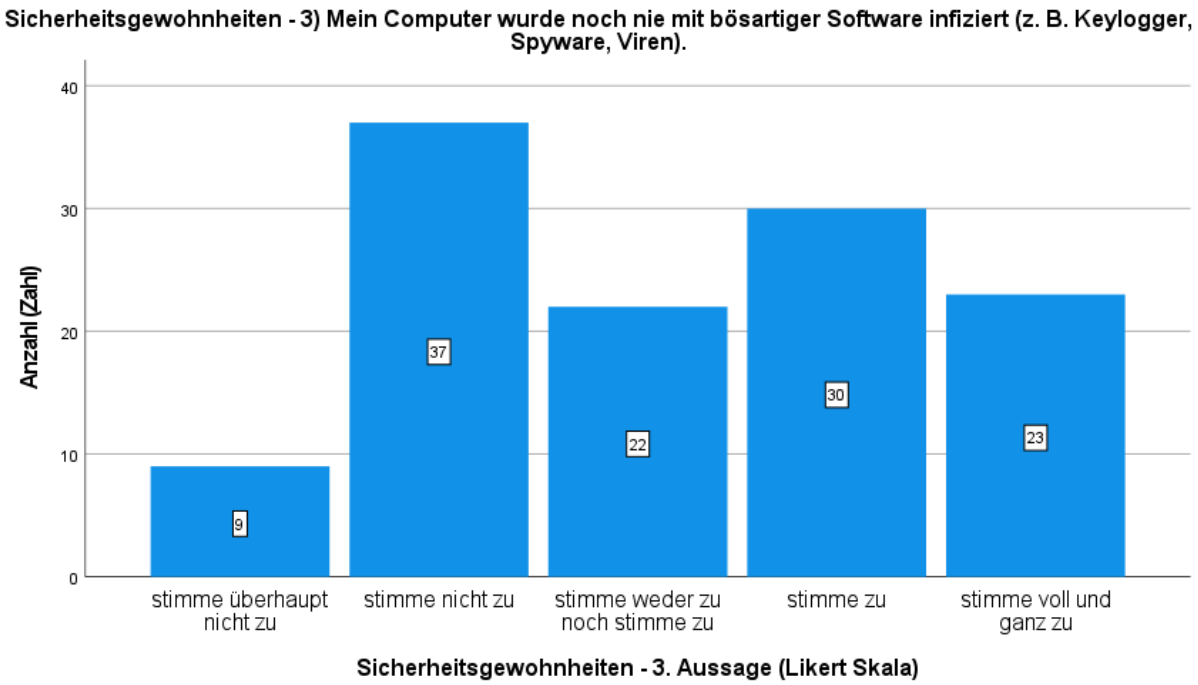



*Abbildung 41: Diskussion - SG (3. Aussage)*

Die dritte Aussage der „Sicherheitsgewohnheiten“ erklärt zum Teil wieso die Werte hierfür schlechter ausgefallen sind, denn einige Personen haben der Aussage: „Mein Computer wurde noch nie mit bösartiger Software infiziert (z.B. Keylogger, Spyware, Viren).“ zugestimmt (Abbildung 41). Als nächstes werden die Passwort Gewohnheiten der Teilnehmer und Teilnehmerinnen genauer betrachtet. Anhand der Tabelle 24 ist zu erkennen, dass mehr als 90% der Teilnehmer und Teilnehmerinnen die Merkmale für ein sicheres Passwort kennen.

| **Sicherheitsgewohnheiten - 5) Ich kenne die Merkmale eines sicheren Passworts.** | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme nicht zu | 2 | 1.7 | 1.7 | 1.7 |
| | stimme weder zu noch stimme zu | 9 | 7.4 | 7.4 | 9.1 |
| | stimme zu | 60 | 49.6 | 49.6 | 58.7 |
| | stimme voll und ganz zu | 50 | 41.3 | 41.3 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 24: Diskussion - SG (5. Aussage)*

Jedoch ist anhand der nächsten Tabellen ersichtlich, dass knappe 75% der Personen die Passwörter für ihre Online-Konten schon mindestens einmal aufgeschrieben haben (siehe Tabelle 25) und auch dazu tendieren, dass sie schwierige Passwörter, die nicht einfach zu merken sind, aufschreiben (siehe Tabelle 27). Des Weiteren verwenden mehr die Hälfte der befragten Personen auch ein Passwort für mehrere Online-Konten gleichzeitig (siehe Tabelle 26).

| Sicherheitsgewohnheiten - 6) Ich habe die Passwörter für alle meine Online-Konten noch nie aufgeschrieben, falls ich sie vergesse. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 21 | 17.4 | 17.4 | 17.4 |
| | stimme nicht zu | 47 | 38.8 | 38.8 | 56.2 |
| | stimme weder zu noch stimme zu | 16 | 13.2 | 13.2 | 69.4 |
| | stimme zu | 19 | 15.7 | 15.7 | 85.1 |
| | stimme voll und ganz zu | 18 | 14.9 | 14.9 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 25: Diskussion - SG (6. Aussage)*

| Sicherheitsgewohnheiten - 7) Ich verwende nicht dasselbe Passwort für mehrere Online-Konten (z. B. persönliches E-Mail-Konto, E-Mail-Konto bei der Arbeit, Konto für soziale Medien, Online-Shopping-Konto). | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 17 | 14.0 | 14.0 | 14.0 |
| | stimme nicht zu | 41 | 33.9 | 33.9 | 47.9 |
| | stimme weder zu noch stimme zu | 22 | 18.2 | 18.2 | 66.1 |
| | stimme zu | 28 | 23.1 | 23.1 | 89.3 |
| | stimme voll und ganz zu | 13 | 10.7 | 10.7 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 26: Diskussion - SG (7. Aussage)*

| Sicherheitsgewohnheiten - 9) Ich schreibe nie ein Passwort auf, das schwer zu merken ist. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | stimme überhaupt nicht zu | 18 | 14.9 | 14.9 | 14.9 |
| | stimme nicht zu | 45 | 37.2 | 37.2 | 52.1 |
| | stimme weder zu noch stimme zu | 19 | 15.7 | 15.7 | 67.8 |
| | stimme zu | 19 | 15.7 | 15.7 | 83.5 |
| | stimme voll und ganz zu | 20 | 16.5 | 16.5 | 100.0 |
| | Total | 121 | 100.0 | 100.0 | |

*Tabelle 27: Diskussion - SG (9. Aussage)*

Diese Ergebnisse erklären wieso die Werte für die „Sicherheitsgewohnheiten“ tendenziell schlechter ausgefallen sind als die Werte von „Phishing Vertrautheit“ und „Phishing Awareness“. Diese Erkenntnisse wurde zum Beispiel von Abroshan et al. (2018) angesprochen. Sie führten eine Reihe von Studien in realen Organisationen durch, um das Verhalten von Mitarbeiter und Mitarbeiterinnen im Umgang mit den Passwortrichtlinien ihrer Organisation zu untersuchen. Diese fanden heraus, dass Mitarbeiter und Mitarbeiterinnen dieselben oder ähnliche Passwörter wiederverwendeten und in den

schlimmsten Fällen das Passwort aufschrieben. Selbst bei strengen Sicherheitsrichtlinien bleibt ein Unternehmen also aufgrund dieser menschlichen Fehler anfällig für Cyberangriffe (Desolda *et al.*, 2021, p. 13). Der nächste Punkt, der besprochen wird, ist die Phishing Anfälligkeit der Teilnehmer und Teilnehmerinnen. Anhand der Abbildung 42 ist zu erkennen, dass 69 Personen (57%) mehr als die Hälfte der Beispiele richtig erkannt haben. Des Weiteren ist es wichtig zu erwähnen, dass mehr als die Hälfte der Teilnehmer und Teilnehmerinnen, die folgenden zwei URLs nicht richtig identifizieren konnten: „https://suppoort.apple.com/“ und „https://147.46.236.55/PayPal/login.html“ (siehe Abbildung 21 und Abbildung 23). Diese Erkenntnis bestätigt, dass die Teilnehmer und Teilnehmerinnen entweder nicht aufmerksam waren bei der Beantwortung von diesem Teil des Fragebogens oder dass das Wissen bezüglich der Phishing URLs tatsächlich fehlt. Aus diesem Grund wird im Leitfaden für die Phishing Schulung ein Augenmerk für den Schulungsinhalt bezüglich Phishing URLs gelegt. Weitere Erkenntnisse bezüglich der Phishing Anfälligkeit werden, nachdem die durchgeführten Phishing Schulungen und bevorzugten Schulungsmethoden besprochen wurden, im Rahmen der Beantwortung der Hypothesen wieder aufgegriffen. Wie bereits erwähnt wird nun auf die durchgeführten Schulungen und der verwendeten Schulungsmethoden eingegangen, die die Teilnehmer und Teilnehmerinnen innerhalb des Großunternehmens in Österreich erhalten haben.

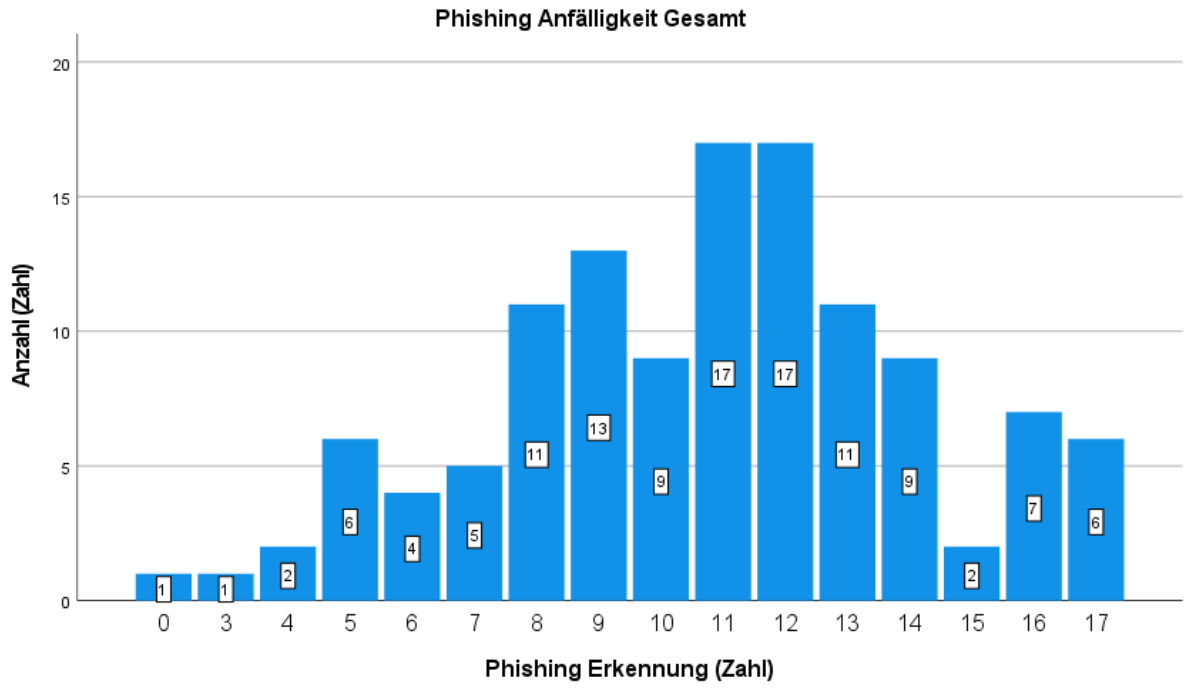



*Abbildung 42: Diskussion - PK (Gesamt)*

Sehr überraschende Ergebnisse liefert die Abbildung 35, denn fast die Hälfte der Teilnehmer und Teilnehmerinnen haben keine Phishing Schulung erhalten in dem Großunternehmen in denen sie tätig waren oder derzeit auch tätig sind. Aus diesem

Grund wurde die dritte Aussage der Phishing Vertrautheit näher betrachtet und es wurde festgestellt, dass wenigstens zwei Drittel der Teilnehmer und Teilnehmerinnen eine Art von Computer-/Informationssicherheit Schulung erhalten haben (siehe Abbildung 36). Die drei meisterhaltenen Schulungsmethoden in Großunternehmen sind die herkömmliche-, eingebettete- und Achtsamkeitsschulung (siehe Abbildung 37). Des Weiteren wurde festgestellt, dass bei fast mehr als die Hälfte der Personen die letzte erhaltene Phishing Schulung bereits länger als fünf Monate zurückliegen. Jedoch wird empfohlen, dass nach einem halben Jahr eine Auffrischung der Phishing Schulungen erfolgen sollte. Schließlich fanden Reinheimer et al. (2020) in ihrer Studie heraus, dass nach sechs Monaten keine korrekten Identifizierung von Phishing- und legitimen E-Mails der Teilnehmer und Teilnehmerinnen möglich war und die Autoren und Autorinnen haben empfohlen, dass eine Auffrischung der Phishing Schulung nach einem halben Jahr empfohlen wird (Reinheimer *et al.*, 2020, p. 259). In ähnlicher Weise stellten Canova et al. (2014) in ihrer Studie fest, dass nach fünf Monaten ein signifikanter Leistungsabfall bei den Teilnehmer und Teilnehmerinnen vorzufinden ist (Jampen *et al.*, 2020, p. 29). Schroeder (2017) hat folgenden Ratschlag erwähnt, dass jede Person mindestens viermal pro Jahr geschult werden soll (Jampen *et al.*, 2020, pp. 28–29). Demnach sollte die Hälfte der Teilnehmer und Teilnehmerinnen der Großunternehmen in Österreich, die bereits eine Phishing Schulung erhalten haben, eine Auffrischung der Kenntnisse erhalten. Des Weiteren sollte die Hälfte der befragten Personen, die keine Phishing Schulung erhalten haben, demnächst eine Schulung in Bezug auf Phishing erhalten.

Als nächstes wird die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen in den Großunternehmen in Österreich in Bezug auf die bevorzugten Phishing Schulungsmethoden näher betrachtet. Es ist aus der Tabelle 3 zu erkennen, dass die Teilnehmer und Teilnehmerinnen keine der vorgeschlagenen Phishing Schulungen eindeutig bevorzugen würden. Wie bereits oben angemerkt, angenommen es müsste anhand der Ergebnisse eine Entscheidung getroffen werden, würde die Achtsamkeitsschulung und die eingebettete Schulung ausgewählt werden. Die Ergebnisse können sich auch durch das Geschlecht oder der Teilnahme einer Phishing Schulung leicht unterscheiden. Männliche Teilnehmer würden sich für die Achtsamkeitsschulung entscheiden, weibliche Teilnehmerinnen würden die eingebettete Schulung bevorzugen. Personen, die bereits eine Phishing Schulung erhalten haben, würden die Achtsamkeitsschulung bevorzugen und die Personen, die noch keine Phishing Schulung erhalten haben, würden die eingebettete Schulungsmethode auswählen. Demzufolge kann festgestellt werden, dass die zwei bevorzugten Schulungsmethoden der Teilnehmer und

Teilnehmerinnen des Fragebogens folgende Methoden sind: „Eingebettete Schulungsmethode“ und „Achtsamkeitsschulung“.

Zuletzt werden die Hypothesen der Masterarbeit besprochen und etwaige Gemeinsamkeiten oder Unterschiede in bereits durchgeführten Studien hervorgehoben. Bei der der ersten Hypothese wurde die Nullhypothese: „Es gibt keine signifikanten Unterschiede zwischen der Phishing Anfälligkeit und dem Geschlecht.“ angenommen, weil der p-Wert des Mann-Whitney-U-Tests nicht signifikant war (siehe Tabelle 11). Es wurden bereits in vielen anderen Studien keine geschlechtsspezifischen Unterschiede in der Anfälligkeit von Phishing-Angriffen festgestellt wie z.B. in den folgenden Studien: „Kumaraguru et al., 2009“, „Zielinska et al., 2014“, „Gavett et al., 2017“, „Moody et al., 2017“, „Butavicius et al., 2017“, „Oliviera et al., 2017“ und „Parsons et al., 2019“ (Tornblad, Jones, *et al.*, 2021, p. 940). Es gibt auch Studien die geschlechtsspezifische Unterschiede festgestellt haben, dass Frauen z.B. anfälliger für Phishing-Angriffe sind als Männer. Es gibt auch wiederum Studien, die belegen, dass Männer eine höhere Phishing Anfälligkeit haben als Frauen (siehe Kapitel 2.3.7.1.1).

Anhand der Tabelle 12 ist zu erkennen, dass es einen signifikanten Unterschied zwischen der Phishing Anfälligkeit und der Teilnahme einer Phishing Schulung gibt, weil im Mann-Whitney-U-Test festgestellt wurde, dass der p-Wert kleiner als $p < 0{,}05$ beträgt. Dementsprechend wurde bei der zweiten Hypothese die Nullhypothese verworfen und die Alternativhypothese: „Es gibt signifikante Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme einer Phishing Schulung.“ angenommen. Es gibt einige Studien, die die gleichen Ergebnisse erzielten wie z.B. die Forschungsergebnisse von Wright und Marett (2010). Diese Studie zeigte, dass Schulung unter anderem das wirksamste Mittel zum Schutz vor Phishing ist (Miller *et al.*, 2020, p. 2). Goel et al. (2017) haben Beweise dafür gefunden, dass die Aufklärung über gängige Phishing-Praktiken die Wahrscheinlichkeit verringert ein Opfer eines Phishing-Angriff zu werden (Goel, Williams and Dincelli, 2017, p. 26). In ähnlicher Weise fanden Caputo et al. (2014) heraus, dass die Klickrate auf Phishing-Links nach einer Schulung um 63% zurückging (Kwak *et al.*, 2020, pp. 1–2). Bei der Masterarbeit wurde nur die allgemeine Betrachtung, ob eine Phishing Schulung durchgeführt worden ist oder nicht, analysiert. Jedoch wurden im theoretischen Teil auch die Ergebnisse von vergangenen Studien zu den einzelnen Schulungsmethoden zusammengefasst (siehe Kapitel 2.3.6.4).

Die nächsten drei Hypothesen beschäftigen sich mit den Faktoren: „Phishing Vertrautheit“, „Phishing Awareness“ und „Sicherheitsgewohnheiten“ in Bezug auf

„Phishing Anfälligkeit“. Die Hypothesen wurden mittels der Spearman Korrelation getestet und dabei wurde festgestellt, dass nur bei „Phishing Vertrautheit“ ein signifikanter Zusammenhang in Bezug auf „Phishing Anfälligkeit“ besteht (siehe Tabelle 13). Aus diesem Grund wurde die Nullhypothese bei der dritten Hypothese verworfen und die folgenden Alternativhypothese: „Es gibt signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit.“ angenommen. Bei der vierten und fünften Hypothese wurde jeweils die Alternativhypothese verworfen und folgende Nullhypothesen: „Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Awareness.“ und „Es gibt keine signifikanten Zusammenhänge zwischen der Phishing Anfälligkeit und der Sicherheitsgewohnheit.“ angenommen, denn hier wurden keine signifikanten Ergebnisse ermittelt (siehe Tabelle 13).

Der Zusammenhang zwischen „Phishing Vertrautheit“ und „Phishing Anfälligkeit“ wurde auch von zwei anderen Studien bestätigt. Gavett et al. (2017) fanden heraus, dass Personen mit Vorwissen über Phishing und/oder die bereits Opfer eines Phishing-Angriffs waren, mehr misstrauisch gegenüber Phishing-Angriffen sind als diejenigen ohne diesem Vorwissen (Tornblad, Jones, *et al.*, 2021, p. 940). Wang et al. (2012) zeigten ebenfalls, dass mit zunehmendem Wissen über Phishing-Betrügereien die Wahrscheinlichkeit sinkt, dass die Personen auf Phishing hereinfallen (Tornblad, Jones, *et al.*, 2021, p. 940).

Hinsichtlich des Zusammenhangs zwischen „Phishing Awareness“ und „Phishing Anfälligkeit“ wurde folgendes aus dem theoretischen Teil entnommen. Alnajim und Munro (2009) fanden heraus, dass die Awareness einen erheblichen Einfluss auf die Effektivität der Nutzer und Nutzerinnen bei der Unterscheidung zwischen legitimen Websites und Phishing-Websites hat (Abbasi *et al.*, 2021, p. 412). Diese Studie bezog sich zwar auf die Erkennung von Websites und die im Rahmen dieser Masterarbeit durchgeführte Studie wiederum bezog sich auf URLs zur Erkennung von Phishing, jedoch konnten hierbei keine signifikanten Ergebnisse erzielt werden. Eine zweite Studie die den Zusammenhang zwischen den beiden Faktoren bestätigt ist die von Halevi et al. (2015). Die Autoren und Autorinnen bestätigten, dass die Awareness den Teilnehmer und Teilnehmerinnen dabei half, nicht Opfer von Phishing zu werden, da die Probanden mehr darauf bedacht waren sich zu schützen (Jampen *et al.*, 2020, p. 12). Ein letztes Beispiel hierzu ist von Alwanain (2019). Die Ergebnisse dieser Studie zeigten eindeutig einen hohen und signifikanten Effekt auf die Phishing Awareness der Nutzer und Nutzerinnen. Denn die Ergebnisse zeigten, dass Phishing-E-Mails korrekt identifiziert wurden und dadurch ein Phishing-Angriff vermieden werden konnte. Dies führte zu einer höheren

Phishing-Vermeidungsrate bei den Nutzer und Nutzerinnen mit Phishing-Awareness im Vergleich zu denen mit weniger Awareness (M. I. Alwanain, 2019, p. 327). Jedoch konnten diese Art von Ergebnissen bzw. der Zusammenhang zwischen „Phishing Awareness“ und „Phishing Anfälligkeit“ in der Studie der Masterarbeit nicht erkannt werden.

Abschließend werden zu „Sicherheitsgewohnheiten“ folgende passende Studien vom theoretischen Teil hervorgehoben. Bakhshi et al. (2009) führten ein E-Mail-basiertes Experiment durch, bei dem 152 Mitarbeiter und Mitarbeiterinnen eine Nachricht erhielten, in der sie aufgefordert wurden, einem Link zu einer externen Website zu folgen und ein angebliches Software-Update zu installieren. Die Ergebnisse zeigten, dass 23% der Empfänger und Empfängerinnen auf den Angriff hereinfielen, was darauf hindeutet, dass vielen Nutzer und Nutzerinnen eine grundlegende Sicherheit fehlt, das für den Online-Schutz erforderlich ist (Purkait, Kumar De and Suar, 2014, pp. 200–201). Albladi und Weir (2018) fanden heraus, dass Bildung, Computerkenntnisse und Sicherheitsgewohnheiten als die wichtigsten Faktoren für den Schutz der Nutzer und Nutzerinnen vor Cyberangriffen angesehen wurden (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021, p. 9). Jedoch konnte in der Masterarbeit kein signifikanter Zusammenhang zwischen „Sicherheitsgewohnheiten“ und „Phishing Anfälligkeit“ festgestellt werden.

## 3.5 Leitfaden für Phishing Schulung

In diesem Kapitel wird ein Leitfaden für eine SETA-Schulung anhand der Literaturrecherche und der Ergebnisse und Auswertungen des Fragebogens für Großunternehmen in Österreich erstellt. Es werden dabei die wichtigsten Informationen aus der Literatur für eine erfolgreiche Schulung zusammengefasst. Dieser Leitfaden soll nur als eine Empfehlung bzw. eine Richtlinie für Unternehmen dienen und soll auf das jeweilige Unternehmen angepasst werden. Dieser Leitfaden kann auch auf Klein- und Mittelbetriebe (KMU) in Österreich umgesetzt werden.

Die Literatur zur technischen und nicht-technischen Anti-Phishing Methoden hat ergeben, dass die Methoden aus mehreren Verteidigungsebenen (technisch und nicht-technisch) bestehen soll (Brickley, Thakur and Kamruzzaman, 2021, p. 38). Demnach sollte bei der Abwehr von Phishing-Angriffen mehrere Verteidigungsebenen (Defense-in-Depth) eingesetzt werden, da jede Ebene ihre Stärken und Schwächen hat (Jampen *et al.*, 2020, p. 7). Einige der aktuellen Verteidigungsansätze umfassen die Verbesserung der physischen Sicherheit und die Verbesserung der Sicherheitsrichtlinien sowie

kontinuierliche Awareness- und Schulungsprogrammen für den Umgang mit Phishing Vorfällen. Ghafir et al. (2016) hat ebenfalls vorgeschlagen, dass all diese Ansätze und Techniken zusammengesetzt werden sollten, um mögliche Risiken in Bezug auf Phishing-Angriffe zu verringern. In ähnlicher Weise stellten Conteh und Schmick (2016) fest, dass mehrere Verteidigungsebenen mit technischen und nicht-technischen Maßnahmen gegen Social-Engineering-Angriffe wirksam sind (Papatsaroucha *et al.*, 2021, p. 25).

Ein wesentlicher Aspekt einer solchen Abwehrstrategie wäre die Schulung der Mitarbeiter und Mitarbeiterinnen eines Unternehmens in Bezug auf Phishing und die Stärkung ihrer Fähigkeit Phishing-Angriffe zu erkennen (Jampen *et al.*, 2020, p. 7). Jedoch können moderne Schulungstechniken, wie Spiele und virtuelle Labore, themenbezogene Videos oder Simulationen realer Szenarien, für die Mitarbeiter und Mitarbeiterinnen zeitaufwändig und stressig sein (aufgrund des hohen Arbeitsdrucks und der Dringlichkeit von Fristen ihrer Tätigkeiten). Es kann auch vorkommen, dass Schulungen möglicherweise nicht einfach gestaltet sind und somit von Mitarbeiter und Mitarbeiterinnen ohne IT-Hintergrund nicht verstanden werden können. Möglicherweise gehen die Schulungen auch nicht auf die individuellen Schwachstellen der einzelnen Personen innerhalb des Unternehmens ein. Herkömmliche Schulungen werden auch oft als langweilig und ermüdend beschrieben. Dennoch stellten Aldawood und Skinner (2020) fest, das Phishing Schulungen wichtig sind. Denn die Autoren und Autroinnen befragten 21 Cybersicherheitsexperten und -expertinnen mit dem Ziel, die kritischsten Schwachstellen im Bereich der Cybersicherheit zu ermitteln und erreichbare Abhilfestrategien zu untersuchen. Die meisten der befragten Personen stimmten darin überein, dass die größte Bedrohung für die Cybersicherheit die menschlichen Schwachstellen einer Person sind. Des Weiteren erwähnten sie, dass die mangelnde Awareness der Person die Cyberverteidigung verkompliziert und erschwert. Aus diesem Grund haben Cybersicherheitsexperten und -expertinnen für die Gegenmaßnahmen Phishing Schulungen vorgeschlagen. Darüber hinaus betonten sie die Notwendigkeit einer kontinuierlichen Schulung sowie die Notwendigkeit, die Mitarbeiter und Mitarbeiterinnen zur Teilnahme an solchen Programmen zu motivieren (Papatsaroucha *et al.*, 2021, pp. 29–30).

Bei so vielen Faktoren, die sich auf die Anfälligkeit des Menschen auswirken und von dem beeinflusst werden, ist es von entscheidender Bedeutung, dass die Phishing Schulungen individuell gestaltet werden, da jeder Mensch für unterschiedliche Cyber-Bedrohungen anfällig ist und über unterschiedliche Computerkenntnisse und -fähigkeiten verfügt (Papatsaroucha *et al.*, 2021, p. 22). Mitarbeiter und Mitarbeiterinnen werden häufig als

das schwächste Glied in der Cybersicherheit eines Unternehmens angesehen und die Unterschiede in der Persönlichkeit der Mitarbeiter Mitarbeiterinnen machen es jedem Unternehmen schwer, eine geeignete Strategie für die Bekämpfung von Phishing-Angriffen zu entwickeln. Darüber hinaus beeinflussen die allgemeine Lebenserfahrung und die technologische Erfahrung der Mitarbeiter und Mitarbeiterinnen auch die Persönlichkeitsmerkmale der jeweiligen Personen. Mitarbeiter und Mitarbeiterinnen sind aufgrund ihrer Anfälligkeit für verschiedene emotionale und kontextbezogene Auslöser leichtere Ziele, und können dabei beim Umgang mit den E-Mails bestimmte Sicherheitsanforderungen missachten (Anawar *et al.*, 2019, pp. 2865–2866). Zwar können technische Anti-Phishing Methoden das Risiko mindern, doch wenn eine Phishing-E-Mail diese Barrieren überwindet, stellen die Mitarbeiter und Mitarbeiterinnen die letzte Verteidigungslinie dar. Aus diesen Gründen ist die SETA-Schulung für Mitarbeiter und Mitarbeiterinnen von entscheidender Bedeutung (Gordon *et al.*, 2019, p. 551).

Es gibt mehrere Leitlinien für Unternehmen, um ein SETA-Programm zu entwickeln. Diese Ansätze lassen sich laut Alshaikh, Maynard and Ahmad, (2021) in drei grundlegende Phasen unterteilen: (1) Entwicklung, (2) Umsetzung und (3) Bewertung (Alshaikh, Maynard and Ahmad, 2021, p. 2).

- Die Entwicklungsphase umfasst Aktivitäten, die dazu dienen, die aktuelle organisatorische Situation zu verstehen, die Unterstützung des Managements zu erhalten und Ressourcen für die Entwicklung eines effektiven Programms zu beschaffen. Zu diesen Aktivitäten gehören die Durchführung einer Bedarfsanalyse für ein SETA-Programm (zu den auch gesetzlichen Anforderungen gehören können), die Festlegung von Zielen, die Zusammenstellung des SETA-Entwicklungsteams und die Identifizierung der Zielgruppe für ein SETA-Programm. Zu den Aktivitäten der Entwicklungsphase gehört auch die Entwicklung von Materialien für eine SETA-Schulung (Alshaikh, Maynard and Ahmad, 2021, p. 2).
- Die Umsetzungsphase konzentriert sich auf die Durchführung des SETA-Programms, dabei können unterschiedliche Lehrmethoden verwendet werden (Alshaikh, Maynard and Ahmad, 2021, p. 2).
- Die letzte SETA-Phase ist die Bewertung, in der das Unternehmen ihre SETA-Initiativen überprüft und bewertet, um deren Wirksamkeit zu messen. Die Effektivität wird in der Regel dadurch gemessen, dass die Phishing Anfälligkeiten der Mitarbeiter und Mitarbeiterinnen festgestellt werden. Best-Practice-Normen wie ISO/IEC 27002 betonen die Notwendigkeit von SETA-Programmen und

empfehlen, dass alle Mitarbeiter eines Unternehmens eine angemessene Awareness, Bildung und Schulung sowie eine regelmäßige Aktualisierung der Unternehmensrichtlinien und -verfahren erhalten sollten, die für ihre jeweilige Funktion relevant sind. Die Normen bieten jedoch keine klare und praktische Anleitung, wie SETA-Programme umgesetzt werden sollten (Alshaikh, Maynard and Ahmad, 2021, pp. 2–3). Aufgrund dessen wurde mithilfe des theoretischen Teils und der Literaturrecherche die wichtigsten Punkte für ein erfolgreiches SETA-Programm in diesem Leitfaden zusammengefasst.

Ein SETA-Programm sollte die Informationssicherheitsstrategie des Unternehmens vorantreiben und die Vision in die Realität umsetzen. Es sollte die Mitarbeiter und Mitarbeiterinnen dazu bringen, die Vision der Sicherheit zu teilen und eine Sicherheitskultur innerhalb des Unternehmens aufzubauen. Unternehmen stehen jedoch vor der Herausforderung, dass die Mitarbeiter und Mitarbeiterinnen nur eine begrenzte Menge an Aufmerksamkeit für Schulungsprogramme wie SETA aufbringen können. Der Umfang der Schulungen hat zugenommen, und die Mitarbeiter und Mitarbeiterinnen müssen in mehreren Bereichen wie Gesundheit und Sicherheit am Arbeitsplatz, sexuelle Belästigung, Diskriminierung und Datenschutz geschult werden. Die Folge davon ist, dass es für die Mitarbeiter und Mitarbeiterinnen schwierig ist, sich zu konzentrieren und sich die vermittelten Informationen in einer SETA-Schulung zu merken. Daher sollte auf die Verwendung verschiedener Methoden und auf das Miteinbeziehen einer kreativen und innovativen Lehrweise, im Hinblick auf wie das Unternehmen ein SETA-Programm durchführt, geachtet werden. Des Weiteren sollte die Effektivität des SETA-Programms durch Reduzierung des Inhalts und Erhöhung der Motivation gesteigert werden. Eine Möglichkeit der Motivationssteigerung ist, dass eine Verknüpfung der Informationssicherheit mit dem persönlichen Leben der Mitarbeiter und Mitarbeiterinnen erfolgt. Zum Beispiel kann das Unternehmen bei der Schulung für die Unternehmensrichtlinien zur Nutzung sozialer Medien (z.B. Facebook und Twitter) sicherstellen, dass das Programm auf Themen wie die Sicherheit von Personen und Kindern bei der Nutzung sozialer Medien eingeht. Eine weitere Möglichkeit der Effektivitätssteigerung liegt darin, sich auf Mitarbeiter und Mitarbeiterinnen zu konzentrieren, die mit sensiblen Informationen und Prozessen innerhalb des Unternehmens auseinandersetzen. In einigen Unternehmen besteht das Hauptziel darin, diese Personen zu identifizieren und ein SETA-Programm zu entwickeln, das auf sie ausgerichtet ist, um die Informationen und Prozesse zu schützen. Ein SETA-Programm sollte auch auf die Bedürfnisse der einzelnen Zielgruppen in Bezug auf den Inhalt, die

Länge/Dauer, die Häufigkeit und die Durchführungsmethoden zugeschnitten sein. Eine SETA-Schulung für die Führungsebene wäre zum Beispiel kurz und prägnant (Alshaikh, Maynard and Ahmad, 2021, pp. 7–9). Nun werden die einzelnen Schritte des SETA-Programmes näher erläutert.

Der Prozess für ein SETA-Programm besteht laut Alshaikh, Maynard and Ahmad, (2021) aus zehn Schritten, die in fünf Phasen unterteilt sind: Ermittlung, Auswahl, Verständnis, Gestaltung und Management (Alshaikh, Maynard and Ahmad, 2021, p. 10).

Die Ermittlungsphase zielt darauf ab, grundlegendes Wissen über die Themen und Probleme aufzubauen. Die Ermittlungsphase besteht aus zwei Schritten: 1) Beschreibung des Themas, Hintergrunds, Zwecks und Schwerpunkts und 2) Durchführung einer Situationsanalyse (Alshaikh, Maynard and Ahmad, 2021, p. 10).

- Schritt 1: Hierbei soll das Unternehmen das bestehende Problem beschreiben und wichtigsten Informationen zu dem Problem zusammenfassen. Ein Beispiel hierfür: Jüngste Sicherheitsberichte zeigen, dass 90% der gesamten Sicherheitsvorfälle innerhalb des Unternehmens durch das Anklicken von Phishing-Links durch Mitarbeiter und Mitarbeiterinnen verursacht wurde. Demnach hat unser Unternehmen einen Betrag von X an Geld/Daten/Reputation verloren, weil Mitarbeiter und Mitarbeiterinnen die Richtlinien unseres Unternehmens zum Umgang mit Phishing-E-Mails nicht eingehalten haben. Der übergeordnete Zweck des Programmes liegt in der Bekämpfung von Phishing-Angriffen und soll unser Unternehmen schützen, indem die Erkennung der Mitarbeiter von Phishing-E-Mails verbessert wird (Alshaikh, Maynard and Ahmad, 2021, p. 11).
- Schritt 2: Durchführung einer Situationsanalyse. Sobald der Zweck und der Schwerpunkt des SETA-Programmes beschrieben sind, sollte das Team damit beginnen, die externen und internen Faktoren zu analysieren, die den Planungsprozess des Programmes beeinflussen könnten. Es wird eine SWOT-Analyse (Stärken, Schwächen, Chancen und Gefahren) durchgeführt, um die Stärken des Unternehmens zu ermitteln und diese zu maximieren, die Schwächen zu minimieren, die Chancen zu nutzen und die Gefahren zu überwinden. Bei den Stärken und Schwächen handelt es sich um interne Faktoren (z.B. verfügbare Ressourcen, Fachwissen, Unterstützung durch das Management, bestehende Allianzen und Partner), während die Chancen und Gefahren externe Faktoren darstellen. Das Ergebnis der Analyse sollte eine Liste von Faktoren sein, an denen

sich der Planungsprozess des SETA-Programmes orientieren wird (Alshaikh, Maynard and Ahmad, 2021, p. 11).

Die Auswahlphase besteht aus zwei Schritten: 1) Auswahl der Zielgruppen und 2) Festlegung von Verhaltenszielen und Zielvorgaben (Alshaikh, Maynard and Ahmad, 2021, p. 11).

- Schritt 1: Die Zielgruppe für das SETA-Programm ist die Gruppe, auf deren Verhalten das Programm ausgerichtet ist. Die Ausarbeitung einer gründlichen Beschreibung der Zielgruppe umfasst die Bestimmung ihrer Demografie, ihrer sozialen Netzwerke und ihrer Größe (Alshaikh, Maynard and Ahmad, 2021, p. 11).
- Schritt 2: Sobald die Zielgruppe ausgewählt und beschrieben ist, sollte das Team spezifische Verhaltensziele und Zielvorgaben festlegen, die erreicht werden sollen. Phishing-Kampagnenstrategien sollten so entwickelt werden, dass sie drei Arten von Zielen unterstützen: (a) Wissensziele zur Awareness (z.B. was sind Phishing-Angriffe, welche Risiken stellen Phishing-E-Mails für die Systeme dar, wie erkennt man Phishing-E-Mails und wie werden Phishing-E-Mails am besten gemeldet), (b) Überzeugungsziele, um die Zielgruppe davon zu überzeugen, dass das Anklicken eines Phishing-Links negative Folgen für die Systeme hat, und (c) Verhaltensziele, um die Zielgruppe zu einer Änderung ihres Verhaltens zu bewegen (Alshaikh, Maynard and Ahmad, 2021, p. 12).

Die Verständnisphase besteht aus einem Schritt (Alshaikh, Maynard and Ahmad, 2021, p. 12):

- Schritt 1: Nach der Auswahl der Zielgruppe und des gewünschten Verhaltens ist es an der Zeit, die Zielgruppe in Bezug auf das gewünschte Verhalten zu verstehen. Das SETA-Team sollte Fragen stellen, um das vorhandene Wissen über Phishing-Angriffe, die Gründe für das Anklicken von Links und die Gründe für das nicht melden von Phishing-E-Mails, zu ermitteln (Alshaikh, Maynard and Ahmad, 2021, p. 12).

Die Gestaltungsphase umfasst zwei Schritte: 1) Entwicklung einer Stellungnahme und 2) Entwicklung einer Strategie (Alshaikh, Maynard and Ahmad, 2021, p. 12).

- Schritt 1: Die Aussage zur Stellungnahme bei Phishing-Angriffen könnte lauten: Unser Unternehmen möchte den Mitarbeiter und Mitarbeiterinnen die schwerwiegenden Folgen durch das Anklicken von Phishing-Links mitteilen und

dass eine angemessene Reaktion auf Phishing-E-Mails (das Anklicken von Links vermeiden und diese melden) das Unternehmen schützt (Alshaikh, Maynard and Ahmad, 2021, pp. 12–13).

- Schritt 2: Eine Strategie könnte darin bestehen, einen neuen Dienst (Melde- und Unterstützungsdienste) für Mitarbeiter und Mitarbeiterinnen einzurichten, die beim Verdacht einer Phishing-E-Mail diese an ein Helpdesk weiterzuleiten. Sobald die gemeldete Phishing-E-Mail beim Helpdesk eingeht, wird sie geprüft, und wenn es sich tatsächlich um eine Phishing-E-Mail handelt, erhält der Mitarbeiter oder die Mitarbeiterin eine E-Mail, in dem sich für die Hilfe beim Schutz des Unternehmens bedankt wird (Alshaikh, Maynard and Ahmad, 2021, p. 13).

Die Verwaltungsphase besteht aus drei Schritten: 1) Entwicklung eines Überwachungs- und Bewertungsplans, 2) Aufstellung eines Budgets und Suche nach Finanzierungsquellen und 3) Entwicklung eines Durchführungsplans (Alshaikh, Maynard and Ahmad, 2021, p. 13).

- Schritt 1: Der Überwachungs- und Bewertungsplan sollte Maßnahmen enthalten, mit denen der Erfolg des SETA-Programmes bewertet werden soll, sowie Angaben dazu, wie und wann diese Messungen vorgenommen werden. Die Entwicklung eines solchen Plans ist von entscheidender Bedeutung. Das Ziel der Phishing-Schulung besteht darin, die Zahl der Meldungen zu erhöhen und die Zahl der Klicks auf Phishing-Links zu verringern (Alshaikh, Maynard and Ahmad, 2021, p. 13). Es können folgende Werte z.B. erhoben werden: Die Anzahl der Mitarbeiter und Mitarbeiterinnen, die die Phishing-E-Mail geöffnet haben. Die Anzahl der Personen, die auf den Link in der Phishing-E-Mail geklickt haben. Die Anzahl der Mitarbeiter und Mitarbeiterinnen, die auf die Phishing-E-Mail geantwortet haben. Die Anzahl der Mitarbeiter und Mitarbeiterinnen pro Abteilung, die der Phishing-E-Mail zum Opfer gefallen sind. Die Anzahl der Personen, die den Anhang der Phishing-E-Mail geöffnet und heruntergeladen haben (Miranda, 2018, p. 8).
- Schritt 2: Das SETA-Team sollte das Budget für die mit der Phishing-Kampagne verbundenen Kosten aufstellen. Dazu gehören in der Regel die Kosten für die Segmentierung und das Verständnis der Zielgruppe, die Gestaltung der Produkte (z. B. Poster), die Schulungen sowie die Überwachung und Bewertung (Phishing-Simulationsübungen) (Alshaikh, Maynard and Ahmad, 2021, p. 13).
- Schritt 3: Der Durchführungsplan enthält detaillierte Informationen über die Rollen und Zuständigkeiten (wer macht was), spezifische Aufgaben und den Zeitplan des SETA-Programmes (Alshaikh, Maynard and Ahmad, 2021, p. 14).

Schulungen zur Erkennung und Meldung von Phishing-E-Mails sind ein Bestandteil des Schulungsprogramms eines Unternehmens zur Informationssicherheit. Laut dem Cybersecurity Framework des National Institute of Standards and Technology (NIST) ist die Schulung und Bildung aller Benutzer und Benutzerinnen in Bezug auf die Awareness für Cybersicherheit und die damit verbundenen Verantwortlichkeiten ein wesentlicher Bestandteil für die Cybersecurity. Außerdem sollten neue Mitarbeiter und Mitarbeiterinnen so schnell wie möglich geschult und die Schulungen für alle beteiligten Personen in regelmäßigen Abständen wiederholt werden (Miranda, 2018, p. 7). Ein umfassendes Schulungsprogramm sollte auch abseits von den zehn Schritten des SETA-Programmes die folgenden Punkte berücksichtigen:

- Für den entscheidenden Erfolg der Phishing-Schulung ist es wichtig, die ethische Freigabe und die Zustimmung der Unternehmensleitung zu erhalten. Ein formeller Projektvorschlag, in dem die Aspekte wie der grundlegende Prozess, verschiedene Phasen, Erfolgsmessungen und mögliche Risiken detailliert beschrieben sind, sollte ebenfalls der Geschäftsleitung zur Genehmigung vorgelegt werden (Kearney and Kruger, 2013, p. 384).
- Bevor Phishing Tests innerhalb eines Unternehmens durchgeführt werden, müssen die Mitarbeiter und Mitarbeiterinnen geschult werden, bevor die Fähigkeiten zur Erkennung von Phishing-Angriffen getestet werden kann (Miranda, 2018, p. 7).
- Die Phishing Beispiele sollte an die Branche des Unternehmens angepasst werden. Die effektivsten Phishing-E-Mails sind diejenigen, die auf die Tätigkeiten des Unternehmens oder der Mitarbeiter und Mitarbeiterinnen zugeschnitten sind. So würde beispielsweise ein Mitarbeiter oder eine Mitarbeiterin im Energiesektor eher auf eine Phishing-E-Mail reagieren die sich auf Solarpaneele bezieht, als auf Schwimmzubehör (Miranda, 2018, p. 8).
- Das Testen der Schulungsmethoden ist entscheidend für die Validierung der Schulungs- und Berichtsziele. Daher sollten die Phishing-E-Mail-Beispiele in der Lage sein, die aktuellen E-Mail- und Netzwerksicherheiten zu umgehen. Die Aufnahme von Phishing-E-Mail-Servern in die Whitelist oder die Anpassung anderer E-Mail-Transportkonfigurationen kann erforderlich sein. Es muss jedoch darauf geachtet werden, dass Konfigurationsänderungen nicht versehentlich dazu führen, dass bösartige Phishing-E-Mails die E-Mail- und Netzwerksicherheitskontrollen umgehen können (Miranda, 2018, p. 9). Außerdem

soll die Privatsphäre der befragten Mitarbeiter und Mitarbeiterinnen und ihrer Daten gewahrt werden (Kearney and Kruger, 2013, p. 384).

- Schulungsmethoden wie z.B. Eingebettete Schulungen müssen angemessen gehandhabt werden, damit die wichtigsten beteiligten Personen in einem Unternehmen diese von tatsächlichen Phishing-Vorfällen unterscheiden können. Für den Umgang mit Phishing-Übungen sollte ein unabhängiger Übungsreaktionsplan entwickelt werden. Zu den wichtigsten Komponenten des Plans gehören. Jede Phishing-Übungs-E-Mail sollte mit einer versteckten Markierung versehen werden. Anhand dieser Markierung können die Sachbearbeiter und -bearbeiterinnen feststellen, ob eine gemeldete Phishing-E-Mail echt oder eine Übungs-E-Mail ist. Die Kennzeichnung sollte außerdem regelmäßig oder bei jeder Phishing-Übung geändert werden. Bei der Markierung kann es sich um eine eindeutige Zahlenfolge oder versteckte Kommentare im HTML-Code handeln. Diese Kennzeichnung sollte unter den durchführenden Personen der Schulung und den beteiligten Personen vertraulich bleiben (Miranda, 2018, p. 9).
- Des Weiteren sollten das Informationssicherheitsteam, der Helpdesk und andere wichtige Personen einen Mitarbeiter oder eine Mitarbeiterin zunächst nicht darüber informieren, dass es sich bei einer E-Mail um eine Übungs-E-Mail handelt. Denn die getesteten Personen können andere Personen im Unternehmen warnen und diese Personen könnten die Übungs-E-Mail ignorieren (Miranda, 2018, p. 9).
- Die Übungen sollten so geplant werden, dass möglichst viele Mitarbeiter und Mitarbeiterinnen die Übungs-E-Mail innerhalb eines kurzen Zeitraums erhalten und öffnen. Eine Empfehlung für Unternehmen die von Montag bis Freitag zu den üblichen Arbeitszeiten arbeiten, wäre die Übung an einem Dienstag zu starten und 72 Stunden lang Daten zu sammeln (Miranda, 2018, p. 10).

Nachdem die wichtigsten Informationen bezüglich der Gestaltung eines SETA-Programmes zusammengefasst worden sind, wird als nächstes die Schulungsmethode ausgewählt. Die ausgewählte Schulungsmethode wurde anhand der Ergebnisse und Auswertung der Teilnehmer und Teilnehmerinnen des Fragebogens für Großunternehmen in Österreich ermittelt. Die zwei bevorzugtesten Schulungsmethoden der befragten Personen sind die „Eingebettete Schulungsmethode“ und die „Achtsamkeitsschulung“.

Kumaraguru et al. (2009) fanden heraus, dass "eingebettete" Schulungen, bei denen reale Angriffe in einer alltäglichen Arbeitsumgebung simuliert wurden, für die Nutzer und

Nutzerinnen effizienter sind, um die Informationen zu lernen und zu merken. Es stellte sich heraus, dass diese Vorgehensweise effektiver war als Schulungen, die nur auf Lehrmaterial basieren. Durch eingebettete Schulungen wird das Thema Sicherheit in den Vordergrund der täglichen Arbeit gerückt und stellt sicher, dass es Teil der Entscheidungsprozesse bleibt (Sebescen and Vitak, 2017, pp. 9–10). Bei eingebetteten Schulungen muss das Schulungsmaterial angezeigt werden, sobald ein Fehler gemacht wird, z.B. unmittelbar nach dem Anklicken eines Links in einer Phishing-E-Mail. Alternativ kann das Schulungsmaterial erst angezeigt werden, nachdem die angestellten Personen die Anmeldedaten auf einer gefälschten Anmeldeseite eingegeben haben. Jedoch können Mitarbeiter und Mitarbeiterinnen auf einen Link klicken und die Anmeldedaten nicht eingeben, dennoch bräuchten diese Personen eine Schulung, weil sie den Phishing-Versuch anhand des E-Mail-Inhalts und des Links erkennen sollten. Das Schulungsmaterial sollte den Mitarbeiter und Mitarbeiterinnen erklären, warum die Schulung nun durchgeführt wird und wie sie den Phishing-Versuch erkennen können. Wenn ein Mitarbeiter oder eine Mitarbeiterin nicht auf die Phishing-E-Mail klickt, sie aber auch nicht meldet, sollte Schulungsmaterial bezüglich des Meldens von Phishing-E-Mails angezeigt werden. Hierbei sollte auch erklärt werden, wieso das Melden von Phishing-E-Mails wichtig ist. Die Schulung sollte als fortlaufender Prozess konzipiert werden und viermal im Jahr durchgeführt werden. Schroeder et al. (2017) hat folgendes zu den Intervallen erwähnt: Die Intervalle sollten so gewählt werden, dass die Mitarbeiter und Mitarbeiterinnen nicht durch zu häufige Wiederholungstests genervt werden, aber dennoch die vom Management gestellten Anforderungen erfüllen (Jampen *et al.*, 2020, pp. 30–31).

Unternehmen verwenden häufig regelbasierte Schulungen, in denen die Mitarbeiter und Mitarbeiterinnen lernen, bestimmte Hinweise zu erkennen oder eine Reihe von Regeln anzuwenden, um Phishing-Angriffe zu vermeiden. Der regelbasierte Ansatz hat die Abwehr von Phishing-Angriffen in Unternehmen verbessert, allerdings führt die regelmäßige Wiederholung von diesen Schulungen nicht unbedingt zu einer höheren Widerstandsfähigkeit gegen Phishing-Angriffe. Forscher und Forscherinnen haben daher vorgeschlagen, den Schwerpunkt auf Vorsichtsmaßnahmen für die Mitarbeiter und Mitarbeiterinnen zu legen (z.B. Verhaltensschulung). Jensen et al. (2017) nutzten die Achtsamkeitsschulung, um einen neuartigen Schulungsansatz zu entwickeln. Dieser Ansatz soll durchgeführt werden, nachdem Personen mit der regelbasierten Schulung (wie der eingebetteten Schulung) vertraut sind. Die eingebettete Schulung und die Achtsamkeitsschulung bilden einen unterschiedlichen Rahmen für die Anti-Phishing-

Schulung. Jedoch können das Verständnis der Unterschiede und die Ergänzung zueinander dabei helfen einen Widerstand gegen Phishing-Angriffe für Mitarbeiter und Mitarbeiterinnen des Unternehmens aufzubauen. Die Achtsamkeitsschulung hat folgende drei Empfehlungen zur Vermeidung von Phishing-Angriffen (Jensen *et al.*, 2017, pp. 597–608):

1. Stop! (Jensen *et al.*, 2017, p. 608)
2. Denken Sie nach...
    a. Fragt die Anfrage nach privaten oder geschützten Informationen?
    b. Kommt die Anfrage unerwartet oder überstürzt?
    c. Ergibt die Anfrage Sinn?
    d. Warum sollte der Absender oder die Absenderin dies von mir verlangen? (Jensen *et al.*, 2017, p. 608)
3. Prüfen Sie. (Jensen *et al.*, 2017, p. 608)

Der erste Schritt, "Stop!", sollte den Personen beibringen zu warten, wenn eine E-Mail eine ausdrückliche Handlungsaufforderung enthält (z.B. Herunterladen eines Anhangs, Klicken auf einen Link). Diese Aufforderungen sind mit einem gewissen Risiko verbunden, und der Schritt "Stop!" ermutigt den Einzelnen zu warten, um die Nachricht zu prüfen, mögliche Konsequenzen zu verstehen und routinemäßige Antworten zu vermeiden. Der zweite Schritt, Denken Sie nach..., ermutigt die Personen, über die aufgeforderten Handlungen, den Kontext, und die mögliche Motivation für die Aufforderung nachzudenken. Die Mitarbeiter und Mitarbeiterinnen sollen über die vier Fragen nachdenken. Diese Fragen sind kurz und leicht zu merken, lenken aber auch die Aufmerksamkeit auf die E-Mail. Nachdem der Bewertungsprozess abgeschlossen ist und bei den Mitarbeiter und Mitarbeiterinnen ein Verdacht aufkommt, sollen sie sich bei einer vertrauenswürdigen dritten Person erkundigen (Jensen *et al.*, 2017, pp. 607–608).

Es ist noch einmal zu erwähnen, dass diese zwei Schulungsmethoden aufgrund der Ergebnisse und Auswertung des Fragebogens ausgewählt worden sind. Jedoch kann auch eine andere Schulungsmethode ausgewählt werden. Nun werden einige Sicherheitsrichtlinien oder Erkennungsmerkmale in Bezug auf Phishing-Attacken zusammengefasst, die in einer Phishing Schulungsmethode enthalten sein sollten:

- Die meisten Phishing-E-Mails enthalten Links zu gefälschten Websites. Die Mitarbeiter und Mitarbeiterinnen sollten über dieses Thema geschult sein und es

vermeiden, auf diese Links zu klicken. Stattdessen können sie ein anderes Fenster öffnen und von dort aus die gewünschte Website aufrufen (Patayo, 2021, p. 15).

- Die Mitarbeiter und Mitarbeiterinnen können die Links überprüfen, indem sie die Maus über den Link bewegen, danach können sie nachsehen ob der angezeigt Link mit dem Link, der in der Nachricht steht, übereinstimmt (Esmat, Alharbi and Karrar, 2021, p. 795).
- Angenommen Mitarbeiter und Mitarbeiterinnen erhalten eine E-Mail von einer Bank, einer Versicherungsgesellschaft oder einer anderen Institution, mit der sie regelmäßig in Kontakt stehen. Sobald in dieser E-Mail nach sensible Informationen gebeten wird, sollten sich die Mitarbeiter und Mitarbeiterinnen mit dieser Organisation direkt in Verbindung setzen, falls sie der E-Mail nicht vertrauen. Dadurch stellen die Mitarbeiter und Mitarbeiterinnen sicher, dass keine sensiblen Daten verloren gehen (Esmat, Alharbi and Karrar, 2021, p. 795).
- Die meisten offiziellen Websites und Banken fordern die Mitarbeiter und Mitarbeiterinnen nicht auf, in den von ihnen gesendeten E-Mails auf Links zu klicken und den Benutzernamen oder das Passwort zu übermitteln (Esmat, Alharbi and Karrar, 2021, p. 796).
- Es soll nicht auf Links zu Websites geklickt werden, die an E-Mails von Personen angehängt sind, die der Benutzer nicht kennt. Beispielsweise erhalten Mitarbeiter und Mitarbeiterinnen die Nachrichten, dass um eine Kontoschließung zu verhindern auf einen Link in der Nachricht geklickt werden sollte. Anstatt auf den Link zu klicken sollten die Mitarbeiter und Mitarbeiterinnen vielmehr die ursprüngliche Website besuchen und sich dort vergewissern (Esmat, Alharbi and Karrar, 2021, p. 796).
- Die Mitarbeiter und Mitarbeiterinnen sollten vermeiden Dateien, die an E-Mail-Nachrichten angehängt sind, zu öffnen, wenn diese von fremden Personen oder unbekannten Unternehmen gesendet werden. Dies ist deshalb wichtig, da diese E-Mail-Anhänge möglicherweise bösartige Programme enthalten (Esmat, Alharbi and Karrar, 2021, p. 796).
- Das Unternehmen und die angestellten Personen müssen sicherstellen, dass das Antiviren-Software auf dem neuesten Stand ist, denn die Software kann bösartige Programme erkennen und sie somit schützen. Angenommen das Gerät eines Mitarbeiter oder einer Mitarbeiterin wurde infiziert, sollte sich diese Person an einen Spezialisten im Unternehmen wenden, um die Malware zu beseitigen (Esmat, Alharbi and Karrar, 2021, p. 796).

- Das Unternehmen kann die Verwendung der zweistufigen Verifizierung einführen. Falls der Mitarbeiter oder die Mitarbeiterin angegriffen wurde und keine PIN oder keinen Code erhält, der die Änderung der Anmeldedaten bestätigt, wird diese Person wissen, dass er oder sie Opfer eines Phishings geworden ist. In diesem Falle müssen die Mitarbeiter und Mitarbeiterinne dies der zuständigen Abteilung melden, um Korrekturmaßnahmen zu ergreifen (Patayo, 2021, pp. 14–15).
- Die Unternehmen können nicht verhindern, dass Phishing-E-Mails ihre Kunden und Kundinnen erreichen, aber sie können Geschäftspraktiken entwickeln, die den Kunden und Kundinnen helfen, sich über Phishing-E-Mails zu informieren. Hier sind zwei Vorschläge: Das Unternehmen und deren angestellten Personen sollen die Kunden und Kundinnen mit dem Namen ansprechen. Des Weiteren werden die Kunden und Kundinnen aufgefordert den Browser zu öffnen und die URL manuell einzugeben, denn das Unternehmen würde keine Links in einer E-Mail verwenden z.B. für die Datenänderung oder Erfragung wichtiger Daten (Esmat, Alharbi and Karrar, 2021, p. 796).

Aufgrund des fehlenden Wissens in Bezug auf die Uniform Resource Locator (URLs) werden Personen Opfer von Phishing-Angriffen (Basit *et al.*, 2021, p. 140). Wie bereits bei Auswertung des Fragebogens festgestellt worden ist, kennt ein Drittel der befragten Personen, die in einem Großunternehmen in Österreich arbeiten oder gearbeitet haben, den Unterschied zwischen „http://“ und „https://“ nicht (siehe Tabelle 18). Aus diesem Grund wurden die wichtigsten Informationen von Gastellier-Prevost et al. (2011) zusammengefasst. Die Autoren und Autorinnen erörterten die folgenden URL-Phishing-Techniken, die von Angreifer und Angreiferinnen verwendet werden können (Purkait, Kumar De and Suar, 2014, p. 204):

- Andere Domänennamen: Phisher und Phisherinnen verlassen sich darauf, dass die angestellten Personen den Domänennamen eines Unternehmens nicht kennen. Auf diese Weise können die Angreifer und Angreiferinnen die gefälschte Website auf einer beliebigen Website ihrer Wahl hosten und davon ausgehen, dass das Opfer die Adressleiste übersieht oder das notwendige Wissen nicht hat (Purkait, Kumar De and Suar, 2014, p. 204).
- Subdomäne oder untergeordnete Domänennamen: Phishing-URLs enthalten einige Teile der ursprünglichen Website-URLs (Purkait, Kumar De and Suar, 2014, p. 204).
- Falsch geschriebene Domänennamen: Es ist sehr einfach, einen oder mehrere Buchstaben einer legitimen URL zu verfälschen, ohne dass dies von Personen

bemerkt wird (Purkait, Kumar De and Suar, 2014, p. 204). Hierzu gab es zwei Beispiele („https://suppoort.apple.com/“ und „https://www.disney_plus.com/de-de/sign-up?type=standard“) im Fragebogen und dabei haben mehr als die Hälfte der Teilnehmer und Teilnehmerinnen die erste Phishing URL nicht erkannt (siehe Abbildung 21) und bei der zweiten Phishing URL haben es 30% der Teilnehmer und Teilnehmerinnen nicht erkannt (siehe Abbildung 22).

- Verwendung anderer Top-Level-Domains (TLD): Phisher und Phisherinnen verwenden eine andere TLD, um die gefälschte Website zu hosten. Mitarbeiter und Mitarbeiterinnen die den ursprünglichen Domänennamen nicht kennen, können mit dieser Technik leicht getäuscht werden (Purkait, Kumar De and Suar, 2014, p. 204).
- Verwendung der IP-Adresse: Phishing-URLs enthalten eine IP-Adresse anstelle eines vollständig qualifizierten Domänennamens (Purkait, Kumar De and Suar, 2014, p. 204). Hierzu gab es auch ein Beispiel („https://147.46.236.55/PayPal/login.html“) und dies konnten 30% der befragten Personen nicht erkennen bzw. haben die Option „Ich weiß es nicht.“ gewählt (siehe Abbildung 23).

Im Anschluss werden einige weitere Phishing Erkennungsmerkmale und Tipps für sichere Vorgehensweisen für Website, URLs und E-Mail zusammengefasst:

Website:

- Prüfung der URL in der Adressleiste, Prüfung auf HTTPS und Schlosssymbol (Fälschung möglich und Zweifelsfalles direkt prüfen) (Mossano *et al.*, 2020, p. 5).
- Prüfung der Legitimität der Website, Setzung von Lesezeichen für sensible Websites (Mossano *et al.*, 2020, p. 5).
- Verwendung von Pop-up-Fenstern für die Passworteingabe (Anzeichen Phishing) (Glăvan *et al.*, 2020, p. 4).
- Keine DNS-Datensätze für bestimmte URL (Anzeichen Phishing) (Glăvan *et al.*, 2020, p. 4).
- Keine Aufzeichnung von Website-Verkehr (Anzeichen Phishing) (Glăvan *et al.*, 2020, p. 4).
- Alter der Domäne weniger als ein Jahr (Anzeichen Phishing) (Glăvan *et al.*, 2020, p. 4).
- Kein Google-Index oder Google-Rang (Anzeichen Phishing) (Bhardwaj *et al.*, 2020, p. 19).

- Mouseover deaktiviert für URL Untersuchung (Anzeichen Phishing) (Bhardwaj *et al.*, 2020, p. 19).
- Rechtsklick deaktiviert (Anzeichen Phishing) (Bhardwaj *et al.*, 2020, p. 19).

URL:

- URL Verkürzungsdienst – werden verwendet, um gefälschte URL zu verbergen (Bhardwaj *et al.*, 2020, p. 19).
- „@“ - Symbol – alphanumerische Zeichen werden nach dem @-Symbol ignoriert (Bhardwaj *et al.*, 2020, p. 19).
- Präfix oder Suffix – hinzufügen von Präfix oder Suffix, getrennt durch ein „-“, weist auf Phishing-Subdomäne hin (Bhardwaj *et al.*, 2020, p. 19).
- Länge der URL – gefälschte Subdomäne oder lange URLs werden verwendet, um Phishing-Seiten zu verbergen (Bhardwaj *et al.*, 2020, p. 19).
- IP-Adresse – es werden IP-Adressen anstelle von gefälschten URL verwendet (Bhardwaj *et al.*, 2020, p. 19).
- Mehrere „.“ - Symbol – mehr als ein „.“ Subdomäne -URL weist auf Phishing-Seiten hin (Bhardwaj *et al.*, 2020, p. 19).
- HTTPS-Token und Port – eine Verwendung von HTTPS-Token und nicht standardmäßigen Ports (8081, 8090, ...) deutet auf Phishing Seiten hin (Bhardwaj *et al.*, 2020, p. 19).
- Doppelte „//“ - Symbol – werden verwendet um die URL umzuleiten und weist auf Phishing-Seiten hin (Bhardwaj *et al.*, 2020, p. 19).

E-Mail:

- Die Absender bzw. Absenderinnenadresse ist der echten Adresse sehr ähnlich, weist aber einige geringfügige Unterschiede auf (z.B. mehrere Buchstaben sind unterschiedlich, synonyme Verwendung) (Rastenis *et al.*, 2020, pp. 315–316).
- Der E-Mail-Text weist einige Rechtschreib- oder Stilfehler auf. Dies ist in der Regel auf die Tatsache zurückzuführen, dass der Text automatisch aus einer anderen Sprache übersetzt wurde (Rastenis *et al.*, 2020, pp. 315–316).
- Die Institution der Absender oder Absenderin und die Zugehörigkeit zu einer bestimmten Organisation wird im E-Mail-Text nicht erwähnt (Rastenis *et al.*, 2020, pp. 315–316).
- Es gibt nicht genügend Informationen, um die Kontakte oder Institution der Absender und Absenderinnen zu identifizieren (Rastenis *et al.*, 2020, pp. 315–316).

- Die E-Mail enthielt ein eingebettetes Bild, das heruntergeladen werden muss, um es zu betrachten. Normalerweise werden Bilder an die E-Mail angehängt, während die eingebetteten Bilder die Verfolgung der gelesenen E-Mails ermöglichen (Rastenis *et al.*, 2020, pp. 315–316).
- Die E-Mail enthält einige externe Links zu anderen Websites (Rastenis *et al.*, 2020, pp. 315–316).
- Der Domänenname der Websites ist sehr ähnlich, aber etwas anders oder völlig anders als die Domäne der sendenden Einrichtung (Rastenis *et al.*, 2020, pp. 315–316).
- Die E-Mail verlangt Daten, obwohl diese bereits bekannt sind (Rastenis *et al.*, 2020, pp. 315–316).
- Der Inhalt der E-Mail scheint zu schön um wahr zu sein (Mossano *et al.*, 2020, p. 5).
- Die E-Mail verwendet generische Begrüßungen für den Empfänger oder die Empfängerin (Mossano *et al.*, 2020, p. 5).
- Die E-Mail weist ein sehr schlechtes Layout auf (Mossano *et al.*, 2020, p. 5).

Es gibt einige Schritte, die beachtet werden sollen, falls eine Phishing-Attacke erfolgreich durchgeführt worden ist. Mitarbeiter und Mitarbeiterinnen müssen das Passwort sofort ändern und die Kontoaktivitäten müssen überprüft werden. Des Weiteren muss dieser Phishing-Angriff gemeldet werden (Mossano *et al.*, 2020, p. 5). In Bezug auf die Meldung von verdächtigen E-Mails gibt es Hinweise darauf, dass die Nutzer und Nutzerinnen nur selten etwas melden. Insofern klickten bei einem simulierten Phishing-Test 1.000 Teilnehmer und Teilnehmerinnen (20,3% der Zielgruppe) auf einen in einer Phishing-E-Mail eingebetteten Link, und nur 7,4% von ihnen meldeten dies dem Helpdesk. Dies geht aus der Bewertung einer Phishing-Kampagne hervor, die 2018 vom Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS) durchgeführt wurde. Ein ähnliches Ergebnis wurde im Jahr 2019 von Verizon durchgeführten Data Breach Investigations Report (DBIR) angesprochen. In einem simulierten Phishing-E-Mail-Test meldete sich die Hälfte der Phishing-Opfer erst einige Wochen später. Diese Tendenz zeigt sich auch bei anderen Arten von Cyberkriminalität wie Datenschutzverletzungen in Unternehmen. Das Internet Crime Complaint Center des FBI in den USA hat Daten veröffentlicht, aus denen hervorgeht, dass nur 15% der Opfer von Cyberkriminalität in Unternehmen ihre jeweiligen Vorfälle im Jahr 2018 den Strafverfolgungsbehörden gemeldet haben, und nur 28% der Cyberangriffe auf Unternehmen im Vereinigten Königreich wurden im Jahr 2016 der Polizei gemeldet. Der

Grundgedanke hinter der Meldung von Phishing-Angriffen ist, dass die Meldung eine frühzeitige Erkennung ermöglicht und es der IT-Abteilung des Unternehmens erlaubt, andere über einen Angriff zu informieren, bevor sich dieser weiter ausbreitet (Kwak *et al.*, 2020, p. 2). Nachdem ein Unternehmen einen Angriff eingedämmt und abgewehrt hat, empfiehlt es alle Daten zum Angriff, die Prozesse und Maßnahmen zur Eindämmung und Abwehr zu dokumentieren. Die Dokumentation sollte dann in der Wissensdatenbank des Unternehmens gespeichert werden. Die Wissensdatenbank (Knowledge Base, KB) ist eine Datenbank in der alle Viren, Malware oder Angriffe gespeichert werden (Patayo, 2021, p. 11).

Obwohl die Schlussfolgerungen den Eindruck erwecken, dass intensive Anti-Phishing-Schulungen in jedem Unternehmen durchgeführt werden sollten, gibt es auch organisatorische Aspekte, die bei der Einführung der Phishing Schulungen beachtet werden sollten. Ein Unternehmen sollte sich die Frage stellen, wie solche Schulungen in innerhalb des Unternehmens von den Mitarbeiter und Mitarbeiterinnen wahrgenommen/aufgenommen werden. Jedes Unternehmen unterscheidet sich in Bezug auf Einstellungen, Sicherheitsvorkehrungen und Organisationskulturen und somit kann sich die Wirkung eines fundierten Schulungsprogramms von Unternehmen zu Unternehmen auch unterscheiden.

Angenommen ein Unternehmen mit einer flachen Organisationsstruktur und einer sehr liberalen Arbeitskultur führt eine eingebettete Schulung durch, könnten die Mitarbeiter und Mitarbeiterinnen die Schulung als eine Art Beobachtung wahrnehmen. In einer Bank hingegen ist die Wahrscheinlichkeit eines solchen Eindrucks möglicherweise geringer. Des Weiteren kann eine eingebettete Schulung dazu führen, dass der Druck der Mitarbeiter und Mitarbeiterinnen erhöht wird, weil sie die Überprüfung bestehen möchten. Daher könnten sie sich von dem Arbeitgeber oder der Arbeitgeberin ständig geprüft oder unter Druck gesetzt fühlen, was sich auf die Gesundheit und/oder Arbeitsleistung der Mitarbeiter und Mitarbeiterinnen auswirken könnte. Daher sollte jede Phishing-Schulung an die Bedürfnisse, dem Marktdruck, den Modernisierungszielen, den Voraussetzungen und dem Budget eines Unternehmens angepasst werden. Im Hinblick auf Phishing-Schulungen muss jedes Unternehmen für sich selbst abwägen, ob die Mitarbeiter und Mitarbeiterinnen in der Lage sind zusätzliche Schulungen zu absolvieren, oder ob sie damit überfordert werden (Jampen *et al.*, 2020, p. 31).

Die Aufmerksamkeitsressourcen der Mitarbeiter und Mitarbeiterinnen sind begrenzt und die Menge an Informationen, die das kognitive System gleichzeitig verarbeiten kann, ist

eingeschränkt. Wenn die Phishing-Schulung mit der Vielzahl anderer Schulungen kombiniert werden und die ebenfalls routinemäßig an die Mitarbeiter und Mitarbeiterinnen weitergegeben werden müssen, wie z.B. Gesundheits- und Sicherheitsinformationen kann dies die Wahrscheinlichkeit und das Ausmaß verringern, dass die Informationen wahrgenommen werden und im Gedächtnis verbleiben oder bei Entscheidungen über die Erkennung von Phishing-E-Mails berücksichtigt werden (Williams, Hinds and Joinson, 2018, p. 2). Ein Unternehmen das beispielsweise bereits über Sicherheitsschulungsprogramme verfügt, könnte das Hinzufügen einer Phishing-Schulung als kontraproduktiv erweisen, da es zu einer Ermüdung der Mitarbeiter und Mitarbeiterinnen führt und der gewünschte Effekt der Sicherheitsverbesserung nicht eintritt (Jampen *et al.*, 2020, p. 31).

Obwohl sich die Phishing-Schulung der Mitarbeiter und Mitarbeiterinnen positiv auf die globalen Bemühungen zur Bekämpfung von Phishing auswirken kann, ist dieser Ansatz mit hohen Kosten verbunden. Nachdem sich die Phishing-Techniken jedoch ständig ändern und weiterentwickeln, verfügen kleine und mittlere Unternehmen möglicherweise nicht über die Ressourcen, die große Organisationen haben, um in die Schulung ihrer Mitarbeiter und Mitarbeiterinnen zu investieren (Qabajeh, Thabtah and Chiclana, 2018, p. 49). Daher kann diese Leitlinie auch für Klein- und Mittelbetriebe (KMU) angepasst werden. Diese Leitlinie und Vorschläge können als Grundbaustein für Cybersicherheitsverantwortliche bei der Planung der SETA-Programme verwendet werden. Dieser Leitfaden kann von jedem Unternehmen verwendet und angepasst werden und stellt die wichtigsten Punkte aus der Literaturrecherche zusammengefasst dar. Dieser Leitfaden stellt eine Hilfestellung für eine erfolgreiche Durchführung eines SETA-Programmes dar.

# 4 Schlussfolgerung

## 4.1 Zusammenfassung

Die Phishing-Angriffe stellen seit mehr als 20 Jahren eine Bedrohung dar und werden könnnen in der Zukunft weiterhin bestehen, aufgrund der Tatsache, dass es für Phisher und Phisherinnen einfach ist diesen Angriff durchzuführen. Es wird auch Mitarbeiter und Mitarbeiterinnen geben die auf fragwürdige Links klicken oder dubiose Anhänge herunterladen (Binks, 2019, pp. 10–11). Daher bleiben Phishing-Angriffe weiterhin ein wichtiges globales Problem (Kaushik *et al.*, 2021, p. 19). Die technischen Anti-Phishing Methoden könne allein nur einen kleinen Beitrag zur Abwehr von Phishing-Angriffen

leisten. Aus diesem Grund sind die Awareness und die Schulung der Personen ein wichtiger Bestandteil für die Abwehr von Phishing-Angriffen. Jedoch müssen technische und nicht-technische Anti-Phishing Methoden zusammen eingesetzt werden um ein wirksamen Schutz für Unternehmen zu gewährleisten (Furnell, Millet and Papadaki, 2019, p. 16). Der Schlüssel zur Eindämmung und Kontrolle von Phishing-Angriffen liegt in der Schulung der Mitarbeiter und Mitarbeiterinnen (Binks, 2019, p. 11). Damit ein Unternehmen Phishing-Angriffe erfolgreich abwehren können, müssen alle Mitarbeiter und Mitarbeiterinnen geschult und regelmäßig überprüft werden (Rutherford, 2018, p. 8).

Im Folgenden werden die wichtigsten Informationen in Bezug auf die Studie der Masterarbeit zusammengefasst. In dieser Studie wurden 121 Teilnehmer und Teilnehmerinnen von Großunternehmen in Österreich zu dem Thema Phishing Schulungen befragt. Obwohl 95% der befragten Personen die Definitionsfrage in Bezug auf Phishing richtig beantwortet haben und mehr als zwei Drittel der Personen noch noch auf eine Phishing-Attacke hereingefallen sind, konnten nur knapp 50% der Teilnehmer und Teilnehmerinnen mehr als 50% der Beispiele zu legitimen- und Phishing-E-Mail bzw. -URLs richtig identifizieren. Aus der Umfrage geht hervor, dass ein Drittel der befragte Personen den Unterschied zwischen „http://“ und „https://“ nicht. Des Weiteren konnten mehr als die Hälfte der Personen folgende zwei Phishing URL Beispiele nicht erkennen: „https://suppoort.apple.com/“ und „https://147.46.236.55/PayPal/login.html“. Diese Erkenntnis lässt vermuten, dass die befragten Personen entweder unaufmerksam bei der Identifizierung der Beispiele waren oder das notwendige Wissen zu URLs nicht vorhanden ist. Es wurde auch festgestellt, dass ein Drittel der Personen den Benutzer- bzw. Benutzerinnennamen, Passwörter und Bankomat-/Kreditkartendaten bereits auf Websites mit „http://“ eingegeben haben. In Gegensatz zu „Phishing Vertrautheit“ und „Phishing Awareness“ sind die Werte zu „Sicherheitsgewohnheiten“ schlechter ausgefallen, weil unter anderem 75% der Teilnehmer und Teilnehmerinnen ihre Passwörter für die Online-Konten aufgeschrieben haben oder dazu tendieren auch Passwörter aufzuschreiben, die schwieriger zu merken sind. Des Weiteren verwenden 50% der befragten Personen ein Passwort für mehrere Online-Konten gleichzeitig.

Einer der wichtigsten Erkenntnisse dieser Studie ist, dass fast die Hälfte der Teilnehmer und Teilnehmerinnen noch nicht eine Phishing Schulung, in dem Großunternehmen in denen sie gearbeitet haben oder derzeit haben, erhalten haben. Jedoch wurde festgestellt, dass zwei Drittel der Personen zumindest eine Computer-/Informationssicherheit Schulung erhalten hat. Dennoch besteht eine dringende Notwendigkeit diese Personen in Bezug auf Phishing zu schulen. Eine weitere wichtige Erkenntnis war, dass bei fast mehr

als 50% der befragten Personen, die eine Phishing Schulung erhalten haben, die letzte Schulung jedoch länger als fünf Monate zurückliegt. Bezüglich der Bevorzugung einer Phishing Schulung wurde ermittelt, dass männliche Teilnehmer sich für die Achtsamkeitsschulung entscheiden würden und weibliche Teilnehmerinnen tendieren eher zu der eingebetteten Schulungsmethode. Personen, die bereits eine Phishing Schulung erhalten haben, würden die Achtsamkeitsschulung bevorzugen und Personen, die noch keine Phishing Schulung erhalten haben, würden die eingebettete Schulung vorziehen.

Es wurden im Rahmen der Masterarbeit auch Hypothesen überprüft und es stellt sich heraus, dass es signifikante Unterschiede zwischen der Phishing Anfälligkeit und der Teilnahme an einer Phishing Schulung gibt, jedoch wurden keine signifikanten Unterschiede in Bezug auf das Geschlecht der Teilnehmer und Teilnehmerinnen ermittelt. Des Weiteren wurde festgestellt, dass es signifikante Zusammenhänge zwischen der Phishing Anfälligkeit und der Phishing Vertrautheit der befragten Personen gibt. Andererseits wurden keine signifikanten Zusammenhänge in Bezug auf Phishing Awareness und Sicherheitsgewohnheiten festgestellt. Mit diesen Erkenntnissen und Ergebnissen wurde ein Leitfaden für eine Phishing Schulung erstellt. Dabei wurden die wichtigsten Informationen, Empfehlungen und Vorschläge zu Phishing Schulungen zusammengefasst. Die Ergebnisse dieser Studie sind wertvoll für IT-Leiter und Sicherheitsmanager, die für den Schutz der Vermögenswerte eines Unternehmens in Österreich vor Phishing-Attacken verantwortlich sind. Die Daten dieser Studie geben Aufschluss über die derzeitige Situation in Bezug auf Phishing Schulungen in Großunternehmen in Österreich. Es wurden auch die wichtigsten Erkenntnisse und bewährte Verfahren vergangener Studien zur Eindämmung und Vermeidung von Phishing-Angriffen im Leitfaden zusammengefasst. Die in dieser Studie gesammelten Informationen können genutzt werden, um effektivere Programme zur Schulung von Personal in Österreich in Bezug auf Phishing zu erstellen.

## 4.2 Limitation

Es wurden zwei Limitationen für diese Masterarbeit festgestellt. Die erste Limitation bestand darin, dass die Teilnehmer und Teilnehmerinnen des Fragebogens die E-Mail-Beispiele anhand eines Screenshots identifizieren mussten. Dementsprechend hatten die befragten Personen auch keine Möglichkeit die Maus über den Link zu bewegen und den Link genauer anzusehen, um festzustellen wohin dieser Link eine Person tatsächlich hinführt. Außerdem war es nicht möglich, die integrierten Links innerhalb einer E-Mail

zu untersuchen oder zusätzliche Informationen wie zum Beispiel die Absender- bzw. Absenderinnenadresse genauer zu überprüfen. Als Folge dessen könnte die Erkennungsrate in Wirklichkeit anders ausfallen. Allerdings hätten diese Bedingungen eine Laborumgebung erfordert und dies war im Rahmen dieser Masterarbeit nicht möglich. Die zweite Limitation bestand darin, dass im Rahmen des Fragebogens aufgrund eines Fehlers, das Alter nicht erhoben wurde. Jedoch wurden viele andere demografische Daten der Teilnehmer und Teilnehmerinnen des Fragebogens erhoben, um die Forschungsfrage der Masterarbeit zu beantworten.

## 4.3 Forschungsbedarf

Es wurden fünf weitere Forschungsmöglichkeiten ermittelt. Erstens, wurden wie bereits erwähnt, aufgrund eines Fehlers das Alter der Teilnehmer und Teilnehmerinnen nicht erhoben. Aufgrund dessen kann die Phishing-Anfälligkeit auf Basis des Alters untersucht werden und entsprechende Schulungsmaßnahmen entwickelt werden. Des Weiteren können weitere Phishing Anfälligkeitsmerkmale zu Personen erforscht werden wie z.B. Herkunft, Persönlichkeitsmerkmale, Psychologische Merkmale, Risikobereitschaft und Informationsverarbeitung. Zweitens können die erhobenen Faktoren: „Phishing Anfälligkeit“ und „Phishing Vertrautheit“ bzw. „Teilnahme Schulung“ mithilfe von Regression weiter analysiert werden. Während bei der Korrelation lediglich festgestellt wird, ob zwei Variablen miteinander in Beziehung stehen, geht die Regression einen Schritt weiter und versucht, die Werte einer Variablen auf der Grundlage einer anderen vorherzusagen. Es wird in den meisten Fällen keine Vorhersage auf der Grundlage einer einzigen unabhängigen Variablen getroffen, sondern in der Regel werden mehrere Variablen verwendet, die wichtig sein könnten (McCormick, Salcedo and Poh, 2015, p. 250). Drittens, der Fragebogen wurde auf Personen, die in einem Großunternehmen in Österreich arbeiten oder gearbeitet haben, beschränkt. Jedoch können auch die Klein- und Mittelbetriebe (KMU) untersucht werden, und im Zuge dessen können die Unternehmensformen miteinander verglichen werden, um Gemeinsamkeiten und Unterschiede festzustellen. Viertens kann die Phishing Anfälligkeit der Menschen in Österreich im Rahmen einer Laboruntersuchung erforscht werden. Fünftens kann die Forschung in Bezug auf Phishing Anfälligkeit auf Smartphones ausgeweitet werden, denn die tägliche Nutzung von Smartphones für soziale Netzwerke und für Transaktionsaktivitäten wie Bankgeschäfte und E-Mails hat drastisch zugenommen (Younis and Musbah, 2020, p. 1).

# 5 Literaturverzeichnis


*A Decade in Digital* (2021) *DataReportal – Global Digital Insights*. Available at: https://datareportal.com/reports/a-decade-in-digital (Accessed: 21 March 2022).

Abbasi, A. *et al.* (2021) 'The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites', *Information Systems Research*, 32(2), pp. 410–436. Available at: https://doi.org/10.1287/isre.2020.0973.

Abroshan, H. *et al.* (2018) 'Phishing Attacks Root Causes', in N. Cuppens et al. (eds) *Risks and Security of Internet and Systems*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 187–202. Available at: https://doi.org/10.1007/978-3-319-76687-4_13.

Abroshan, H. *et al.* (2021a) 'A phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks', in *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*. New York, NY, USA: Association for Computing Machinery (UMAP '21), pp. 345–350. Available at: https://doi.org/10.1145/3450614.3464472.

Abroshan, H. *et al.* (2021b) 'COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic', *IEEE Access*, 9, pp. 121916–121929. Available at: https://doi.org/10.1109/ACCESS.2021.3109091.

Abroshan, H. *et al.* (2021c) 'Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process', *IEEE Access*, 9, pp. 44928–44949. Available at: https://doi.org/10.1109/ACCESS.2021.3066383.

Adil, M., Khan, R. and Nawaz Ul Ghani, M.A. (2020) 'Preventive Techniques of Phishing Attacks in Networks', in *2020 3rd International Conference on Advancements in Computational Sciences (ICACS). 2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*, pp. 1–8. Available at: https://doi.org/10.1109/ICACS47775.2020.9055943.

Akpon-Ebiyonare, D.E. (2019) 'Cyber Insecurity: End User Vulnerability Awareness and Perception Assessment', . *Number*, 20(2), p. 7.

Alabdan, R. (2020) 'Phishing Attacks Survey: Types, Vectors, and Technical Approaches', *Future Internet*, 12(10), p. 168. Available at: https://doi.org/10.3390/fi12100168.

Aldawood, H. and Skinner, G. (2018) 'Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review', in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 62–68. Available at: https://doi.org/10.1109/TALE.2018.8615162.

Aleroud, A. and Zhou, L. (2017) 'Phishing environments, techniques, and countermeasures: A survey', *Computers & Security*, 68, pp. 160–196. Available at: https://doi.org/10.1016/j.cose.2017.04.006.

Allodi, L. *et al.* (2020) 'The Need for New Antiphishing Measures Against Spear-Phishing Attacks', *IEEE Security Privacy*, 18(2), pp. 23–34. Available at: https://doi.org/10.1109/MSEC.2019.2940952.

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021) 'Applying social marketing to evaluate current security education training and awareness programs in organisations', *Computers & Security*, 100, p. 102090. Available at: https://doi.org/10.1016/j.cose.2020.102090.

Alsharnouby, M., Alaca, F. and Chiasson, S. (2015) 'Why phishing still works: User strategies for combating phishing attacks', *International Journal of Human-Computer Studies*, 82, pp. 69–82. Available at: https://doi.org/10.1016/j.ijhcs.2015.05.005.

Alwanain, M. (2019) 'Effects of user-awareness on the detection of phishing emails: A case study', *International Journal of Innovative Technology and Exploring Engineering*, 8, pp. 480–484.

Alwanain, M. (2020) 'Phishing Awareness and Elderly Users in Social Media'.

Alwanain, M.I. (2019) 'An Evaluation of User Awareness for the Detection of Phishing Emails', *International Journal of Advanced Computer Science and Applications*, 10(10). Available at: https://doi.org/10.14569/IJACSA.2019.0101046.

*Amazon - Phishing* (2019) *ANTENNE BAYERN*. Available at: https://www.antenne.de/experten-tipps/technik/amazon-fake-mail-vorsicht-vor-dieser-betrugsmasche (Accessed: 2 August 2022).

Anawar, S. *et al.* (2019) 'ANALYSIS OF PHISHING SUSCEPTIBILITY IN A WORKPLACE: A BIG-FIVE PERSONALITY PERSPECTIVES', 14, p. 18.

Antonucci, A. *et al.* (2020) 'Towards an Assessment of Pause Periods on User Habituation in Mitigation of Phishing Attacks', *KSU Proceedings on Cybersecurity Education, Research and Practice* [Preprint]. Available at: https://digitalcommons.kennesaw.edu/ccerp/2020/Research/2.

Anwar, M. *et al.* (2017) 'Gender difference and employees' cybersecurity behaviors', *Computers in Human Behavior*, 69, pp. 437–443. Available at: https://doi.org/10.1016/j.chb.2016.12.040.

Apandi, S.H., Sallim, J. and Sidek, R.M. (2020) 'Types of anti-phishing solutions for phishing attack', *IOP Conference Series: Materials Science and Engineering*, 769(1), p. 012072. Available at: https://doi.org/10.1088/1757-899X/769/1/012072.

Arachchilage, N.A.G. and Love, S. (2014) 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behavior*, 38, pp. 304–312. Available at: https://doi.org/10.1016/j.chb.2014.05.046.

Arachchilage, N.A.G., Love, S. and Beznosov, K. (2016) 'Phishing threat avoidance behaviour: An empirical investigation', *Computers in Human Behavior*, 60, pp. 185–197. Available at: https://doi.org/10.1016/j.chb.2016.02.065.

Arduin, P.-E. (2020) 'A cognitive approach to the decision to trust or distrust phishing emails', *International Transactions in Operational Research*, n/a(n/a). Available at: https://doi.org/10.1111/itor.12963.

Arend, I. *et al.* (2020) 'Passive- and not active-risk tendencies predict cyber security behavior', *Computers & Security*, 97, p. 101964. Available at: https://doi.org/10.1016/j.cose.2020.101964.

Arshad, A. *et al.* (2021) 'A Systematic Literature Review on Phishing and Anti-Phishing Techniques', *arXiv:2104.01255 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2104.01255 (Accessed: 3 December 2021).

B. Kim, E. (2014) 'Recommendations for information security awareness training for college students', *Information Management & Computer Security*, 22(1), pp. 115–126. Available at: https://doi.org/10.1108/IMCS-01-2013-0005.

Back, S. and Guerette, R.T. (2021) 'Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks', *Journal of Contemporary Criminal Justice*, 37(3), pp. 427–451. Available at: https://doi.org/10.1177/10439862211001628.

Baillon, A. *et al.* (2019) 'Informing, simulating experience, or both: A field experiment on phishing risks', *PLOS ONE*, 14(12), p. e0224216. Available at: https://doi.org/10.1371/journal.pone.0224216.

Baki, S. and Verma, R. (2021) 'Sixteen Years of Phishing User Studies: What Have We Learned?', *arXiv:2109.04661 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2109.04661 (Accessed: 6 December 2021).

*Bank Austria - Phishing* (2021). Available at: https://www.bankaustria.at/ueber-uns-bank-austria-online-sicherheit-online-vorsicht-vor-gefaelschten-mails.jsp (Accessed: 2 August 2022).

Bansal, G. (2018) 'Got Phished! Role of Top Management Support in Creating Phishing Safe Organizations', *MWAIS 2018 Proceedings* [Preprint]. Available at: https://aisel.aisnet.org/mwais2018/6.

Basit, A. *et al.* (2021) 'A comprehensive survey of AI-enabled phishing attacks detection techniques', *Telecommunication Systems*, 76(1), pp. 139–154. Available at: https://doi.org/10.1007/s11235-020-00733-2.

Benenson, Z., Gassmann, F. and Landwirth, R. (2017) 'Unpacking Spear Phishing Susceptibility', in M. Brenner et al. (eds) *Financial Cryptography and Data Security*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 610–627. Available at: https://doi.org/10.1007/978-3-319-70278-0_39.

Bhadane, A. and Mane, D.S.B. (2018) 'State of Research on User Training against Phishing with Recent Trends of Attacks', p. 16.

Bhardwaj, A. *et al.* (2020) 'Why is phishing still successful?', *Computer Fraud & Security*, 2020(9), pp. 15–19. Available at: https://doi.org/10.1016/S1361-3723(20)30098-1.

Bildungspolitik, W.-A.- und (2022) *Klein- und Mittelbetriebe (KMU): Definition*. Available at: https://www.wko.at/service/zahlen-daten-fakten/KMU-definition.html (Accessed: 21 August 2022).

Binks, A. (2019) 'The art of phishing: past, present and future', *Computer Fraud & Security*, 2019(4), pp. 9–11. Available at: https://doi.org/10.1016/S1361-3723(19)30040-5.

Boddy, M. (2018) 'Phishing 2.0: the new evolution in cybercrime', *Computer Fraud & Security*, 2018(11), pp. 8–10. Available at: https://doi.org/10.1016/S1361-3723(18)30108-8.

Brickley, J., Thakur, K. and Kamruzzaman, A. (2021) 'A Comparative Analysis between Technical and Non-Technical Phishing Defences', *International Journal of Cyber-Security and Digital Forensics*, 10, pp. 28–41.

Broadhurst, R. *et al.* (2018) *Phishing and Cybercrime Risks in a University Student Community*. SSRN Scholarly Paper ID 3176319. Rochester, NY: Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.3176319.

Burda, P. *et al.* (2020) 'Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment', in *Proceedings of the 15th International Conference on Availability, Reliability and Security*. New York, NY, USA: Association for Computing Machinery (ARES '20), pp. 1–10. Available at: https://doi.org/10.1145/3407023.3409178.

Burda, P., Allodi, L. and Zannone, N. (2020) 'Don't Forget the Human: a Crowdsourced Approach to Automate Response and Containment Against Spear Phishing Attacks', in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 471–476. Available at: https://doi.org/10.1109/EuroSPW51379.2020.00069.

Canham, M. *et al.* (2021) 'Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards', *SAGE Open*, 11(1), p. 2158244021990656. Available at: https://doi.org/10.1177/2158244021990656.

Chaudhry, J.A. and Rittenhouse, R.G. (2015) 'Phishing: Classification and Countermeasures', in *2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB). 2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB)*, pp. 28–31. Available at: https://doi.org/10.1109/MulGraB.2015.17.

Chiew, K.L., Yong, K.S.C. and Tan, C.L. (2018) 'A survey of phishing attacks: Their types, vectors and technical approaches', *Expert Systems with Applications*, 106, pp. 1–20. Available at: https://doi.org/10.1016/j.eswa.2018.03.050.

Chigada, J. and Madzinga, R. (2021) 'Cyberattacks and threats during COVID-19: A systematic literature review', *South African Journal of Information Management*, 23(1), pp. 1–11. Available at: https://doi.org/10.4102/sajim.v23i1.1277.

CJ, G. *et al.* (2018) 'PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness', in *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*. New York, NY, USA: Association for Computing Machinery (CHI PLAY '18 Extended Abstracts), pp. 169–181. Available at: https://doi.org/10.1145/3270316.3273042.

Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. (2021) 'Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks', *Education and Information Technologies* [Preprint]. Available at: https://doi.org/10.1007/s10639-021-10806-7.

Damodaram, D.R. (2016) 'STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS', 03(01), p. 7.

Das, S. *et al.* (2019) 'All About Phishing: Exploring User Research through a Systematic Literature Review', *arXiv:1908.05897 [cs]* [Preprint]. Available at: http://arxiv.org/abs/1908.05897 (Accessed: 6 December 2021).

Davis, C. (2013) *SPSS for applied sciences: basic statistical testing*. Collingwood, Vic.: CSIRO Publishing.

De Bona, M. and Paci, F. (2020) 'A real world study on employees' susceptibility to phishing attacks', in *Proceedings of the 15th International Conference on Availability, Reliability and Security*. New York, NY, USA: Association for Computing Machinery (ARES '20), pp. 1–10. Available at: https://doi.org/10.1145/3407023.3409179.

Desolda, G. *et al.* (2021) 'Human Factors in Phishing Attacks: A Systematic Literature Review', *ACM Computing Surveys*, 54(8), p. 173:1-173:35. Available at: https://doi.org/10.1145/3469886.

Esmat, H., Alharbi, A. and Karrar, A. (2021) 'The Impact of Phishing on the Business Sector in KSA: Analytical Study', *International Journal of Advanced Trends in Computer Science and Engineering*, 10, pp. 791–799. Available at: https://doi.org/10.30534/ijatcse/2021/471022021.

Fernando, M. and Arachchilage, N.A.G. (2020) 'Why Johnny can't rely on anti-phishing educational interventions to protect himself against contemporary phishing attacks?', *arXiv:2004.13262 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2004.13262 (Accessed: 3 December 2021).

Ferreira, A. and Vieira-Marques, P. (2018) 'Phishing Through Time: A Ten Year Story based on Abstracts':, in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. *4th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, pp. 225–232. Available at: https://doi.org/10.5220/0006552602250232.

Franz, A. *et al.* (2021) 'Still Plenty of Phish in the Sea — A Taxonomy of {User-Oriented} Phishing Interventions and Avenues for Future Research', in. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pp. 339–358. Available at: https://www.usenix.org/conference/soups2021/presentation/franz (Accessed: 4 December 2021).

Frauenstein, E.D. and Flowerday, S. (2020) 'Susceptibility to phishing on social network sites: A personality information processing model', *Computers & Security*, 94, p. 101862. Available at: https://doi.org/10.1016/j.cose.2020.101862.

Frauenstein, E.D. and von Solms, R. (2013) 'An Enterprise Anti-phishing Framework', in R.C. Dodge and L. Futcher (eds) *Information Assurance and Security Education and Training*. Berlin, Heidelberg: Springer (IFIP Advances in Information and Communication Technology), pp. 196–203. Available at: https://doi.org/10.1007/978-3-642-39377-8_22.

Furnell, S., Millet, K. and Papadaki, M. (2019) 'Fifteen years of phishing: can technology save us?', *Computer Fraud & Security*, 2019(7), pp. 11–16. Available at: https://doi.org/10.1016/S1361-3723(19)30074-0.

Gavett, B.E. *et al.* (2017) 'Phishing suspiciousness in older and younger adults: The role of executive functioning', *PLOS ONE*, 12(2), p. e0171620. Available at: https://doi.org/10.1371/journal.pone.0171620.

Glăvan, D. *et al.* (2020) 'Detection of phishing attacks using the anti-phishing framework', *Scientific Bulletin 'Mircea cel Batran' Naval Academy*, 23(1), pp. 208-212,208A. Available at: http://dx.doi.org/10.21279/1454-864X-20-I1-028.

Goel, S., Williams, K. and Dincelli, E. (2017) 'Got Phished? Internet Security and Human Vulnerability', *Journal of the Association for Information Systems*, 18(1). Available at: https://doi.org/10.17705/1jais.00447.

Gordon, W.J. *et al.* (2019) 'Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system', *Journal of the American Medical Informatics Association*, 26(6), pp. 547–552. Available at: https://doi.org/10.1093/jamia/ocz005.

Gupta, B.B. *et al.* (2017) 'Fighting against phishing attacks: state of the art and future challenges', *Neural Computing and Applications*, 28(12), pp. 3629–3654. Available at: https://doi.org/10.1007/s00521-016-2275-y.

Gupta, B.B., Arachchilage, N.A.G. and Psannis, K.E. (2018) 'Defending against phishing attacks: taxonomy of methods, current issues and future directions', *Telecommunication Systems*, 67(2), pp. 247–267. Available at: https://doi.org/10.1007/s11235-017-0334-z.

Hakim, Z.M. *et al.* (2021) 'The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection', *Behavior Research Methods*, 53(3), pp. 1342–1352. Available at: https://doi.org/10.3758/s13428-020-01495-0.

Ifham, A. (2020) 'How to do Normality Test using SPSS?', *Medium*, 8 May. Available at: https://medium.com/@ahamedifham/how-to-do-normality-test-using-spss-de5234080f6d (Accessed: 25 August 2022).

Jakobsson, M. (2018) 'Two-factor inauthentication – the rise in SMS phishing attacks', *Computer Fraud & Security*, 2018(6), pp. 6–8. Available at: https://doi.org/10.1016/S1361-3723(18)30052-6.

Jalali, M.S. *et al.* (2020) 'Why Employees (Still) Click on Phishing Links: Investigation in Hospitals', *Journal of Medical Internet Research*, 22(1), p. e16775. Available at: https://doi.org/10.2196/16775.

Jampen, D. *et al.* (2020) 'Don't click: towards an effective anti-phishing training. A comparative literature review', *Human-centric Computing and Information Sciences*, 10(1), p. 33. Available at: https://doi.org/10.1186/s13673-020-00237-7.

Jansson, K. and von Solms, R. (2013) 'Phishing for phishing awareness', *Behaviour & Information Technology*, 32(6), pp. 584–593. Available at: https://doi.org/10.1080/0144929X.2011.632650.

Jayatilaka, A., Arachchilage, N.A.G. and Babar, M.A. (2021) 'Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors', *arXiv:2108.04766 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2108.04766 (Accessed: 3 December 2021).

Jensen, M., Durcikova, A. and Wright, R. (2017) 'Combating Phishing Attacks: A Knowledge Management Approach', in. Available at: https://doi.org/10.24251/HICSS.2017.520.

Jensen, M.L. *et al.* (2017) 'Training to Mitigate Phishing Attacks Using Mindfulness Techniques', *Journal of Management Information Systems*, 34(2), pp. 597–626. Available at: https://doi.org/10.1080/07421222.2017.1334499.

Kaushik, K. *et al.* (2021) 'Exploring the mechanisms of phishing', *Computer Fraud & Security*, 2021(11), pp. 14–19. Available at: https://doi.org/10.1016/S1361-3723(21)00118-4.

Kearney, W.D. and Kruger, H.A. (2013) 'Phishing and Organisational Learning', in L.J. Janczewski, H.B. Wolfe, and S. Shenoi (eds) *Security and Privacy Protection in Information Processing Systems*. Berlin, Heidelberg: Springer (IFIP Advances in Information and Communication Technology), pp. 379–390. Available at: https://doi.org/10.1007/978-3-642-39218-4_28.

Kirlappos, I. and Sasse, M.A. (2012) 'Security Education against Phishing: A Modest Proposal for a Major Rethink', *IEEE Security Privacy*, 10(2), pp. 24–32. Available at: https://doi.org/10.1109/MSP.2011.179.

Kumaraguru, P. *et al.* (2009) 'School of phish: a real-word evaluation of anti-phishing training', in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. the 5th Symposium*, Mountain View, California: ACM Press, p. 1. Available at: https://doi.org/10.1145/1572532.1572536.

Kwak, Y. *et al.* (2020) 'Why do users not report spear phishing emails?', *Telematics and Informatics*, 48, p. 101343. Available at: https://doi.org/10.1016/j.tele.2020.101343.

Linkov, V. *et al.* (2019) 'Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research', *Frontiers in Psychology*, 10, p. 995. Available at: https://doi.org/10.3389/fpsyg.2019.00995.

López-Aguilar, P. and Solanas, A. (2021) 'Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism', in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 1363–1368. Available at: https://doi.org/10.1109/COMPSAC51774.2021.00192.

Ltd, I.-I.B. (2018) 'A Users' Awareness Study and Influence of Socio-Demography Perception of Anti-Phishing Security Tips', *Acta Informatica Pragensia*, 7(2), pp. 138–151.

*Lufthansa Group* (2022). Available at: https://www.austrian.com/at/en/lufthansa-group (Accessed: 23 August 2022).

Manoharan, S. *et al.* (2021) 'To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails', *Information & Computer Security*, ahead-of-print(ahead-of-print). Available at: https://doi.org/10.1108/ICS-04-2021-0046.

Mansfield-Devine, S. (2018) 'The ever-changing face of phishing', *Computer Fraud & Security*, 2018(11), pp. 17–19. Available at: https://doi.org/10.1016/S1361-3723(18)30111-8.

Martin, S.R., Lee, J.J. and Parmar, B.L. (2021) 'Social distance, trust and getting "hooked": A phishing expedition', *Organizational Behavior and Human Decision Processes*, 166, pp. 39–48. Available at: https://doi.org/10.1016/j.obhdp.2019.08.001.

Mashtalyar, N. *et al.* (2021) 'Social Engineering Attacks: Recent Advances and Challenges', in A. Moallem (ed.) *HCI for Cybersecurity, Privacy and Trust*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 417–431. Available at: https://doi.org/10.1007/978-3-030-77392-2_27.

McCormick, K., Salcedo, J. and Poh, A. (2015) *SPSS® statistics for Dummies®: a Wiley brand; [make everything easier! ; learn to: configure SPSS to produce better results ; get data into and out of SPSS ; produce graphs that best display your data ; extend SPSS with programming options]*. 3. ed. Hoboken, NJ: Wiley (for dummies).

Meyers, J.J. *et al.* (2018) 'Training Future Cybersecurity Professionals in Spear Phishing using SiEVE', in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. New York, NY, USA: Association for Computing Machinery (SIGITE '18), pp. 135–140. Available at: https://doi.org/10.1145/3241815.3241871.

Meyers, L.S. (2013) *Performing data analysis using IBM SPSS(R)*. Hoboken: Wiley.

Miller, B. *et al.* (2020) 'PREVENTION OF PHISHING ATTACKS: A THREE-PILLARED APPROACH', *Issues In Information Systems* [Preprint]. Available at: https://doi.org/10.48009/2_iis_2020_1-8.

Miranda, M.J.A. (2018) 'Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach', 14(2), p. 6.

Mitchell, A. (2020) 'Improving Cybersecurity Behaviors: A Proposal for Analyzing Four Types of Phishing Training', *WISP 2020 Proceedings* [Preprint]. Available at: https://aisel.aisnet.org/wisp2020/2.

Moody, G.D., Galletta, D.F. and Dunn, B.K. (2017) 'Which phish get caught? An exploratory study of individuals′ susceptibility to phishing', *European Journal of Information Systems*, 26(6), pp. 564–584. Available at: https://doi.org/10.1057/s41303-017-0058-x.

Morgan, G.A. (2010) *SPSS for introductory statistics: use and interpretation*. Third edition. New York: Psychology Press.

Mossano, M. *et al.* (2020) 'Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector', in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 130–139. Available at: https://doi.org/10.1109/EuroSPW51379.2020.00026.

Nicholson, J. *et al.* (2020) 'Investigating Teenagers' Ability to Detect Phishing Messages', in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 140–149. Available at: https://doi.org/10.1109/EuroSPW51379.2020.00027.

*Number of e-mail users worldwide 2025* (2021) *Statista*. Available at: https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ (Accessed: 21 March 2022).

Ovelgönne, M. *et al.* (2017) 'Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach', *ACM Transactions on Intelligent Systems and Technology*, 8(4), pp. 1–25. Available at: https://doi.org/10.1145/2890509.

Papatsaroucha, D. *et al.* (2021) 'A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues', *arXiv:2106.09986 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2106.09986 (Accessed: 6 December 2021).

Patayo, C. (2021) *A Preventive and Detective Model for Phishing Attack in Small and Medium Size Businesses*. SSRN Scholarly Paper ID 3777065. Rochester, NY: Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.3777065.

*PayPal - Phishing* (2020). Available at: https://www.oe24.at/digital/mega-betrug-mit-paypal-teure-abzockmasche-in-oesterreich/455077525 (Accessed: 23 August 2022).

Purkait, S., Kumar De, S. and Suar, D. (2014) 'An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website', *Information Management & Computer Security*, 22(3), pp. 194–234. Available at: https://doi.org/10.1108/IMCS-05-2013-0032.

Qabajeh, I., Thabtah, F. and Chiclana, F. (2018) 'A recent review of conventional vs. automated cybersecurity anti-phishing techniques', *Computer Science Review*, 29, pp. 44–55. Available at: https://doi.org/10.1016/j.cosrev.2018.05.003.

Rastenis, J. *et al.* (2020) 'Impact of Information Security Training on Recognition of Phishing Attacks: A Case Study of Vilnius Gediminas Technical University', in T. Robal et al. (eds) *Databases and Information Systems*. Cham: Springer International Publishing (Communications in Computer and Information Science), pp. 311–324. Available at: https://doi.org/10.1007/978-3-030-57672-1_23.

Redaktionsteam, S. de (2019) 'Netflix - Phishing', *Anti-Spam Info*, 22 October. Available at: https://www.spam-info.de/12115/netflix-phishing-ihr-konto-ist-gesperrt/ (Accessed: 2 August 2022).

Redaktionsteam, S. de (2020a) 'Media Markt - Phishing', *Anti-Spam Info*, 7 December. Available at: https://www.spam-info.de/13299/datensammler-verschenken-media-markt-geschenkkarten-fake/ (Accessed: 2 August 2022).

Redaktionsteam, S. de (2020b) 'PayPal - Phishing', *Anti-Spam Info*, 26 July. Available at: https://www.spam-info.de/12956/paypal-phishing-ihr-konto-wurde-begrenzt-2/ (Accessed: 2 August 2022).

Reinheimer, B. *et al.* (2020) 'An investigation of phishing awareness and education over time: When and how to best remind users', in. *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pp. 259–284. Available at: https://www.usenix.org/conference/soups2020/presentation/reinheimer (Accessed: 6 December 2021).

Rutherford, R. (2018) 'The changing face of phishing', *Computer Fraud & Security*, 2018(11), pp. 6–8. Available at: https://doi.org/10.1016/S1361-3723(18)30107-6.

Sarginson, N. (2020) 'Securing your remote workforce against new phishing attacks', *Computer Fraud & Security*, 2020(9), pp. 9–12. Available at: https://doi.org/10.1016/S1361-3723(20)30096-8.

Sebescen, N. and Vitak, J. (2017) 'Securing the human: Employee security vulnerability risk in organizational settings', *Journal of the Association for Information Science and Technology*, 68(9), pp. 2237–2247. Available at: https://doi.org/10.1002/asi.23851.

*SoSciSurvey* (2022). Available at: https://www.soscisurvey.de/help/doku.php/de:start (Accessed: 21 August 2022).

Sözen, E. and Güven, U. (2019) 'The Effect of Online Assessments on Students' Attitudes towards Undergraduate-Level Geography Courses', *International Education Studies*, 12(10), pp. 1–8.

*SPSS für Studierende* (2022) *FernFH*. Available at: https://shop.fernfh.ac.at/software/25-spss-fuer-studierende.html (Accessed: 23 August 2022).

*Statista - Durchschnittliche Bilanzsumme Banken 2021* (2021) *Statista*. Available at: https://de.statista.com/statistik/daten/studie/298774/umfrage/bilanzsumme-der-banken-in-oesterreich/ (Accessed: 21 August 2022).

*Statista - Nutzung von Videoportalen 2022* (2022) *Statista*. Available at: https://de.statista.com/statistik/daten/studie/879284/umfrage/umfrage-zur-nutzung-von-videoportalen-in-oesterreich/ (Accessed: 21 August 2022).

*Statista - Paketsendungen 2021* (2021) *Statista*. Available at: https://de.statista.com/statistik/daten/studie/297444/umfrage/paketsendungen-oesterreischische-post/ (Accessed: 21 August 2022).

*Statista - Top 10 der Online-Shops* (2020) *Statista Infografiken*. Available at: https://de.statista.com/infografik/716/die-top-10-online-shops-in-oesterreich-nach-umsatz/ (Accessed: 21 August 2022).

*Statista - Zahlungsmethoden am Handy 2020* (2020) *Statista*. Available at: https://de.statista.com/statistik/daten/studie/455026/umfrage/nutzung-von-zahlungsmitteln-beim-mobile-commerce-in-oesterreich/ (Accessed: 21 August 2022).

Sumner, A. *et al.* (2021) 'Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings', *Journal of Computer Information Systems*, 0(0), pp. 1–23. Available at: https://doi.org/10.1080/08874417.2021.1955638.

Thomas, J. (2018) *Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks*. SSRN Scholarly Paper ID 3171727. Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=3171727 (Accessed: 6 December 2021).

Tornblad, M.K., Jones, K.S., *et al.* (2021) 'Characteristics that Predict Phishing Susceptibility: A Review', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 65(1), pp. 938–942. Available at: https://doi.org/10.1177/1071181321651330.

Tornblad, M.K., Armstrong, M.E., *et al.* (2021) 'Unrealistic Promises and Urgent Wording Differently Affect Suspicion of Phishing and Legitimate Emails', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 65(1), pp. 363–367. Available at: https://doi.org/10.1177/1071181321651277.

Verma, J.P. and Abdel-Salam, A.-S.G. (2019) *Testing statistical assumptions in research*. Hoboken, NJ: Wiley.

Williams, E.J., Hinds, J. and Joinson, A.N. (2018) 'Exploring susceptibility to phishing in the workplace', *International Journal of Human-Computer Studies*, 120, pp. 1–13. Available at: https://doi.org/10.1016/j.ijhcs.2018.06.004.

Wosah, N.P. and Win, T. (2021) 'Phishing Mitigation Techniques: A Literature Survey', *International Journal of Network Security & Its Applications*, 13(2), pp. 63–72. Available at: https://doi.org/10.5121/ijnsa.2021.13205.

Yan, Z. *et al.* (2018) 'Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?', *Computers in Human Behavior*, 84, pp. 375–382. Available at: https://doi.org/10.1016/j.chb.2018.02.019.

Yanakiev, Y. *et al.* (2020) *Human Systems Integration Approach to Cyber Security NATO STO Technical Report*. Available at: https://doi.org/10.14339/STO-TR-HFM-259.

Yang, W. *et al.* (2017) 'Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experiment', in *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp*. New York, NY, USA: Association for Computing Machinery (HoTSoS), pp. 52–61. Available at: https://doi.org/10.1145/3055305.3055310.

Yeoh, W. *et al.* (2021) 'Simulated Phishing Attack and Embedded Training Campaign', *Journal of Computer Information Systems*, 0(0), pp. 1–20. Available at: https://doi.org/10.1080/08874417.2021.1919941.

Younis, Y.A. and Musbah, M. (2020) 'A Framework to Protect Against Phishing Attacks', in *Proceedings of the 6th International Conference on Engineering & MIS 2020*. New York, NY, USA: Association for Computing Machinery (ICEMIS'20), pp. 1–6. Available at: https://doi.org/10.1145/3410352.3410825.

Zielinska, O.A. *et al.* (2014) 'One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), pp. 1466–1470. Available at: https://doi.org/10.1177/1541931214581306.

# 6 Abbildungsverzeichnis

Abbildung 1: Ergebnis - Geschlecht ..... 109

Abbildung 2: Ergebnis - Höchste abgeschlossene Ausbildung ..... 110

Abbildung 3: Ergebnis - Arbeitsbereich ..... 111

Abbildung 4: Ergebnis - Arbeitsjahre ..... 111

Abbildung 5: Ergebnis – Wochenstundenanzahl ..... 112

Abbildung 6: Ergebnis - Phishing Vertrautheit (Gesamt) ..... 113

Abbildung 7: Ergebnis - Phishing Awareness (Gesamt) ..... 114

Abbildung 8: Ergebnis - Sicherheitsgewohnheiten (Gesamt) ..... 114

Abbildung 9: Ergebnis - UniCredit Bank Austria AG (Phishing-E-Mail) ..... 116

Abbildung 10: Ergebnis - Austrian Airlines AG (Legitime E-Mail) ..... 117

Abbildung 11: Ergebnis - Media Markt (Phishing-E-Mail) ..... 117

Abbildung 12: Ergebnis - Amazon (Phishing-E-Mail) ..... 118

Abbildung 13: Ergebnis - Wiener Linien (Legitime E-Mail) ..... 119

Abbildung 14: Ergebnis - Netflix (Phishing-E-Mail) ..... 120

Abbildung 15: Ergebnis - Lieferando (Legitime E-Mail) ..... 121

Abbildung 16: Ergebnis - FinanzOnline (Legitime E-Mail) ..... 121

Abbildung 17: Ergebnis - PayPal (Phishing-E-Mail) ..... 122

Abbildung 18: Ergebnis - Österreichische Post AG (Phishing-E-Mail) ..... 123

Abbildung 19: Ergebnis - Phishing Anfälligkeit (E-Mail) anhand des Geschlechts ..... 123

Abbildung 20: Ergebnis - Phishing Anfälligkeit (E-Mail) anhand Teilnahme Schulung 124

Abbildung 21: Ergebnis - Phishing URL 1 ..... 125

Abbildung 22: Ergebnis - Phishing URL 2 ..... 125

Abbildung 23: Ergebnis - Phishing URL 3 ..... 126

Abbildung 24: Ergebnis - Phishing URL 4 ..... 127

Abbildung 25: Ergebnis - Phishing URL 5 ..... 127

Abbildung 26: Ergebnis - Legitime URL 1 ..... 128

Abbildung 27: Ergebnis - Legitime URL 2 ..... 129

Abbildung 28: Ergebnis - Legitime URL 3 ..... 129

Abbildung 29: Ergebnis - Legitime URL 4 ..... 130

Abbildung 30: Ergebnis - Legitime URL 5 ..... 130

Abbildung 31: Ergebnis - Phishing Anfälligkeit (URL) anhand des Geschlechts ..... 131

Abbildung 32: Ergebnis - Phishing Anfälligkeit (URL) anhand Teilnahme Schulung ... 132

Abbildung 33: Ergebnis - Phishing Anfälligkeit (E-Mail und URL) anhand des Geschlechts ..... 133

Abbildung 34: Ergebnis - Phishing Anfälligkeit (E-Mail und URL) anhand Teilnahme Schulung ..... 133

Abbildung 35: Ergebnis - Teilnahme Schulung ..... 134

Abbildung 36: Ergebnis - Phishing Vertrautheit (3. Aussage) ..... 135

Abbildung 37: Ergebnis - Schulungsmethode ..... 136

Abbildung 38: Ergebnis - Letzte Phishing Schulung ..... 136

Abbildung 39: Diskussion - PV (1. Aussage) ..... 146

Abbildung 40: Diskussion - PA (7. Aussage) ..... 149

Abbildung 41: Diskussion - SG (3. Aussage) ..... 151

Abbildung 42: Diskussion - PK (Gesamt) ..... 153

Abbildung 43: Rücklaufstatistik Fragebogen ..... 1

Abbildung 44: Fragebogen Seite 0 (Ausschlussverfahren Text) ..... 2

Abbildung 45: Fragebogen Seite 1 (Willkommenstext) und 2 (Frage Ausschlussverfahren) ..... 3

Abbildung 46: Fragebogen Seite 3 (Phishing Definition) und 4 (Phishing Vertrautheit) .. 4

Abbildung 47: Fragebogen Seite 5 (Phishing Awareness) ..... 5

Abbildung 48: Fragebogen Seite 6 (Sicherheitsgewohnheiten) ..... 6

Abbildung 49: Fragebogen Seite 7 (Unicredit Bank Austria AG - Phishing-E-Mail) ..... 7

Abbildung 50: Fragebogen Seite 8 (Austrian Airlines AG - Legitime E-Mail) ..... 8

Abbildung 51: Fragebogen Seite 9 (Media Markt - Phishing-E-Mail) ..... 9

Abbildung 52: Fragebogen Seite 10 (Amazon - Phishing-E-Mail) .....10

Abbildung 53: Fragebogen Seite 11 (Wiener Linien - Legitime E-Mail) .....11

Abbildung 54: Fragebogen Seite 12 (Netflix - Phishing-E-Mail) .....12

Abbildung 55: Fragebogen Seite 13 (Lieferando - Legitime E-Mail) .....13

Abbildung 56: Fragebogen Seite 14 (FinanzOnline - Legitime E-Mail) .....14

Abbildung 57: Fragebogen Seite 15 (Paypal - Phishing-E-Mail) .....15

Abbildung 58: Fragebogen Seite 16 (Österreichische Post AG - Phishing-E-Mail).....16

Abbildung 59: Fragebogen Seite 17 (URL Phishing und Legitim) und 18 (Teilnahme Phishing Schulung).....17

Abbildung 60: Fragebogen Seite 19 (Erhaltene Schulung) und 20 (Letzte Schulung).....18

Abbildung 61: Fragebogen Seite 21 - 0. Teil (Jump1) .....18

Abbildung 62: Fragebogen Seite 21 - 1. Teil (Bevorzugte Phishing Schulung).....19

Abbildung 63: Fragebogen Seite 21 - 2. Teil (Bevorzugte Phishing Schulung) und 22 (Geschlecht).....20

Abbildung 64: Fragebogen Seite 23 (Höchste abgeschlossene Ausbildung) und 24 (Arbeitsbereich)....21

Abbildung 65: Fragebogen Seite 25 (Arbeitsjahre), Seite 26 (Wochenstundenanzahl) und Seite 27 (Danke Text)....22

Abbildung 66: Bevorzugte Phishing Schulungsmethode (Herkömmlich) anhand des Geschlechts....23

Abbildung 67: Bevorzugte Phishing Schulungsmethode (Eingebettet) anhand des Geschlechts....23

Abbildung 68: Bevorzugte Phishing Schulungsmethode (Simuliert) anhand des Geschlechts....24

Abbildung 69: Bevorzugte Phishing Schulungsmethode (Spielbasiert) anhand des Geschlechts....24

Abbildung 70: Bevorzugte Phishing Schulungsmethode (Achtsamkeit) anhand des Geschlechts....25

Abbildung 71: Bevorzugte Phishing Schulungsmethode (Herkömmlich) anhand Teilnahme Schulung....25

Abbildung 72: Bevorzugte Phishing Schulungsmethode (Eingebettet) anhand Teilnahme Schulung....26

Abbildung 73: Bevorzugte Phishing Schulungsmethode (Simuliert) anhand Teilnahme Schulung....26

Abbildung 74: Bevorzugte Phishing Schulungsmethode (Spielbasiert) anhand Teilnahme Schulung....27

Abbildung 75: Bevorzugte Phishing Schulungsmethode (Achtsamkeit) anhand Teilnahme Schulung....27

Abbildung 76: Streudiagramm - Phishing Anfälligkeit Gesamt und Phishing Vertrautheit....28

Abbildung 77: Streudiagramm - Phishing Anfälligkeit Gesamt und Phishing Awareness....28

Abbildung 78: Streudiagramm - Phishing Anfälligkeit Gesamt und Sicherheitsgewohnheiten.....29

# 7 Tabellenverzeichnis

Tabelle 1: Bewertungsbereich Likert Skala ..... 113

Tabelle 2: Ergebnis - Phishing Definition ..... 115

Tabelle 3: Ergebnis - Bevorzugte Phishing Schulungsmethode ..... 137

Tabelle 4: Auswertung - Cronbach´s Alpha (Phishing Vertrautheit) ..... 138

Tabelle 5: Auswertung - Cronbach´s Alpha (Phishing Awareness) ..... 138

Tabelle 6: Auswertung - Cronbach´s Alpha (Sicherheitsgewohnheiten) ..... 139

Tabelle 7: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit Gesamt) ..... 139

Tabelle 8: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit E-Mail) ..... 139

Tabelle 9: Auswertung - Cronbach´s Alpha (Phishing Anfälligkeit URL) ..... 139

Tabelle 10: Auswertung - Test für Normalverteilung PK Ges ..... 140

Tabelle 11: Auswertung - Mann-Whitney U Test (PKGes & Geschlecht) ..... 141

Tabelle 12: Auswertung - Mann-Whitney U Test (PKGes & Teilnahme Phishing Schulung) ..... 141

Tabelle 13: Auswertung - Spearman Korrelation (PK Ges, PV, PA und SG) ..... 143

Tabelle 14: Diskussion - Spearman Korrelation (PK Ges und PV - 1. & 5. Aussage) ..... 145

Tabelle 15: Diskussion - PV (8. Aussage) ..... 146

Tabelle 16: Diskussion - PV (9. Aussage) ..... 147

Tabelle 17: Diskussion - PV (10. Aussage) ..... 147

Tabelle 18. Diskussion - PA (2. Aussage) ..... 147

Tabelle 19: Diskussion - PA (3. Aussage) ..... 148

Tabelle 20: Diskussion - PA (4. Aussage) ..... 148

Tabelle 21: Diskussion - PA (10. Aussage) ..... 149

Tabelle 22: Diskussion - PA (11. Aussage) ..... 150

Tabelle 23: Diskussion - PA (9. Aussage) ..... 150

Tabelle 24: Diskussion - SG (5. Aussage) ..... 151

Tabelle 25: Diskussion - SG (6. Aussage) ..... 152

Tabelle 26: Diskussion - SG (7. Aussage) ..... 152

Tabelle 27: Diskussion - SG (9. Aussage) ..... 152

# Anhang A

Bisher wurden **178** Interviews abgeschlossen.

Interviews: 178
Gültige Fälle: 135 **Auswahlkriterien**
Pretests: 0
Datensätze inkl. Testdaten: 178
Stand: 13.08.2022, 19:08 Uhr

| Fragebogen | Klicks | Datensätze abgeschlossen | Interviews gesamt | Gültige Fälle (Download) |
|---|---|---|---|---|
| **Fragebogen** MA-FB | 279 | 135 | 178 | 135 |
| **Gesamt** | **279** | **135** | **178** | **135** |

**Einzelstatistik zu Ausstiegsseiten**
Bitte oben den entsprechenden Fragebogen anklicken
**Fragebogen**

| Letzte bearbeitete Seite | Datensätze abgeschlossen | Interviews gesamt | kumulativ |
|---|---|---|---|
| Seite **26** | 121 | 121 | 121 |
| Seite **21** | 0 | 1 | 122 |
| Seite **18** | 0 | 2 | 124 |
| Seite **16** | 0 | 3 | 127 |
| Seite **12** | 0 | 1 | 128 |
| Seite **10** | 0 | 1 | 129 |
| Seite **9** | 0 | 2 | 131 |
| Seite **6** | 0 | 5 | 136 |
| Seite **5** | 0 | 7 | 143 |
| Seite **4** | 0 | 11 | 154 |
| Seite **3** | 0 | 5 | 159 |
| Seite **2** | 14 | 19 | 178 |
| **Gesamt** | **135** | **178** | |

Insgesamt wurden 279 Aufrufe (Klicks) für diesen Fragebogen aufgezeichnet (einschließlich versehentlicher doppelter Klicks, Aufrufe durch Suchmaschinen, ...).

**Rücklauf im Zeitverlauf**

Sie können das Diagramm per Rechtsklick → *Grafik speichern unter* in Druckauflösung herunterladen.

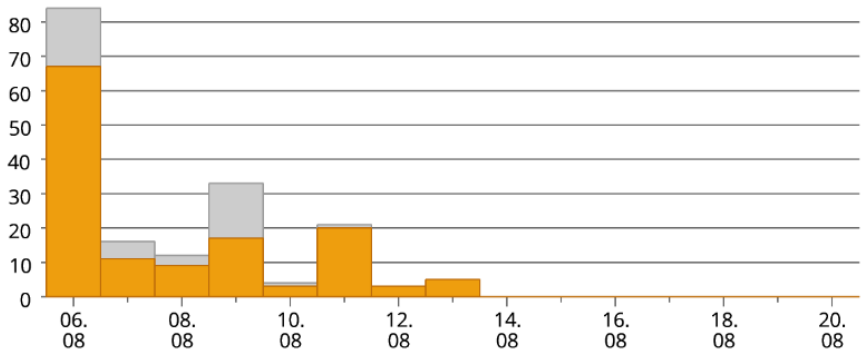



*Abbildung 43: Rücklaufstatistik Fragebogen*

## Danke!

Liebe Teilnehmerin, lieber Teilnehmer,

Sie haben bei der ersten Frage die Antwortmöglichkeit: „Nein, ich habe noch nie in einem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet." ausgewählt und sind somit am Ende dieser Umfrage.

Falls Sie doch jemals in einem Unternehmen in Österreich mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet haben, würde ich Sie bitten die Umfrage von neu zu starten. Vielleicht haben Sie ein Praktikum oder eine geringfügige/Teilzeit Beschäftigung ausgeübt und dies auch nur für eine kurze Zeit.

Falls dies nicht der Fall sein sollte, bedanke ich mich recht herzlich für Ihre Teilnahme an meiner Studie. Sie haben einen wichtigen Beitrag zu dieser Studie geleistet und mir dabei geholfen einen Schritt näher zum Abschluss meines Masterstudiums zu kommen.

Umfragelink: www.soscisurvey.de/phishingschulungsmethoden/
Dieser Link kann gerne geteilt werden.

Wenn Sie Fragen zu der Umfrage haben, senden Sie mir eine E-Mail an: sharon.velikkakath@mail.fernfh.ac.at.

Mit freundlichen Grüßen,
Velikkakath Sharon

---

B.Sc. Sharon Velikkakath, Ferdinand Porsche FernFH – 2022

*Abbildung 44: Fragebogen Seite 0 (Ausschlussverfahren Text)*

**Seite 01**

FT01

# Willkommen!

Liebe Teilnehmerin, lieber Teilnehmer,

mein Name ist Sharon Velikkakath, ich studiere Wirtschaftsinformatik und verfasse derzeit meine Masterarbeit. Ich bedanke mich recht herzlich für die Teilnahme zu der Umfrage über die Sichtweise der Arbeitnehmer und Arbeitnehmerinnen in Österreich in Bezug auf Phishing Schulungsmethoden. Falls Sie jemals in einem Unternehmen in Österreich mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet haben, sei es als Praktikum, Teilzeit- oder Vollzeit-Position, bitte ich Sie diesen Fragebogen auszufüllen.

Die Bearbeitungsdauer dieser Umfrage beträgt ca. 8-10 Minuten. Für den Erfolg der Studie ist es mir sehr wichtig, dass Sie den Fragebogen vollständig ausfüllen und keine Fragen auslassen. Bitte benutzen Sie nicht die "Zurück"-Taste Ihres Browsers, ansonsten kann der Fragebogen nicht mehr fortgesetzt werden und Ihr Fortschritt geht verloren.

Alle Daten werden anonym erhoben und streng vertraulich behandelt. Wenn Sie Fragen zu der Umfrage haben, senden Sie mir eine E-Mail an: sharon.velikkakath@mail.fernfh.ac.at.

Umfragelink: www.soscisurvey.de/phishingschulungsmethoden/
Dieser Link kann gerne geteilt werden.

Ich bedanke mich schon im Voraus für die Teilnahme und über Ihre wertvolle Zeit.

Mit freundlichen Grüßen,
Velikkakath Sharon

**Seite 02**

AV01

**1. Haben Sie jemals in einem Unternehmen in Österreich mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet?**

- ◯ **Ja**, ich arbeite **derzeit** in einem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen.
- ◯ **Ja**, ich habe **bereits** in einem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet.
- ◯ **Nein**, ich habe noch **nie** in einem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet.

**1 aktive(r) Filter**

**Filter AV01/F1**
Wenn eine der folgenden Antwortoption(en) ausgewählt wurde: **3**
Dann nach dem Klick auf "Weiter" den Text **FT03** anzeigen und das Interview beenden

*Abbildung 45: Fragebogen Seite 1 (Willkommenstext) und 2 (Frage Ausschlussverfahren)*

**Seite 03**

PV01

**2. Bitte beantworten Sie die folgende Frage.**

**Phishing ist:**

Sie können nur eine Antwortmöglichkeit auswählen.

- ◯ Eine Art von Social-Engineering-Angriff, der darauf abzielt, sensible Daten wie Passwörter und Kreditkarten von Ihnen zu stehlen, indem es sich als vertrauenswürdiges Unternehmen oder Person tarnt.
- ◯ Eine Art bösartiges Programm, das darauf abzielt, Ihr Gerät zu beschädigen, und das wie ein legitimes Programm aussieht.
- ◯ Ein Virus, der sich selbst duplizieren und auf Ihren Geräten verbreiten kann.
- ◯ Keine der Antwortmöglichkeiten stimmt.

**Seite 04**

PV02

**3. Wie vertraut sind Sie mit dem Thema: „Phishing“?**

Bitte beantworten Sie die nachfolgenden Aussagen anhand folgender Skala:

| | stimme überhaupt nicht zu | stimme nicht zu | stimme weder zu noch stimme zu | stimme zu | stimme voll und ganz zu |
|---|---|---|---|---|---|
| Ich bin selbst auf eine Phishing-Attacke hereingefallen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ich kenne jemanden, der auf eine Phishing-Attacke hereingefallen ist. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ich habe eine Schulung zum Thema Computer-/Informationssicherheit erhalten. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ich weiß allgemein über Phishing-Angriffe Bescheid. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ich weiß, wie man einen Phishing-Angriff verhindern kann. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Wenn ich das Internet benutze, kann ich eine Phishing-Website erkennen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Wenn ich meine E-Mail benutze, kann ich eine Phishing-E-Mail erkennen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ein Phishing-Angriff kann durch Telefonanrufe erfolgen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ein Phishing-Angriff kann über SMS erfolgen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Ein Phishing-Angriff kann über Soziale Medien erfolgen. | ◯ | ◯ | ◯ | ◯ | ◯ |
| Eine Phishing-E-Mail enthält immer Links zu Webseiten. | ◯ | ◯ | ◯ | ◯ | ◯ |

*Abbildung 46: Fragebogen Seite 3 (Phishing Definition) und 4 (Phishing Vertrautheit)*

PA01

**4. Wie würden Sie ihre Awareness Kenntnisse einschätzen?**

Bitte beantworten Sie die nachfolgenden Aussagen anhand folgender Skala:

| | stimme überhaupt nicht zu | stimme nicht zu | stimme weder zu noch stimme zu | stimme zu | stimme voll und ganz zu |
|---|---|---|---|---|---|
| Ich vergewissere mich oft, ob eine Website seriös ist. | ○ | ○ | ○ | ○ | ○ |
| Ich kenne den Unterschied zwischen Website-Adressen, die mit „http://" und „https://" beginnen. | ○ | ○ | ○ | ○ | ○ |
| Ich habe meinen Benutzernamen und mein Passwort noch **nie** auf einer Website eingegeben, deren Adresse mit „http://" beginnt. | ○ | ○ | ○ | ○ | ○ |
| Ich habe meine Bankomat-/Kreditkartendaten noch **nie** auf einer Website eingegeben, deren Adresse mit „http://" beginnt. | ○ | ○ | ○ | ○ | ○ |
| Ich habe meine Bankomat -/Kreditkartendaten noch **nie** per Telefon (per Sprach- oder Textnachricht) weitergegeben. | ○ | ○ | ○ | ○ | ○ |
| Ich öffne **nie** E-Mails von unbekannten Absendern. | ○ | ○ | ○ | ○ | ○ |
| Ich prüfe sorgfältig, ob eine E-Mail, die ich erhalten habe, verdächtige Links oder Anhänge enthält, auch wenn sie von einem mir bekannten Absender kommt. | ○ | ○ | ○ | ○ | ○ |
| Ich bin misstrauisch gegenüber E-Mails, die einen Link enthalten, dessen Absender ich **nicht** kenne. | ○ | ○ | ○ | ○ | ○ |
| Ich scrolle über einen Link in der E-Mail und sehe mir die Adresse genau an, bevor ich auf den Link klicke. | ○ | ○ | ○ | ○ | ○ |
| Ich bin mir des Risikos bewusst, das mit dem Anklicken von E-Mail-Links verbunden ist. | ○ | ○ | ○ | ○ | ○ |
| Ich bin mir des Risikos bewusst, das mit dem Öffnen und/oder Herunterladen von E-Mail-Anhängen verbunden ist. | ○ | ○ | ○ | ○ | ○ |
| Ich öffne **nie** E-Mail-Anhänge. | ○ | ○ | ○ | ○ | ○ |

*Abbildung 47: Fragebogen Seite 5 (Phishing Awareness)*

SG01

**5. Wie würden Sie ihre Sicherheitsgewohnheiten einschätzen?**

Bitte beantworten Sie die nachfolgenden Aussagen anhand folgender Skala:

| | stimme überhaupt nicht zu | stimme nicht zu | stimme weder zu noch stimme zu | stimme zu | stimme voll und ganz zu |
|---|---|---|---|---|---|
| Ich habe ein Virenschutzprogramm auf meinem Computer. | ○ | ○ | ○ | ○ | ○ |
| Ich fühle mich online **nicht** sicher, wenn ich kein aktuelles Antivirenprogramm auf meinem Computer habe. | ○ | ○ | ○ | ○ | ○ |
| Mein Computer wurde noch **nie** mit bösartiger Software infiziert (z.B. Keylogger, Spyware, Viren). | ○ | ○ | ○ | ○ | ○ |
| Ich vergesse mich **nie** abzumelden, wenn mein Computer unbeaufsichtigt ist. | ○ | ○ | ○ | ○ | ○ |
| Ich kenne die Merkmale eines sicheren Passworts. | ○ | ○ | ○ | ○ | ○ |
| Ich habe die Passwörter für alle meine Online-Konten noch **nie** aufgeschrieben. | ○ | ○ | ○ | ○ | ○ |
| Ich verwende **nicht** dasselbe Passwort für mehrere Online-Konten (z. B. persönliches E-Mail-Konto, E-Mail-Konto bei der Arbeit, Konto für soziale Medien, Online-Shopping-Konto). | ○ | ○ | ○ | ○ | ○ |
| Ich ändere mein Passwort regelmäßig aus Sicherheitsgründen. | ○ | ○ | ○ | ○ | ○ |
| Ich schreibe **nie** ein Passwort auf, das schwer zu merken ist. | ○ | ○ | ○ | ○ | ○ |
| Ich habe meinen Kontostand noch **nie** überprüft, während ich in einem öffentlichen WLAN-Netzwerk angemeldet war. | ○ | ○ | ○ | ○ | ○ |
| Ich habe noch **nie** Geld überwiesen, während ich in einem öffentlichen WLAN-Netzwerk angemeldet war. | ○ | ○ | ○ | ○ | ○ |
| Ich habe noch **nie** einen Online-Einkauf getätigt, während ich in einem öffentlichen WLAN-Netzwerk angemeldet war. | ○ | ○ | ○ | ○ | ○ |

*Abbildung 48: Fragebogen Seite 6 (Sicherheitsgewohnheiten)*

PK05

**6. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**

**Betreff:** Die Zugangsdaten Ihres Kundenbereichs sind abgelaufen.
**Von:** "Unicredit AG" <results@kenmbarnes.com>
**Datum:** 18.12.2021, 17:19
**An:**

Sehrgeehrter Kunde.

***Nach mehreren erfolglosen Versuchen, Sie über den Kundenservice anzurufen. Wir haben in Ihrem Kundenbereich eine vertrauliche Nachricht hinterlassen, um Ihnen wichtige Informationen zu Ihrem Konto zu geben. Sie wurden eingeladen, es zu lesen und Ihr Profil so schnell wie möglich zu aktualisieren.***

Öffne die App jetzt

***Mit freundlichen Grüßen.***

Copyright © 2021 Unicredit Bank Austria

Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 49: Fragebogen Seite 7 (Unicredit Bank Austria AG - Phishing-E-Mail)*

PK01

**7. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**


Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.

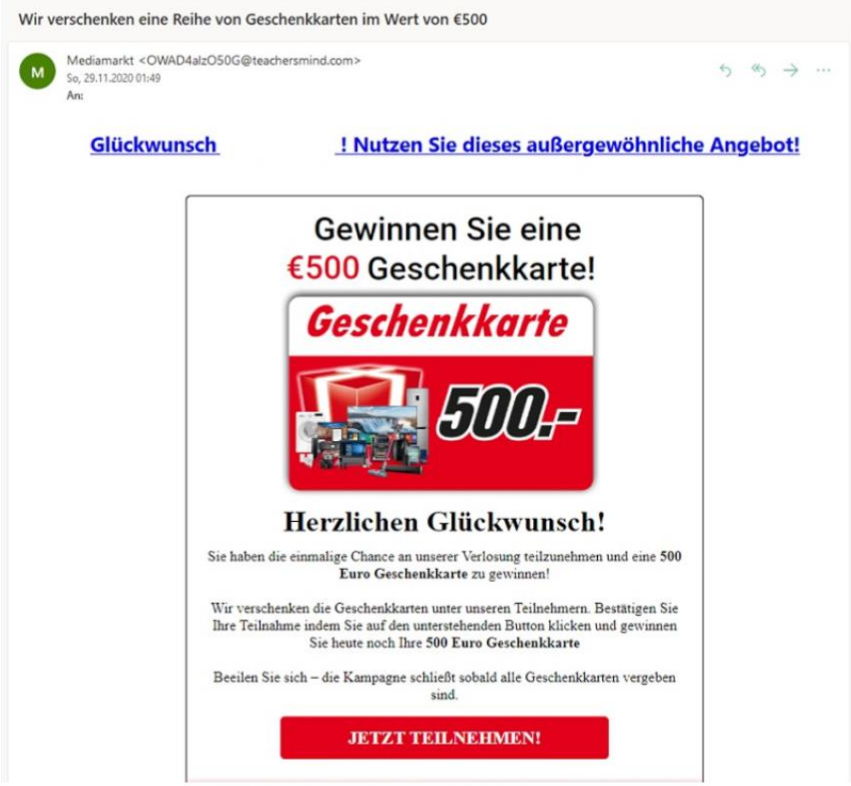
---

- ◯ Ich weiß es nicht.

*Abbildung 50: Fragebogen Seite 8 (Austrian Airlines AG - Legitime E-Mail)*

PK10

**8. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**




Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 51: Fragebogen Seite 9 (Media Markt - Phishing-E-Mail)*

PK07

**9. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**

**Von:** Amazon.de <versandbestaetigung@amazon.de>
**Datum:** 23. Januar 2019 um 10:43:00 MEZ
**An**
**Betreff:** Amazon.de - **Ihre Bestellung 302-6752858-0069827 details**

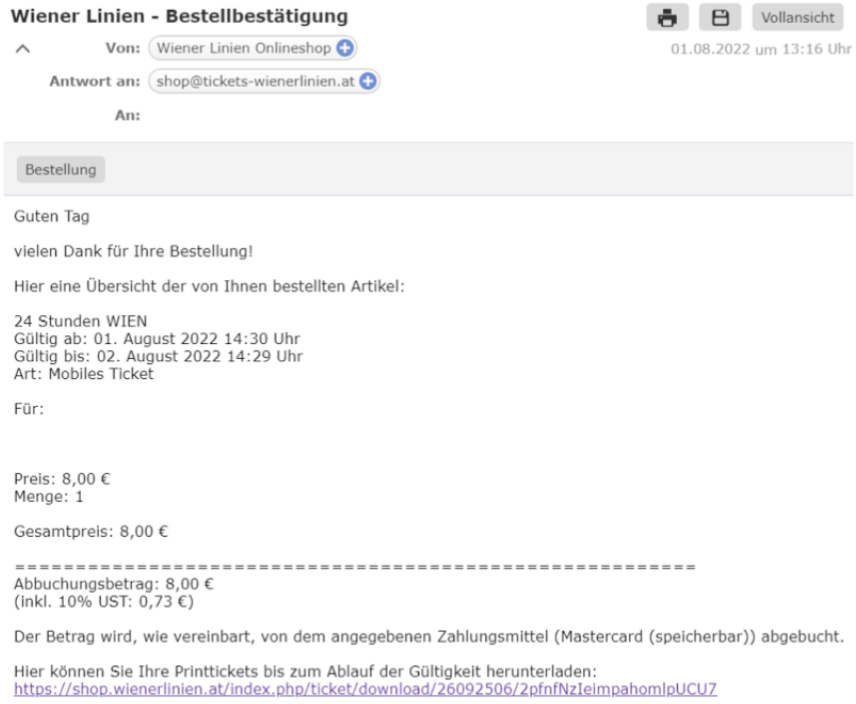

Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 52: Fragebogen Seite 10 (Amazon - Phishing-E-Mail)*

PK02

**10. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**



**Wiener Linien - Bestellbestätigung**

Vollansicht

Von: Wiener Linien Onlineshop 01.08.2022 um 13:16 Uhr

Antwort an: shop@tickets-wienerlinien.at

An:

Bestellung

Guten Tag

vielen Dank für Ihre Bestellung!

Hier eine Übersicht der von Ihnen bestellten Artikel:

24 Stunden WIEN
Gültig ab: 01. August 2022 14:30 Uhr
Gültig bis: 02. August 2022 14:29 Uhr
Art: Mobiles Ticket

Für:

Preis: 8,00 €
Menge: 1

Gesamtpreis: 8,00 €

==========
Abbuchungsbetrag: 8,00 €
(inkl. 10% UST: 0,73 €)

Der Betrag wird, wie vereinbart, von dem angegebenen Zahlungsmittel (Mastercard (speicherbar)) abgebucht.

Hier können Sie Ihre Printtickets bis zum Ablauf der Gültigkeit herunterladen:
https://shop.wienerlinien.at/index.php/ticket/download/26092506/2pfnfNzIeimpahomlpUCU7

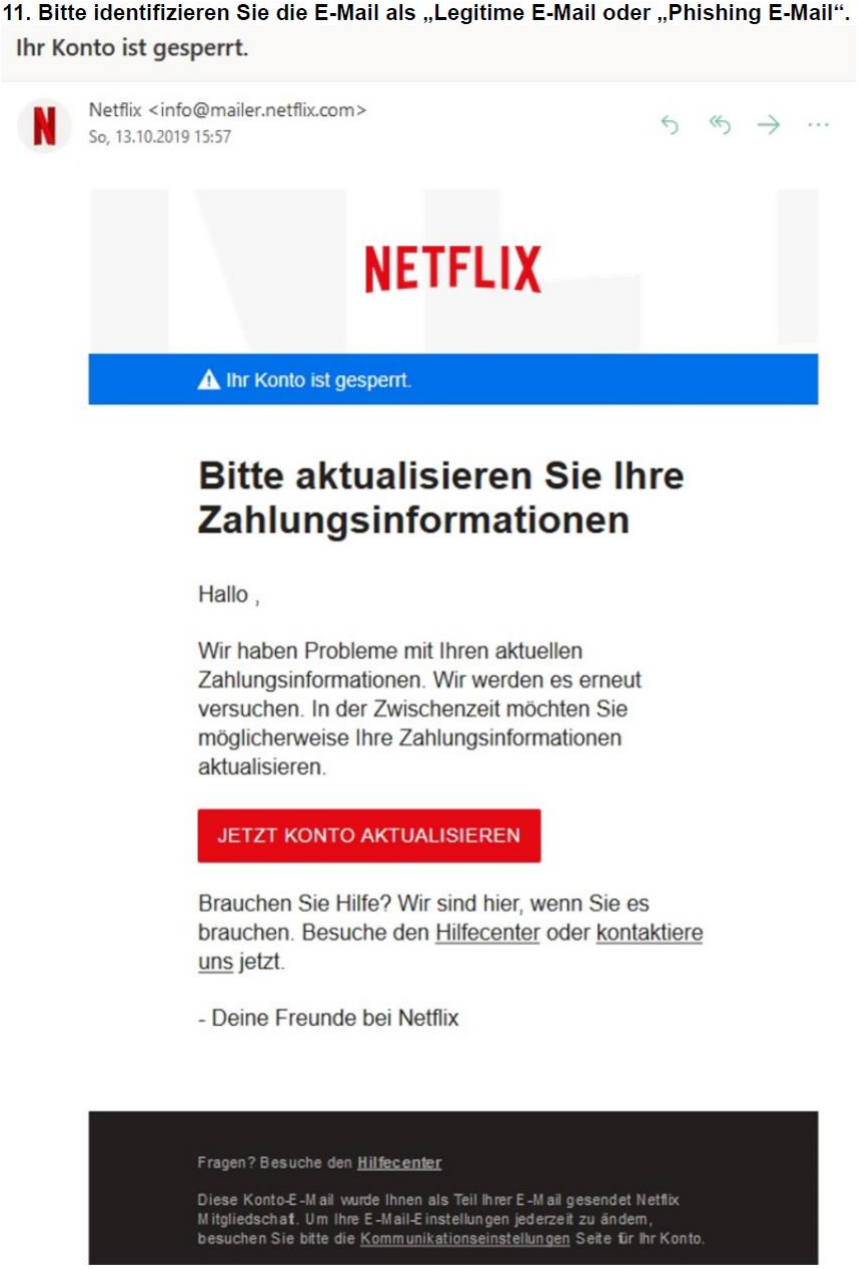
Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 53: Fragebogen Seite 11 (Wiener Linien - Legitime E-Mail)*

PK08

**11. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**



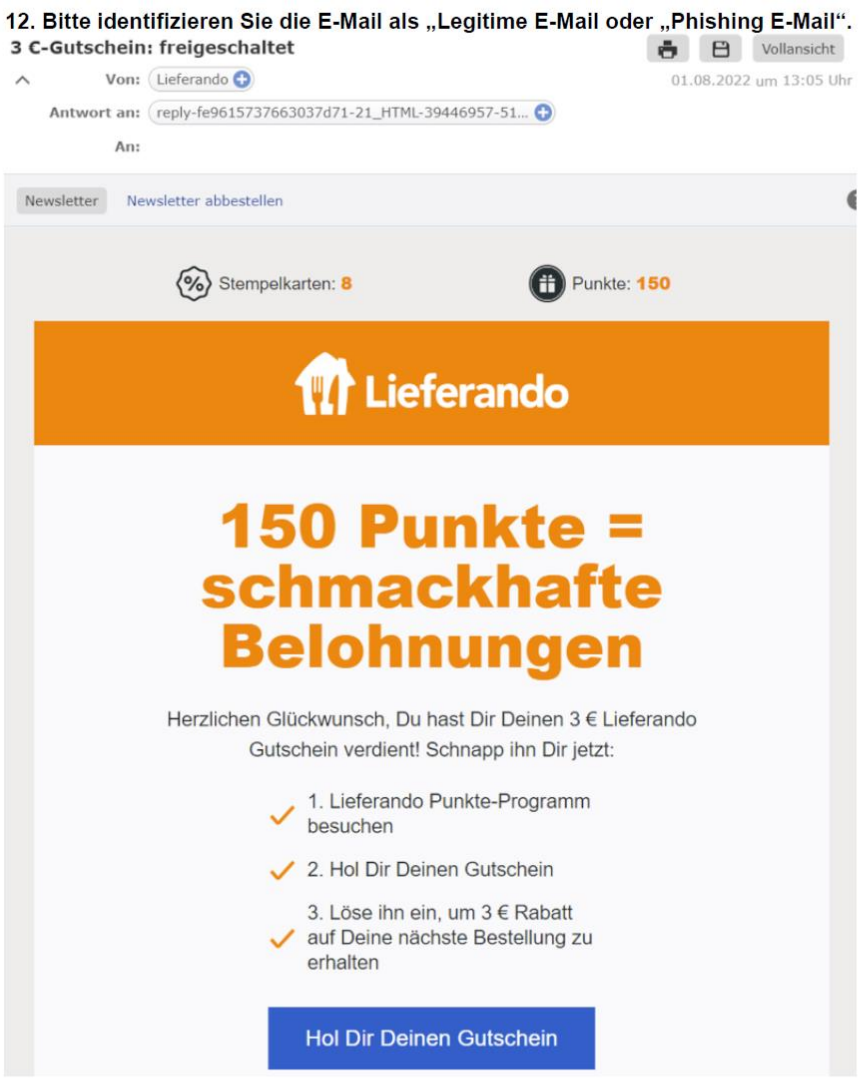

Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 54: Fragebogen Seite 12 (Netflix - Phishing-E-Mail)*

PK03

**12. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**




Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 55: Fragebogen Seite 13 (Lieferando - Legitime E-Mail)*

PK04

**13. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**

Mitteilung von FinanzOnline

F finanzOnline@bmf.gv.at <finanzOnline@bmf.gv.at>
08.07.2022 06:35

An:

Sehr geehrte FinanzOnline-Teilnehmerin, sehr geehrter FinanzOnline-Teilnehmer,

diese E-Mail-Adresse ist als Kontaktadresse für gespeichert.

Sie haben einen neuen Bescheid in Ihren Nachrichten.
Klicken Sie einfach auf https://finanzonline.bmf.gv.at/ und melden Sie sich wie gewohnt an.

Hinweis: Diese Nachricht wurde automatisiert erstellt. Bitte antworten Sie nicht darauf.

Sie haben eine Frage zum System FinanzOnline? Dann rufen Sie bitte 050 233 790 an. Wir sind Montag bis Freitag von 8 bis 17 Uhr für Sie da.
Wenn Sie eine steuerliche Frage haben, wenden Sie sich an Ihr Finanzamt.
Unsere Öffnungszeiten finden Sie unter https://service.bmf.gv.at/service/anwend/behoerden/.

Freundliche Grüße
Ihr Finanzamt

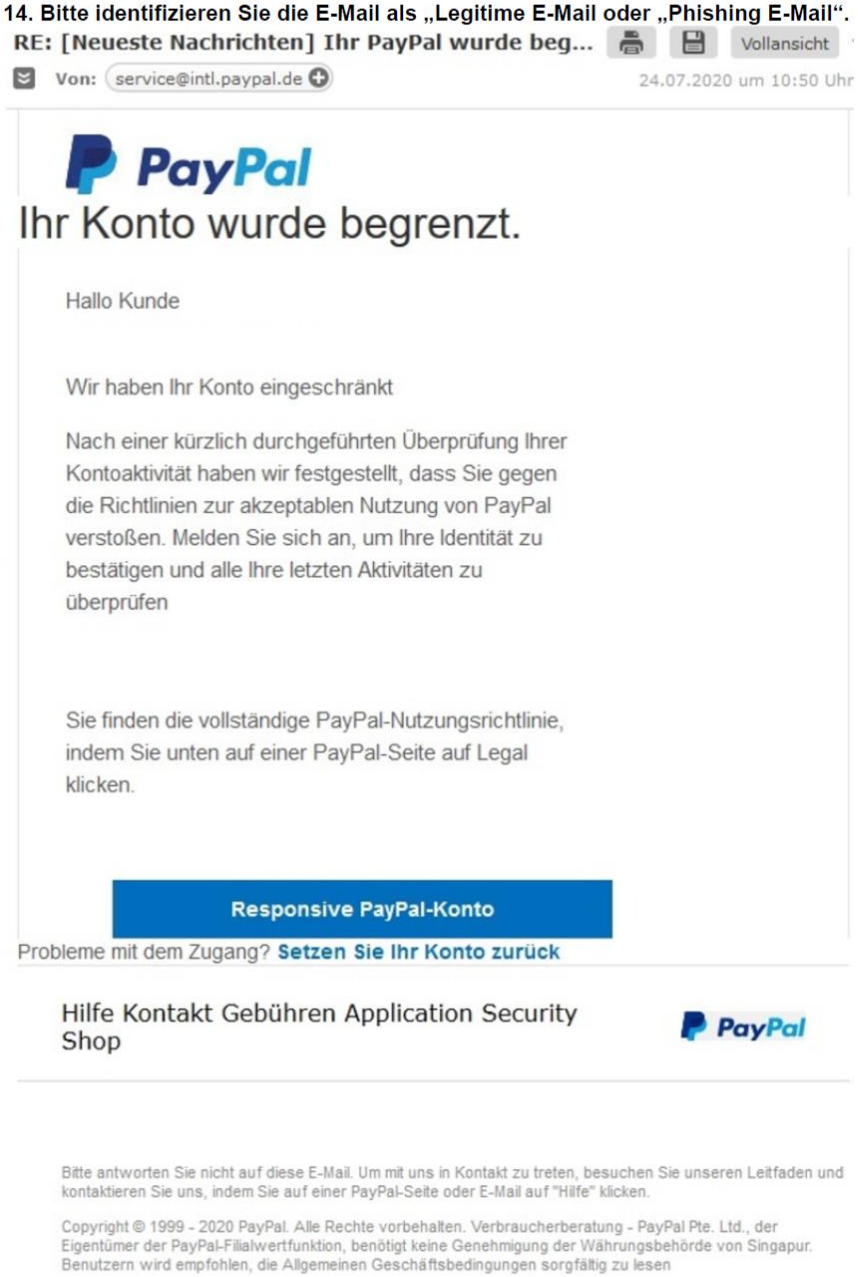
Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 56: Fragebogen Seite 14 (FinanzOnline - Legitime E-Mail)*

PK06

**14. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**




Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 57: Fragebogen Seite 15 (Paypal - Phishing-E-Mail)*

PK09

**15. Bitte identifizieren Sie die E-Mail als „Legitime E-Mail oder „Phishing E-Mail“.**

**Von:** Meine Post [send@meinepost.com]
**Gesendet:** 17.02.2022, 09:21

**Thema:** Dein Paket wartet !

**Bestätigung Ihrer Registrierung**

Dein Paket ist bei uns eingetroffen
Wir informieren Sie, dass für Ihr Paket noch eine Liefergebühr in Höhe
von 2,11 EUR zu zahlen ist.

https://www.post.at/sh/double-optin?token=KYWAwcEDGVI3

Bitte zahlen Sie die Versandkosten für die Lieferung morgen

Freundliche Grüße,
Ihr Post-Team

**Österreichische Post AG**

Aktiengesellschaft
Unternehmenszentrale
Rochusplatz 1, 1030 Wien,
Österreich

**zum Kontaktformular** **Zur Post Website**

Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

- ◯ Legitime E-Mail.
- ◯ Phishing E-Mail.
- ◯ Ich weiß es nicht.

*Abbildung 58: Fragebogen Seite 16 (Österreichische Post AG - Phishing-E-Mail)*

**Seite 17**

PK11

**16. Bitte identifizieren Sie die nachfolgenden URL als „Legitime URL oder „Phishing URL“.**

Wenn Sie sich nicht sicher sind, können Sie die Antwortmöglichkeit „Ich weiß es nicht“ auswählen.

| | Legitime URL | Phishing URL | Ich weiß es nicht |
|---|---|---|---|
| https://www.msn-verify.com/ | ○ | ○ | ○ |
| https://www.amazon.de/gp/help/customer/display.html?nodeId=508510&ref_=nav_cs_help | ○ | ○ | ○ |
| https://www.facebook.com/help/1434403039959381/?helpref=hc_fnav | ○ | ○ | ○ |
| https://www.google.at/?gws_rd=ssl | ○ | ○ | ○ |
| https://www.youtube.com/results?search_query=orf | ○ | ○ | ○ |
| https://www.ebay-security.com | ○ | ○ | ○ |
| https://suppoort.apple.com/ | ○ | ○ | ○ |
| https://www.disney_plus.com/de-de/sign-up?type=standard | ○ | ○ | ○ |
| https://www.netflix.com/at/browse/genre/3652 | ○ | ○ | ○ |
| https://147.46.236.55/PayPal/login.html | ○ | ○ | ○ |

**Seite 18**

DS01

**17. Haben Sie schon einmal an einer Phishing Schulung teilgenommen?**

Beachten Sie bei der Beantwortung der nachfolgenden Fragen, dass diese sich auf das Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen bezieht.

○ Ja, ich habe an einer Schulung teilgenommen, die das Thema Phishing behandelt hat.

○ Nein, ich habe an keiner Schulung teilgenommen, die das Thema Phishing behandelt hat.

○ Ich weiß es nicht.

**2 aktive(r) Filter**

**Filter DS01/F1**
Wenn eine der folgenden Antwortoption(en) ausgewählt wurde: **1, -1**
Dann Frage/Text **DS02** später im Fragebogen anzeigen (sonst ausblenden)

**Filter DS01/F2**
Wenn eine der folgenden Antwortoption(en) ausgewählt wurde: **2**
Dann nach dem Klick auf "Weiter" direkt zur Seite **jump1** springen

*Abbildung 59: Fragebogen Seite 17 (URL Phishing und Legitim) und 18 (Teilnahme Phishing Schulung)*

**Seite 19**

DS02

**18. Welche Art von Schulung haben Sie erhalten?**

Beachten Sie bei der Beantwortung der nachfolgenden Fragen, dass diese sich auf das Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen bezieht.

- ◯ **Herkömmliche Schulung**
  (ist eine Methode, bei der Ausbilder und Ausbilderinnen in einem Seminar mithilfe von video-, grafik- oder textbasiertem Material eine Schulung durchführen.)
- ◯ **Eingebettete Schulung**
  (ist eine Methode, bei der die Mitarbeiter und Mitarbeiterinnen während ihrer Arbeitszeit Phishing-E-Mails erhalten und nicht wissen, dass sie getestet werden. Sobald ein Link angeklickt wurde, werden sofort Rückmeldungen getätigt und Anweisungen angezeigt, sodass der Fehler erkannt wird.)
- ◯ **Simulierte Schulung**
  (ist eine Methode, bei der die Mitarbeiter und Mitarbeiterinnen Phishing-E-Mails erhalten, dies passiert aber nicht während der Arbeitszeit und sie sind sich bewusst sind, dass sie getestet werden. Sobald ein Link angeklickt wurde, werden sofort Rückmeldungen getätigt und Anweisungen angezeigt, sodass der Fehler erkannt wird.)
- ◯ **Spielbasierte Schulung**
  (ist eine Methode, bei der Mitarbeiter und Mitarbeiterinnen mit Hilfe eines Spiels über Phishing-Angriffe lernen)
- ◯ **Achtsamkeitsschulung**
  (ist eine Methode, die den Schutz vor Phishing verbessert, indem die Aufmerksamkeit der Mitarbeiter und Mitarbeiterinnen während der Bewertung einer E-Mail darauf gerichtet wird, ob eine Nachricht eine ausdrückliche Aufforderung (zum Beispiel: "Klicken Sie auf diesen Link") zum Handeln enthält oder nicht. Des Weiteren wird das Bewusstsein des Einzelnen durch aktives Hinterfragen erhöht und verhindert Handlungen im Zusammenhang mit einer verdächtigen Nachricht.)
- ◯ **Keine dieser genannten Schulung habe ich erhalten.**

**2 aktive(r) Filter**

**Filter DS02/F1**
Wenn eine der folgenden Antwortoption(en) ausgewählt wurde: **1, 2, 3, 4, 5**
Dann Frage/Text **DS03** später im Fragebogen anzeigen (sonst ausblenden)

**Filter DS02/F2**
Wenn eine der folgenden Antwortoption(en) ausgewählt wurde: **6**
Dann nach dem Klick auf "Weiter" direkt zur Seite **jump1** springen

**Seite 20**

DS03

**19. Wann haben Sie ihre letzte Phishing Schulung absolviert?**

Beachten Sie bei der Beantwortung der nachfolgenden Fragen, dass diese sich auf das Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen bezieht.

- ◯ Weniger als 1 Monat
- ◯ 1-3 Monate
- ◯ 3-5 Monate
- ◯ Mehr als 5 Monate
- ◯ Ich weiß es nicht.

*Abbildung 60: Fragebogen Seite 19 (Erhaltene Schulung) und 20 (Letzte Schulung)*

**Seite 21**

**jump1**

BS01

*Abbildung 61: Fragebogen Seite 21 - 0. Teil (Jump1)*

**20. Welche Schulungsmethode würden Sie bevorzugen?**

**Erklärung zu den Schulungsmethoden:**

**Herkömmliche Schulung**
(ist eine Methode, bei der Ausbilder und Ausbilderinnen in einem Seminar mithilfe von video-, grafik- oder textbasiertem Material eine Schulung durchführen.)
**Eingebettete Schulung**
(ist eine Methode, bei der die Mitarbeiter und Mitarbeiterinnen während ihrer Arbeitszeit Phishing-E-Mails erhalten und nicht wissen, dass sie getestet werden. Sobald ein Link angeklickt wurde, werden sofort Rückmeldungen getätigt und Anweisungen angezeigt, sodass der Fehler erkannt wird.)
**Simulierte Schulung**
(ist eine Methode, bei der die Mitarbeiter und Mitarbeiterinnen Phishing-E-Mails erhalten, dies passiert aber nicht während der Arbeitszeit und sie sind sich bewusst sind, dass sie getestet werden. Sobald ein Link angeklickt wurde, werden sofort Rückmeldungen getätigt und Anweisungen angezeigt, sodass der Fehler erkannt wird.)
**Spielbasierte Schulung**
(ist eine Methode, bei der Mitarbeiter und Mitarbeiterinnen mit Hilfe eines Spiels über Phishing-Angriffe lernen)
**Achtsamkeitsschulung**
(ist eine Methode, die den Schutz vor Phishing verbessert, indem die Aufmerksamkeit der Mitarbeiter und Mitarbeiterinnen während der Bewertung einer E-Mail darauf gerichtet wird, ob eine Nachricht eine ausdrückliche Aufforderung (zum Beispiel: "Klicken Sie auf diesen Link") zum Handeln enthält oder nicht. Des Weiteren wird das Bewusstsein des Einzelnen durch aktives Hinterfragen erhöht und verhindert Handlungen im Zusammenhang mit einer verdächtigen Nachricht.)

Bitte beantworten Sie die nachfolgenden Aussagen anhand folgender Skala:

| | stimme überhaupt nicht zu | stimme nicht zu | stimme weder zu noch stimme zu | stimme zu | stimme voll und ganz zu |
|---|---|---|---|---|---|
| Die **Herkömmliche Schulung** wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen. | ○ | ○ | ○ | ○ | ○ |
| Die **Herkömmliche Schulung** wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann. | ○ | ○ | ○ | ○ | ○ |
| Die **Herkömmliche Schulung** ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können. | ○ | ○ | ○ | ○ | ○ |
| Die **Herkömmliche Schulung** ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können. | ○ | ○ | ○ | ○ | ○ |
| Die **Eingebettete Schulung** wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen. | ○ | ○ | ○ | ○ | ○ |
| Die **Eingebettete Schulung** wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann. | ○ | ○ | ○ | ○ | ○ |
| Die **Eingebettete Schulung** ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können. | ○ | ○ | ○ | ○ | ○ |
| Die **Eingebettete Schulung** ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können. | ○ | ○ | ○ | ○ | ○ |
| Die **Simulierte Schulung** wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen. | ○ | ○ | ○ | ○ | ○ |

*Abbildung 62: Fragebogen Seite 21 - 1. Teil (Bevorzugte Phishing Schulung)*

| | | | | | |
|---|---|---|---|---|---|
| Die **Simulierte Schulung** wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann. | ○ | ○ | ○ | ○ | ○ |
| Die **Simulierte Schulung** ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können. | ○ | ○ | ○ | ○ | ○ |
| Die **Simulierte Schulung** ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können. | ○ | ○ | ○ | ○ | ○ |
| Die **Spielbasierte Schulung** wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen. | ○ | ○ | ○ | ○ | ○ |
| Die **Spielbasierte Schulung** wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann. | ○ | ○ | ○ | ○ | ○ |
| Die **Spielbasierte Schulung** ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können. | ○ | ○ | ○ | ○ | ○ |
| Die **Spielbasierte Schulung** ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können. | ○ | ○ | ○ | ○ | ○ |
| Die **Achtsamkeitsschulung** wird es mir erleichtern, eine Phishing-E-Mail in Zukunft zu erkennen. | ○ | ○ | ○ | ○ | ○ |
| Die **Achtsamkeitsschulung** wird mir helfen zu verstehen, wie ich Phishing-Angriffe verhindern kann. | ○ | ○ | ○ | ○ | ○ |
| Die **Achtsamkeitsschulung** ist die richtige Methode, um Menschen beizubringen, wie sie Phishing-E-Mails erkennen können. | ○ | ○ | ○ | ○ | ○ |
| Die **Achtsamkeitsschulung** ist eine effektive Methode, um Menschen beizubringen, wie sie Phishing-Angriffe verhindern können. | ○ | ○ | ○ | ○ | ○ |

**Seite 22**

DM01

**21. Bitte wählen Sie ihr Geschlecht aus.**

- ○ Weiblich
- ○ Männlich
- ○ Divers
- ○ Ohne Angabe

*Abbildung 63: Fragebogen Seite 21 - 2. Teil (Bevorzugte Phishing Schulung) und 22 (Geschlecht)*

**Seite 23**

DM02

**22. Bitte wählen Sie die höchste abgeschlossene Ausbildung aus.**

- ◯ Allgemeinbildende Pflichtschule (inkl. Personen ohne Pflichtschulabschluss)
- ◯ Berufsschule und Lehre
- ◯ Berufsbildende mittlere Schule
- ◯ Berufsbildende höhere Schule
- ◯ Allgemeinbildende höhere Schule
- ◯ Akademie
- ◯ Tertiäre Kurzausbildung (Schule für Berufstätige, Aufbaulehrgang, Werkmeister-, Bauhandwerker- & Meisterschule, Kolleg)
- ◯ Bachelorstudium
- ◯ Masterstudium
- ◯ PhD-/Doktorstudium

**Seite 24**

DM03

**23. In welchem Bereich haben Sie bei dem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet oder arbeiten derzeit?**

- ◯ Bau, Baunebengewerbe, Holz, Gebäudetechnik
- ◯ Bergbau, Rohstoffe, Glas, Keramik, Stein
- ◯ Büro, Marketing, Finanz, Recht, Sicherheit
- ◯ Chemie, Biotechnologie, Lebensmittel, Kunststoffe
- ◯ Elektrotechnik, Elektronik, Telekommunikation, IT
- ◯ Handel, Logistik, Verkehr
- ◯ Landwirtschaft, Gartenbau, Forstwirtschaft
- ◯ Maschinenbau, Kfz, Metall
- ◯ Medien, Grafik, Design, Druck, Kunst, Kunsthandwerk
- ◯ Reinigung, Hausbetreuung, Anlern- und Hilfsberufe
- ◯ Soziales, Gesundheit, Schönheitspflege
- ◯ Textil und Bekleidung, Mode, Leder
- ◯ Tourismus, Gastgewerbe, Freizeit
- ◯ Umwelt
- ◯ Wissenschaft, Bildung, Forschung und Entwicklung
- ◯ Andere

*Abbildung 64: Fragebogen Seite 23 (Höchste abgeschlossene Ausbildung) und 24 (Arbeitsbereich)*

**Seite 25**

DM04

**24. Wie lange haben Sie bei dem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet oder arbeiten derzeit schon?**

- ◯ Weniger als 1 Jahr
- ◯ 1–3 Jahre
- ◯ 3–6 Jahre
- ◯ 6–9 Jahre
- ◯ Mehr als 9 Jahre

**Seite 26**

DM05

**25. Welche Wochenstundenanzahl haben Sie bei dem Unternehmen mit mehr als 250 Mitarbeiter und Mitarbeiterinnen gearbeitet oder arbeiten derzeit?**

- ◯ 1-10 Wochenstunden
- ◯ 11-20 Wochenstunden
- ◯ 21-30 Wochenstunden
- ◯ 31-40 Wochenstunden
- ◯ 40+ Wochenstunden

**Letzte Seite**

# Danke!

Liebe Teilnehmerin, lieber Teilnehmer,

ich bedanke mich recht herzlich für Ihre Teilnahme an meiner Studie. Sie haben einen äußerst wichtigen Beitrag zu dieser Studie geleistet und mir mit dem Ausfüllen dieses Fragebogens dabei geholfen, meine Masterarbeit erfolgreich zu absolvieren.

Umfragelink: https://www.soscisurvey.de/phishingschulungsmethoden/"

Dieser Link kann gerne geteilt werden.

Wenn Sie Fragen zu der Umfrage haben, senden Sie mir eine E-Mail an: sharon.velikkakath@mail.fernfh.ac.at.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

Mit freundlichen Grüßen,

Velikkakath Sharon



*Abbildung 65: Fragebogen Seite 25 (Arbeitsjahre), Seite 26 (Wochenstundenanzahl) und Seite 27 (Danke Text)*

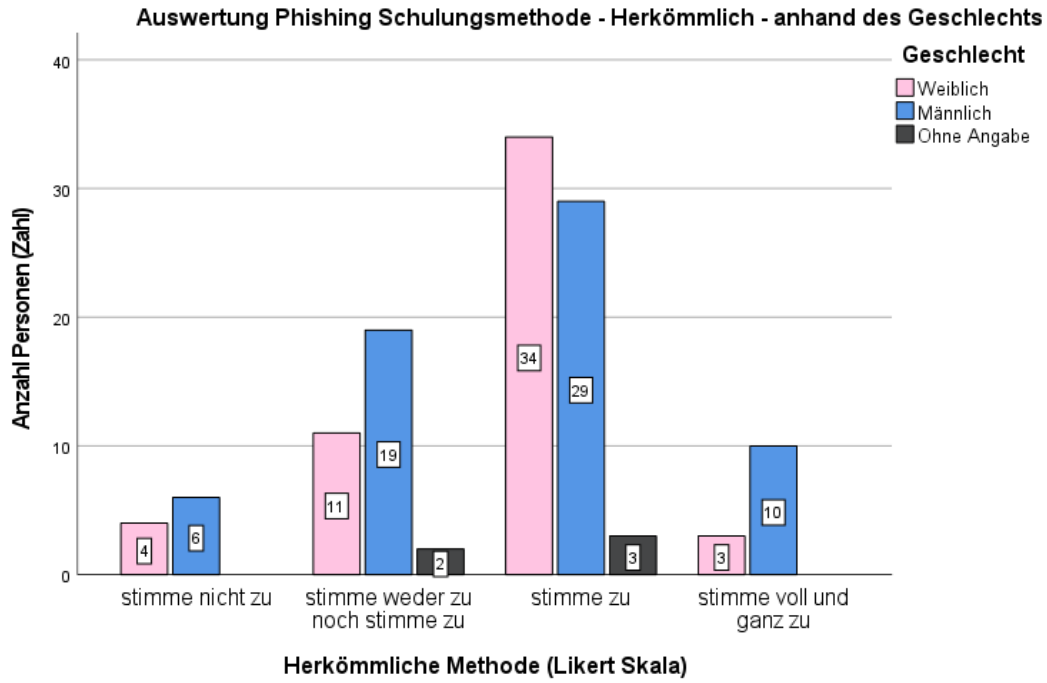



*Abbildung 66: Bevorzugte Phishing Schulungsmethode (Herkömmlich) anhand des Geschlechts*

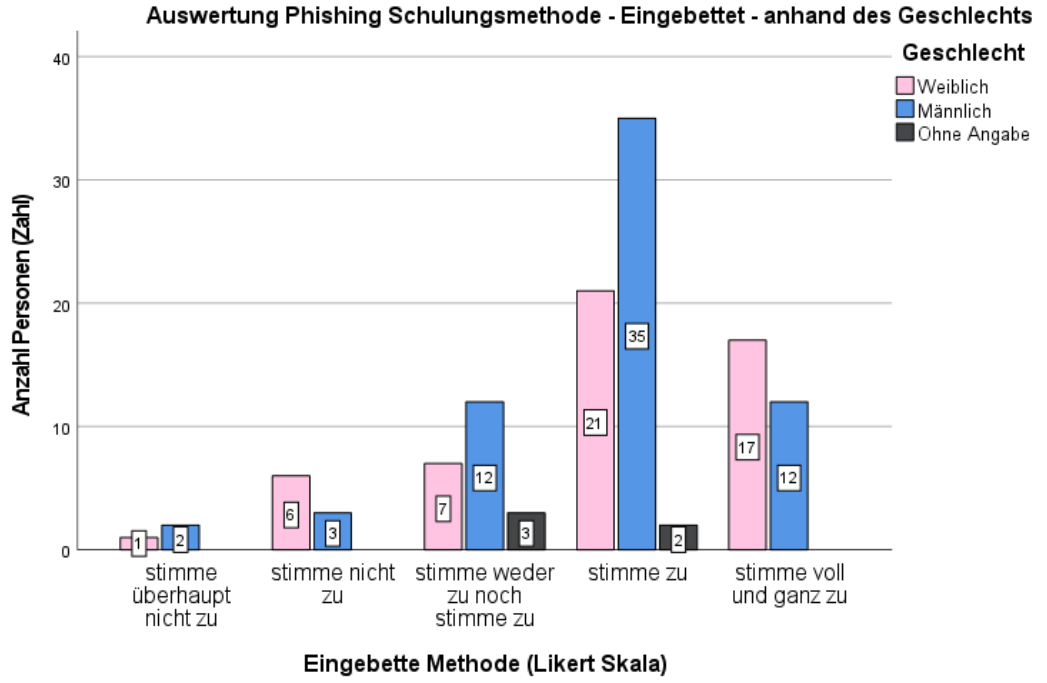



*Abbildung 67: Bevorzugte Phishing Schulungsmethode (Eingebettet) anhand des Geschlechts*

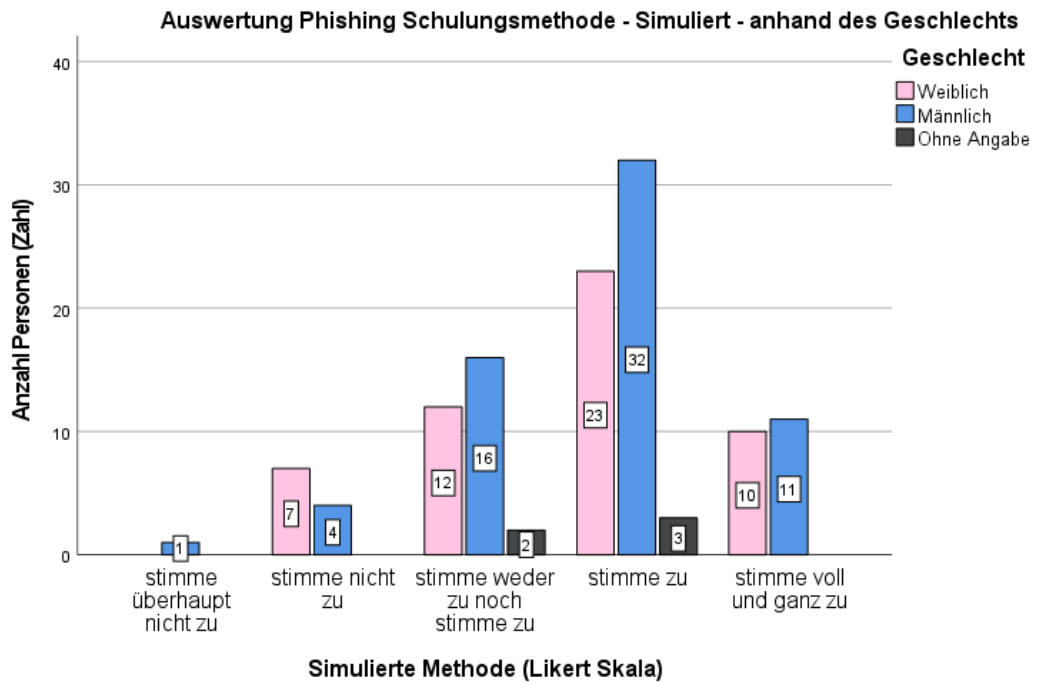



*Abbildung 68: Bevorzugte Phishing Schulungsmethode (Simuliert) anhand des Geschlechts*

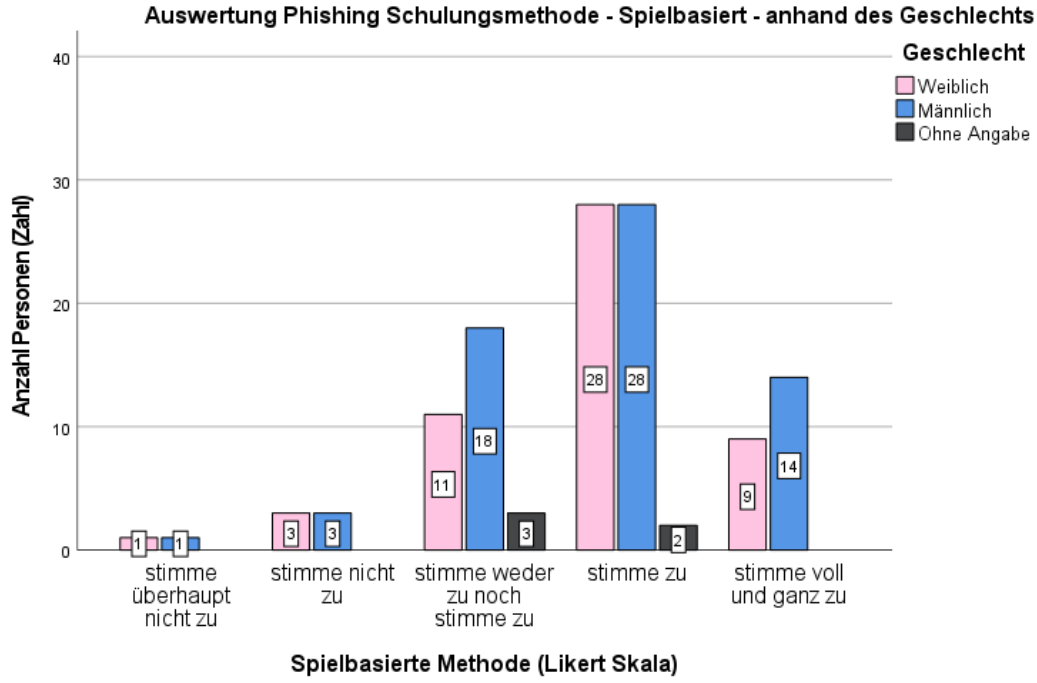



*Abbildung 69: Bevorzugte Phishing Schulungsmethode (Spielbasiert) anhand des Geschlechts*

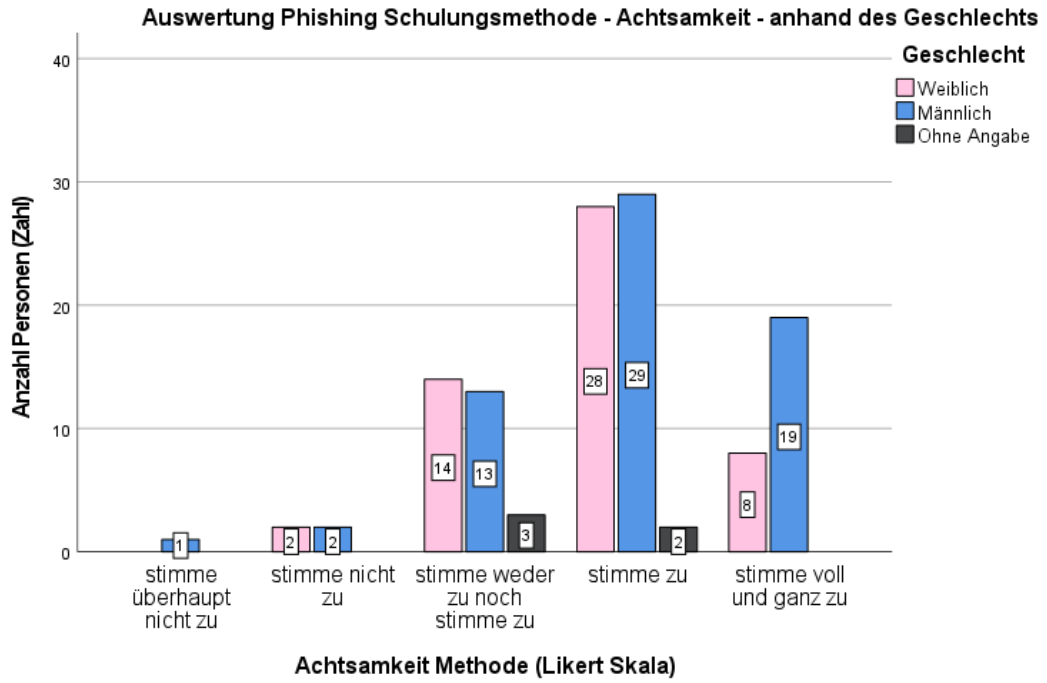



*Abbildung 70: Bevorzugte Phishing Schulungsmethode (Achtsamkeit) anhand des Geschlechts*

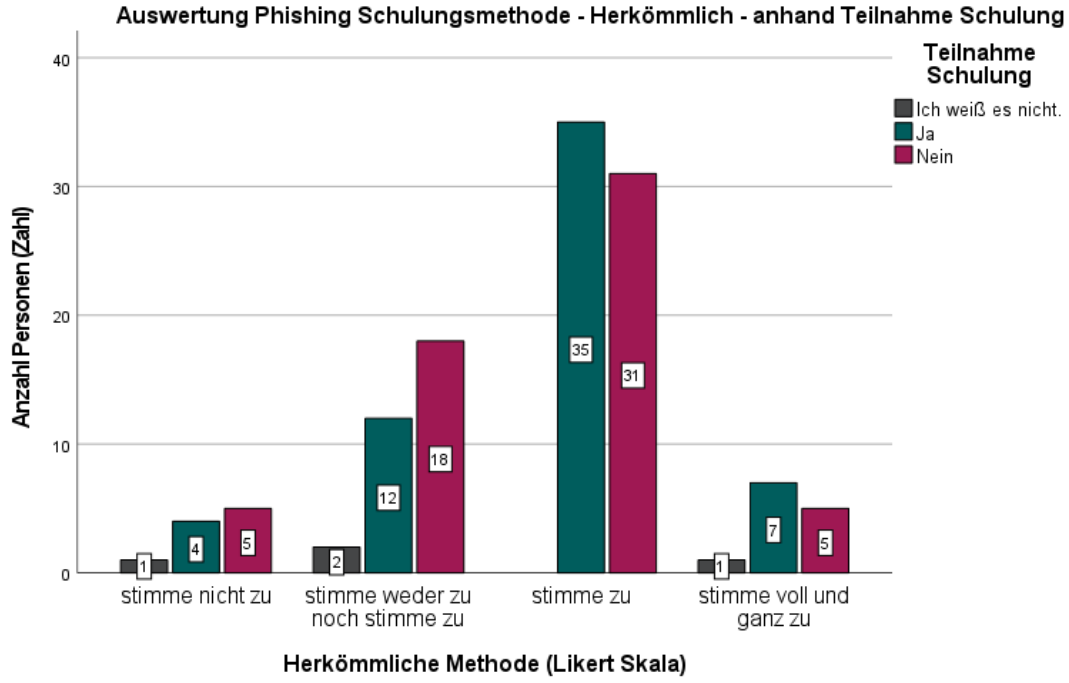



*Abbildung 71: Bevorzugte Phishing Schulungsmethode (Herkömmlich) anhand Teilnahme Schulung*

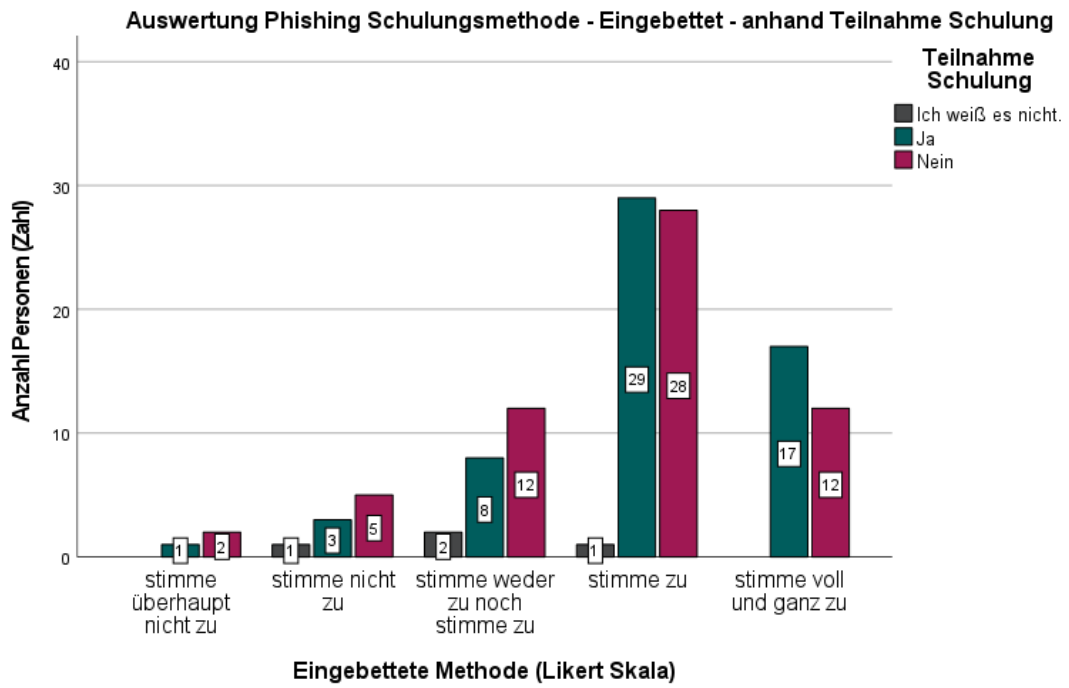



*Abbildung 72: Bevorzugte Phishing Schulungsmethode (Eingebettet) anhand Teilnahme Schulung*

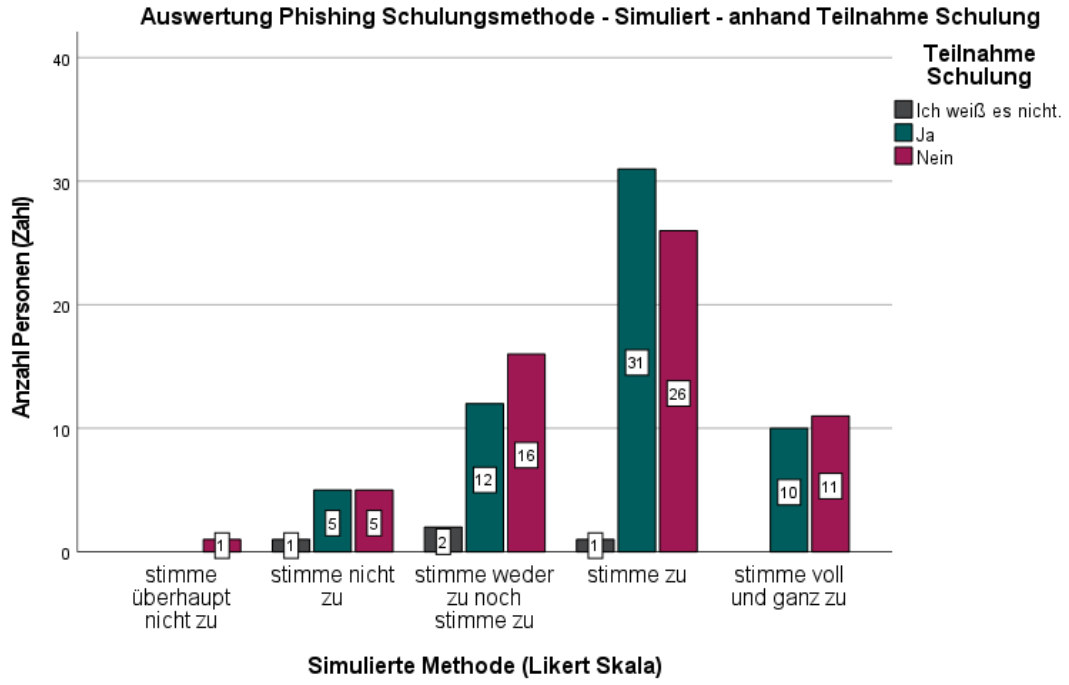



*Abbildung 73: Bevorzugte Phishing Schulungsmethode (Simuliert) anhand Teilnahme Schulung*

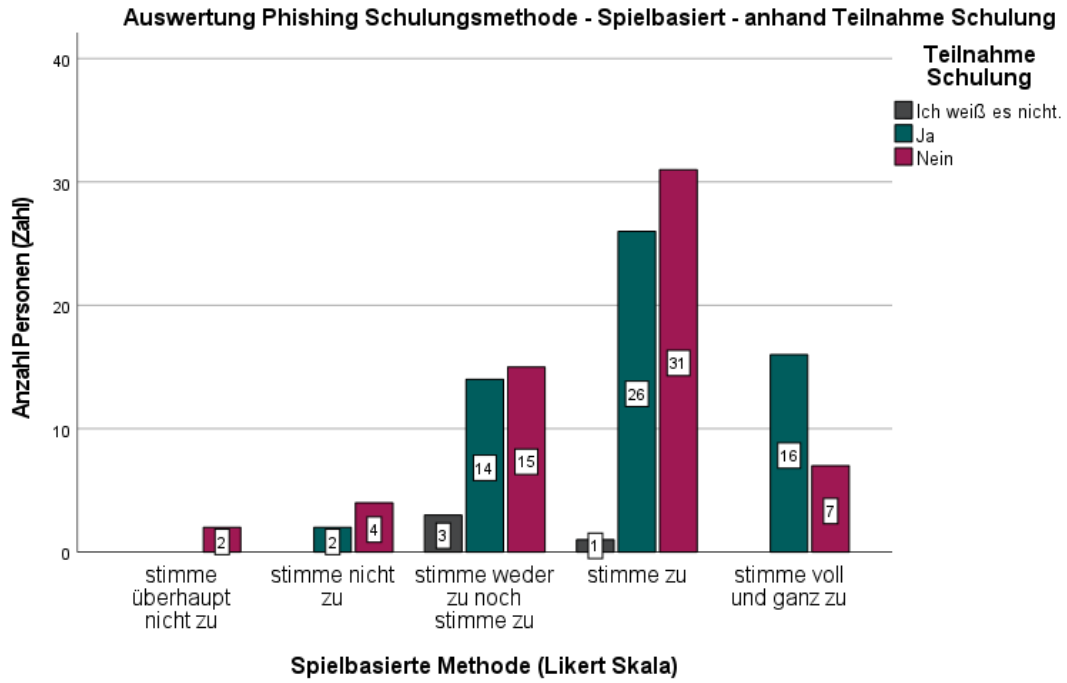



*Abbildung 74: Bevorzugte Phishing Schulungsmethode (Spielbasiert) anhand Teilnahme Schulung*

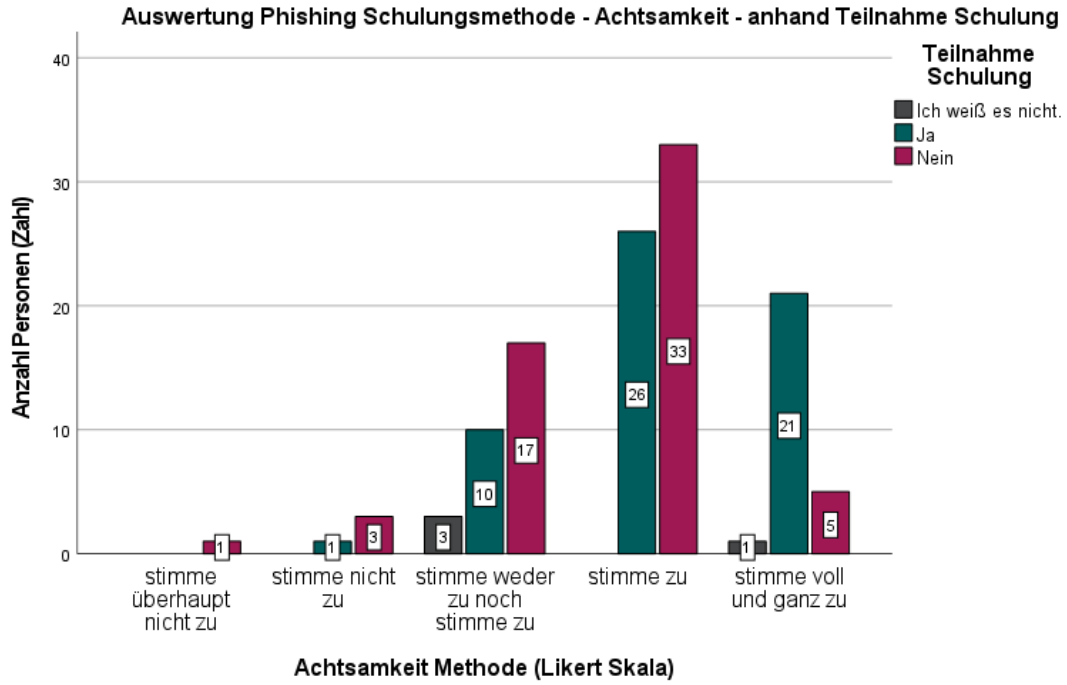



*Abbildung 75: Bevorzugte Phishing Schulungsmethode (Achtsamkeit) anhand Teilnahme Schulung*

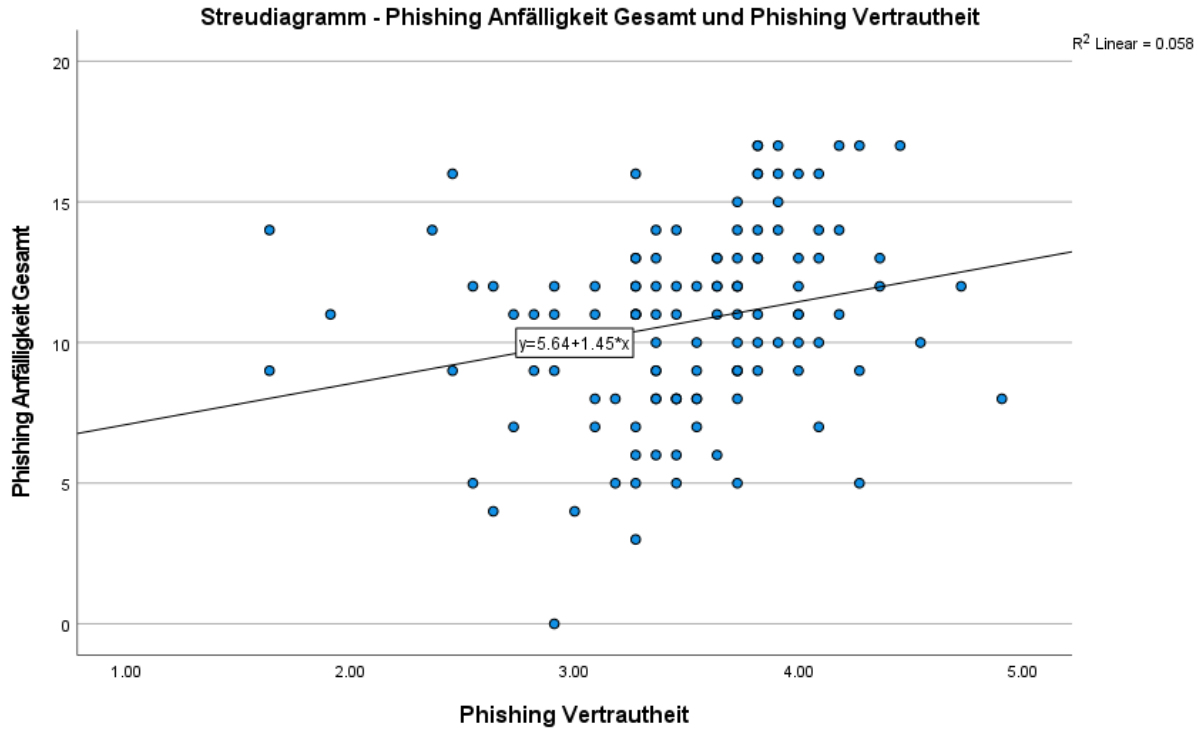



*Abbildung 76: Streudiagramm - Phishing Anfälligkeit Gesamt und Phishing Vertrautheit*

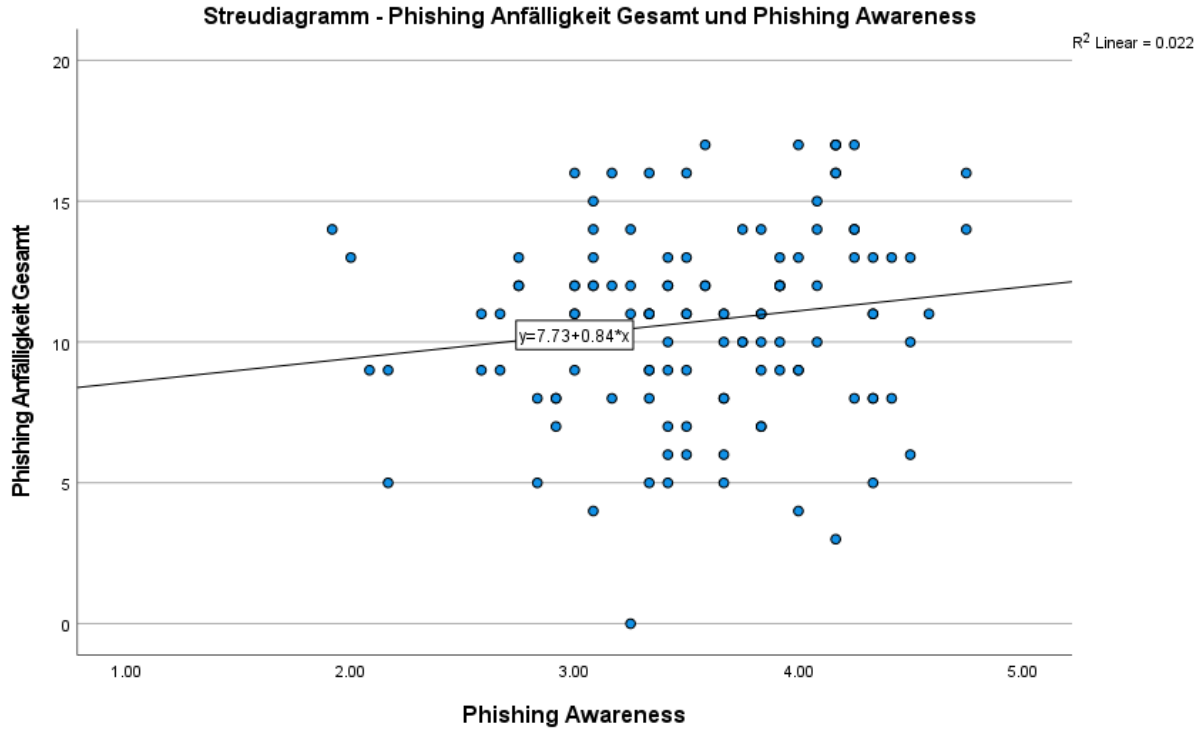



*Abbildung 77: Streudiagramm - Phishing Anfälligkeit Gesamt und Phishing Awareness*

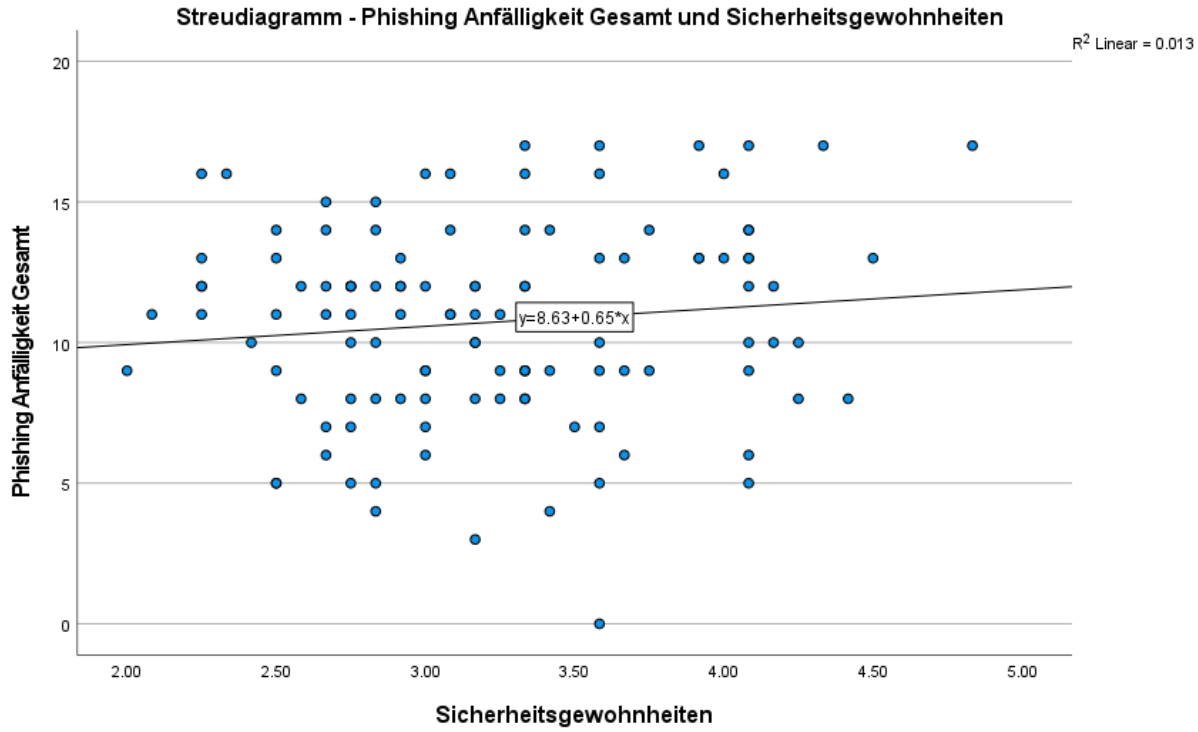



*Abbildung 78: Streudiagramm - Phishing Anfälligkeit Gesamt und Sicherheitsgewohnheiten*