Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

Masterthesis

Social Engineering Risk Mitigation

Entwicklung & Validierung eines Anti-Phishing-Trainings

Hochschule	**ZHAW**
Department	**School of Management and Law**
Studiengang	**MSc Wirtschaftsinformatik**
Semester	**Frühlingssemester 2018**
Modul	**Masterarbeit**
ECTS	**12**
Version	**3.1**
Matrikelnr.	**12-198-248**
Eingereicht	**Winterthur, 25. Mai 2018**

Verfasser
Moritz Zollinger
Research Associate
Glärnischweg 21
CH-8400 Winterthur
mo.zollinger@gmail.com

Gutachter
Dr. Roger Seiler
Dozent
St.-Georgen-Platz 2
CH-8400 Winterthur
roger.seiler@zhaw.ch

Abstract

Monatlich werden circa hunderttausend verschiedene Phishing-E-Mails versandt, welche für einen jährlichen Schaden in Milliardenhöhe verantwortlich sind. Diese Arbeit beschäftigt sich deshalb mit der Frage, wie das Phishing-Risiko gesenkt werden kann. Während technische Gegenmassnahmen einen positiven Beitrag zur Cyber-Abwehr leisten, können diese nicht alle Phishing-Angriffe abwehren. Letzten Endes muss der Anwender bei Social-Engineering-Angriffen wie Phishing über genügend Sicherheitsbewusstsein und Wissen verfügen, um einen Angriff zu verhindern. Um die Wahrscheinlichkeit eines Schadens durch Phishing für Internetanwender zu reduzieren, wurde ein Anti-Phishing-Training entwickelt. Das Online-Training klärt Anwender zum Thema Phishing und über dessen Risiken auf und lehrt den Umgang mit Phishing-E-Mails sowie deren Identifikation. Um die Effektivität des Trainings zu prüfen, wurde eine Pilot-Studie und ein randomisiertes Kontrollgruppenexperiment durchgeführt. Unter Verwendung eines Mittelwertvergleiches konnte ein schwacher, positiver Trainingseffekt gefunden werden. Um den Beitrag zur Cyber-Abwehr zu maximieren, steht das Training für Anwender, Forscher und Entwickler unter AGPL-Lizenz frei zur Verfügung.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AGPL	GNU Affero General Public License
APWG	Anti-Phishing Working Group
BEC	Business Email Compromise
Bit	Binary Digit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	Certification Authority Authorization
CDN	Content Delivery Network
CEO	Chief Executive Officer
COBIT	Control Objectives for Information and Related Technologies
CSP	Content Security Policy
DKIM	Domain Keys Identified Mail
DMARC	Domain Message Authentication Reporting & Conformance
DNS	Domain Name System
DNSSEC	DNS Security Extensions
EKL	Phishing-Erkennungsleistung
FBI	Federal Bureau of Investigations
GDPR	General Data Protection Regulation
GovCERT	Computer Emergency Response Team
GPL	GNU General Public License
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IC3	Internet Crime Complaint Center
IEC	International Electrotechnical Commission
IP	Internet Protokoll
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization

Abkürzung	Bedeutung
ITK	Informatikkenntnisse
MELANI	Melde- und Analysestelle Informationssicherung
MFA	Multi-Faktor-Authentifizierung
MITM	Man-in-the-Middle
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
PAV	Phishing-Anhang-Vermeidung
PLV	Phishing-Link-Vermeidung
PRNG	Pseudorandom Number Generator
SISA	Swiss Internet Security Alliance
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
SPSS	Statistical Package for the Social Sciences
SSL	Secure Sockets Layer
StGB	Schweizerisches Strafgesetzbuch
TAM	Technology Acceptance Model
TLS	Transport Layer Security
TTAT	Technology Threat Avoidance Theory
URL	Uniform Resource Locator
XSS	Cross-Site Scripting
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

In der Post findet sich eine Rechnung nie bestellter Ware (SRF, 2018). Es fehlen Tausende von Franken auf dem Bankkonto oder alle Dokumente und Fotos auf dem Computer wurden von Ransomware (Crypto-Trojaner, Computer-Virus) verschlüsselt und können via Lösegeldzahlung freigekauft werden (MELANI, 2017b). Dies kann auf Internetanwender zukommen, falls sie sich durch Phishing-E-Mails täuschen lassen. Denn Phishing ist ein Versuch mit psychologischen Taktiken, auch Social Engineering genannt, Anwender dazu zu bringen, sich selbst zu schädigen, indem sie Zugangsdaten weitergeben oder Malware (Überbegriff für Schadprogramme wie Computer-Viren) ausführen.

Der Fall der schweizerischen Post ist ein aktuelles Phishing-Beispiel. In über hundert Fällen gerieten Cyber-Kriminelle an Adress- und Anmeldedaten von Postkunden (Polizei Schweiz, 2018). Unter Verwendung der entwendeten Daten und den Online-Diensten der Post leiteten die Kriminellen im Namen der Kunden bestellte Pakete zu sich um und schädigten dabei Postkunde und Online-Shop zugleich (Polizei Schweiz, 2018). Während die Lieferung des Online-Shops bei den Kriminellen einging, erhielt der Postkunde die Rechnung. Aufgrund der Betrugsfälle sah sich die Post gezwungen, den Umleitungsdienst einzuschränken (SRF, 2018). Dieses und weitere Beispiele werden in dieser Arbeit behandelt.

Die Schweizer Banken: Züricher Kantonalbank (2018), Credit Suisse (2015) und UBS (2018) stellen alle Informationen zum Thema Phishing bereit, um sich und ihre Kunden vor dieser Betrugsart zu schützen. Denn mit den via Phishing erbeuteten Anmeldeinformationen ist es unter Umständen möglich, Finanztransaktionen auszuführen (Beobachter, 2017). Laut dem russischen Sicherheitssoftwarehersteller Kaspersky Lab

(2018) richteten sich im Jahr 2017 so viele Phishing-E-Mails wie in keinem Jahr zuvor gegen Finanzdienstleister (54 %). Davon waren im Speziellen die Banken mit einem Anteil von 25 % aller Phishing-E-Mails betroffen (Kaspersky Lab, 2018). Aus diesem Grund behandelt ein Teil dieser Arbeit Phishing-E-Mails von Finanzinstituten.

Als Phishing wird der Versuch bezeichnet, via E-Mail, Messenger-Dienst oder anderer Kommunikationskanäle an persönliche oder sensitive Daten wie Benutzername, Passwort oder Kreditkartendetails zu gelangen (Ramanathan & Wechsler, 2013; Moore & Clayton, 2007). Beim klassischen Phishing imitieren Angreifer bestehende Unternehmen, um Anwender auf gefälschte Webseiten zu leiten, welche dann die Daten der Anwender speichern (Moore & Clayton, 2007). Lastdrager (2014) suchte nach einer in der Forschergemeinschaft breit akzeptierten Definition für Phishing. Dafür wurden in einer Literaturrecherche aus 2485 Publikationen 113 Definitionen zur Analyse selektioniert. Gemäss Lastdrager (2014) ist die gemeinsame Definition von Phishing über alle Studien hinweg, ein skalierbarer Akt der Täuschung, bei welchem Imitation genutzt wird, um Informationen von Anwendern zu erlangen.

Phishing ist somit eine Form von Social Engineering (S. Gupta, Singhal & Kapoor, 2016). Denn laut Evans (2009) akademischer Definition verwendet ein Social-Engineering-Angriff soziale Methoden, wie Täuschung oder Manipulation, um Zugang auf Informationssysteme zu erlangen (Atkins & Huang, 2013; Muscanell, Guadagno & Murphy, 2014). Social Engineering ist eine effiziente (Symantec, 2017) und oft genutzte Cyber-Angriffs-Methode (BSI, 2016), da es für den Angreifer oft einfacher ist, den Menschen als schwächstes Glied der Sicherheitskette zu überwinden (BSI, 2016; Williams & Li, 2017; Bulgurcu, Cavusoglu & Benbasat, 2010). Social Engineering-Angriffe, wie Phishing, stellen eine ernsthafte Cyber-Bedrohung für Internetanwender und Unternehmen dar (Aleroud & Zhou, 2017; Chandrasekaran, Narayanan & Upadhyaya, 2006; R. T. Wright & Marett, 2010; Arachchilage, Love & Beznosov, 2016).

1.1 Ausgangslage

Phishing ist ein einfacher, von Kriminellen verwendeter Cyber-Angriff, mit hoher Verbreitung. Gemäss dem schweizerischen Computer Emergency Response Team (GovCERT) (2018) wurden in der zweiten Jahreshälfte 2017 und im ersten Quartal 2018 zwischen 53 und 189 Phishing-Webseiten pro Woche über die Anti-Phishing-Meldestelle Antiphishing.ch der MELANI (2015a) registriert. Die schweizerische Melde- und Analysestelle Informationssicherung (MELANI) (o. J.), zu welcher GovCERT und die Meldestelle gehören, weisen in ihrem Lagebericht (MELANI, 2017a) 2343 verschiedene Phishing-Webseiten für das erste Halbjahr 2017 aus. Die MELANI teilt ihre Informationen mit der globalen NGO Anti-Phishing Working Group (APWG) (2018b). Pro Monat verzeichnet die APWG in ihrem Phishing Activity Trend Report circa 100'000 Phising-E-Mail-Kampagnen und 50'000 Phishing-Webseiten weltweit (APWG, 2017a, 2017b). Die Anzahl der Phishing-Angriffe von 2012 bis 2017 fluktuiert, ist in der Tendenz jedoch steigend (APWG, 2016).

Phishing verursacht einen wirtschaftlichen Schaden, denn es ist ein Cyber-Angriff mit finanziellen Auswirkungen. Beim Internet Crime Complaint Center (IC3) des FBIs wurde der Schaden in den Vereinigten Staaten auf ungefähr 391 Millionen Franken pro Jahr beziffert (FBI IC3, 2016). Bei einem weiteren zu Phishing gehörendem, jedoch separat ausgewiesenem Betrug namens Business Email Compromise (BEC), bei welchem Phishing verwendet wird um Überweisungen zu erwirken, beläuft sich die Schadenssumme auf circa 360 Millionen Franken (FBI IC3, 2016). Hierbei handelt es sich um den gemeldeten und nicht um den Gesamtschaden. Die Dunkelziffer liegt vermutlich höher. Das Marktforschungsinstitut Gartner schätzt den Schaden auf 3,2 Milliarden Schweizer Franken mit 3,6 Millionen Betroffenen (McCall, 2007). Eine weitere Schätzung liegt bei 12 Milliarden (Netsafe, 2017). Die Wissenschaft scheint vorsichtiger mit einer Gesamtschätzung des weltweiten Phishing-Schadens zu sein. Selbst X. Chen, Bose, Leung und Guo (2011), die sich explizit mit dem durch Phishing verursachten Schaden befassten, geben keine konkrete Schätzung ab. In ihrer Studie untersuchten sie, um den Schaden zu schätzen, den Einfluss von Phishing-Meldungen auf die Aktienpreise der jeweiligen

Unternehmen. Da in diesem Modell die Kunden nicht berücksichtigt werden und Aktienmärkte als volatil gelten, ist diese Zahl als Basis für eine Schätzung des weltweiten Phishing-Schadens möglicherweise ungeeignet. Eine Studie von Herley und Florêncio (2008), welche zum Schluss kommt, dass sich Phishing für Angreifer nicht lohnt, kritisiert Phishing-Schätzungen. Unter anderem werden auch die Schätzungen von Gartner zwischen 2005 und 2007 kritisiert (Herley & Florêncio, 2008). Ausserdem gehen Herley und Florêncio (2008) von einer Überschätzung um bis zu Faktor 50 aus. Die Schätzungen von 391 Millionen in den USA und 3,2 respektive 12 Milliarden Franken weltweit lassen vermuten, dass Phishing ein nicht trivial zu lösendes Problem ist.

Die Erfolgsrate von Phishing-E-Mails liegt zwischen 2–100 %, wie mehre Studien gezeigt haben (siehe Unterabschnitt 2.1.4). Somit würde es im Schnitt ausreichen 50 Phishing-E-Mails an ein Unternehmen zu senden, um die Zugangsdaten von mindestens einem Benutzerkonto zu erlangen. Für Unternehmen mit mehreren hundert Mitarbeiten kann Phishing somit eine ernsthafte Cyber-Bedrohung darstellen, da die Erfolgschancen für Angreifer entsprechend hoch sind.

1.2 Problemstellung

Da Phishing ein globales Problem mit einer Schadenssumme in Milliardenhöhe ist, wurden bereits Gegenmassnahmen ergriffen. Rein technische Massnahmen schützen vor Phishing via E-Mail nur partiell (Hong, 2012; Purkait, 2013; Siadati, Nguyen & Memon, 2017). Selbst die Entwickler der Browser-Erweiterung ‘AntiPhish’ sehen ihre Software nur als Ergänzung und nicht als Lösung an (Kirda & Kruegel, 2005; Rosiello, Kirda, Kruegel & Ferrandi, 2007). Es scheint nicht auszureichen, technisch sichere Systeme zu entwickeln, solange die Anwender über zu wenig Sicherheitsbewusstsein (engl. security awareness) verfügen (McCoy & Fowler, 2004). Während technische Massnahmen einen Beitrag zur Reduktion des Phishing-Risikos leisten, gelingt es ihnen nicht, das Risiko vollständig zu vermeiden.

Das Versenden von Phishing-E-Mails ist in der Schweiz ein Delikt. Im Schweizerischen Strafgesetzbuch (StGB) ist Phishing gemäss der Schweizerischen Kriminalprävention (2018) nicht als eigener Strafbestand verankert. Art. 143, 143bis, 144, 147 und 254 sind jedoch anwendbar. Gemäss Art. 147 StGB "Betrügerischer Missbrauch einer Datenverarbeitungsanlage", ist die unbefugte Verwendung von Daten für einen Datenverarbeitungsvorgang welcher eine Vermögensverschiebung herbeiführt mit Freiheitsentzug von bis zu 10 Jahren strafbar. Jagatic, Johnson, Jakobsson und Menczer (2007) als auch Herley und Florêncio (2008) unterstellen den Angreifern betrügerische Absichten und X. Chen et al. (2011) sehen beim Phishing primär die kriminelle und finanzielle Motivation. Das Verbot von Phishing in der Schweiz löst das Problem der Phishing-E-Mails nicht vollständig, denn der Versand von Phishing-E-Mails wird dadurch nicht ganzheitlich verhindert. Mit technischen Massnahmen und gesetzlichen Verboten gelingt es demnach nicht Phishing zu verhindern.

1.3 Zielsetzung

Weil Phishing ein verbreitetes und ernst zu nehmendes Risiko darstellt, wird in dieser Arbeit ein Ansatz zur Milderung des Phishing-Risikos evaluiert. Mit rein technischen oder regulatorischen Massnahmen kann das Risiko nicht ganzheitlich beseitigt werden, deshalb wurde nach anwenderfokussierten Lösungsansätzen gesucht. Es hat sich gezeigt, dass Anwender explizit auf das Thema IT-Sicherheit sensibilisiert werden können (Puhakainen & Siponen, 2010; Bulgurcu et al., 2010; McCoy & Fowler, 2004; ISO/IEC, 2013; Wilson & Hash, 2003) und einen wichtigen Beitrag zu dieser leisten (Arachchilage & Love, 2014; Dodge, Carver & Ferguson, 2007). IT-Sicherheit kann durch Anwender-Training erhöht werden (M. A. Wright, 1998; Dodge et al., 2007), somit wirkt sich Training positiv auf die IT-Sicherheit aus (Arachchilage & Love, 2014; Liang & Xue, 2009, 2010; Harrington, Anderson & Agarwal, 2006). In diesem Punkt scheint sich die Forschungsgemeinschaft einig zu sein. Werden Anwender zum Thema IT-Sicherheit aufgeklärt, steigert sich ihr Sicherheitsbewusstsein (C. C. Chen, Shaw & Yang, 2006). Ein gesteigertes Sicherheitsbewusstsein senkt möglicherweise das Phi-

shing-Risiko (Long, 2013). Liang und Xue (2009) schlagen neben der Aufklärung über IT-Risiken auch eine Schulung der Anwender über die möglichen Konsequenzen von Phishing vor. Gemäss des von Liang und Xue (2009) entwickelten Modells werden sowohl Informationen über die Möglichkeit eines Angriffs als auch dessen Konsequenzen benötigt, um die Anwender zu sensibilisieren (Liang & Xue, 2009). Viele Forscher schlagen explizit vor, Anwender auf Phishing zu schulen (Arachchilage et al., 2016; Liang & Xue, 2010; Downs, Holbrook & Cranor, 2007; S. Sheng et al., 2007; S. Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010; Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2010; Kumaraguru, Rhee, Sheng et al., 2007; Kumaraguru, Rhee, Acquisti et al., 2007; Kumaraguru et al., 2009; Atkins & Huang, 2013; Abraham & Chengalur-Smith, 2010). Training scheint somit eine akzeptierte Methode im Sicherheitsbereich zu sein, um das Sicherheitsbewusstsein der Anwender zu steigern. Ebenfalls wird Anwender-Training auch als Mittel gegen die Phishing-Bedrohung empfohlen.

Anwender-Training wird im Sicherheitsbereich bereits angewendet. Im europäischen Standard ISO/IEC (2013) ist Sicherheitsbewusstseinstraining eine Zielvorgabe. Wilson und Hash von der amerikanischen NIST veröffentlichten eine Spezialpublikation über die Entwicklung von Trainings-Programmen zur Steigerung des Sicherheitsbewusstseins (Wilson & Hash, 2003). Da Anwender-Training empfohlen wird und sich in der Fachliteratur Hinweise finden, dass Training und Schulung im Bereich Phishing effektiv sein kann, setzt diese Studie auf Trainingsmassnahmen. Hierzu wurde eine Schulung, sowie ein interaktives Anwender-Training realisiert und überprüft, um das Phishing-Risiko, respektive die Eintrittswahrscheinlichkeit eines Schadens durch Phishing, zu senken. In der Vergangenheit hat sich gezeigt, dass Phishing-Spiele einen positiven Effekt haben können (S. Sheng et al., 2007; Wen, Li, Wade, Huang & Wang, 2017; Arachchilage & Cole, 2011; Misra, Arachchilage & Berkovsky, 2017; Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2008; ISO/IEC, 2013). Deshalb beinhaltet das Training ebenfalls eine spielerische Komponente.

1.4 Methode

Um die Ursache-Wirkungs-Zusammenhänge (Cook, Campbell & Shadish, 2002, S. 5–7) zwischen Anwender-Training und der Wahrscheinlichkeit Phishing zu identifizieren zu untersuchen, wird auf ein experimentelles Forschungsdesign (Stein, 2014) gesetzt. Anhand eines Experimentes (Eifler, 2014) werden die Probanden randomisiert (Yates, 1964; Fisher, 1926) einer Experimental- oder Kontrollgruppe zugeordnet.

Die Experimentalgruppe erhält das entwickelte Phishing-Training. Die Kontrollgruppe löst in diesem Feldexperiment (Eifler, 2014) keine vergleichbare Aufgabe. Die Phishing-Erkennungsleistung beider Gruppen werden in einer Nachher-Messung durch eine Online-Umfrage (Wagner & Hering, 2014) erfasst (Stein, 2014). Das randomisierte Kontrollgruppenexperiment soll die hypothetische Ursache der unabhängigen Variable ‘Training’ auf die abhängige ‘Phishing-Erkennungsleistung’ ergründen. Der kausale Effekt (Kühnel & Dingelstedt, 2014) des Trainings wird mit einer Mittelwertanalyse bestimmt. Weitere Informationen zum Experimentaldesign finden sich in Abschnitt 3.4 und die Analysemethoden sind in Abschnitt 3.5 festgehalten.

Kapitel 2

Theoretischer Hintergrund

In diesem Kapitel wird die Thematik der Phishing-E-Mails aufgearbeitet (siehe Abschnitt 2.1). Ebenfalls werden bereits bestehende, technische Anti-Phishing-Massnahmen (siehe Abschnitt 2.2) vorgestellt. In Abschnitt 2.4 sind wissenschaftliche Arbeiten beschrieben, die einen Bezug zum Thema Anti-Phishing-Training haben.

2.1 Phishing-E-Mails

In diesem Abschnitt wird die Effektivität von Phishing aufgezeigt und Phishing wird nach unterschiedlichen Arten klassifiziert. Es werden Erkennungsmerkmale identifiziert, der generelle Umgang mit Phishing diskutiert, sowie die betroffenen Wirtschaftssektoren aufgezeigt.

2.1.1 Klassifikation

Wie in Kapitel 1 beschrieben, ist Phishing ein Akt der Täuschung, bei welchem Imitation genutzt wird, um Informationen von Anwendern zu erlangen. Die für diesen Cyber-Angriff verwendeten E-Mails werden als Phishing-E-Mails bezeichnet. Das Antonym zu Phishing-E-Mail ist die legitime E-Mail. Legitim steht hier für das echte, zulässige, originale, unverfälschte, valide E-Mail. Mit Phishing-E-Mails können verschieden Ziele verfolgt werden. Sie reichen vom Entwenden von Anmeldedaten via Phishing-Webseite über das Auslösen einer Zahlung bis hin zur Infektion eins Unternehmens mit Malware. Weiter kann Phishing in verschiedene Typen unterteilt werden.

Klassisches, Deceptive Phishing

Beim klassischen oder deceptive Phishing, zu Deutsch täuschendes Phishing, werden legitime Unternehmen imitiert (Huang, Tan & Liu, 2009). Die Webseite des Unternehmens wird dabei inklusive Anmeldemaske von Angreifern kopiert und unter einer Phishing-URL angeboten. Die Angreifer fälschen ebenfalls E-Mails des Unternehmens und verlinken darin ihre Phishing-URL. Die mit dem Phishing-Link präparierten E-Mails werden danach zu tausenden versandt. Die Absenderadresse der E-Mail kann dabei gefälscht sein (Chaudhary, 2014) und somit dem legitimen Absender entsprechen. Ist der Angriff erfolgreich, folgen Anwender dem Phishing-Link und geben auf der geklonten Webseite ihre Daten an die Angreifer weiter. Diese Art von Phishing wird auch als Klon-Phishing (engl. clone phishing) bezeichnet (Banu & Banu, 2013).

Spear-Phishing

Eine weitere Art von Phishing ist das Spear-Phishing, auf Deutsch Speer-Phishing. Während beim deceptive Phishing E-Mails in Massen versendet werden, bezeichnet Spear-Phishing einen gezielten Angriff auf ein Unternehmen oder eine Gruppe von Individuen (Parmar, 2012). Der Angreifer sammelt dabei Informationen über sein Ziel, wie Name oder bekannte Entitäten, um unter Verwendung der Methoden des klassischen Phishings, gezieltere Phishing-E-Mails zu versenden.

Whaling

Die Bezeichnung ‘Whaling’ leitet sich vom englischen Wort ‘whale’ (deutsch Walfisch) ab. Der Name kommt daher, dass beim Whaling die ‘grossen Fische’, wie der Chief Executive Officer (CEO) oder das Top-Management angegriffen werden, denn diese können lukrative Ziele darstellen (Hong, 2012).

Business Email Compromise und CEO-Betrug

Business Email Compromise (BEC) ist ein Angriff auf Unternehmen, welche regelmässig Zahlungen an Lieferanten durchführen (FBI IC3, 2014). Beim BEC wird via Social-Engineering und Phishing versucht eine Überweisung auf ein Konto der

Angreifer auszulösen. Der Absender der Phising-E-Mails wird dabei gefälscht oder das sendende Konto wurde zuvor via Phishing oder andern Methoden kompromittiert (FBI IC3, 2014). Das Internet Crime Complaint Center (IC3) des Federal Bureau of Investigations (FBI) (2014) listet fünf Unterarten von BEC. Eine davon ist der CEO-Betrug, bei welchem Phishing-E-Mails mit dem Absender des CEOs oder einem anderen Mitglied des oberen Managements an Mitarbeiter derselbigen Unternehmens versandt werden (Mansfield-Devine, 2016). Die Phishing-E-Mails fordern die Mitarbeiter auf, Überweisungen oder andere für die Angreifer profitablen Handlungen auszuführen. Die Symantec (2016) setzt den CEO-Betrug gar mit BEC gleich. Ein Unterschied zum Whaling ist, dass beim CEO-Betrug die Mitarbeiter angegriffen werden, während das Whaling den CEO attackiert.

Phishing und Malware

Eine weitere Kategorie von Phishing verwendet Malware, wie Ransomware oder Trojaner. Während das klassische Klon-Phishing, Spear-Phishing, Whaling, BEC und der CEO-Betrug ausschliesslich auf Social-Engineering basieren und auf die Gutgläubigkeit der Anwender vertrauen, wird Phishing mit Malware durch technische Methoden unterstützt. Es können unterschiedliche Arten von Malware via E-Mail-Anhang oder Link verbreitet werden (Brewer, 2016). Phishing-E-Mails sind gemäss Richardson und North (2017) die am häufigsten verwendete Methode Ransomware zu verbreiten. Ransomware-Angriffe differenzieren sich vom klassischen Phishing neben der Verwendung von Software auch darin, dass keine Anmeldedaten entwendet werden. Finanzielle Vorteile für die Angreifer ergeben sich bei Ransomware durch die Verschlüsselung von Dateien der Anwender und anschliessender Forderung von Lösegeld für deren Entschlüsselung. Trojaner können ebenfalls verbreitet werden, um Zugangsdaten durch mitlesen von Tastatureingaben zu entwenden, sowie Überweisungen oder einen Man-in-the-Middle-Angriff durchzuführen (Aaron, 2010).

DNS-Spoofing und Pharming

Als Unterkategorie von Phishing mit Malware kann DNS-Spoofing mit Malware gesehen werden (Klein & Golan, 2006). DNS-Abfragen werden dabei von Trojanern so manipuliert, dass Anwender beim Ansteuern einer legitimen Webseite auf einem von den Angreifern kontrollierten Server landen (Bin, Qiaoyan & Xiaoying, 2010). Dies kann durch Modifikation der 'hosts'-Datei (Bin et al., 2010) vonstattengehen, welche ähnlich wie ein Telefonbuch Domain-Namen (Teil der URL) auf IP-Adressen abbildet. Diese Art von Angriff wird auch als Pharming bezeichnet (Chaudhry, Chaudhry & Rittenhouse, 2016), wie beim klassischen Phishing wird dazu eine geklonte Webseite eines Unternehmens benötigt.

2.1.2 Erkennungsmerkmale

Dieses Kapitel behandelt die Merkmale anhand deren Phishing-E-Mails erkannt werden können und wie mit Phishing umgegangen werden sollte. Eine E-Mail kann unter anderem die Elemente Absender, Empfänger, Betreff, Inhalt, Link und Anhang beinhalten. Diese Elemente können auf Hinweise von Phishing geprüft werden, denn die Elemente weisen charakteristische Erkennungsmerkmale auf. Dieses Wissen über die Merkmale von Phishing-E-Mails kann möglicherweise an Anwender vermittelt werden, um diese vor Phishing zu schützen.

Links und die URL

Phishing-E-Mails weisen auch für Laien identifizierbare Erkennungsmerkmale auf. Die URL, auch als Adresse einer Webseite bezeichnet, welche sich hinter einem Link verbirgt, ist ein zentrales Merkmal. Es existieren schwarze Listen (Ulevitch, o. J.; Georgiev, 2015) mit Phishing-URLs und Google-Ingenieure klassifizieren Phishing-E-Mails anhand der URL (Whittaker, Ryner & Nazif, 2010). Viele Anwender-Trainings fokussieren ebenfalls auf URL (Kumaraguru, Rhee, Acquisti et al., 2007; S. Sheng et al., 2007; Wen et al., 2017; Arachchilage & Cole, 2011). Ausserdem wurden Browser-Erweiterungen zur Bekämpfung von Phishing entwickelt, welche die URL berücksich-

tigen (Dunlop, Groat & Shelly, 2010). Einige Publikationen beschreiben wie Angreifer URLs in Phishing-E-Mails mit ähnlichen Buchstaben anhand des kyrillischen Alphabetes oder mit weiteren Methoden aufbauen, um möglichst authentisch zu wirken (Siadati, Jafarikhah & Jakobsson, 2016; APWG, 2016; Ollmann, 2004; Dhamija, Tygar & Hearst, 2006). Dies legt nahe, dass Phishing-E-Mails anhand der URL identifizierbar sind. URLs können zudem direkt Malware verlinken (Hardy et al., 2014). Die APWG (o. J.) rät, Links in E-Mails nicht zu vertrauen und diesen nicht zu folgen.

Der Absender

Die Absenderadresse einer E-Mail ist ebenfalls ein potentielles Erkennungsmerkmal (Hardy et al., 2014). Einige Trainings-Ansätze (Lastdrager, Gallardo, Hartel & Junger, 2017; Wen et al., 2017) nutzen den Absender als Klassifikationsmerkmal. Und eine Sammlung von Phishing-Fällen (Konsumenteninfo AG, 2018) beinhalten mehrere E-Mails mit falschem oder gefälschtem Absender. Falsche Absender können mit dem originalen, legitimen beinahe übereinstimmen, während gefälschte Absender exakt dem legitimen entsprechen. E-Mail-Absender können und werden von Angreifern gefälscht (Banu & Banu, 2013; AlamgirKhan, 2013; FBI IC3, 2014; Downs, Holbrook & Cranor, 2006). Die Fälschung des Absenders geschieht mit dem Ziel, Phishing-E-Mails legitimer erscheinen zu lassen. Um Phishing zu erschweren, wurden Massnahmen (siehe Abschnitt 2.2) ergriffen, welche das Fälschen eines Absenders verhindern sollen. Während falsche Absender von Laien erkannt werden können, erfordert die Identifikation von gefälschten Absendern mehr Expertise.

Der Betreff und Inhalt

Phishing-E-Mails können teilweise am Nachrichteninhalt oder bereits am Betreff erkannt werden. Die Fachliteratur erwähnt hier, dass manche Phishing-E-Mails versuchen, einen Handlungsdruck oder ein Gefühl der Dringlichkeit zu erzeugen (engl. sense of urgency), mit der Absicht Anwender zu einer Handlung zu motivieren. (Rajalingam, Alomari & Sumari, 2012; Lastdrager et al., 2017; Atkins & Huang, 2013). Abraham und Chengalur-Smith (2010) erwähnen, dass Anwendern in Phishing-E-Mails gedroht

wird, Rajalingam et al. (2012) führen ein Beispiel auf mit der Drohung, dass ein Online-Account gelöscht wird, falls nicht innerhalb von 48 Stunden auf die E-Mail reagiert wird. Lastdrager et al. (2017) führen Dringlichkeitsbewusstsein und Drohung ebenfalls als Phishing-Hinweis auf und ergänzen, dass Rechtschreibung, Grammatik und Stil ebenfalls zur Klassifikation herbeigezogen werden können. In einer Studie kamen Atkins und Huang (2013), welche die Phishing-E-Mail genutzten Überzeugungstechniken anhand von 200 E-Mails untersuchten, ebenfalls zum Schluss, dass ein bedrohender Stil verwendet wurde. Ihre Studie (Atkins & Huang, 2013) zeigte, dass autoritative Überzeugungstechniken kombiniert mit Dringlichkeit verwendet wurden, um Entscheidungen der Anwender zu beeinflussen. Der Handlungsdruck führt möglicherweise dazu, dass Anwender schneller und unüberlegter agieren. In einer Sammlung von Phishing-E-Mails finden sich sowohl Versuche einen Handlungsdruck zu erzeugen als auch E-Mails, welche Grammatik- und Stilfehler beinhalten (Konsumenteninfo AG, 2018).

Der E-Mail-Anhang

E-Mails können Anhänge mit Malware enthalten (Richardson & North, 2017). Wen et al. (2017) schulen deshalb in ihrem Anti-Phishing-Training, nur 'sichere' Anhänge, mit Endung .pdf oder .docx zu öffnen und implizieren damit, dass andere Endungen wie .exe unsicher sind. Es ist jedoch nicht der Fall, dass diese Dateiformate sicher sind. Gemäss Li, Lai und Ddl (2011) wurde ein Politiker in Hong Kong mehrmals mit Spear-Phishing-E-Mails und Malware-Anhängen im Word- (.docx) oder PDF-Format (.pdf) angegriffen. Li et al. (2011) untersuchten in ihrer Studie die Malware-Anhänge genauer und kamen zu dem Schluss, dass sie eine echte Bedrohung darstellen. Es scheint somit nicht möglich, einen Anhang anhand der Endung als sicher zu klassifizieren. Abraham und Chengalur-Smith (2010) untersuchten Social-Engineering-Taktiken im Zusammenhang mit Malware und stellten fest, dass E-Mail Anhänge der beliebteste Kanal zur Infiltration sind. Hardy et al. (2014) analysierten die E-Mails von drei tibetischen Organisationen und fanden, dass 95 % der Malware-Angriffe via E-Mail durch Ignorieren des E-Mail-Anhangs verhindert werden. Es scheint somit eine gute Strategie, Anhänge von Phishing-E-Mails selbst in einem Dokumentenformat nicht zu öffnen. Die Banken

UBS (2018) und Züricher Kantonalbank (2018) sowie die Hochschule Luzern (2018b) weisen ihre Kunden explizit darauf hin, Links und Anhänge in E-Mails nicht zu öffnen.

Das Schlosssymbol und HTTPS/TLS

Das Schlosssymbol, welches bei Webbrowsern in der Adressleiste erscheint, falls eine mit TLS gesicherte Webseite angesteuert wird, kann ebenfalls als Erkennungsmerkmal herangezogen werden (Dhamija et al., 2006; Purkait, 2013). Dass eine Webseite TLS, den Nachfolger von SSL (Rescorla & Dierks, T., 2008), verwendet, lässt sich anhand des HTTPS-Protokolls erkennen. Bei TLS beginnt die URL mit 'https://' anstatt mit 'http://' wie beim ungesicherten HTTP-Protokoll. TLS soll garantieren, dass Daten unverändert übermittelt werden, ist jedoch kein Indikator für die Vertrauenswürdigkeit einer Webseite (Rescorla & Dierks, T., 2008). Gemäss Downs et al. (2006) wurde das Symbol von einigen Probanden dahingehend missinterpretiert, dass Webseiten mit Schlosssymbol vertrauenswürdig sind. Während im Jahr 2014 circa 25 % der von Firefox-Browser aufgerufenen Webseiten mit HTTPS gesichert waren, sind es im Jahr 2018 bereits gegen 75 % (Internet Security Research Group, 2018). Der Chrome-Browser wird HTTP-Webseiten ab Juli 2018 als unsicher kennzeichnen (Emily Schechter, 2018b). Ab September 2018 werden Chrome-Anwender auf HTTP-Webseiten mit Eingabefeldern verstärkt visuell gewarnt und bei HTTPS-Webseiten wird auf die Angabe 'Sicher' und möglicherweise auch auf das Schlosssymbol verzichtet (Emily Schechter, 2018a). Auf Grund von Missinterpretationen durch Anwender, zunehmender Verbreitung von TLS und des Verzichtes seitens Google dies anzuzeigen, ist das Schlosssymbol in der Browser-Adressleiste als Erkennungsmerkmal ungeeignet. Um Phishing-E-Mails zu identifizieren bleiben somit die URL, der Absender, sowie der Betreff und Inhalt geeignete Merkmale

2.1.3 Handlungsempfehlungen

Die Anti-Phishing Working Group (APWG) (o. J.) rät, Links in E-Mails nicht zu vertrauen und die URL stattdessen direkt in den Browser einzugeben. Ebenfalls wird davon abgeraten, Anhänge zu öffnen. Die APWG (2018a) ist eine im Jahr 2013 gegründete

internationale Koalition gegen Cyber-Kriminalität mit über 1800 Mitgliedern aus den Bereichen Wirtschaft, Politik, Polizei und Non-Profit. Die APWG Anti-Phishing Information APWG (o. J.) wurde von der Wombat Security erstellt, welche von Kumaraguru (UMBC, 2018) gegründet wurde. Kumaraguru's Studien sind in Abschnitt 2.4 ausgeführt. Weiter ist den Informationen der APWG (o. J.) zu entnehmen, dass auf gefälschte Absender sowie auf einen ausgeübten Handlungsdruck geachtet werden sollte.

Die STOP. THINK. CONNECT. (STC) (APWG & SISA, 2018) ist eine Cyber-Sicherheitsbewussteinskampagne und weist auf gefälschte Absender hin. Die STC empfiehlt, bei E-Mails von einem bekannten Absender mit ungewöhnlicher E-Mail-Adresse vorsichtig zu sein. Die STC gehört zur APWG (2018a) und hat eine eigene von Swiss Internet Security Alliance (SISA) betriebene Web-Präsenz in der Schweiz (APWG & SISA, 2018). Zu den Mitgliedern der SISA gehören neben Banken, Behörden, Internet-Dienstleistern auch die MELANI, die Kantonspolizei Zürich und die Hochschule Luzern (APWG & SISA, 2018). STC weist zudem auf die Gefahr von Anhängen hin. Es wird erklärt, Links mit der Maus zu überprüfen und bei E-Mails mit Rechtschreibfehlern vorsichtig zu sein. Ebenfalls wird der Handlungsdruck sowie eine unpersönliche Anrede thematisiert (APWG & SISA, 2018).

Kaspersky Lab (2015) empfiehlt generell misstrauisch gegenüber E-Mails zu sein und Links vor dem Anklicken immer zu überprüfen, selbst wenn der Absender bekannt ist, da der Absender gefälscht sein könnte. Ebenfalls warnt Kaspersky Lab (2015) vor Klon-Phishing. Allgemein kann somit zum Thema E-Mail empfohlen werden, generell misstrauisch zu sein, Inhalt, Anhang und im speziellen Links zu überprüfen.

2.1.4 Effektivität

Wie bereits in Abschnitt 1.2 Problemstellung beschrieben, wird die Verbreitung von Phishing von einigen Organisationen untersucht. Über die Effektivität von Phishing ist sich die Forschergemeinschaft jedoch uneins. Long (2013) fand in ihrer Masterarbeit, dass 2–3 % der Mitarbeiter im Finanzsektor aufgrund von Phishing-E-Mails ihre Zugangsdaten weitergaben. Im Experiment von Jakobsson und Ratkiewicz (2006) folgten

11 % der 237 Anwender dem Phishing-Link zu einem Onlineauktionshaus und gaben dort ihre Anmeldedaten unbewusst weiter. In ihrem Experiment sandten sie jedem Anwender jeweils vier E-Mails, unter der unbelegten Annahme, es bestehe kein Lerneffekt durch vorangegangene E-Mails. Benenson, Gassmann und Landwirth (2017) fanden eine Phishing-Link-Klickrate von 20 % via E-Mail und eine von 42.5 % auf Facebook. Sie verschickten einen Link zu nichtexistierenden Partybildern einer fiktiven Party von einem unbekannten E-Mail-Konto an 1'200 Studenten. Die meisten Studenten, welche dem Phishing-Link folgten gaben Neugierde als Motiv an. Möglicherweise könnte die Klickrate mit einer echter wirkenden E-Mail erhöht werden, beispielsweise von einer realen Party, und mit gefälschtem Absender der Organisatoren. Dieses Forschungsresultat von Benenson et al. (2017) lässt sich auf Grund des Nachrichteninhaltes nicht direkt in die Geschäftswelt übertragen, zeigt aber, dass 20 % der Anwender auf ein unbekanntes Phishing-E-Mail reagieren.

In einem Experiment fand Kumaraguru, Rhee, Acquisti et al. (2007), dass bis zu 100 % der Probanden auf Phishing-Links klicken. Das Experiment bestand aus drei Gruppen zu je zehn Teilnehmern deren Aufgabe es war, Phishing-E-Mails zu erkennen. Die Phishing-E-Mails wurden als Embedded-Training direkt an die E-Mail-Adresse der Teilnehmer versandt, danach erhielten die Teilnehmer, je nach Gruppe, ein Phishing-Training in Textform, als Text mit Bildern oder als Comic. Am Ende des Quasi-Experimentes erhielten die Teilnehmer ein weiteres Phishing-E-Mail zugesandt. Bei der Gruppe, welche das Training als Text erhielt, veränderte sich die Klickrate von 90 % nicht. Beim Hinweis mit Bildern sank die Rate von 80 % auf 70 % und beim Comic von 100 % auf 30 %. Die Aussagekraft der Studie von Kumaraguru, Rhee, Acquisti et al. ohne Kontrollgruppe und mit nur zehn, absichtlich ohne Informatikkenntnisse selektionierten, Probanden pro Gruppe ist jedoch beschränkt. In einer weitere Studie von Kumaraguru et al. (2008), folgten 88 % anstatt 100 % der Anwender dem Link.

Eine Klickrate von 100 % fanden auch Siadati et al. (2017). Die Autoren missbrauchten die Benachrichtigungsfunktion von GitHub.com, einer Plattform für gemeinsame Softwareentwicklung. GitHub versandte für die Forscher mit Phishing-Links ver-

sehene E-Mails an 20 Studenten mit Informatikkenntnissen, welche die Plattform nutzten. Für diese Art von Angriff, welche Siadati et al., in Anlehnung an XSS 'X-Plattform Phishing' nennen, sind ebenfalls weitere Plattformen wie LinkedIn, Dropbox oder Amazon anfällig (Siadati et al., 2017). Siadati et al. (2017) untersuchten die Phishing-Link-Klickrate. Es wurde jedoch nicht untersucht, wie viele der 20 Studenten sich auf der Phishing-Kopie von Github, tatsächlich angemeldet hätten. Um eine Phishing-Webseite zu erstellen, können Teile der echten Webseite, in diesem Falle von Github, übernommen werden. Mit dieser Technik kann ein Klon der originale Webseite kreiert werden (Chaudhry et al., 2016). Dhamija et al. (2006) fanden in ihrer Studie, dass bei effektiven Phishing-Webseiten 90 % der Anwender ihre privaten Daten hinterlassen. Die Erfolgsrate von Phishing-E-Mails liegt somit je nach Studie und abhängig vom E-Mail und Empfänger zwischen 2–100 %. Dies würde bedeuten, dass mit 50 Phishing-E-Mails im Durchschnitt mindestens ein Benutzerkonto des angegriffenen Unternehmens kompromittiert werden kann.

2.1.5 Betroffene Wirtschaftssektoren

Vom klassischen Klon-Phishing kann jede Unternehmung betroffen sein. Der Finanzsektor scheint besonders gefährdet (Kaspersky Lab, 2018; PhishLabs, 2018). Ein weiteres Indiz dafür sind die von den Banken zur Verfügung gestellten Anti-Phishing-Information. Der Phishing-Test der Hochschule Luzern (2018a) fragt Erkennungsmerkmale ab und verwendet sowohl PayPal als auch die PostFinance als Beispiel. Der Test ist Teil der Plattform "eBanking - aber sicher!", welche mehrere Partner aus dem Finanzsektor hat und zur Hochschule Luzern (2018a) gehört. Die Firma PayPal wird in mehreren Quellen zwischen 2004 und 2018 genannt (PhishLabs, 2018; Symantec, 2017; Siadati et al., 2016; Parsons, McCormac, Pattinson, Butavicius & Jerram, 2015; Arachchilage & Love, 2014; Atkins & Huang, 2013; Rajalingam et al., 2012; X. Sheng, 2009; Whittaker et al., 2010; Aburrous, Hossain, Dahal & Thabtah, 2010; Rosiello et al., 2007; Chandrasekaran et al., 2006; Ollmann, 2004). Amazon, eBay, Gmail, Google, Dropbox und Banken werden ebenfalls genannt.

PhishLabs (2018) sieht wie Kaspersky Lab (2018) und die MELANI (2015b) Finanzdienstleister im Fokus der Phishing-Angriffen, allerdings nur mit einem Anteil von 33.9% anstatt 54%. Auf die Finanzdienstleister (23%) und Zahlungsdienste (13.9%) folgen gemäss PhishLabs (2018) Cloud-Speicherdienste (22.6%) wie Dropbox und Online-Dienstleister (20.6%) wie Google und Online-Handel (11%) wie Amazon.

Ein Training sollte deshalb Beispiele dieser Sektoren beinhalten. In dieser Studie werden Phishing-E-Mails in Anlehnung an die Unternehmen Viseca und Paypal aus dem Finanzsektor, Dropbox stellvertretend für die Cloud-Speicherdienstleister und Google als Online-Dienstleister behandelt. Der schweizerische Mobilfunk-Provider Salt wird als ein Vertreter aus dem Online-Handel gewählt. Die schweizerische Post wurde aufgrund des aktuellen Angriffs gewählt.

2.2 Anti-Phishing-Massnahmen

Es wurden Anstrengungen unternommen, dem Phishing-Problem zu begegnen. Dieser Abschnitt verschafft einen Überblick über technische Massnahmen zur Verhinderung von Phishing-Angriffen. Nicht-technische Massnahmen wie Anwender-Training werden in Abschnitt 2.4 beschrieben.

Schwarze Listen

Eine Methode um Phishing zu verhindern, ist das Führen einer Schwarzen Liste (engl. blacklist) (Huang et al., 2009) mit bekannten Phishing-URLs, wie dies im US-Patent von Georgiev (2015) beschrieben wird. PhishTank (Ulevitch, o. J.) stellt beispielsweise eine solche kollaborativ erstellte Liste kostenfrei zur Verfügung. Schwarze Listen helfen aufgrund ihrer Funktionsweise nur, bei bereits bekannten Phishing-URLs. Ein weiterer Ansatz, welcher auch neue Phishing Webseiten erkennen kann, wurde von D. S. Gupta, Tanbeer und Mohandas (2017) patentiert. Dabei werden die Inhalte der zu analysierenden Seiten mit bekannten legitimen Webseiten verglichen und falls eine hohe Übereinstimmung besteht, wird die Webseite als Phishing klassifiziert. Ein älteres Patent wendet eine vergleichbare Methode an (J. T. Goodman et al., 2005), jedoch wird

dabei nur die URL verglichen.

Microsoft hält zwei Patente, um mit maschinellem Lernen Phishing-Webseiten zu erkennen (Zhu, Choi, KR, Lee & KR, 2013; Xue & Zhu, 2015). Google (2018) setzt ebenfalls auf maschinelles Lernen. Eine von drei Google-Ingenieuren verfasste wissenschaftliche Arbeit (Whittaker et al., 2010) beschreibt, wie Google maschinelles Lernen nutzt, um Millionen von Webseiten täglich zu analysieren und auf Phishing hin zu überprüfen. Ihre Lösung klassifiziert Phishing-Webseiten zu 90 % korrekt mit einer False-Positive-Rate von unter 0.1 %. Wird eine legitime E-Mail fälschlicherweise als Phishing klassifiziert, wird dies als False-Positive bezeichnet. Bei einem False-Negative wird eine Phishing-E-Mail nicht erkannt und als legitimes klassifiziert. Eine hohe False-Positive-Rate kann den Anwender verärgern (Purkait, 2013), da legitime E-Mails möglicherweise nicht zugestellt werden. Laut Whittaker et al. (2010) ist der Ansatz einer automatischen Phishing-Klassifikation manuell gepflegten schwarzen Listen dadurch überlegen, dass weniger Zeit bis zur Erkennung einer Phishing-Webseite vergeht. Viele Phishing-Webseiten sind weniger als einen Tag online, wenige Stunden Verzögerung können deshalb die Qualität einer schwarzen Liste signifikant beeinträchtigen (Whittaker et al., 2010). Schwarze Listen scheinen ein effektives Mittel gegen Phishing darzustellen, welches bis zu 90 % der Phishing-URLs erkennt.

Browser-Leisten (engl. browser toolbars), welche die Vertrauenswürdigkeit angesteuerter Webseiten, unter anderem via schwarzen Listen, überprüfen, können ebenfalls eingesetzt werden. Browser-Leisten haben sich nicht als effektiv erwiesen (Wu, Miller & Garfinkel, 2006; Cranor, Egelman, Hong & Zhang, 2007). Es sind wenig aktuelle Publikationen zu diesem Thema vorhanden, was darauf hindeutet, dass der Ansatz mit Browser-Leisten nicht mehr länger verfolgt wird.

Vertrauenswürdige Absender

Eine weitere Massnahme ist das Fälschen des Absenders zu erschweren. Mit Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) und Domain Message Authentication Reporting & Conformance (DMARC) existieren technische Möglich-

keiten, den Absender einer E-Mail zu authentifizieren und damit Phishing zu erschweren (Siadati et al., 2016). SPF (Kitterman, 2014) bietet die Möglichkeit das Fälschen eines E-Mail-Absenders (engl. spoofing) zu erschweren. Via DNS wird überprüft, welchen E-Mail-Servern gestattet ist, E-Mails für eine bestimmte Domain (steht hier für die URL nach dem @) zu versenden. Mit DKIM (Hansen, Kucherawy & Crocker, 2011; Kitterman, 2018) lassen sich E-Mails beim Senden vom Server digital signieren. Anhand der Signatur und dem DNS kann der Empfänger den Inhalt und Absender einer E-Mail verifizieren. DMARC (Kucherawy & Zwicky, 2015) ist ein Regelset und Framework, welches SPF & DKIM verwendet, um E-Mails zu klassifizieren. Mit DMARC lassen sich gefälschte Absender erkennen, falls die beteiligten E-Mail-Server diese Protokolle einsetzen. Ähnliche Absender können mit dieser Massnahme nicht erkannt werden. Die in dieser Studie entworfenen Phishing-E-Mails konnten mit gefälschtem Absender erfolgreich an die E-Mail-Dienste von Google und Microsoft gesendet werden.

Multi-Faktor-Authentifizierung (MFA)

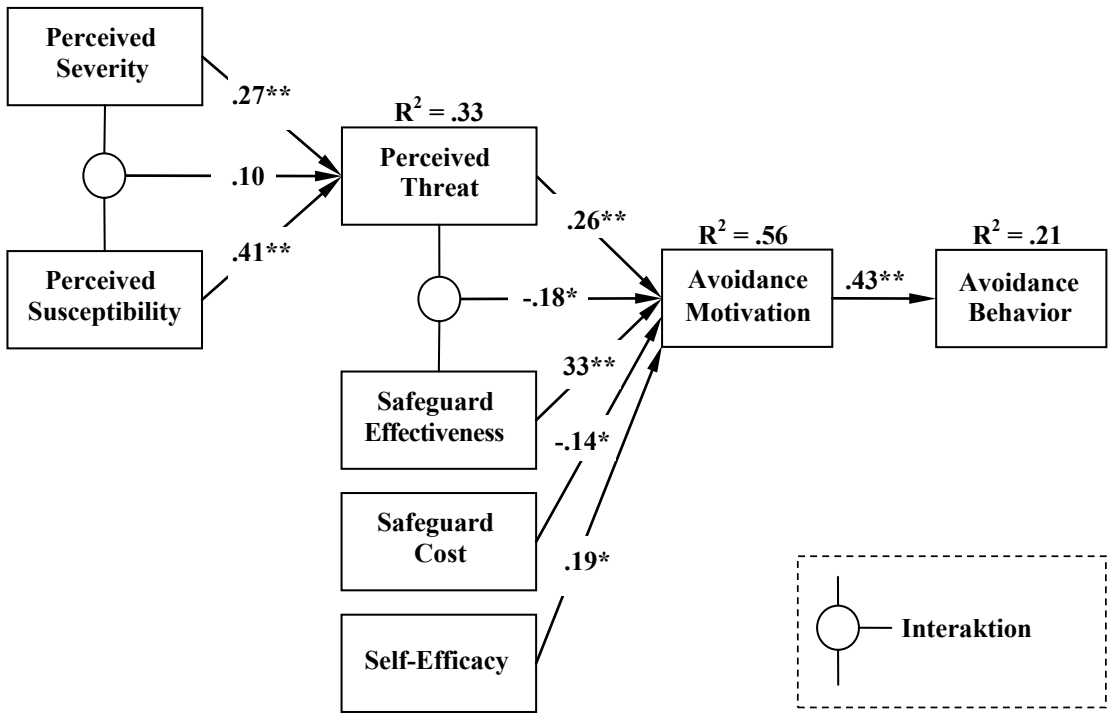
Multi-Faktor-Authentifizierung (MFA) wird ebenfalls als Option gegen Phishing genannt (Ramzan, 2010). Beim Anmelden via MFA muss ein Anwender, zusätzlich zu seinem Passwort, noch mindestens einen weiteren Faktor vorweisen. Dies kann beispielsweise ein auf dem Mobiltelefon generierter TOTP-Code (Time-Based One-Time Password Algorithm-Code) sein (Rydell, M'Raihi, Pei & Machani, 2011). MFA erschwert Phishing-Angriffe, kann diese jedoch nicht immer verhindern. Ein Man-in-the-Middle (MITM)-Angriff (Schneier, 2005) oder Malware auf dem Mobiltelefon kann MFA umgehen (Zollinger & Monsorno, 2015).

Trotz Massnahmen wie MFA, DMARC, dem Führen von schwarzen Listen und der maschinellen Klassifikation von Phishing-Webseiten durch Firmen wie Microsoft oder Google ist Phishing ein ungelöstes Problem. Gemäss Hong (2012) bieten technische Massnahmen keinen Schutz, solange sich die Anwender durch Phishing täuschen lassen. Wie in Abschnitt 1.3 beschrieben, kann Anwender-Training möglicherweise das Schadensausmass von Phishing-E-Mails reduzieren.

2.3 Modelle

Dieser Abschnitt beschreibt die Anwendbarkeit der Technology Threat Avoidance Theory (TTAT), des Technology Acceptance Models (TAM) und der Fennema-Sherman Attitude Scale in Bezug auf Training. Diese Modelle bilden die theoretische Grundlage dieser Arbeit und einiger in Abschnitt 2.4 beschriebenen verwandten Arbeiten

Die TTAT erklärt das *Vermeidungsverhalten* von Anwendern bei Cyber-Bedrohung und wurde von Liang und Xue (2009) unter Berücksichtigung mehrerer Theorien aus unterschiedlichen Bereichen hergeleitet. Aus der TTAT, der bisher ersten Theorie für Cyber-Bedrohung-Vermeidungsverhalten, entwickelten Liang und Xue (2010) das TTAT-Modell (siehe Abbildung 2.1) und testeten dieses empirisch. Das TTAT-Modell stützt die Wichtigkeit von Anwender-Training und hilft dessen Effektivität zu erhöhen (Liang & Xue, 2010).



Beziehung: β = Regressionskoeffizient, ** p < .01; * p < .05, R^2 = Bestimmtheitsmass

Abbildung 2.1: Technology Threat Avoidance Theory (TTAT) nach Liang und Xue (2010)

Die Abbildung 2.1 beschreibt das TTAT-Modell, welches Einflüsse auf die *Vermeidungsmotivation* (engl. Avoidance Motivation), die zu *Vermeidungsverhalten* (engl. Avoidance Behavoir) führen (Liang & Xue, 2010). Auf die *Vermeidungsmotivation* wirken die *wahrgenommene Bedrohung* (engl. Perceived Threat), *Effektivität und Aufwand der Sicherheitsmassnahmen* (engl. Safeguard Effectiveness und Cost) sowie die *Selbstwirksamkeitserwartung* bei Anwendung der Sicherheitsmassnahmen (engl. Self-Efficacy).

Die *wahrgenommene Bedrohung* definiert die Einschätzung der Gefahr durch den Anwender und setzt sich aus dem *wahrgenommenen Schweregrad und Anfälligkeit* zusammen. Der *wahrgenommene Schweregrad* (engl. Perceived Severity) steht für das, durch den Anwender antizipierte, Schadensausmass der negativen Konsequenzen durch die Bedrohung. *Die wahrgenommene Anfälligkeit* oder Suszeptibilität (engl. Perceived Susceptibility) definiert sich durch die geschätzte Wahrscheinlichkeit von der Bedrohung betroffen zu sein (Liang & Xue, 2010). Dieses Konstrukt gleicht der Risikodefinition, welche Risiko als Produkt von Schadensausmass und Eintrittswahrscheinlichkeit festlegt (Ropohl, 1986, S. 97).

Die *Effektivität der Sicherheitsmassnahmen* beschreibt den Grad an Kontrolle, welche Anwender über die Bedrohung durch Anwendung der Massnahme erlangen. Der *Aufwand der Sicherheitsmassnahmen* bezieht sich auf den physischen und kognitiven Aufwand, welchen Anwender betreiben müssen, um die Sicherheitsmassnahme anzuwenden. Die *Selbstwirksamkeitserwartung* definiert die Selbstsicherheit, welche ein Anwender beim Benutzen der Sicherheitsmassnahme empfindet. Allgemeiner bezeichnet *Selbstwirksamkeitserwartung* die Zuversicht eines Anwenders, Handlungen aufgrund eigener Kompetenzen selbst auszuführen (Bandura, 1977).

Gemäss dem TTAT-Modell sollte Anwender-Training die Cyber-Bedrohung, deren Eintrittswahrscheinlichkeit, Konsequenzen und Vermeidbarkeit aufzeigen (*wahrgenommene Bedrohung, Schweregrad und Anfälligkeit*). Ebenfalls muss die Effektivität und die Einfachheit der Sicherheitsmassnahmen aufgezeigt (*Effektivität und Aufwand der Sicherheitsmassnahmen*) und die *Selbstwirksamkeitserwartung* erhöht werden. Die ne-

gative Interaktion zwischen der *wahrgenommenen Bedrohung* und der *Effektivität der Sicherheitsmassnahmen* lässt vermuten, dass die *Effektivität der Sicherheitsmassnahmen* sinkt, falls die *wahrgenommene Bedrohung* steigt (Liang & Xue, 2010). Deshalb empfehlen Liang und Xue (2010) die Cyber-Bedrohung nicht in extremis aufzuzeigen.

Das TTAT-Modell (Liang & Xue, 2010) enthält unter anderem Elemente des Technology Acceptance Models (TAM) von Davis (1985). Dieses ist zur Voraussage der Nutzung eines Systems durch Anwender geeignet ist und von Venkatesh und Davis (2000) weiter entwickelt und getestet wurde (Venkatesh, Morris, Davis & Davis, 2003). Das TAM seinerseits basiert auf dem Fishbein-Modell (Fishbein & Ajzen, 1975; Ajzen & Fishbein, 1977, 1980). Das TAM (Venkatesh & Davis, 2000) untersucht den Effekt der wahrgenommenen Nützlichkeit (Perceived Usefulness) eines Systems und die Einfachheit der Nutzung (Perceived Ease of Use) auf die Absicht eines Anwenders ein System zu nutzen (Intention to Use (Venkatesh & Davis, 2000) / Attitude Toward Using (Davis, 1989)), sowie dessen tatsächliches Nutzungsverhalten vorherzusagen (Usage Behavior). Die wahrgenommene Nützlichkeit des TAMs gleicht der Effektivität der Sicherheitsmassnahmen aus dem TTAT-Modell. Die Einfachheit der Systemnutzung aus dem TAM scheint gegenteilig als Aufwand anstatt Einfachheit in der Anwendung von Sicherheitsmassnahmen im TTAT-Modell reflektiert zu sein.

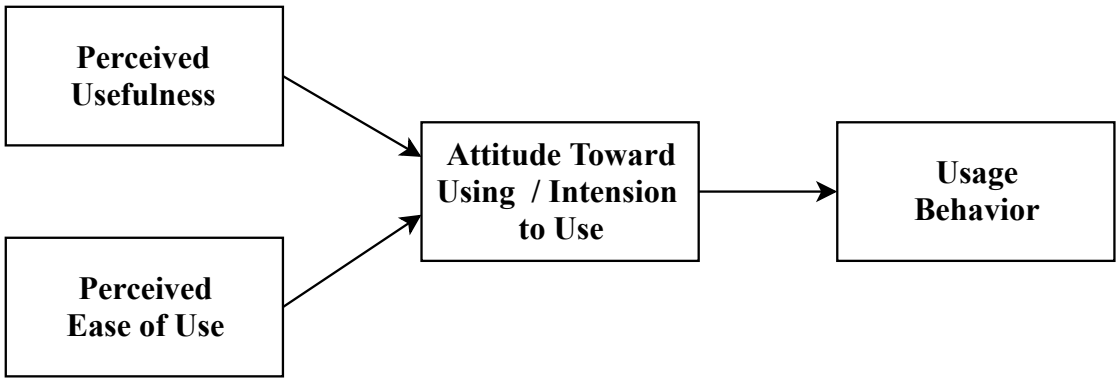


Abbildung 2.2: Technology Acceptance Model (TAM) nach Venkatesh und Davis (2000)

Das TAM scheint nützlich zur Erhebung der Einstellung gegenüber E-Mail-Diensten zu sein. Da keine Belege gefunden wurden, dass durch den Anwender wahrgenommene Nützlichkeit oder Einfachheit eines Systems das Bedrohungsvermeidungsverhal-

ten beeinflusst, wird das TAM in dieser Arbeit lediglich als Basis des TTAT-Models verwendet. Aus demselben Grund wird auch auf andere Modelle zur Messung einer Einstellung (engl. Attitude) gegenüber einem System oder Sache verzichtet. Eines dieser Modelle ist die Fennema-Sherman Mathematics Attitude Scale (Fennema & Sherman, 1976) beziehungsweise deren Modifikationen für die Informationstechnologie (Kahveci, 2010). Das TTAT-Modell erklärt das Vermeidungsverhalten von Bedrohungen und ist deshalb besser für ein Phishing-Training geeignet als das TAM, welches die Nutzung eines Systems vorauszusagen versucht, indem die Einstellung der Anwender erhoben wird.

Das in dieser Studie entwickelte Anti-Phishing-Training stützt sich auf das TTAT-Modell, welches bereits Anwendung in Sicherheitstrainings fand (Arachchilage & Cole, 2011) (siehe Abschnitt 2.4). Im entwickelten Training wird dem Anwender vermittelt, dass Phishing eine verbreitete Bedrohung ist, von welcher alle Anwender betroffen sein können (*wahrgenommenen Anfälligkeit*) und dass durch Phishing entwendete Anmeldedaten unautorisierte Kontoüberweisungen möglich machen. Ebenfalls wird aufgezeigt, dass durch Ransomware im Anhang private Dateien verloren gehen können (*wahrgenommener Schweregrad*). Es wird erklärt, dass es einfach ist, die Webseitenadresse der Links mithilfe der Maus in Erfahrung zu bringen und wie die Adresse überprüft werden kann (*Aufwand der Sicherheitsmassnahmen*). Durch interaktives Training sollen die Anwender die Wirksamkeit der Sicherheitsmassnahmen selbst überprüfen können (*Effektivität der Sicherheitsmassnahmen*). Das Training soll den Anwendern ebenfalls Sicherheit im Umgang mit Phishing-E-Mails und Anwendung der Sicherheitsmassnahmen geben, um die *Selbstwirksamkeitserwartung* zu steigern. Als Kontrollvariablen werden, statt dem TAM gestützten Nutzungsverhalten, Informatikkenntnisse, Alter und Geschlecht erhoben. Die Informatikkenntnisse sollen reflektieren wie gut sich ein Anwender mit Informatik im Speziellen mit E-Mails auskennt. Obwohl laut (Liang & Xue, 2010) Alter, Geschlecht und Internet-Erfahrung keinen Einfluss auf das Vermeidungsverhalten einer Bedrohung haben, könnten diese die Erkennungsleistung von Phishing beeinflussen. Die Phishing-Erkennungsleistung definiert, wie gut Anwender in der Lage sind, Phishing-E-Mails von legitimen zu unterscheiden.

Ein weiteres Modell zur Lerntheorie aus der Didaktik unterscheidet zwischen prozeduralem und deklarativem Wissen. Prozedurales Wissen bezeichnet Handlungswissen (Wissen wie, engl. knowing how), während deklaratives Sachwissen (Wissen was, engl. knowing what) bezeichnet (Anderson, 1976; Tenberg, 2006, S. 88; Rampillon & Zimmermann, 1997, S. 59). In einem theoretischen Teil des Trainings wird deshalb deklaratives Wissen vermittelt, während beim interaktiven Training das prozedurale Wissen aufgebaut werden soll.

2.4 Verwandte Arbeiten

In der Vergangenheit wurden bereits zu nicht technischen Anti-Phishing-Massnahmen wie Trainings geforscht. Dieses Kapitel beschreibt verwandte Studien und Publikationen, welche sich mit Anti-Phishing-Training beschäftigen.

Phish-Guru & Anti-Phishing-Phil von Kumaraguru et al.

Kumaraguru und Sheng setzen sich in mehreren Studien mit dem Thema Phishing auseinander (Kumaraguru, Rhee, Acquisti et al., 2007; Kumaraguru, Rhee, Sheng et al., 2007; S. Sheng et al., 2007; Kumaraguru et al., 2008, 2009, 2009; S. Sheng et al., 2010). In einer Studie liessen Kumaraguru, Rhee, Acquisti et al. (2007) drei Gruppen zu je zehn Probanden in einem Laborexperiment ohne Kontrollgruppe 18 E-Mails erkennen. Dazwischen präsentierte sie jeweils auf unterschiedliche Weise Informationen über Phishing. In der Studie schnitt die Gruppe, welche die Phishing-Informationen als Comic erhalten hatte, besser ab als die Gruppen, welche die Informationen als Text oder als Text mit Bildern erhalten hatte. In ihrer Studie entschieden sie sich Kumaraguru, Rhee, Acquisti et al. (2007) für die Grundsätze, Links in E-Mails nicht zu folgen und persönliche Daten nicht anzugeben. Alternativ könnte den Anwendern die Kompetenz Phishing von legitimen E-Mails zu unterscheiden vermittelt werden.

In einer weiteren Laborstudie mit je 14 Studenten ohne Informatikkenntnisse pro Gruppe verglichen Kumaraguru, Rhee, Sheng et al. (2007) die Effektivität von Phishing-Informationen als Comic in zwei Szenarien. Die Informationen wurden entweder di-

rekt im E-Mail bereitgestellt oder die Anwender erhielten eine Phishing-E-Mail dessen Link zu Informationen führte. Letztere Methode nennen sie Embedded-Training. Kumaraguru, Rhee, Sheng et al. (2007) fanden, dass die Embedded-Methode bei welcher eine Phishing-E-Mail versandt wird, im Labor wirkungsvoller war. Begründet wurde dies damit, dass Anwender, nachdem sie Phishing zum Opfer gefallen sind, empfänglicher für Informationen darüber sind. Im Gegensatz zu ihrer letzten Studie setzten sie in dieser auf Lernprinzipien wie, Learning-by-doing, sofortige Rückmeldung und auf Story-basierte Lernmethoden. Den entwickelten 'Phish-Guru' Comic in fünf Bildern, verwendeten Kumaraguru et al. (2008) in einer weiteren Studie zusammen mit einem Firmenpartner und einer Spear-Phishing Variante des Phish-Gurus mit mehr Teilnehmern ($N = 111$). Ein drittes Mal zum Einsatz kam der Phish-Guru mit dem Ziel, die Wirkungsdauer des Trainings zu untersuchen (Kumaraguru et al., 2009). Das Experiment umfasste 515 Teilnehmer, inklusive einer Kontrollgruppe. Alle drei Studien (Kumaraguru, Rhee, Sheng et al., 2007; Kumaraguru et al., 2008, 2009) wurden unter anderem mit t-Tests ohne Angabe der Effektstärke ausgewertet. Der t-Test ist ein statistischer Test zur Analyse der Mittelwertdifferenz (Universität Zürich, 2018). Das Training hatte einen positiven Effekt und es wurde kein Effekt bei demografischen Merkmalen festgestellt.

S. Sheng et al. (2007) publizierte zusammen mit Kumaraguru das Spiel 'Anti-Phishing Phil'. Das Spiel ist komplett losgelöst von E-Mails und es gilt in einem Aquarium Phishing-URLs zu erkennen. Würmer repräsentieren dabei URLs, welche via Tastendruck von einem Fisch gegessen werden können. Der Vater des Fisches kann um Hilfe gebeten werden. Es scheint als hätten Kumaraguru, Rhee, Acquisti et al. (2007) ihre Meinung den Anwendern nur die Grundsätze zu schulen im selben Jahr revidiert. Jedenfalls ist eines ihrer Prinzipien nun, Anwender zu lehren, Phishing-URLs zu identifizieren und nicht Links generell zu ignorieren. Wen et al. (2017) kritisiert an dieser Studie, dass dieses Spieldesign kein realistisches Training bietet. Um ihr Phishing-Training zu prüfen, wurde ein Quasi-Experiment (Eifler, 2014) ohne Kontrollgruppe mit den Gruppen Spiel, Tutorial und bestehendem Trainingsmaterial an je 14 Probanden durchgeführt. Das Spiel hatte den grössten Effekt. Aufgrund einer Vorher-Nachher-Messung (Eifler,

2014; Stein, 2014) und der kleinen Stichprobe sind die Resultate zu relativieren. Ebenfalls ist der relativ kleine Fokus und Umfang des Spiels zu kritisieren, da es lediglich gilt URLs zu identifizieren.

Phish-Guru und Anti-Phishing Phil wurden in einer weiteren Studie mit dem Titel 'Teaching Johnny not to Fall for Phish' (Kumaraguru et al., 2010) untersucht. Der Titel ist möglicherweise an 'Why Johnny can't encrypt' (Whitten & Tygar, 1999) angelehnt. Aus den beiden Trainings wurden Schulungsprinzipien abgeleitet und in einer Literaturrecherche von drei Webseiten und einem Video wurden E-Mail-Erkennungsmerkmale identifiziert. In dieser Studie fanden Kumaraguru et al. (2010) einen demografischen Zusammenhang, und zwar dass 13- bis 17-Jährige besonders anfällig für Phishing sind. Dies könnte ein Grund für die weitere Studie von S. Sheng et al. (2010) zusammen mit Kumaraguru sein, in welcher sie den Zusammenhang zwischen Demografie und Phishing-Anfälligkeit untersuchten. Dabei fanden sie, dass weibliche und Probanden zwischen 18 und 25 Jahren besonders anfällig sind. Aufgrund dieser Befunde berücksichtigt diese Studie ebenfalls Alter und Geschlecht der Probanden.

Control-Alt-Hack von Denning, Lerner, Shostack und Kohno

Denning et al. (2013) entwickelten ein physisches Kartenspiel mit dem Ziel, das Sicherheitsbewusstsein zu steigern, und versandten es an Bildungsinstitutionen. Aus qualitativem Feedback von 22 Institutionen und über 450 Studenten lasen sie, dass ihr Kartenspiel das Ziel erreicht hatte. Ebenfalls zeigen Denning et al. (2013) anhand weiterer Spiele im Bereich Cyber-Sicherheit auf, dass für Training insbesondere Spiele eingesetzt werden, deshalb enthält das in dieser Studie entwickelte Training ebenfalls spielerische Elemente.

Anti-Phishing Spiele 1–3 von Arachchilage und Hameed

Arachchilage und Cole (2011) entwickelten ein Spiel für das Mobiltelefon und stützen sich dabei auf die Technology Threat Avoidance Theory (TTAT) von Liang und Xue (2010). Anhand der Publikation ist der Bezug des TTAT-Modells zum Spiel schwer nachvollziehbar. Sie beziehen sich dabei auf die wahrgenommene Bedrohung

(engl. Perceived Threat) (Liang & Xue, 2009) und treffen die Aussage, dass Anwender realisieren, dass die Effektivität der absichernden Massnahmen (engl. Safeguard Effectiveness) die Kosten der Absicherungsmassnahmen (Safeguard Cost) senken und Selbstwirksamkeitserwartung (engl. Self-Efficacy) steigern (Arachchilage & Cole, 2011), was so nicht durch das TTAT-Modell von Liang und Xue (2010) erklärt werden kann (siehe Abbildung 2.1). Im von Arachchilage und Cole (2011) entwickelten Spiel isst der vom Anwender kontrollierte kleine Fisch, Würmer, welche URLs repräsentieren. Hilfe kann der Anwender vom grossen Fisch anfordern. Das Anti-Phishing-Spiel von Arachchilage und Cole (2011) und der Anti-Phishing Phil von S. Sheng et al. (2007) unterscheiden sich im Konzept nicht massgeblich. Arachchilage und Cole (2011) referenziert die Anti-Phishing Phil Studie von S. Sheng et al. (2007), jedoch nicht im Kontext des Spiels. Die gleiche von Wen et al. (2017) angebrachte Kritik der Realitätsferne kann bemerkt werden.

Arachchilage und Love (2013) analysierten das TTAT-Modell und evaluierten es erneut anhand einer Online-Umfrage ($N = 150$), um ein Spieldesign-Framework für Phishing-Training zu erhalten. Die Autoren kamen zu dem Schluss, dass das TTAT als Spieldesign-Framework geeignet ist. In einer weiteren Studie unter Verwendung des TTAT-Modells (Arachchilage & Love, 2014) wurde via Online-Umfrage mit Studenten ($N = 20$) der Effekt von prozeduralem und deklarativem Wissen durch die Bewertung von fünf URLs, auf die Selbstwirksamkeitserwartung (engl. Self-Efficacy) ausgewertet. Deklaratives ($p = .132$) und prozedurales Wissen ($p = .132$) waren einzeln nicht signifikant. Zusammen in einer ANOVA ($p = .033$) konnte ein signifikanter Einfluss auf Selbstwirksamkeitserwartung (engl. Self-Efficacy) des TTAT-Modells gemessen werden. Auf die Angabe einer Effektstärke wurde bei diesen Beziehungen verzichtet. Die Urheber des TTAT-Modells (Liang & Xue, 2010) verwendeten stattdessen Regressionen und setzten die Variablen unter Angabe des β-Koeffizienten und der Signifikanz in Beziehung miteinander.

Im Jahr 2016 entwickelten Arachchilage et al. (2016) ein weiteres Spiel unter Berücksichtigung des TTAT-Modells und des von ihnen entwickelten Design-Frameworks

(Arachchilage & Love, 2013). Die Konzepte des prozeduralen- und konzeptionellen-Wissens (Arachchilage & Love, 2014) wurden nicht integriert, deren Integration wird in einer Folgestudie (Arachchilage & Hameed, 2017) diskutiert. Das aus der Studie resultierende Spiel entspricht im Funktionsumfang, Design und Konzept dem von Arachchilage und Cole (2011) entwickelten. In einer Vorher-Nachher-Messung ($N = 20$) wurde die Phishing-Erkennungsleistung durch das Spiel um 28 % verbessert. Im Quasi-Experiment (Eifler, 2014) mussten jeweils zehn URLs im Pre-, Spiel und Post-Test als Phishing oder legitim klassifiziert werden. Obwohl der Vergleich der Erkennungsleistung in Prozent mittels t-Test ($p < 0.005$) signifikant war, ist bei der Interpretation des Resultates der Studie auf die kleine Stichprobengrösse und das Experimentaldesign ohne Kontrollgruppe zu achten.

Die von Arachchilage und Hameed (2017) vorgeschlagenen Konzepte im Zusammenhang mit prozeduralem und deklarativem Wissen, sowie der Selbstwirksamkeitserwartung (engl. Self-Efficacy) werden in einer Studie von Misra et al. (2017) in einem Spiel namens Phish-Phinder implementiert, mit dem Ziel die Selbstsicherheit der Anwender zu erhöhen. Der Phish-Phinder aus dem Jahr 2017 unterscheidet sich nicht wesentlich von den zwei vorhergehenden Spielen (Arachchilage & Cole, 2011; Arachchilage et al., 2016) und bezieht sich auf den 2007 entwickelten Anti-Phishing Phil von S. Sheng et al. (2007) mit beinahe identischer Funktionalität.

Die Studien von Arachchilage erforschten wie sich das TTAT-Modell und weitere Konzepte in Anti-Phishing-Spiele einbinden lassen. Das TTAT-Modell aus dem Bereich der Cyber-Sicherheit lässt sich demnach auch spezifisch für die Bedrohung durch Phishing und die Entwicklung von Anwender-Training einsetzen. Die Konzepte der von Arachchilage entwickelten Anti-Phishing-Spiele haben sich durch die Anwendung des Modells jedoch nur marginal verändert. Für diese Arbeit wurde ein anderes, realistischeres Schulungskonzept unter Berücksichtigung des TTAT-Modells gewählt. Die URL wird im Anwender-Training dieser Studie ebenfalls berücksichtigt, jedoch nicht als einziger Bestandteil, da reine URL-Identifikation Spiele bereits mehrfach entwickelt und erforscht wurden.

What.Hack von Wen et al.

Wen et al. (2017) entwickelten das Online-Anti-Phising-Spiel What.Hack basierend auf dem Spiel 'Papers Please' um Anwender im Umgang mit E-Mails, URLs und Anhängen zu schulen. Ebenfalls zeigt das Spiel die negativen Konsequenzen von Phishing auf. Im Szenario des Spiels werden die Anwender in einer fiktiven Bank zum E-Mail-Filter und müssen nach einem vorgegebenen Regelwerk die eingehenden E-Mails kategorisieren, um im Level aufzusteigen. Es handelt sich dabei um E-Mails mit reinem Text und Links. Der Schwierigkeitsgrad steigt mit jedem Level an und das Regelwerk, welches vertrauenswürdige und nicht vertrauenswürdige Domain-Namen (steht hier für die URL nach dem @) und Dateiendungen enthält, erweitert sich. Durch das Abgleichen des Domain-Namen aus dem Regelwerk mit demjenigen des Absenders sind die Phishing-E-Mails grösstenteils klassifizierbar. Dies ist zu kritisieren, da ein Anwender im Normalfall nicht über ein Regelwerk mit einer solchen Filterliste verfügt. Eine Filterliste kann ausserdem technisch umgesetzt werden, um Anwender nicht weiter zu belasten. Im Anwender-Training dieser Studie wird daher auf eine Auflistung von vertrauenswürdigen URLs verzichtet. Ein Regelwerk mit generellen Regeln wird als sinnvoll erachtet. In What.Hack werden Anwender darauf trainiert, die URL des Links zu prüfen, indem mit der Maus darübergefahren wird. Dieses Vorgehen ist realitätsnäher (Wen et al., 2017) als der Ansatz, URLs dem Anwender direkt zur Bewertung vorzulegen, wie dies im Anti-Phishing Phil (S. Sheng et al., 2007) und der Phish-Phinder Serie gemacht wurde (Arachchilage & Cole, 2011; Arachchilage et al., 2016; Misra et al., 2017). Beim in dieser Studie entwickelten Training müssen Anwender die Links auf die selbe Weise überprüfen. Ebenfalls sollen die Konsequenzen beim Öffnen von Anhängen mit Malware aufgezeigt werden und die E-Mails realer erscheinen. Die Effektivität von What.Hack wurde nicht überprüft, doch die Autoren Wen et al. (2017) planen dies in Zukunft zu tun. Die Messung des Anwender-Trainings ist integraler Bestandteil dieser Studie.

Kapitel 3

Methodik

Dieses Kapitel führt die Forschungsfrage (siehe Abschnitt 3.1) und Hypothesen (siehe Abschnitt 3.2) aus. Zur empirischen Überprüfung der Hypothesen wird ein randomisiertes Kontrollgruppenexperiment verwendet, dessen Stichprobe in Abschnitt 3.3 festgehalten ist. Das Experimentaldesign und der detaillierte Ablauf des Experiments sind in Abschnitt 3.4 und die statistische Analyse des Experiments ist in Abschnitt 3.5 beschrieben. Die angewandten Methoden werden kritisch hinterfragt und es werden Alternativen dazu aufgezeigt. Um die Methodik, inklusive Experimentaldesign, Stimuli und den statistischen Analysemethoden zu testen, wurde eine Pilot-Studie (siehe Abschnitt 4.1) durchgeführt. Mit den neu gewonnen Erkenntnissen aus der Pilot-Studie wurde die Methodik erneut kritisch reflektiert.

3.1 Forschungsfrage

Erklärtes Ziel dieser Arbeit ist, das Risiko von Phishing-E-Mails zu senken (siehe Abschnitt 1.3). Eine allgemein gefasste, explorative Fragestellung dazu lautet: "*Wie kann das Phishing-Risiko für Internetanwender vermindert werden*". Der deutsche Technikphilosoph Ropohl (1986, S. 97) definiert Risiko als Produkt der Eintrittswahrscheinlichkeit und Höhe des Schadens pro Ereignis. Diese Risikodefinition scheint im Feld der Informationssicherheit breit akzeptiert zu sein. Der ISO/IEC (2013) Standard 27001:2013, der BSI- (2008) Standard 100-2 und die ISACA (2013), welchen COBIT (ISACA, 2012) herausgibt, verwenden diese. Um das Phishing-Risiko gemäss Definition zu senken, kann die Wahrscheinlichkeit oder das Schadensausmass reduziert werden. Das Schadensausmass kann durch unterschiedliche technische Massnahmen (siehe Abschnitt 2.2),

im Falle von Ransomware als Anhang via Anti-Viren-Software, gesenkt werden. Im Falle eines entwendeten Passwortes zum Online-Banking könnte ein Schaden möglicherweise durch MFA verhindert werden (Geer, 2005). Die Arbeit versucht deshalb das Risiko, welches von Phishing ausgeht, via Reduktion der Eintrittswahrscheinlichkeit zu senken. Anwender-Training hat sich im Sicherheitsbereich effektiv gezeigt (siehe Abschnitt 1.3). Deshalb wird versucht, die Wahrscheinlichkeit eins Schadens und somit des Phishing-Risikos, durch ein Anti-Phishing-Training für Anwender zu senken.

Forschungsfrage

Kann die Wahrscheinlichkeit eines Schadens durch Phishing-E-Mails für Internetanwender durch Training vermindert werden?

3.2 Hypothesen

Da Anwender-Training womöglich die Wahrscheinlichkeit eines Schadens und somit das Risiko von Phishing senkt, soll der Einfluss von Anwendertraining auf die Wahrscheinlichkeit Phishing zu erkennen untersucht werden. Als erster Schritt in der Operationalisierung der Forschungsfrage (Stein, 2014) soll die Nullhypothese aufgestellt werden. Die Nullhypothese besagt, dass kein Zusammenhang besteht und wird, falls Hypothese 1 angenommen wird, verworfen.

Nullhypothese

Das Training hat keinen Einfluss auf die Erkennungsleistung von Phishing-E-Mails.

Die Antithese zur Nullhypothese besagt, dass ein Zusammenhang zwischen Training und der Erkennungsleistung von Phishing besteht. In Hypothese 1 wird der Zusammenhang der unabhängigen Variable Training auf die abhänge Phishing-Erkennungsleistung (EKL) als positiv postuliert. Es wird angenommen, dass Anwender ohne Trai-

ning Phishing nicht zuverlässig erkennen können und dass Training die Phishing-Erkennungsleistung steigert. Diese Ursache-Wirkungs-Beziehung ist als Hypothese 1 formuliert. Ein negativer Einfluss der Trainings wird nicht vermutet und ist deshalb nicht als Hypothese formuliert.

Hypothese 1

Auf Phishing trainierte Anwender erkennen Phishing-E-Mails besser als untrainierte Anwender.

Neben einem positiven Einfluss des Trainings auf die Phishing-Erkennungsleistung wird vermutet, dass Anwender welche ein Training erhalten haben, Links in Phishing-E-Mails öfters ignorieren und diesen weniger oft folgen. Beispielsweise aufgrund des Wissens über die negative Konsequenzen, welche das Öffnen von Links nach sich ziehen kann. Die folgende Hypothese 2.1 vergleicht den Unterschied der beiden Gruppen auf die Häufigkeit der Phishing-Link-Vermeidung (PLV).

Hypothese 2.1

Auf Phishing trainierte Anwender folgen Links in Phishing-E-Mails weniger oft als untrainierte Anwender.

Die Hypothese 2.2 vergleicht den Zusammenhang von Training auf das Öffnen von E-Mail-Anhängen. Es wird vermutet, dass die trainierte Gruppe Anhänge weniger oft öffnet. Trainierte Anwender sollten demnach eine höhere Phishing-Anhang-Vermeidung (PAV) aufweisen als untrainierte.

Hypothese 2.2

Auf Phishing trainierte Anwender öffnen Anhänge an Phishing-E-Mails weniger oft als untrainierte Anwender.

3.3 Stichprobe

Die Stichprobe wurde zufällig aus der Gesamtbevölkerung gezogen. Es gab keine demografischen Einschränkungen wie Alter oder Geschlecht für die Teilnahmen an der Studie. Ebenfalls waren Bildung oder das Anstellungsverhältnis keine Einschränkungen, da alle Bevölkerungsschichten von Phishing betroffen sein können. Weil die Studie online durchgeführt wurde, war ein Computer mit Internetzugang Bedingung zur Teilnahme. Die Probanden wurden via E-Mail und Social-Media rekrutiert. Diese Kanäle werden ebenfalls zur Verbreitung von Phishing-Nachrichten benutzt, somit konnte sichergestellt werden, dass die Probanden potenziell von Phishing betroffen sind. Die Teilnahme an der Studie erfolgte auf freiwilliger Basis und ohne Bezahlung. Es wurden bewusst keine finanziellen Anreize, wie Kino- oder Einkaufsgutscheine geboten, weil dies im Zusammenhang mit Phishing verdächtig wirken könnte. Die Teilname an der Studie war anonym, da die Zuordnung eines Datensatzes zu einer Person verhindert wurde oder nur mit aussergewöhnlichem Aufwand möglich ist (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 2018). Sobald dies der Bearbeitungszweck zuliess, wurden die Daten weiter anonymisiert, indem die IP-Adresse entfernt wurde. Es wurden keine Personenbezogen im Sinne der General Data Protection Regulation (GDPR) (European Union, 2016) verarbeitet. Es gab keine minderjährige Teilnehmer, diese wären im Hinblick auf die GDPR aus der Stichprobe entfernt worden.

3.3.1 Stichprobe der Pilot-Studie

Die Stichprobe der Pilot-Studie besteht aus zehn Probanden ($N = 10$), davon sind vier weiblich und sechs männlich (siehe Abbildung A.28). In der Experimentalgruppe ($n = 6$) sind die Geschlechter gleich verteilt (siehe Abbildung A.30), in der Kontrollgruppe ($n = 4$) überwiegt der Männeranteil mit drei zu eins (siehe Abbildung A.29). Die Altersverteilung reicht von 21 bis 60 Jahre (siehe Abbildung A.31) in der Experimental- sowie Kontrollgruppe sind Probanden im Alter zwischen 20–30 und um die 60 enthalten (Siehe Abbildung A.33 und Abbildung A.32), wobei in der grösseren Experimentalgruppe die 20–30 Jährigen öfters vertreten sind.

3.3.2 Stichprobe der Hauptstudie

Die Stichprobe ($N = 76$) beinhaltet nach Bereinigung 76 Probanden. Ausgefiltert wurden Probanden, welche die Umfrage nicht bis zum Ende ausgefüllt haben. Die Grösse der Experimentalgruppe ist 29 und die Kontrollgruppe umfasst 47 Probanden. Von den 76 haben 74 ihr Geschlecht angegeben (siehe Abbildung A.36). In der gesamten Stichprobe überwiegt der Männeranteil leicht ($M = .55$, $0 = Weiblich$, $1 = Männlich$), ebenso in der Kontrollgruppe ($M = .65$) (siehe Abbildung A.3.2.1). In der Experimentalgruppe sind die Frauen stärker repräsentiert ($M = .39$) (siehe Abbildung A.38). An der Studie nahmen Probanden im Alter von 20 bis 61 teil ($Min = 20$, $Max = 61$, $M = 30.01$) (siehe Abbildung A.39). Die Altersverteilung über die Kontroll- ($Min = 22$, $Max = 61$, $M = 29.47$) (siehe Abbildung A.40) und Experimentalgruppe ($Min = 20$, $Max = 61$, $M = 30.9$) (siehe Abbildung A.41) ist sehr ähnlich. In beiden Gruppen sind Probanden zwischen 20 und 30 Jahren am stärksten vertreten. Die Altersverteilung ist damit derjenigen der Pilot-Studie sehr ähnlich.

3.4 Experimentaldesign

Wie in Abschnitt 1.4 eingeführt, wird, um die Hypothese und die Effektivität des Trainings zu prüfen, auf ein experimentelles Forschungsdesign (Stein, 2014) mit einem Kontrollgruppenexperiment (Kühl, 2009; Eifler, 2014) gesetzt, um die Kausalität empirisch zu untersuchen. Die Gruppeneinteilung erfolgt dabei randomisiert, wie Fisher (1935) dies vorschlägt. Für die zufällige, randomisierte Zuordnung wird eine Pseudorandom Number Generator (PRNG) Implementation verwendet, basierend auf Matsumoto und Nishimuras (1998) Mersenne-Twister. Die Entropie (Shannon, 1948) des PRNG wird auf ein Bit reduziert, damit die Wahrscheinlichkeit in etwa der eines Münzwurfes (Ford, 1983) entspricht. Um den Ursache-Wirkungs-Zusammenhang (Cook et al., 2002, S. 5–7) zwischen der unabhängigen Variable ‘Training’ auf die abhängigen Variablen zu untersuchen, wird die Experimentalgruppe mit dem Training manipuliert, während die Kontrollgruppe keine Stimuli erhält. Die E-Mails als Stimulus-Material sind in Unterabschnitt 3.4.1 beschrieben. Die abhängigen Variablen, die wie Phishing-Erkennungs-

leistung (EKL), werden via einer Online-Umfrage (Wagner & Hering, 2014) in beiden Gruppen gemessen. Das Training bestehend aus einem Schulungs- und interaktiven Teil sowie die Umfrage sind in der Webapplikation 'Phishing-Studie-Applikation', kurz App, gebündelt und werden den Probanden zur Verfügung gestellt. Die App automatisiert ebenfalls Teile der statistischen Analyse. Die Items des Trainings und der Umfrage werden in Unterabschnitt 3.4.4 erläutert. Details zur Auswertung des Experimentaldesigns finden sich in Abschnitt 3.5 Analyse.

Im Experimentalablauf (siehe Abbildung 3.1) erhält die Experimentalgruppe zuerst ein Training und füllt danach die Online-Umfrage aus, während die Kontrollgruppe das Training überspringt und direkt zur Umfrage gelangt. Das Experiment wird als Feldexperiment (Eifler, 2014) durchgeführt. Die Datenerhebung findet somit bei den Probanden zu Hause oder im Büro statt und nicht in einem Labor. Der Vorteil eines Fel-

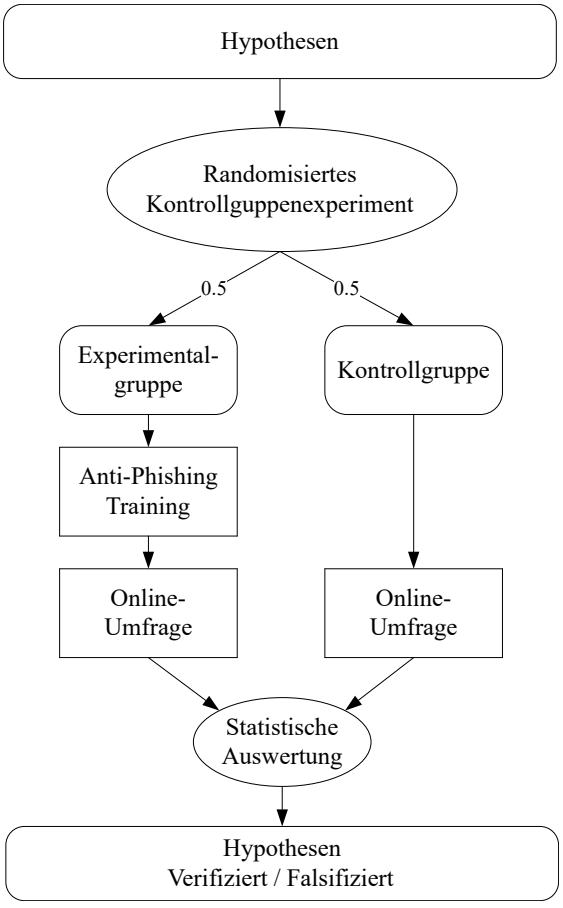


Abbildung 3.1: Ablauf des Kontrollgruppenexperimentes

dexperimentes gegenüber dem Laborexperiment liegt in der hohen externen Validität (Krebs & Menold, 2014), da sie in der natürlichen Umgebung stattfinden, in welcher Probanden normalerweise ihre E-Mails bearbeiten (Kühl, 2009). Laborexperimente haben auf Kosten der externen eine höhere interne Validität. Störfaktoren können besser kontrolliert werden und der Effekt lässt sich stärker auf das Experiment zurückführen (Kühl, 2009; Eifler, 2014). Im Dilemma zwischen interner und externer Validität wurde ein Mittelweg gewählt. Das Feldexperiment sorgt für eine externe Validität während das labornahe Training für die interne sorgt. Gemäss Kühl (2009) sind die Klassifikationen von Experimenten idealtypisch und miteinander kombinierbar.

Alternative Designs

Echte Experimente wie das randomisierte Kontrollgruppenexperiment sind quasi-experimentellen Forschungsdesigns vorzuziehen, da bei Quasi-Experimenten (Cook et al., 2002, S. 5–7) die Kausalaussage erschwert wird (Kühl, 2009; Eifler, 2014). Auch eine vorexperimentelle Vorher-Nachher-Messung eignet sich nicht, weil bei der Vorher-Messung bereits ein Lerneffekt auftreten könnte. (Eifler, 2014; Kühnel & Dingelstedt, 2014). Anstatt eines Experimentes könnte auch die Delphi-Methode (Linstone, 1985; Rowe & Wright, 2001) eingesetzt werden, um die Effektivität der Trainings zu schätzen. Hierbei würde es sich jedoch nur um eine Schätzung und nicht um eine Messung handeln und es besteht ein Risiko, dass die Experten falsch liegen. Das Kontrollgruppenexperiment wurde aus diesen Gründen der Delphi-Methode und anderen Experimenten vorgezogen, um die hypothetische Ursache der unabhängigen Variable ‘Training’ auf die abhängige ‘Phishing-Erkennungsleistung’ zu ergründen.

Bei diesem Design dient die Online-Umfrage zur Messung der Effektivität des Trainings. Anstatt der Umfrage hätte zur Messung auch ein Versand von Test-Phishing-E-Mails stattfinden können. Beim Testversand von Phishing-E-Mails dürfte die externe Validität höher sein, da bei diesem Setting die Probanden ihre gewohnte E-Mail-Applikation verwenden und sich des Tests nicht zwingend bewusst sind. Doch gerade für die Rückführung des Effektes auf die Variation im Experiment ist interne Validität relevant (Kühl, 2009). Nachteile dieses Ansatzes sind, dass die E-Mail-Adresse der Pro-

banden erhoben werden muss und die Probanden nicht nach ihrer Einschätzung zu den jeweiligen E-Mails befragt werden können. Während es möglich ist zu erheben, welche Probanden welchem Link gefolgt sind, ist es nicht mit abschliessender Gewissheit feststellbar, ob die E-Mails im Posteingang eingetroffen sind oder geöffnet wurden. Ein weiterer Nachteil ist, dass reale anstatt fiktive Firmen verwendet werden müssten. Bei fiktiven Firmen ist es trivial diese als Test-E-Mail zu identifizieren. Auf die Verwendung von real existierenden Firmen wurde verzichtet. Zudem würden Probanden, die ihre E-Mail-Adresse aus Gründen der Privatsphäre nicht oder falsch angeben, aus dem Experiment ausgeschlossen. Das Versenden von Test-Phishing-E-Mails müsste zudem ethisch hinterfragt werden. Ausserdem ist durch Angabe der E-Mail die Anonymität der Probanden gefährdet. Da diese Studie am 25. Mai 2018 exakt zum Inkrafttreten des verschärften Europäischen Datenschutzgesetzes GDPR abgeschlossen ist (European Union, o. J.), hätte die Verarbeitung von personenbezogenen Daten, wie E-Mail-Adressen, noch unter weniger strikten Auflagen erfolgen können. Das Versenden von Test-E-Mails wurde zur Messung der Langzeitwirkung des Trainings in Betracht gezogen, aufgrund rechtlicher und ethischen Gründen sowie Bedenken zum Schutz der Privatsphäre jedoch nicht durchgeführt.

Eine weitere Option ist der Vergleich unterschiedlicher Trainingsmethoden gewesen, um das beste Training zu ermitteln. Beispielsweise könnte das entwickelte Training gegen das Training anderer Studien oder gegenüber eingekauften Lösungen verglichen werden. Da keine finanziellen Mittel zur Durchführung der Studie bereitstehen, können keine kommerziell verfügbaren Trainings verwendet werden. Weil kein existierendes Instrument zur Erhebung der Phishing-Erkennungsleistung gefunden werden konnte, wurde mit der Umfrage selbst eines entwickelt. Die Fairness eines Vergleiches zwischen diesem Training und Trainings Dritter ist mit einem neuen Instrument nicht gewährleistet.

3.4.1 Stimulus-Material

Die Experimental- und Kontrollgruppe unterscheiden sich in den erfahrenen Stimuli. Die Experimentalgruppe erhält im Training Informationen über Phishing und drei E-Mails zur Bearbeitung, wovon zwei Phishing-E-Mails sind. In den nächsten zwei Abschnitten werden die Stimuli über Phishing und die E-Mail-Fälle erläutert.

Informationen über Phishing

Vor der Bearbeitung der E-Mail-Fälle erhalten die Probanden der Experimentalgruppe Informationen über Phishing und E-Mails. Dies legt die Grundlage Phishing zu erkennen. Als erstes werden die Probanden mit den Elementen einer E-Mail (siehe Abbildung A.3) wie Absender, Empfänger, Anhang und Link vertraut gemacht, denn diese werden als Basiswissen benötigt. In einem nächsten Schritt werden den Probanden, auf Basis der in Unterabschnitt 2.1.2 gewonnenen Erkenntnissen, Verhaltensgrundsätze gelehrt (siehe Abbildung A.4), wie verdächtige E-Mails zu ignorieren und Links sowie Anhänge nicht zu öffnen. Nach den Verhaltensgrundsätzen werden drei Schritte zur Identifikation von Phishing (siehe Abbildung A.5) vermittelt. Die Schritte stützen sich dabei auf die erarbeiteten theoretischen Grundlagen. Den Probanden wird kurz erläutert, wie Absender, Links und Inhalt einer E-Mail überprüft werden können. Es werden falsche, ähnliche sowie gefälschte Absender geschult (siehe Abbildung A.6). Danach wird den Probanden vermittelt, wie die Adresse eines Links, auch URL genannt, überprüft werden kann (siehe Abbildung A.7). Folgend wird vermittelt, wie legitime Links von Phishing-Links unterschieden werden können (siehe Abbildung A.8). Diese Informationen sollen den Probanden helfen, die E-Mails der Fälle des nachfolgenden Trainings richtig zu klassifizieren und ebenfalls die Phishing-E-Mails in der Umfrage zu erkennen.

Die E-Mail-Fälle

Insgesamt wurden sechs Fälle entwickelt. Pro Fall werden Probanden gebeten je eine E-Mail als Phishing-E-Mail oder legitime E-Mail zu klassifizieren. Jeder Fall enthält zusätzlich zur kategorisierenden E-Mail noch ein weitere erklärende E-Mail zum

Vergleich. Somit existierten pro Fall zwei E-Mails, jeweils in einer Phishing- und legitimen Variante. In einem Phishing-Fall wird die Phishing-E-Mail vorgelegt und in einem legitimen Fall die legitime E-Mail. Falls nicht explizit vermerkt, wird jeweils bei den Fällen die zu kategorisierende E-Mail referenziert.

Im Training wird die Experimentalgruppe mit den Fällen MyAccount (Google) (siehe Abbildung A.12), MyDelivery (Post) (siehe Abbildung A.14) und MyCreditCard (Viseca) (siehe Abbildung A.16) konfrontiert. Dies soll zu einem Lerneffekt führen und bezwecken, dass die Probanden Phishing in Zukunft besser erkennen können. In der auf das Training folgenden Umfrage werden beide Gruppen gebeten, die drei E-Mails MyMobile (Salt) (siehe Abbildung A.24), MyBox (Dropbox) (siehe Abbildung A.26) und MyPay (PayPal) (siehe Abbildung A.27) zu kategorisieren, wovon ebenfalls zwei E-Mails als Phishing kategorisiert sind. Insgesamt muss die Experimentalgruppe sechs und die Kontrollgruppe drei E-Mails klassifizieren. Die Fälle MyAccount und MyPay sind legitim, bei den anderen Fällen handelt es sich um klassisches Klon-Phishing, wobei der Fall MyBox Elemente des Spear-Phishings beinhaltet und die Fälle MyCreditCard und MyMobile als Phishing mit Malware typisiert werden können (siehe Unterabschnitt 2.1.1). Nachfolgend werden die Erkennungsmerkmale (Siehe: Tabelle 3.1 und Tabelle 3.2) beschrieben, sowie die Fälle des Trainings mit denjenigen der Umfrage verglichen. Daraufhin werden die zwei legitimen E-Mails gefolgt von den Phishing-E-Mails erläutert und es wird begründet, weshalb diese Fälle gewählt wurden. Alle in Tabelle 3.1 und Tabelle 3.2 referenzierten E-Mails befinden sich im Anhang dieser Arbeit. Die im Training verwendeten E-Mails befinden sich in Anhang in Abschnitt A.1 und diejenigen der Umfrage in Abschnitt A.2.

In Tabelle 3.1 sind alle sechs Fälle aufgeführt. Pro Fall werden die Klassifizierung und die Erkennungsmerkmale der dazugehörigen E-Mails aufgelistet. Bei allen Phishing-E-Mails wird der Link modifiziert. Diese Modifikation wird benötigt, um den Anwender auf eine Phishing-Seite zu führen. Um Anwender auf Phishing-Seiten zu führen, ohne den Link zu modifizieren, braucht es einen MITM-Angriff oder DNS-Spoofing welche durch Phishing unterstützt werden können (siehe Abschnitt 2.1.1). Ist

eine DNS-Modifikation bereits vorhanden, entfällt die Notwendigkeit eines Phishing-Angriffs. Bei den E-Mails MyDelivery und MyMobile deutet der Stil, Inhalt sowie die Rechtschreibung auf Phishing hin. Dieses Merkmal wird wahrscheinlich auch von Laien erkannt. Bei MyCreditCard und MyBox wurden neben dem Link auch der Absender und Empfänger modifiziert. An die E-Mails von MyCreditCard und MyMobile ist zudem ein verdächtig wirkender Anhang angefügt. Bei MyDelivery und MyMobile wurde der Absender gefälscht (siehe Abschnitt 2.2). Details der Charakteristika können aus der Tabelle 3.2 entnommen werden.

Fall			Erkennungsmerkmale				
ID	*Name*	*Klass.*	*Abs.*	*Empf.*	*Link*	*Inhalt*	*Anhang*
Training							
A	MyAccount	Legitim					
D	MyDelivery	Phishing			✓	✓	
C	MyCreditCard	Phishing	✓	✓	✓		✓
Umfrage							
M	MyMobile	Phishing			✓	✓	✓
B	MyBox	Phishing	✓	✓	✓		
P	MyPay	Legitim					

ID = Identifikation, Klass. = Klassifizierung, Abs. = Absender, Empf. = Empfänger

Tabelle 3.1: Matrix der E-Mail-Fälle mit den Erkennungsmerkmalen

Die Erkennungsmerkmale der Phishing-E-Mail des Trainings und der Umfrage sind aneinander angepasst, sodass Aussagen über die Erkennungsleistung und den Lernfortschritt von Probanden innerhalb der Experimentalgruppe möglich sind. Möglicherweise haben Probanden im Training einen Phishing-Absender nicht erkannt, erkennen diesen aber später jedoch in der Umfrage. Daraus könnte man auf einen Lerneffekt schliessen. Hierbei würde es sich um ein Quasi-Experiment (Eifler, 2014) handeln, was nicht den Standards eines Experimentes entspricht. Da sich Aussagen innerhalb der Kontrollgruppe nicht wissenschaftlich fundiert belegen lassen, wird darauf verzichtet. Weil diese Daten als Nebeneffekt zum Training anfallen, werden sie dennoch erhoben.

Fall	Variante	
Merkmal	*Phishing*	*Legitim*
MyDelivery (Post) T		
Link	https://steal.com/ service.mydelivery.ch/login	https://service.mydelivery.ch/ ekp-web/secure/external/view/ 2257228633?lang=DE
Inhalt	Drohung, Handlungsdruck, Orthographie, Grammatik	-
MyCreditCard (Viseca) T		
Absender	no-reply@mycreditcard.cc	no-reply@mycreditcard.ch
Empfänger	verborgene Empfänger	<name>@phishing-studie.org
Link	https://account.mycreditcard.cc/ one?email=<name>@phishing-studie.org	Kein Link vorhanden
Anhang	rechnung.pdf.exe	rechnung.pdf
MyMobile (Salt) U		
Link	https://mymobile.ch.cn/ login?id=fce4ffd1158ff84	-
Inhalt	Stil, Orthographie	-
Anhang	Vertrag-nr-3TR0B0178.pdf	-
MyBox (Dropbox) U		
Absender	mybox@outlook.com	-
Empfänger	verborgene Empfänger	-
Link	https://www.673ab7.cf/ mybox.com/l/scl/3d6baac83...	-

T = Training, U = Umfrage, <name> = Verwendeter Name.

Alle E-Mails sind in einer legitimen und Phishing-Variante vorhanden, es sind nur die relevanten Angaben aufgelistet.

Die legitimen Fälle MyAccount (Google) und MyPay (PayPal) sind nicht aufgelistet.

Tabelle 3.2: Vergleich der Phishing-E-Mail mit dem Legitimen pro Fall

Bei den Fällen MyPay (PayPal) und MyCreditCard (Viseca) handelt es sich um Klone von Finanzinstituten. Die beiden Fälle wurden gewählt, weil Finanzinstitute besonders häufig betroffen sind (siehe Kapitel 1) und PayPal oft als Beispiel verwendet wird (siehe Unterabschnitt 2.1.5). Der Fall MyDelivery wurde aufgrund der Aktualität

der Phishing-Angriffe gegen die Postkunden gewählt (siehe Kapitel 1) und MyBox, weil Dropbox ebenfalls betroffen ist (siehe Unterabschnitt 2.1.5). Mit MyDelivery, MyCreditCard und MyMobile wurden zudem in der Schweiz tätige Unternehmen ausgewählt, da das Training explizit auf die Deutschschweiz ausgerichtet ist. Informationen über die Charakteristika der E-Mails können der Tabelle 3.1 entnommen werden.

MyAccount (Google) & MyPay (PayPal) sind legitime Fälle. MyAccount ist eine Anmeldewarnung, die ursprünglich von Google stammt und der ebenfalls legitime von PayPal kopierte Fall MyPay informiert über den Erhalt der monatlichen Kontoübersicht. Der Fall MyAccount könnte verdächtig wirken, da der Anwender darin zu einer Handlung gedrängt wird. Die legitime E-Mail von MyPay enthält einen Link zu MyPay, welcher ebenfalls etwas verdächtig ist. Die originale E-Mail von PayPal enthielt Links zu einer PayPal fremden Domain, dies wurde für das Training verändert, damit die E-Mail legitimer wirkt. Nachfolgend sind die Phishing-Fälle aufgelistet.

MyDelivery (Post) ist klassisches Phishing und versucht den Empfänger durch Drohungen auf eine Phishing-Webseite zu führen. Der Fall wurde aufgrund der Aktualität gewählt (siehe Kapitel 1).

MyCreditCard (Viseca) ist ein Fall eines in der Schweiz tätigen Unternehmens und wurde aufgrund der Zugehörigkeit zum Finanzsektor gewählt. Als Malware-Phishing wird zusätzlich zur Phishing-Webseite versucht, mit einem fiktiven, hohen Rechnungsbetrag den Empfänger dazu zu bewegen, Ransomware zu installieren. Neugierde und ein gefühlter Handlungsdruck motivieren den Empfänger möglicherweise.

MyMobile (Salt) ist ein Phishing-Fall mit Malware eines in der Schweiz tätigen Mobilfunkanbieters. Durch eine nicht georderte Bestellung wird neben der klassischen Phishing-Webseite versucht, den Empfänger zu motivieren, einen Anhang mit Malware zu öffnen.

MyBox (Dropbox) ist ein Fall mit Spear-Phishing Elementen (siehe Abschnitt 2.1.1). Es wird vorgetäuscht. dass die E-Mail von einer bekannten Person stammt.

3.4.2 Training

Das Anti-Phishing-Training besteht aus der Schulung, welche Informationen über Phishing beinhaltet und einem interaktiven, spielerischen Trainingsteil in welchem E-Mail-Fälle nach Phishing oder legitim klassifiziert werden müssen. Für diese Studie wurden die drei Fälle MyAccount, MyDelivery, MyCreditCard mit je zwei E-Mails entworfen (siehe Unterabschnitt 3.4.1). Die Fälle werden wie in Tabelle 3.3 beschrieben zu Items kodiert. Die den Probanden präsentierten E-Mails mit ihren Eigenschaften sind in der Tabelle 3.1 und Tabelle 3.2 aufgelistet. Das Anti-Phishing ist der Hauptteil der Phishing-Studie-Applikation und vollständig in diese integriert. Bildschirmfotos der App sind im Anhang (siehe Abschnitt A.1) abgedruckt. Die Phishing-Studie-Applikation integriert neben der Schulung und dem interaktiven Training auch die Online-Umfrage. Die ganze Studie kann mit der App durchgeführt werden, folglich kommt die App sowohl bei der Kontrollgruppe als auch für die Experimentalgruppe zum Einsatz. Dieser Abschnitt schildert schrittweise den Ablauf des Trainings unter Verwendung der App bezogen auf die Experimentalgruppe.

Item Id	*Item*	*Skala*
Training		
A.1	Fall MyAccount richtig gelöst.	1 oder 7
D.1	Fall MyDelivery richtig gelöst.	1 oder 7
C.1	Fall MyCreditCard richtig gelöst.	1 oder 7
C.5	Anhang an MyCreditCard geöffnet.	1 oder 7

Wird ein Fall im Training korrekt klassifiziert, wird der Wert 7 zugewiesen, ansonsten der Wert 1.

Tabelle 3.3: Die Items des Trainings

Entscheiden sich Internetanwender zur Teilnahme an dieser Studie, landen sie auf der Willkommensseite der App (siehe Abbildung 3.2), welche den Ablauf der Studie kurz vorstellt und allgemeine Informationen zu Phishing und dessen Risiken vermittelt. Entscheiden sich die Besucher der Willkommensseite zur Teilnahme, werden sie randomisiert der Kontroll- oder Experimentalgruppe zugewiesen. Für diesen Abschnitt wird

von einer Zuteilung in die Experimentalgruppe ausgegangen. Die Experimentalgruppe durchläuft die Schritte: Schulung, Interaktives Training und Umfrage während die Kontrollgruppe direkt zur Umfrage gelangt.

Abbildung 3.2: Phishing-Studie-Applikation - Willkommen

Schulung

Mittels einer Präsentation werden die Probanden der Experimentalgruppe kurz über den Ablauf der Studie informiert (siehe Abbildung A.2). Danach erhalten sie die Informationen über Phishing. Auf der letzten virtuellen Folie (siehe Abbildung A.9) werden die Probanden gebeten mit dem interaktiven Anti-Phishing-Training fortzufahren.

Interaktives Training

Auf der Startseite des Training-Spiels (siehe Abbildung 3.3) wird die Aufgabe erläutert, Phishing-E-Mails als legitim oder Phishing zu klassifizieren. Das Ziel ist möglichst viele Punkte zu sammeln. Es wird hervorgehoben, dass Anhänge geöffnet werden können, dies jedoch Risiken birgt, und erklärt wie Links mit der Maus überprüft werden sollten. Den Probanden wird erklärt, dass sie als fiktive Person spielen und sämtliche

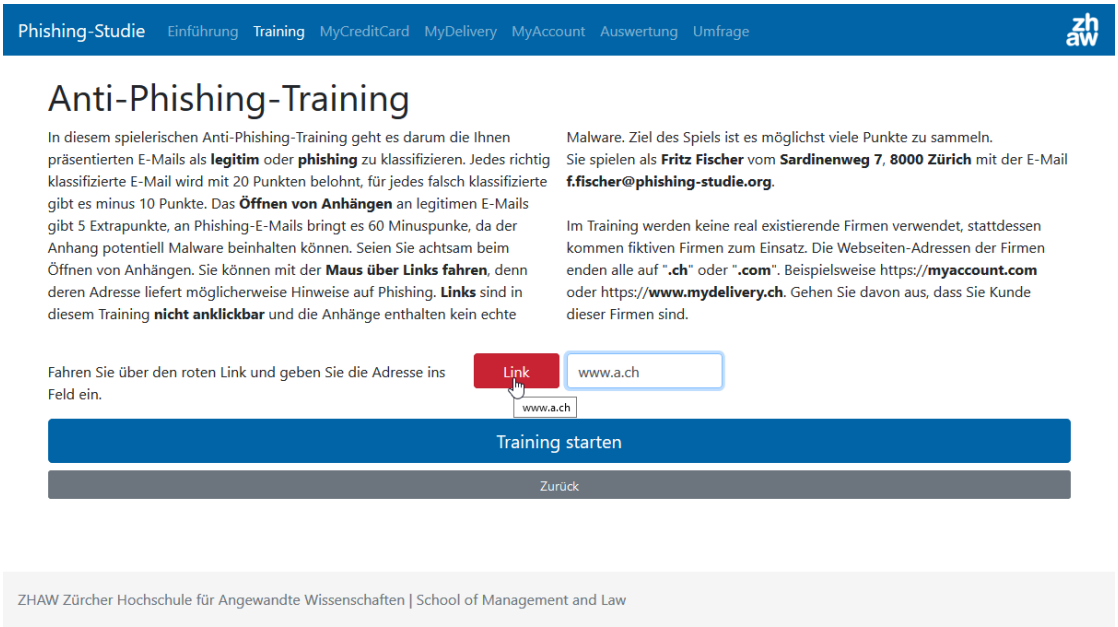


Abbildung 3.3: Phishing-Studie-Applikation - Training - Startseite

in den E-Mails vorkommenden Firmen nicht real sind. Um die Qualität der erhobenen Daten zu verbessern, müssen die Probanden verifizieren, dass sie die Fähigkeit besitzen, Links zu überprüfen. Dafür werden sie gebeten, mit der Maus, über einen Link zu fahren und die URL in ein Textfeld einzugeben. Nach der Verifikation wird das Training

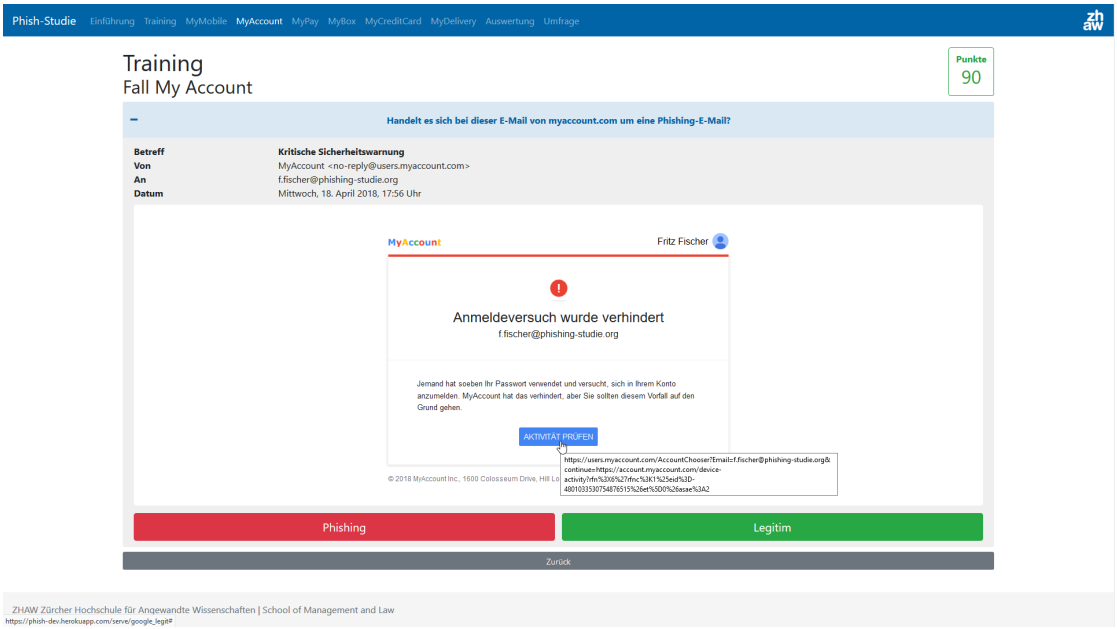


Abbildung 3.4: Phishing-Studie-Applikation - Training - Fall MyAccount - ungelöst

gestartet. Dies verhindert die Teilnahme von Probanden welche, trotz Erklärung in der Schulung (siehe Abschnitt 3.4.2), nicht in der Lage sind, Links zu verifizieren.

Während des Trainings werden den Probanden zufällig Fälle zur Beurteilung vorgelegt. Zu jedem Fall gehört eine E-Mail in einer legitimen und einer Phishing-Fassung sowie eine Erklärung. Je nach Fall wird die legitime oder Phishing-Variante zur Inspektion präsentiert (siehe Abbildung 3.4). Der erste Fall erhält zusätzliche Hilfestellungen. Die Probanden müssen daraufhin entscheiden, ob eine legitime oder eine Phishing-E-Mail vorliegt. Als Entscheidungsgrundlage kann, wie in der Schulung (siehe Abschnitt 3.4.2) vermittelt, der Absender, Empfänger, Inhalt und der Link inklusive URL herangezogen werden.

Nach der Entscheidung erhält der Proband Rückmeldung zu seiner Antwort und die Erklärung mit weiteren Informationen zum Fall und zu Phishing im Allgemeinen. Ebenfalls werden beide E-Mail-Varianten zum Vergleich nebeneinander dargestellt (siehe Abbildung 3.5). Die Anhänge von Phishing-E-Mails werden in diesem Training behandelt als enthielten sie Ransomware (Erpressungs- auch Crypto-Trojaner). Wird ein Malware-Anhang geöffnet, erscheint eine Warnung, dass Anwenderdaten nun durch

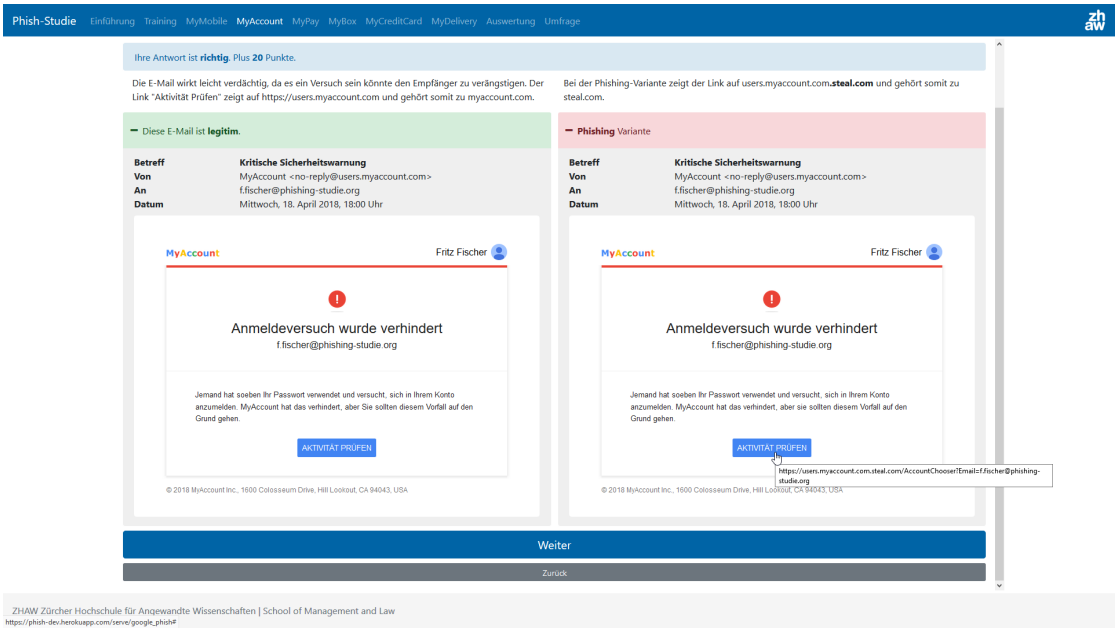


Abbildung 3.5: Phishing-Studie-Applikation - Training - Fall MyAccount - gelöst

Ransomware verschlüsselt sein könnten und möglicherweise verloren sind (siehe Abbildung A.18). Nach Bearbeitung der drei Fälle wird die Zusammenfassung der Resultate in Form einer Auswertung kommuniziert. Die Auswertung präsentiert die Summe aller korrekt und falsch gelösten Fälle, sowie die Gesamtpunktzahl (siehe Abbildung A.11). Auf einen Vergleich mit anderen Probanden wird während der Studie verzichtet, da dessen Effekt auf die Resultate der Studie nicht abgeschätzt werden kann. Vor einer Danksagung werden die wichtigsten Punkte nochmals in einem Fazit zusammengefasst. Danach wird der Proband gebeten, an der Umfrage im folgenden Unterabschnitt 3.4.3 teilzunehmen.

3.4.3 Umfrage

Die Online-Umfrage dient zur Messung der Effektivität des Trainings und erhebt die Phishing-Erkennungsleistung (EKL) der Probanden. Zusätzlich werden demografische Angaben und Informatikkenntnisse erhoben. Alle Items sind in der Tabelle 3.4 gelistet. Um die EKL zu bestimmen, werden E-Mails eingesetzt, die durch den Probanden anhand einer siebenstufigen Likert-Skala (Likert, 1932) von ‘trifft überhaupt nicht zu’ bis ’trifft voll zu’ eingeschätzt werden (siehe Tabelle 3.4). Die Mitte der Skala steht für ‘unentschieden’. Es steht den Probanden offen, die Frage explizit nicht zu beantworten. Die siebenstufige Skala erreicht das obere Limit der Reliabilität. Es wird empfohlen, eine weite Skala zu wählen, da es immer möglich ist, die Daten zur Analyse kompakter zu kategorisieren (Allen & Seaman, 2007). Für die E-Mails von MyBox und MyPay antworten die Probanden, ob es sich um Phishing handelt, ob der Link bedenkenlos angeklickt werden kann und ob sie den Link öffnen würden. Für den Fall MyMobile wird zusätzlich befragt, ob der Anhang bedenkenlos geöffnet werden kann und ob sie dies tun würden. Die Fälle MyBox und MyMobile sind Phishing, während es sich bei MyPay um eine legitime E-Mail handelt. Es wird angenommen, dass Informatikkenntnisse einen Einfluss auf die EKL haben. Möglicherweise hat das Training bei Probanden mit hohen Vorkenntnissen in Informatik und Phishing keinen Effekt, da diese bereits über Phishing aufgeklärt sind. Die Items: Alter, Geschlecht, Bildung und Hauptbeschäftigung werden erhoben, da bei diesen ebenfalls ein Zusammenhang mit der EKL bestehen könnte.

Item Id	*Item*	*Skala*
1–2. Demografie		
1	Alter	0–100
2	Geschlecht	F,M,A,K
3. Informatikkenntnisse		
3.1	Ich kenne mich mit Informatik aus.	Likert
3.2	Ich kannte mich vor dieser Studie bereits mit Phishing aus.	Likert
3.3	Ich war vor dieser Studie mit dem Aufbau einer URL vertraut.	Likert
3.4	Ich kenne die Technologie SMTP	Likert
4-5 Ausbildung und Hauptbeschäftigung		
4	Höchste abgeschlossene Ausbildung	0–15
5	Aktuelle Hauptbeschäftigung	0–9
B. E-Mail von MyBox (Phishing)		
B.1	Hierbei handelt es sich um eine Phishing-E-Mail.	Likert
B.2	Der Link in dieser E-Mail kann bedenkenlos geklickt werden.	Likert
B.3	Ich würde den Link in dieser E-Mail anklicken.	Likert
M. E-Mail von MyMobile (Phishing)		
M.1	Hierbei handelt es sich um eine Phishing-E-Mail.	Likert
M.2	Der Link in dieser E-Mail kann bedenkenlos geklickt werden.	Likert
M.3	Ich würde den Link in dieser E-Mail anklicken.	Likert
M.4	Der Anhang an dieser E-Mail kann bedenkenlos geöffnet werden.	Likert
M.5	Ich würde den Anhang an dieser E-Mail öffnen.	Likert
P. E-Mail von MyPay (Legitim)		
P.1	Hierbei handelt es sich um eine Phishing-E-Mail.	Likert
P.2	Der Link in dieser E-Mail kann bedenkenlos geklickt werden.	Likert
P.3	Ich würde den Link in dieser E-Mail anklicken.	Likert

F = Weiblich (0), M = Männlich (1), A = Anderes (2). Item-Text wurden gekürzt.

Alle Fragen sind Pflichtfragen, es kann mit ‘Keine Antwort’ geantwortet werden.

Tabelle 3.4: Die Items der Umfrage

Die Items B2, M2 und P2 ‘Der Link/Anhang kann bedenkenlos angeklickt werden’ sind ähnlich zu B3, M3 und P3 ‘Ich würde den Link/Anhang dieser E-Mail anklicken’, messen jedoch nicht dasselbe. Während die erste Item-Gruppe danach fragt, ob es sich um einen Phishing-Link handelt, fragt die Zweite nach der Intention diesen zu öffnen. Das erste Konstrukt dient dem Aufbau des Zweiten, die Probanden sollen zuerst das Erkennungsmerkmal reflektieren, um darauffolgend zu entscheiden, ob sie auf den Link oder Anhang öffnen würden. Risikoaffine Probanden folgen möglicherweise Links, obwohl sie Phishing vermuten und risikoaverse verzichten darauf, einem Link zu folgen, selbst wenn sie eine legitime E-Mail vermuten. Die Risikobereitschaft wird nicht erhoben, weil das Primärziel die Effektivitätsmessung des Trainings ist. Möglich ist auch, dass Probanden dem Link nicht folgen möchten, weil der Inhalt für sie nicht von Interesse ist. Durch Verwendung des Konjunktivs ‘würde’ in der Item-Formulierung und Doppelerhebung wird versucht diese Problematik zu entschärfen. Eisinga, Te Grotenhuis und Pelzer (2013) empfehlen zur Messung der Reliabilität eins Zwei-Item-Konstruktes Spearman-Brown Statistik anstatt Cronbachs α (Cortina, 1993) oder Pearson-Korrelation zu verwenden. Um die Effektivität der Trainings zu messen wird ausgewertet, wie viele der Probanden den Link oder Anhang öffnen und nicht ob diese nur erkannt werden, denn das Öffnen ist im Endeffekt für die Sicherheit entscheidend. Aus dem Zwei-Item-Konstrukt wird somit das besser passende gewählt und eine Ein-Item-Skala zur Erhebung der PLV und PAV gebildet (Diamantopoulos, Sarstedt, Fuchs, Wilczynski & Kaiser, 2012), eine Item-Korrelation entfällt somit.

Die Online-Umfrage wird sowohl von der Kontroll- als auch der Experimentalgruppe ausgefüllt. Aus Gründen der Anwenderfreundlichkeit ist die Umfrage in die Phishing-Studie-Applikation integriert (siehe Abbildung A.19). Die Umfrage ist in ihrer gesamten Länge im Anhang (Abschnitt A.2) abgedruckt. Informationen über die Verwendung der Umfrageresultate finden im nächsten Abschnitt und in Abschnitt 3.5 Analyse.

3.4.4 Forschungsdesign

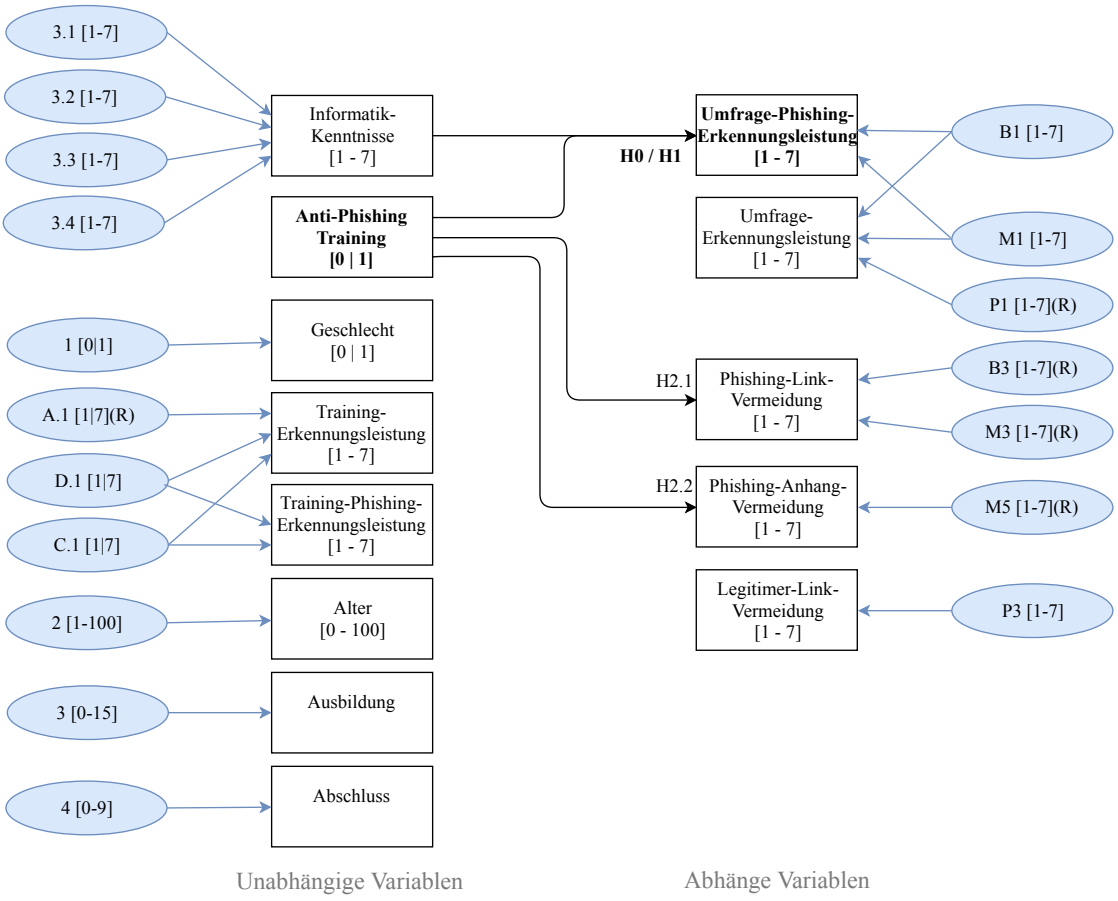
Die Abbildung 3.6 des konzeptionellen Modells schafft einen Überblick über das Forschungsdesign und die während des Experimentes erhobenen Daten. Das konzeptionelle Modell zeigt, wie die Items der Umfrage und des Trainings (als Ovale dargestellt) zu Variablen (als Rechtecke visualisiert) verrechnet werden. Im konzeptionellen Modell sind die zu prüfenden Hypothesen als Beziehungen zwischen den Variablen modelliert.

Hypothese 1 beschreibt die Auswirkung der Variable Training auf die Variable Phishing-Erkennungsleistung (EKL), welche aus den Items B1 und M1 gebildet wird. Die Frage hinter den Items ist, ob es sich bei der E-Mail um Phishing handelt. Das Item P1 (legitime E-Mail) wird für diese Variable nicht benötigt, denn es geht um die Erkennung von Phishing und nicht darum, ob legitime E-Mails richtig erkannt werden können. Ebenfalls wird nicht berücksichtigt, ob das legitim E-Mail fälschlicherweise als Phishing deklariert wurde, da dies auf die Internet-Sicherheit keine Auswirkung hat. Um prüfen zu können, ob das Training negative Einflüsse auf die Klassifizierung legitimer E-Mails hat, wurde das Item P1 dennoch erhoben. Das Item P1 wird zur Verrechnung umgekehrt (engl. reversed), um die gleiche Aussage wie B1 und M1 zu treffen. Die Nullhypothese welche besagt, dass kein Einfluss besteht, ist entsprechend der ersten Hypothese modelliert.

Hypothese 2.1 bezieht sich auf die Variable Phishing-Link-Vermeidung (PLV), gebildet aus den umgekehrten Items B3 und M3. Die Items B3 und M3 fragen nach der Klick-Bereitschaft auf Phishing-Links. Hypothese 2.1 besagt, dass trainierte Anwender Phishing-Links weniger oft anklicken und somit vermeiden. Je höher die Phishing-Link-Vermeidung (PLV) desto besser. Hypothese 2.2 beschreibt den Sachverhalt analog zur Hypothese 2.1, berücksichtigt aber den E-Mail-Anhang. Die Variable Phishing-Anhang-Vermeidung (PAV) wird aus dem umgekehrten Item M5 gebildet.

Die Erkennungsleistung aus dem Training wird, wie in Unterabschnitt 3.4.1 ausgeführt, nicht zur Prüfung von Hypothesen verwendet werden, da es sich um ein Quasi-Experiment (Eifler, 2014) handeln würde und dessen Aussagen nicht wissenschaftlich fundiert zu belegen sind. Weil diese Daten als Nebeneffekt zum Training anfallen, wer-

den sie dennoch erhoben. Die Informatikkenntnisse (ITK) beeinflussen möglicherweise die Phishing-Erkennungsleistung (EKL), deshalb werden diese ebenfalls erhoben.



Ovale = Items mit Aufbau: Identifikation [Wertebereich], (Reversed), Rechtecke = Variablen mit Aufbau: Bezeichnung [Wertebereich]

Abbildung 3.6: Konzeptionelles Modell

3.5 Analyse

Um Nullhypothese und Hypothese 1 zu testen, wird die Mittelwertdifferenz der Phishing-Erkennungsleistung (EKL) analysiert. Um zu entscheiden, ob sich der Mittelwert der beiden Gruppen signifikant unterscheidet, kann der parametrische Student's t-Test (Johnston, 1970), Welch's t-Test heterogener Varianzen (Welch, 1947) oder der nicht-parametrische Mann-Withney U-Test (Mann & Whitney, 1947) durchgeführt werden (Ruxton, 2006). Es wird angenommen, dass das Merkmal der EKL in der Grundge-

samtheit normalverteilt ist. Neben der Normalverteilung setzt Student's t-Test Varianzhomogenität voraus. Bei Varianzheterogenität wird teilweise empfohlen, einen Mann-Whitney-U- anstatt t-Test durchzuführen (McKnight & Najab, 2010). Ruxton (2006) untersuchte die Tests und kamen zum Schluss, dass bei ungleichen Varianzen der Welch's t-Test anstatt des U-Tests durchgeführt werden sollte. Zimmerman (1987) fand ebenfalls, dass die Ersetzung des t-Testes durch eine nichtparametrische Alternative bei Verletzung der Varianzhomogenität und Normalverteilung nicht zwingend zu besseren Resultaten führt. De Winter und Dodou (2010) untersuchten die Problematik t-Test versus U-Test bei Likert-Skalen und kamen zum Schluss, dass sich beide Tests eignen um Differenzen nachzuweisen. Die Stichprobengrösse N für den t-Test sollte 30 übersteigen (Browner, Newman & Hulley, 2007). Bei kleinen Strichproben ($N < 30$) liefert der t-Test möglicherweise unzuverlässige Resultate (Wisz et al., 2008). Deshalb wird für die Auswertung dieser Studie Student's t-Test verwendet, falls die Varianzen sich nicht signifikant unterscheiden, ansonsten wird Welch's t-Test angewandt.

Um auf Varianzhomogenität zu prüfen, wird Levene's F-Test verwendet, denn dieser hat sich als robust (Lim & Loh, 1996; Brown & Forsythe, 1974) erwiesen. Liefert der Levene-Test kein signifikantes Ergebnis ($p >= .05$) (Stigler, 2008), liegt Varianzhomogenität vor, denn der Test prüft die Nullhypothese der Varianzgleichheit. Ist das Ergebnis signifikant, wird von heterogenen Varianzen ausgegangen. Ein $p - Wert <= .05$ wird als Signifikant angesehen (W. R. Rice, 1989; Stigler, 2008) (Universität Zürich, 2018). Der p-Wert ist kein Mass für die Effektstärke (S. Goodman, 2008; Wasserstein & Lazar, 2016). Die meistgenutzten Masse dafür sind Cohen's d (1992) und der Korrelationskoeffizient r nach Pearson (M. E. Rice & Harris, 2005; Lin, 1989). Zur Bewertung der Effektstärke von Mittelwertdifferenzen wird deshalb Cohen's (1992) d verwendet. Ein $d = .2$ entspricht dabei einem kleinen, .5 einem mittleren und .8 einem grossen Effekt. Als Effektstärke r ausgedrückt entspricht .1 einem kleinen, .3 einem mittleren und .5 einem grossen Effekt (Cohen, 1992; M. E. Rice & Harris, 2005). Zusätzlich wird der Korrelationskoeffizient r nach Pearson ermittelt (Benesty, Chen, Huang & Cohen, 2009; M. E. Rice & Harris, 2005).

Kapitel 4

Resultate

Vor der Hauptstudie ($N = 76$) wurde eine Pilot-Studie ($N = 10$) durchgeführt. Die Resultate der Pilot-Studie finden sich in Abschnitt 4.1 und diejenigen der Hauptstudie in Abschnitt 4.2. Die Statistiken und Diagramme wurden mit dem Statistical Package for the Social Sciences (SPSS) (*IBM SPSS Statistics for Windows*, 2017) und WolframAlpha (Wolfram Alpha, 2018) erstellt. Die Prüfung der Hypothesen und die Interpretation der Resultate sind in Kapitel 5 Diskussion in Abschnitt 5.1 beschrieben.

4.1 Pilot-Studie

Die Pilot-Studie wurde vor der Hauptstudie durchgeführt, denn wie De Vaus (2013) vermerkt, sollte das Risiko nicht eingegangen werden, eine Studie ohne vorgängige Pilot-Studie durchzuführen. Die Pilot-Studie diente dazu, die Machbarkeit, inklusive korrekter Funktionsweise der Applikation, zu überprüfen und die Erhebungsinstrumente Umfrage und Training vorgängig zu testen und zu optimieren (Van Teijlingen & Hundley, 2002). Die Pilot-Studie wurde nach dem in Abschnitt 3.4 vorgestellten Experimentaldesign durchgeführt.

4.1.1 Deskriptive Statistik

Eine erste Analyse der Daten zeigt (siehe Tabelle 4.1), dass die Phishing-Erkennungsleistung (EKL) der Gruppe mit Training im Mittel ($M = 6.5$) höher liegt, als diejenige der Gruppe ohne Training ($M = 4.88$). Im Minimum erzielten trainierte Anwender eine höhere EKL ($Min = 5$) im Vergleich zu untrainierten Anwendern ($Min = 3.55$). Diese

	Minimum		*Maximum*		*Mittelwert*		*Standardabw.*	
Training	*Nein*	*Ja*	*Nein*	*Ja*	*Nein*	*Ja*	*Nein*	*Ja*
EKL	3.5	5	6	7	4.88	6.5	1.11	.84
ITK	1.25	1.25	5.50	6	2.69	4	1.92	1.74

n = 4 für Training = Nein | n = 6 für Training = Ja

EKL = Phishing-Erkennungsleistung, ITK = Informatikkenntnisse

Standardabw. = Standardabweichung (*SD*)

Tabelle 4.1: Pilot-Studie - Deskriptive Statistik

Daten lassen vermuten, dass das Training einen positiven Einfluss auf die Erkennungsleistung von Phishing hat. Die Aussagekraft der Pilot-Studie ist aufgrund der kleinen Stichprobengrösse ($N = 10$) zu relativieren. Die Informatikkenntnisse sind in der Experimentalgruppe ($M = 4$) verglichen mit Kontrollgruppe ($M = 2.69$) ebenfalls höher, somit könnte der Effekt des Trainings überbewertet sein. Die Phishing-Erkennungsleistung der beiden Gruppen ist auf Abbildung 4.1 als Boxplot visualisiert. Die Informatikkenntnisse sind auf Abbildung 4.2 gegenübergestellt. Die Histogramme (Abbildung A.35 und Abbildung A.34) vergleichen die Phishing-Erkennungsleistung der beiden Gruppen. Abbildung A.35 zeigt, dass in der Gruppe mit Training gute Phishing-Erkennungsleistung häufiger auftreten als in der Gruppe ohne Training (siehe Abbildung A.34).

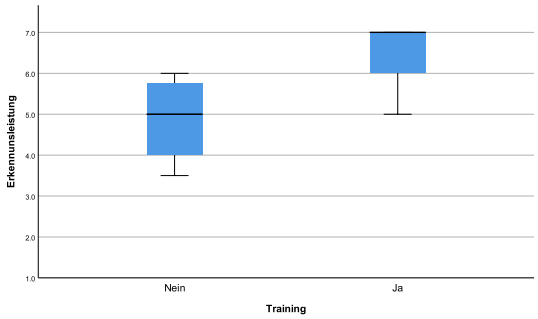


Abbildung 4.1: Pilot-Studie - Box-Plot der EKL

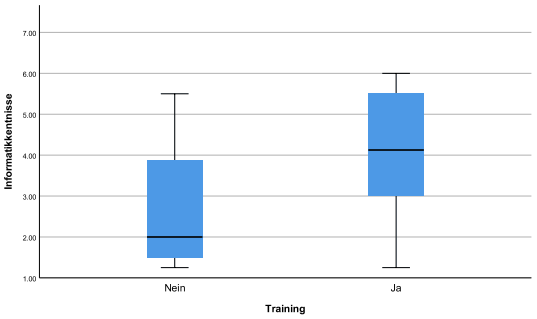


Abbildung 4.2: Pilot-Studie - Box-Plot der ITK

4.1.2 Statistische Analyse

Wie in Abschnitt 3.5 beschrieben, wird der t-Test zur Untersuchung der Mittelwertdifferenz und zur Prüfung der Hypothesen angewendet. Für die Auswertung der Pilot-Studie kann Student's t-Test verwendet werden, da nach Levene ($F(1,10) = .571$, $p = .471$, $n = 10$) Varianzhomogenität für die Phishing-Erkennungsleistung (EKL) vorliegt (siehe Tabelle 4.2). Es existiert ein signifikanter Unterschied ($t(8) = 2.656$, $p = .029$.) in der EKL zwischen der Gruppe welche Training erhalten hat ($M = 6.5$, $SD = .84$) und der untrainierten Gruppe ($M = 4.88$, $SD = 1.11$). Das Training hat nach Cohen (1992) ($d = 1.65$) einen starken Effekt. Cohen's d kann als r ($r = .64$) ausgedrückt werden und wird damit mit dem Korrelationskoeffizienten von Pearson ($r = .68$) vergleichbar. Nach Cohen (1992) entspricht der Korrelationskoeffizient nach Pearson ($r = .68$) ebenfalls einem starken Effekt.

	Levene-Test		*t-Test*		
	F	p	t	df	p
EKL	.571	.471	2.656	8	.029
ITK	.013	.911	1.124	8	.294

p = Signifikanz, N = 4 für Training = Nein | N = 6 für Training = Ja

EKL = Phishing-Erkennungsleistung, ITK = Informatikkenntnisse

t = t-Wert, df = Freiheitsgrade, p = Statistische Signifikanz

Tabelle 4.2: Pilot-Studie - Levene-Test und t-Test der EKL und ITK

4.1.3 Erkenntnis

Aufgrund der Pilot-Studie wurde festgestellt, dass der Fall MyBox einen Bodeneffekt (engl. floor effect) zeigte (Döring & Bortz, 2016, S. 738), da er von Probanden mit und ohne Training zuverlässig klassifiziert werden konnte und somit über wenig Aussagekraft verfügt. Um die Trennschärfe des Items (Straka & Macke, 2002) zu erhöhen, wurde deshalb der Schwierigkeitsgrad des Falles leicht erhöht, ohne die Art der Erkennungsmerkmale zu verändern. Im Konkreten wurde die URL von steal.com/www.mybox.com

auf www.673ab7.cf/mybox.com geändert und der Absender bcd2456e5eae2@hotmail-.com durch mybox@outlook.com ersetzt.

Die Modifikation impliziert, dass die Daten der Pilot-Studie nicht mit den Daten der Studie vereint werden dürfen (Van Teijlingen & Hundley, 2002). Neben dem Einschluss von Pilot-Daten weisen Van Teijlingen und Hundley (2002) in ihrer Studie über die Wichtigkeit von Pilot-Studien auf ein weiteres Problem hin, nämlich die Verfälschung der Daten durch die Teilnahmen von Probanden an beiden Studien. Um das Problem der doppelten Teilnahme und die damit einhergehende Verfälschung der Resultate zu verhindern, wurden Probanden der Pilot-Studie von der Hauptstudie ausgeschlossen.

Die Effekte der Pilot-Studie gehen in die von Hypothese 1 beschriebene Richtung. Die kleine Stichprobengrösse ($N = 10$) verhindert jedoch eine aussagekräftige Interpretation der Daten. Anhand der Pilot-Studie konnte das Experimentaldesign getestet und in Hinblick auf die Hauptstudie optimiert werden.

4.2 Hauptstudie

Auf die Pilot-Studie (siehe Abschnitt 4.1) folgend wurde die umfassendere Hauptstudie durchgeführt. in welche die Erkenntnisse der Pilotstudie eingeflossen sind. Um die Daten zu erheben wurde das in Abschnitt 3.4 beschriebene Experimentaldesign verwendet. Ziel der Hauptstudie, folgend Studie genannt, ist die in Kapitel 3 Methodik aufgestellten Hypothesen (siehe Abschnitt 3.2) mathematisch zu prüfen (siehe Abschnitt 3.5). In einem ersten Schritt werden die Daten anhand deskriptiver Statistik erläutert und danach statistisch ausgewertet.

4.2.1 Deskriptive Statistik

Dieses Kapitel liefert Informationen über die Verteilung und Kennzahlen der erhobenen Daten. In der Tabelle 4.3 ist das Minimum (*Min*), Maximum (*Max*) und der Mittelwert (*M*) sowie die Standardabweichung (*SD*) der Variablen Alter, Geschlecht, Phishing-Erkennungsleistung (EKL) und Informatikkenntnisse (ITK) jeweils für die Experimental-

Variable	*Minimum*		*Maximum*		*Mittelwert*			*Standardabw.*		
Training	*Nein*	*Ja*	*Nein*	*Ja*	*Nein*	*Ja*	*Alle*	*Nein*	*Ja*	*Alle*
Alter	22	20	61	61	29.47	30.9	30.01	8.554	10.335	9.24
Geschlecht	0	0	1	1	.65	.39	.55	.482	.497	.500
EKL	1	1.5	7	7	5.245	5.707	5.421	1.703	1.573	1.659
ITK	1	1.25	7	7	4.532	4.328	4.454	1.899	1.757	1.837
PLV	1	2	7	7	5.713	5.948	5.80	1.51	1.577	1.53
PAV	1	1	7	7	4.79	5.69	5.13	2.303	2.254	2.311

Alle = Beide Gruppen zusammen, Alle: N = 76, Training Nein: n = 47, Training Ja: n = 29

ITK = Informatikkenntnisse, EKL = Phishing-Erkennungsleistung, PLV = Phishing-Link-Vermeidung

PAV = Phishing-Anhang-Vermeidung, Standardabw. = Standardabweichung (*SD*)

Geschlecht: 0 = Weiblich, 1 = Männlich, N = 74, Je einmal 'Keine Angabe' pro Gruppe

Tabelle 4.3: Studie - Deskriptive Statistik

gruppe ($Training = Ja,\ n = 29$) und die Kontrollgruppe ($Training = Nein,\ n = 47$) dokumentiert. Der Mittelwert und die Standardabweichung sind zusätzlich noch für beide Gruppen zusammen ($N = 76$) angegeben. Der Mittelwert der Phishing-Erkennungsleistung, welcher zur Prüfung von Hypothese 1 verwendet wird, ist bei der Experimentalgruppe ($M = 5.707$) etwas höher als bei der Kontrollgruppe ($M = 5.245$). Die Signifikanz dieser Differenz ist im nächsten Abschnitt aufgeführt. Die Informatikkenntnisse dagegen sind im Durchschnitt gegenüber der Experimentalgruppe ($M = 4.328$), in der Kontrollgruppe leicht höher ($M = 4.532$). Eine Auswertung pro Fall ist im Anhang aufgeführt (siehe Unterabschnitt A.3.3).

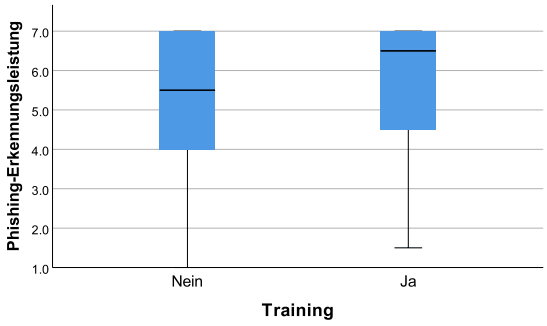


Abbildung 4.3: Studie - Box-Plot der EKL

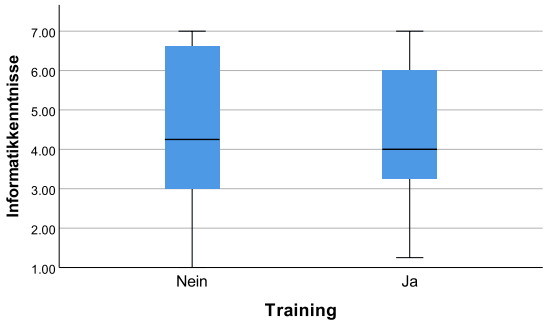


Abbildung 4.4: Studie - Box-Plot der ITK

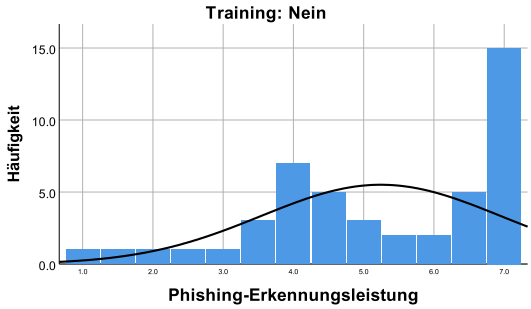


Abbildung 4.5: Studie - Histogramm der EKL in der Kontrollgruppe

Abbildung 4.6: Studie - Histogramm der EKL in der Experimentalgruppe

Die Variablen Phishing-Erkennungsleistung und Informatikkenntnisse sind, nach Gruppen separiert, in den Box-Plots in Abbildung 4.3 und Abbildung 4.4 verglichen. Die EKL (siehe Abbildung 4.3) ist bei der Gruppe, welche ein Training erhalten hat ($Mdn = 6.5$, $Q_1 = 5.24$, $Q_2 = 6.5$, $Q_3 = 7$) leicht höher als bei der untrainierten Gruppe ($Mdn = 5.5$, $Q_1 = 4$, $Q_2 = 5.5$, $Q_3 = 7$). Der Median (Mdn) der beiden Gruppen unterscheidet sich um 1. Gleich ist hingegen das dritte Quartil ($Q_3 = 7$) welches zugleich dem Maximum entspricht ($Max = 7$). Bei den ITK sind sich die beiden Gruppen ähnlicher. Der Unterschied des Medians zwischen der Kontrollgruppe ($Mdn = 4.25$, $Q_1 = 3$, $Q_2 = 4.25$, $Q_3 = 6.75$) und der Experimentalgruppe ($Mdn = 4$, $Q_1 = 3.125$, $Q_2 = 4$, $Q_3 = 6$) ist 0.25, das dritte Quartil weicht um 0.75 ab. Die Experimentalgruppe hat somit geringere ITK als die Kontrollgruppe.

Normalverteilung

Die EKL der beiden Gruppen ist als Histogramm in Abbildung 4.5 und Abbildung 4.6 dargestellt. Der häufigste Wert bei beiden Gruppen ist, entgegen der Normalverteilung, der Wert 7. Die Histogramme der Informatikkenntnisse sind in Abbildung A.42 und Abbildung A.43 ersichtlich. In der Kontrollgruppe treten Informatikkenntnisse mit dem höchsten Wert 7 am häufigsten auf, während diese Häufung bei der Experimentalgruppe nicht zu beobachten ist. Abbildung A.44 und Abbildung A.45 zeigen ein Quantil-Quantil-Diagramm (Q-Q-Plot) der Variablen EKL und ITK der Stichprobe, um diese auf Normalverteilung zu prüfen. Die Daten sind nicht optimal normalverteilt.

Geschlechtsspezifische Unterschiede

Es konnten geschlechtsspezifische Unterschiede festgestellt werden. Die weiblichen Probanden schätzten ihre ITK ($n = 33$, $Min = 1.25$, $Max = 7$, $M = 3.538$) im Mittel tiefer ein als die männlichen ($n = 41$, $Min = 1$, $Max = 7$, $M = 5.11$) (siehe Abbildung A.46). Ebenfalls liegt die EKL der weiblichen Probanden ($Min = 1$, $Max = 7$, $M = 4.939$) tiefer als diejenige der männlichen ($Min = 1.5$, $Max = 7$, $M = 5.732$) (siehe Abbildung A.47). Die EKL der weiblichen Probanden ohne Training ($n = 16$, $Min = 1$, $Max =$, $M = 4.344$) steigerte sich im Vergleich zu der Gruppe mit Training ($n = 17$, $Min = 4$, $Max =$, $M = 5.5$). Ebenfalls steigerte sich die männliche Gruppe ohne Training ($n = 30$, $Min = 3$ $Max =$, $M = 5.667$) im Vergleich zu der Gruppe mit Training ($n = 11$, $Min = 1.5$, $Max =$, $M = 5.9$) (siehe Abbildung A.48) (siehe Abbildung A.49). Das Training scheint bei allen Probanden eine Wirkung zu zeigen. Die tiefere EKL der Frauen ist möglicherweise auf die tiefere ITK zurückzuführen,da 51 % der weiblichen Probanden im Gegensatz zu 25 % der männlichen Probanden ein Training erhielten.

Altersspezifische Unterschiede

Die ITK scheinen mit dem Alter abzunehmen (siehe Abbildung A.50), während die EKL über beide Gruppen hinweg circa konstant bleibt (siehe Abbildung A.51). Ohne Training nimmt die EKL in der Stichprobe mit dem Alter ebenfalls ab (siehe Abbildung A.53). Bei der Gruppe, welche ein Training erhalten hat, nahm die EKL mit dem Alter zu (siehe Abbildung A.53). Die Stichprobe ist jedoch zu klein, um hier allgemeingültige Aussagen zu treffen.

4.2.2 Statistische Analyse

Es werden t-Tests zur Prüfung der Hypothesen und zur Untersuchung der Mittelwertdifferenzen angewendet. Vorbedingung für Student's t-Test ist unter anderem (siehe Abschnitt 3.5) die Varianzhomogenität. Die Varianzen der Phishing-Erkennungsleistung, Informatikkenntnisse und Phishing-Link- sowie -Anhang-Vermeidung unterscheiden sich nicht signifikant. Es kann somit bei allen Variablen von Varianzhomogenität ausgegangen werden, wie Levene-Tests (siehe Tabelle 4.4) via t-Test zeigen (EKL: $F(1,74) = .558,\ p = .475,\ n = 74$), (ITK: $F(1,74) = .674,\ p = .414,\ n = 74$), (PLV: $F(1,74) = .009, p = .925, n = 74$), (PAV: $F(1,74) = .1.720, p = .194, n = 74$). Deshalb kann, wie bereits zur Auswertung der Pilot-Studie, Student's t-Test verwendet werden und es muss nicht auf den t-Test für heterogene Varianzen zurückgegriffen werden.

	Levene-Test	
	F	*p*
Phishing-Erkennungsleistung (EKL)	.558	.457
Informatikkenntnisse (ITK)	.674	.414
Phishing-Link-Vermeidung (PLV)	.009	.925
Phishing-Anhang-Vermeidung (PAV)	1.720	.194

p = Statistische Signifikanz

Tabelle 4.4: Studie - Levene-Test der Varianzhomogenität

Die Ergebnisse der t-Tests sind in der Tabelle 4.5 aufgeführt. Der t-Test der Phishing-Erkennungsleistung ($t(74) = 1.183,\ p = .241$) weist eine Signifikanz von $p = .241$ auf und wurde zur Prüfung der Hypothese 1 durchgeführt. Die Phishing-Link-Vermeidung hat, gemäss dem t-Test ($t(74) = .649,\ p = .518$), eine statistische Signifikanz von $p = .518$ und die Phishing-Anhang-Vermeidung ($t(74) = 1.673,\ p = .099$) weist ein p von .099 aus. p-Werte von über 5 % werden in dem von Fisher (1925) geprägten Masse als nicht ausreichend signifikant betrachtet (Stigler, 2008). Unter dieser Annahme müssen die durchgeführten Student's t-Tests als statistisch nicht signifikant betrachtet werden.

	t-Test			*Effektstärke*	
	t	df	p	d	r
EKL	1.183	74	.241	.275	.136
ITK	–.469	74	.641	−.109	.054
PLV	.649	74	.518	.151	.075
PAV	1.673	74	.099	.389	.191

n = 29 für Training = Nein, n = 47 für Training = Ja, N = 74 Total

t = t-Wert, df = Freiheitsgrade, p = Statistische Signifikanz

d = Cohen's d, r = Pearson's r als Mass der Effektstärke

Tabelle 4.5: Studie - Student's t-Test unter Angabe der Effektstärke

Da die Signifikanz keine Kennzahl der Effektstärke ist (siehe Abschnitt 3.5) wurden zu dessen Bestimmung Cohen's (1992) d und r nach Pearson (M. E. Rice & Harris, 2005) berechnet (siehe Tabelle 4.5). Eine kleiner Effekt nach Cohen tritt bei der Phishing-Erkennungsleistung ($d = .275$, $r = .136$) und bei der Phishing-Anhang-Vermeidung ($d = .389$, $r = .191$) auf. Ein sehr kleiner Effekt tritt bei der Phishing-Link-Vermeidung ($d = .151$, $r = .075$) auf. Der negative t-Wert der Informatikkenntnisse ($t(74) = -.469$, $p = .641$, $d = -.109$, $r = .054$) weist auf einen Effekt in die entgegengesetzte Richtung hin. Dies zeigt, dass sich die Informatikkenntnisse der beiden Gruppen nicht signifikant unterscheiden und dass in der Gruppe ohne Training mehr Informatikkenntnisse vorhanden sind. Die Prüfung der Hypothesen und Beantwortung der Forschungsfrage sind in Kapitel 5 zu finden.

Kapitel 5

Diskussion

Diese Studie hat die Effektivität von Anwender-Training auf die Erkennungsleistung von Phishing untersucht. Im Folgenden werden die Resultate der statistischen Analyse interpretiert und die Hypothesen geprüft. Weiter werden die Limitationen dieser Arbeit kritisch reflektiert und mögliche Optionen für zukünftige Forschung aufgezeigt.

5.1 Resultate

Als Erstes wird, um Hypothese 1 zu prüfen, der Einfluss des Anti-Phishing-Trainings auf die Phishing-Erkennungsleistung (EKL) analysiert. Die Experimentalgruppe ($M = 5.707$, $SD = 1.537$, $n = 29$), welche ein Training erhalten hat, schneidet in der EKL besser ab als die Kontrollgruppe ($M = 5.245$, $SD = 1.703$, $n = 47$) welche kein Training erhalten hat ($t(74) = 1.183$, $p = .241$). Die Effektstärke der EKL liegt bei $r = .136$ und entspricht damit nach Cohen (1992) einem, schwachen positiven Effekt (siehe Abschnitt 3.5). Mit einem p-Wert von $p = .241$ ist die Mittelwertdifferenz der EKL aus den beiden Gruppen statistisch nicht signifikant. Hypothese 1 wird daher verworfen ($t(74) = 1.183$, $p = .241$, $d = .275$, $r = .136$). Bis zu ihrer Widerlegung wird die Nullhypothese mit der Aussage angenommen, dass Training keinen Einfluss auf die EKL hat.

Hypothese 2.1 und Hypothese 2.2 besagen, dass auf Phishing trainierte Anwender Links weniger oft folgen, respektive Anhänge seltener öffnen, als Anwender welche kein Training erhalten haben. Um Hypothese 2.1 und Hypothese 2.2 zu prüfen, werden die Variablen Phishing-Link-Vermeidung (PLV) und Phishing-Anhang-Vermeidung (PAV) ausgewertet. Die trainierte Gruppe zeigt im Mittel die bessere PLV ($M = 5.948$,

$SD = 1.577$, $n = 29$) und PAV ($M = 5.69$, $SD = 2.254$, $n = 29$) gegenüber der PLV ($M = 5.713$, $SD = 1.51$, $n = 47$) und PAV ($M = 4.79$, $SD = 2.303$, $n = 47$) der untrainierten Gruppe (PLV: $t(74) = .649$, $p = .518$), (PAV: $t(74) = 1.673$, $p = .099$). Gemäss Cohen (1992) entspricht die Effektstärke der PAV mit $r = .19$ einem schwachen positiven Effekt. Statistische Signifikanz ist für die Effekte der PLV ($p = .518$) und für die PAV ($p = .099$) nicht gegeben. Aufgrund mangelnder Signifikanz werden Hypothese 2.1 und Hypothese 2.2 abgelehnt.

Die Forschungsfrage, ob die Wahrscheinlichkeit eines Schadens durch Phishing-E-Mails für Internetanwender durch Training vermindert wird, kann nicht eindeutig beantwortet werden. Für die Phishing-Erkennungsleistung wurde ein nicht signifikanter ($p = .241$), schwacher Effekt ($d = 0.28$, $r = 0.14$) nach Cohen (1992) festgestellt. Die Hypothesen konnten nicht mit statistischer Signifikanz gestützt werden, daher müssen sie mit Ausnahme der Nullhypothese abgelehnt werden. Gründe weshalb die Tests nicht statistisch signifikant waren, und wie das gewünschte Signifikanzniveau erreicht werden könnte, sind im folgenden Kapitel beschrieben.

5.2 Limitationen

Dieser Abschnitt behandelt die Einschränkungen sowie Auffälligkeiten dieser Studie. Obwohl mit grösster Sorgfalt und rigoros auf wissenschaftlicher Basis gearbeitet wurde, sind einige Limitationen zu beachten. Die Stichprobe enthält nach Bereinigung die Daten von 76 Probanden, welche nicht zu gleichen Teilen auf die beiden Gruppen verteilt sind. Die Experimentalgruppe enthält 29 und die Kontrollgruppe 47 Probanden. Bei einem Verhältnis von .5 gelten die Gruppen als gleich gross. Davon weichen die beiden Gruppen mit einem Verhältnis von .617 lediglich um .117 ab. Die Verteilung der Phishing-Erkennungsleistung (EKL) bildet die Normalverteilung nicht exakt ab (siehe Abbildung A.44). In der Fachliteratur finden sich Hinweise, dass der t-Test auch bei nicht normalverteilten Daten robust ist, solange die Gruppengrössen ungefähr gleich sind (Posten, Rasch & Tiku, 1984). Die Methodenberatung der Universität Zürich (2018) empfiehlt bei ungleichen Gruppengrössen Cohen's d (1992) zu verwenden, da r ver-

zogen sein könnte. Um die Reliabilität der Effektstärke zu steigern, wurde deshalb *d* zusätzlich zu *r* berechnet.

Der Unterschied in den Gruppengrössen ist mit hoher Wahrscheinlichkeit nicht durch inakkurat randomisierte Zuteilung der Probanden entstanden, da diese automatisiert getestet wurde. Die visuelle Analyse der Daten legt nahe, dass einige Probanden, vermutlich aus zeitlichen Gründen, nach dem Training aber noch vor der Umfrage abgebrochen haben. Möglicherweise wurde auch die Schaltfläche übersehen, welche zur Umfrage führt (siehe Abbildung A.11). Ein weiterer Grund könnte die eingeschränkte Mobile-Tauglichkeit des für den Computer entwickelten interaktiven Training-Teils gewesen sein. Obwohl es grundsätzlich möglich ist, alle Teile der Studie auf dem Mobiltelefon zu verwenden. Im Gegensatz zur Kontrollgruppe findet sich in der Experimentalgruppe kein Datensatz, welcher unter Verwendung eines mobilen Browser erzeugt wurde. Die erhobenen Datensätze enthalten nicht personenbezogene Browser-Daten und Zeitstempel pro passierten Abschnitt, was eine solche Analyse ermöglicht. In der Einladung zur Studie wurde explizit auf die Verwendung eines Computers hingewiesen.

Mehrfachteilnahmen und Manipulationsversuche wurden mit technischen Massnahmen wie dem Setzen von Browser-Cookies (Barth, 2011) und der Auswertung der Browser-Metadaten sowie der temporär gespeicherten IP-Adresse so gut wie möglich verhindert. Dazu wurde die Gruppeneinteilung beim Aufruf jeder Seite erneut überprüft. Dies verhindert, dass Probanden der Kontrollgruppe an Informationen über den Stimulus der Experimentalgruppe gelangen. Jedoch können Probanden nach dem Wechsel eines Gerätes und Standorts aus technischen Gründen nicht wiedererkannt werden. Deshalb werden sie erneut randomisiert zugeteilt. Dieser Effekt kann beispielsweise beim Wechsel vom Mobiltelefon auf den Computer auftreten. Werden Probanden nach dem Wechsel von Geräten einer anderen Gruppe zugeteilt ($Wahrscheinlichkeit = .5$) können unerwünschte Effekte entstehen, welche die Resultate verfälschen. Falls Probanden via Mobiltelefon der Experimentalgruppe zugeteilt wurden, sich aber danach aufgrund eines ungenügenden Nutzungserlebnisses für ein Ausfüllen am Computer entscheiden, liegt die Wahrscheinlichkeit der Experimentalgruppe zugeteilt zu werden, erneut bei 50

%. Wird davon ausgegangen, dass nur die Experimentalgruppe die Geräte wechseln, liegt die totale Wahrscheinlichkeit in die Experimentalgruppe zu gelangen noch bei 25 % anstatt der ursprünglichen 50 % ($.25 = .5 * .5$). Dieser Effekt könnte ebenfalls für die ungleichen Gruppengrössen oder einer Verfälschung der Resultate verantwortlich sein.

In der Kontrollgruppe tritt eine Häufung von Probanden mit sehr hohen Informatikkenntnissen auf. Dieser nicht normalverteilte Ausreisser der Häufigkeit könnte die Resultate verfälscht haben, denn es wird vermutet, dass hohe Informatikkenntnisse sich positiv auf die Phishing-Erkennungsleistung auswirken. Eine lineare Regression mit ITK als unabhängige und EKL als abhängige Variable über den gesamten Datensatz stützt diese Annahme ($F(1,74) = 13.658$, $p = .000$, $\beta = .375$). Das Modell erklärt 14.4 % (korrigiertes $r^2 = .144$) der Varianz und entspricht nach Cohen's d (Cohen, 1992) einem starken Effekt ($r = .410$). Der Einfluss auf die Studie wird durch die geringe ausgewiesene ITK-Mittelwertdifferenz der Kontrollgruppe ($M = 4.532$) verglichen mit der Experimentalgruppe ($M = 4.328$) relativiert. Möglich ist, dass der Effekt des Trainings bei Probanden mit hohen ITK geringer ausfällt, da sie aufgrund ihrer Vorkenntnisse wenig dazulernen. Werden Probanden mit $ITK >= 6$ aus dem Datensatz entfernt, führt dies nicht zu statistischer Signifikanz ($p <= .05$).

Nachweislich verfälschte Datensätze wurden aussortiert. Es kann jedoch nicht ausgeschlossen werden, dass bewusst falsche Angaben gemacht wurden. Möglichkeiten diese Effekte zu verhindern, sowie Optionen für die Zukunft, werden im nächsten Abschnitt diskutiert.

5.3 Ausblick

Dieser Abschnitt führt Optionen aus, welche in Zukunft umgesetzt werden können und beschreibt offene Forschungsfragen. Diese Studie könnte erneut mit einer grösseren Stichprobe reproduziert werden, um die Wirksamkeit des Trainings differenziell zu prüfen. Die Rekrutierung der Probanden könnte beispielsweise in Zusammenarbeit mit Wirtschaftspartnern oder Bildungsinstitutionen geschehen, indem diese ihre Mitar-

beiter zur Teilnahme an der Studie aufrufen. Ebenfalls könnte mit Sicherheitsfirmen kooperiert werden, welche das Anti-Phishing-Training ihren Kunden anbieten. Somit könnte die Stichprobengrösse um ein Vielfaches erhöht werden. Um unterschiedliche Gruppengrössen zu vermeiden, könnte das Training für Mobilgeräte ganz gesperrt oder das Nutzungserlebnis gesteigert werden. Zudem wäre es möglich, die Randomisierung so zu modifizieren, dass Probanden mit einer höheren Wahrscheinlichkeit der Experimentalgruppe zugeteilt werden. Anstatt eines Feldexperiments könnte die Studie auch als Laborexperiment durchgeführt werden. Im Labor kann sichergestellt werden, dass alle Probanden die komplette Studie unter konstanten Bedingungen durchlaufen. Die Häufung der Informatikkenntnisse der Probanden ist wahrscheinlich auf das Umfeld des Autors zurückzuführen. Eine grössere und diversere Stichprobe würde diesen Effekt mindern. Das Erhebungsinstrument für die Informatikkenntnisse kann in Zukunft ebenfalls erweitert werden, um die Kenntnisse präziser zu erfassen.

Anhand einer grösseren Stichprobe könnte überprüft werden, ob sich der positive Effekt des Trainings wiederholt und mit höherer Signifikanz finden lässt. Anstatt mit nur einer Experimentalgruppe könnten neben einer Kontrollgruppe auf verschiedene Experimentalgruppen gesetzt werden, welche unterschiedliche Arten von Trainings erhalten. Anhand dieses Experimentaldesigns könnten zusätzlich Aussagen darüber gemacht werden, welcher der Training-Ansätze die höchste Effizienz aufweist.

Die in dieser Studie verwendete Phishing-Studie-Applikation (App) ist derart aufgebaut, dass sie im Firmenumfeld eingesetzt werden kann und die Verarbeitung von grösseren Stichproben unterstützt. Ebenfalls ist die App darauf ausgelegt, in andere Sprachen übersetzt zu werden, um zu erforschen, ob in anderen Sprach- und Kulturräumen die gleichen Effekte beobachtet werden können. Ebenfalls denkbar ist, das Training in Zukunft mit einem Versand von Test-Phishing-E-Mails zu kombinieren. Beim Testversand wird beispielsweise eine von den Forschern speziell präparierte Phishing-E-Mail an Mitarbeiter eines Unternehmens versendet. Der Link der Phishing-E-Mails wird dabei von den Forschern kontrolliert. Diese Rekrutierungsmethode bietet den Vorteil, dass ausschliesslich Anwendern ein Training angeboten wird, welche dem Link

der Test-Phishing-E-Mails gefolgt sind. Diese Anwender haben möglicherweise einen höheren Trainingsbedarf und das Training ist für sie relevanter. Ebenfalls könnte das Interesse am Training höher sein, da sie eine Phishing-E-Mail nicht erkennen konnten (Kumaraguru, Rhee, Sheng et al., 2007).

Eine mögliche Weiterentwicklung des Training-Teils der App ist die Integration von Phishing-Webseiten. Die Anwender könnten den Links in E-Mails folgen, um auf Webseiten zu gelangen. Dort könnten Probanden entscheiden, ob sie Daten weitergeben. Damit das Spielprinzip weiterhin funktioniert, müssten die Ziele des Trainings so angepasst werden, dass Anwender für Anmeldevorgänge auf legitimen Webseiten belohnt werden. Ebenfalls könnten sich in Anhängen legitimer E-Mails Informationen befinden, welche für die Zielerreichung zwingend benötigt werden. Damit könnten Anwender motiviert werden, Anhänge zu öffnen und Links zu folgen. Diese Erweiterungen stehen jedoch im Widerspruch zum Grundsatz, generell vorsichtig zu sein. Der Schulungsteil könnte mit Charakteren in einem Handlungsstrang oder mit Comicfiguren erweitert werden, wie bereits in anderen Arbeiten getan wurde (Wen et al., 2017; Kumaraguru, Rhee, Acquisti et al., 2007).

Die App soll im Rahmen weitere Arbeiten weiterentwickelt werden können. Deshalb soll die App als Open-Source unter der AGPL-Lizenz (Free Software Foundation, 2007a) veröffentlicht werden. Die Free Software Foundation (2015) empfiehlt die AGPL- der GPL-Lizenz (Free Software Foundation, 2007b) bei serverbasierter Software vorzuziehen. Interessierten Parteien wird es damit ermöglicht, die App zu nutzen und anzupassen, solange die Weiterentwicklung ebenfalls frei verfügbar ist. Das Anti-Phishing-Training wird nach dieser Studie online verfügbar bleiben, damit Interessierte sich zum Thema Phishing bilden und mit Phishing-E-Mails trainieren können.

5.4 Fazit

Diese Studie beschäftigte sich mit der Frage, wie das Phishing-Risiko für Internetanwender vermindert werden kann. Basierend auf dem Stand der Forschung und dem TTAT-Modell, wurde deshalb ein Anwender-Training zur Steigerung des Sicherheitsbewusstseins und der Phishing-Erkennungsleistung entwickelt. Um den Effekt des Trainings zu untersuchen, wurde ein randomisiertes Kontrollgruppenexperiment durchgeführt. Um das Forschungsdesign inklusive des Messinstrumentes zu testen, wurde eine Pilot-Studie durchgeführt. In der Pilot-Studie waren die Mittelwerte der beiden Gruppen gemäss Student (1908)'s t-Test statistisch signifikant verschieden (Fisher, 1925) und das Anwender-Training hatte, nach Cohen (1992), einen starken, positiven Effekt auf die Phishing-Erkennungsleistung. In der Hauptstudie wurde unter Anwendung der selben Methodik ein statistisch nicht signifikanter, schwacher Effekt gefunden. Dies zeigt die Bedeutung von Stichproben auf und deutet darauf hin, dass ein Effekt vorhanden ist, welcher durch Wiederholung der Studie mit einer grösseren Stichprobe gefunden werden könnte.

Diese Studie liefert weitere Hinweise, dass bereits ein kurzes Anwender-Training einen positiven Effekt auf die Erkennungsleistung von Phishing haben kann und stützt damit die Wichtigkeit von Massnahmen zur Stärkung der Sicherheitsbewusstseins. Mit dem Anti-Phishing-Training wurde ein frei verfügbares und erweiterbares Anwender-Training geschaffen und getestet, welches Anwender über die Risiken von Phishing aufklärt und lehrt, Phishing-E-Mails zu erkennen. Das Training leistet damit einen Beitrag zur Cyber-Sicherheit.

Anhang

A.1 Die Phishing-Studie-Applikation

A.1.1 Technische Informationen

Die App ist in der Programmiersprache Ruby[1] 2.5.1 geschrieben und wurde mit dem Web-Applikations-Framework Rails 5.1 entwickelt[2]. Für das Web-Frontend kommt das Boostrap-Famework[3] 4.1 zum Einsatz. Die App wird via der Cloudplattform von Heroku[4] im Internet verfügbar gemacht. Die dazugehörige Postgres Datenbank wird in den Rechenzentren von Amazon[5] betrieben. DNS-Anfragen, der bei Name.com[6] registrierte Domain, werden vom Cloudflare[7] beantwortet und aus Gründer der Performance und Sicherheit durch deren Content Delivery Network (CDN) geroutet. Die App ist sorgfältig entwickelt und wurde manuell sowie automatisiert[8] getestet. Ebenfalls sind Sicherheitsfunktionen wie HTTPS, HSTS, CSP, DNSSEC, CAA, XSS-Protection, SecureCookies und weitere Sicherheitsfunktionen aktiv[9] [10] [11]. Die Datenbank ist gegen ungewollte Zugriffe abgesichert und verfügt über eine Benutzer- und Rollenverwaltung.

[1] https://www.ruby-lang.org
[2] https://rubyonrails.org
[3] https://getbootstrap.com
[4] https://www.heroku.com
[5] https://aws.amazon.com/
[6] https://www.name.com/
[7] https://www.cloudflare.com/
[8] https://circleci.com/gh/mo-zo/phisher
[9] https://www.hardenize.com/report/phishing-studie.org/
[10] https://securityheaders.com/?q=phishing-studie.org
[11] https://www.ssllabs.com/ssltest/analyze.html?d=phishing-studie.org

Neben dem Benutzer mit allen Rechten, werden automatisch Rollen für Server, sowie für den rein lesenden Zugriff zwecks Analyse erstellt. Um Datenverlust zu verhindern, werden regelmässig Sicherungskopien der Datenbank angefertigt. Via der Quellcode-Hosting und Kollaborationsplattform GitHub[12] ist der Quellcode der App allgemein verfügbar. Die Umfrage wurde unter der Zuhilfenahme des von UmfrageOnline[13] zu Verfügung gestellten Services realisiert. Die App kann unter https://phishing-studie.org aufgerufen werden.

A.1.2 Umfang

Die App ist einfach erweiter- und internationalisierbar. Neue Folien und Fälle können leicht hinzugefügt werden, wie dies beispielsweise nach der Pilot-Studie geschehen ist. Tatsächlich verfügt die App bereits über sechs anstelle der drei in der Studie verwendeten Fälle. Die gesamte Textausgabe ist für die Internationalisierung vorbereitet und könnte übersetzt werden. Es besteht die Möglichkeit optional alle E-Mail mit Name und Adresse zu personalisieren (siehe Abbildung A.1). Dazu können die Probanden zu Beginn des Trainings ihre persönlichen Daten angeben, welche nicht in einer Datenbank gespeichert werden. Für ein Mitarbeiter-Training könnten die Daten alternativ auch aus dem Adressbuch des Unternehmens stammen. Obwohl Personalisierung zu realistischeren E-Mails führen kann, wurde die Funktion nicht für die Studie verwendet. Ein Grund dafür ist die mangelnde Vergleichbarkeit von Probanden, welche die Personalisierungsfunktion genutzt haben, gegenüber denjenigen, die sie nicht oder mit eigenen, fiktiven Daten genutzt haben. Wäre die Eingabe der Angaben Pflicht könnte dies, gerade bei einer Phishing-Studie, Probanden zum Abbruch der Teilnahmen motivieren. Die Fälle können den Probanden in randomisierter Reihenfolge präsentiert werden. Diese Funktion wurde zur Durchführungen der Studie genutzt. Ebenfalls kann die Zeit, welche ein Proband für die einzelnen Schritte braucht, aufgezeichnet werden. Diese Information kann, neben den ebenfalls speicherbaren Browser- und Plattformdaten, für Auswertungen genutzt werden. So kann beispielsweise analysiert werden, wann ein Proband auf

[12] https://github.com/mo-zo/phisher
[13] https://www.umfrageonline.ch

welchem Gerät abbricht. Die App ermöglicht die Vereinigung von Umfrageresultaten im Excel-Format mit den Auswertungen der Datenbank. Die so zusammen geführten Daten können als in SPSS verwendbarer Excel-Datei exportiert werden.

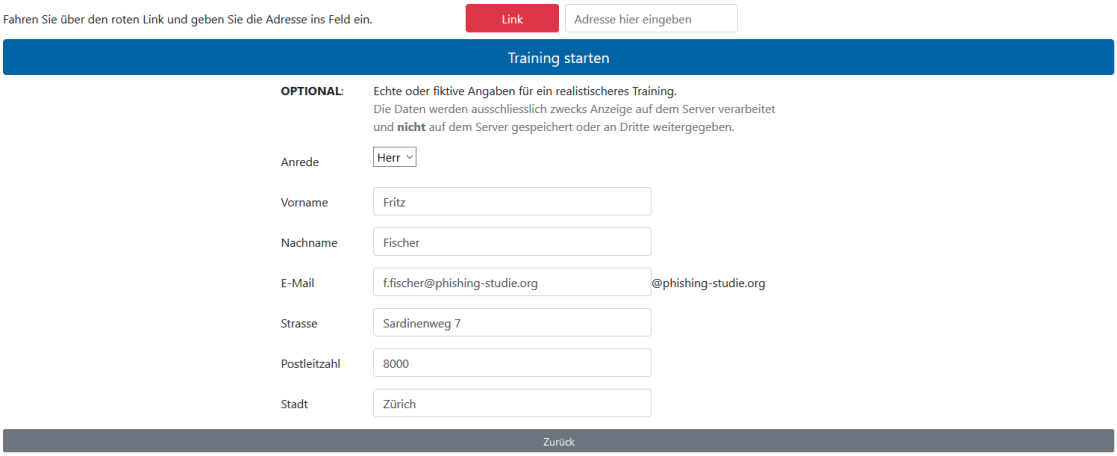


Abbildung A.1: Phishing-Studie-Applikation - Training - Personalisierung

A.1.3 Bildschirmfotos der Schulung

Abbildung A.2: Phishing-Studie-Applikation - Schulung - Folie 1 - Ablauf der Studie

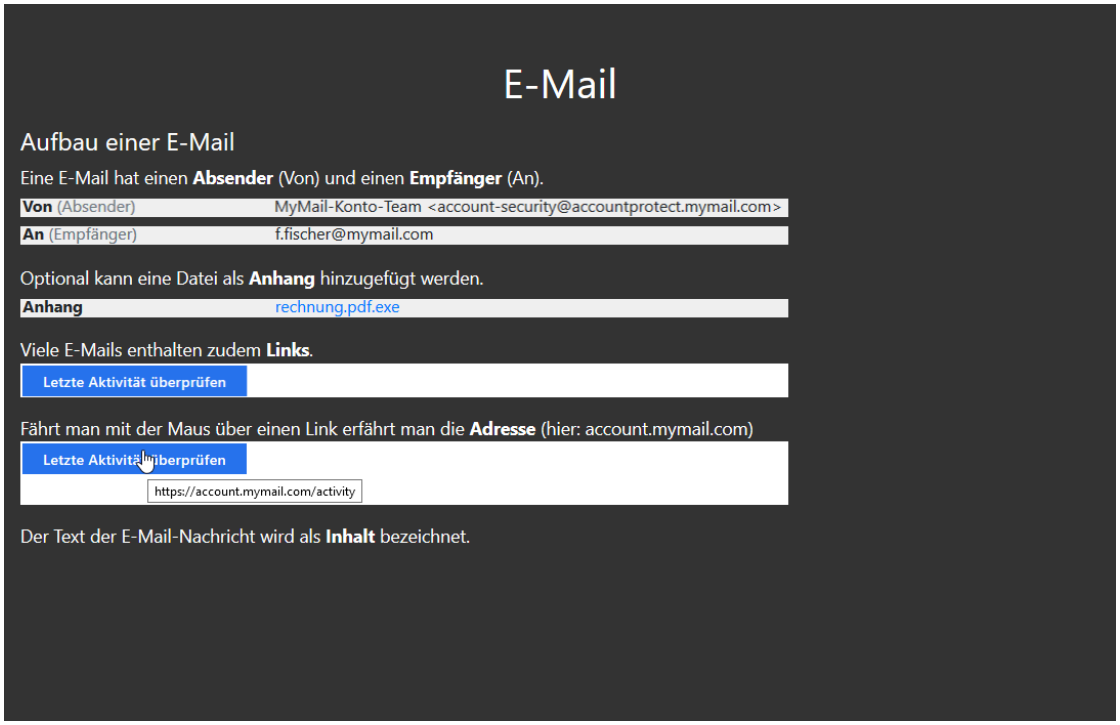


Abbildung A.3: Phishing-Studie-Applikation - Schulung - Folie 2 - Aufbau einer E-Mail

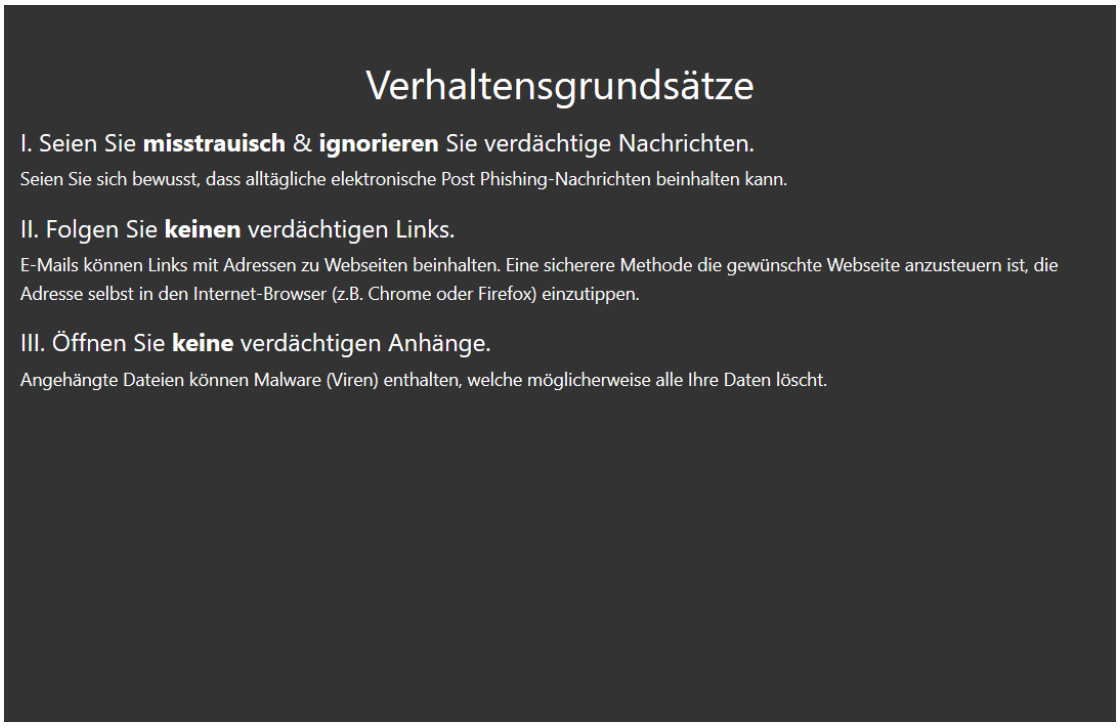


Abbildung A.4: Phishing-Studie-Applikation - Schulung - Folie 3 - Verhaltensgrundsätze

Abbildung A.5: Phishing-Studie-Applikation - Schulung - Folie 4 - Phishing Erkennen

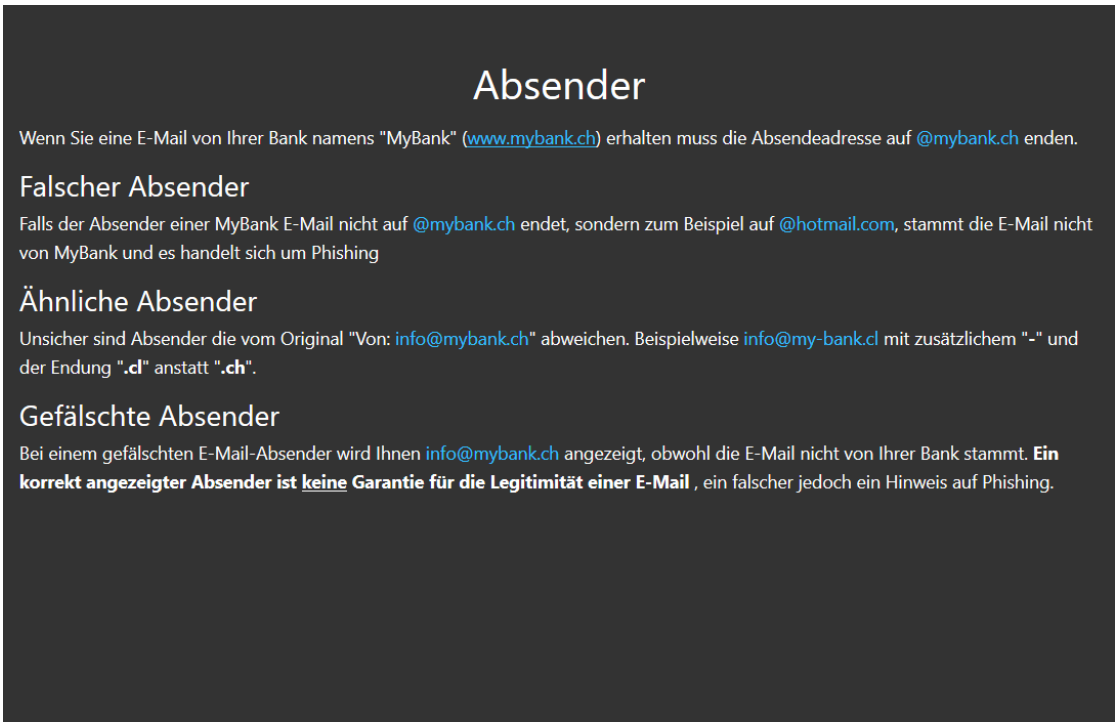


Abbildung A.6: Phishing-Studie-Applikation - Schulung - Folie 5 - Absender

Abbildung A.7: Phishing-Studie-Applikation - Schulung - Folie 6 - Link überprüfen

Abbildung A.8: Phishing-Studie-Applikation - Schulung - Folie 7 - Link

Abbildung A.9: Phishing-Studie-Applikation - Schulung - Folie 8 - Weiter zum Training

A.1.4 Bildschirmfotos des interaktiven Trainings

Abbildung A.10: Phishing-Studie-Applikation - Training - Willkommen

Abbildung A.11: Phishing-Studie-Applikation - Training - Auswertung

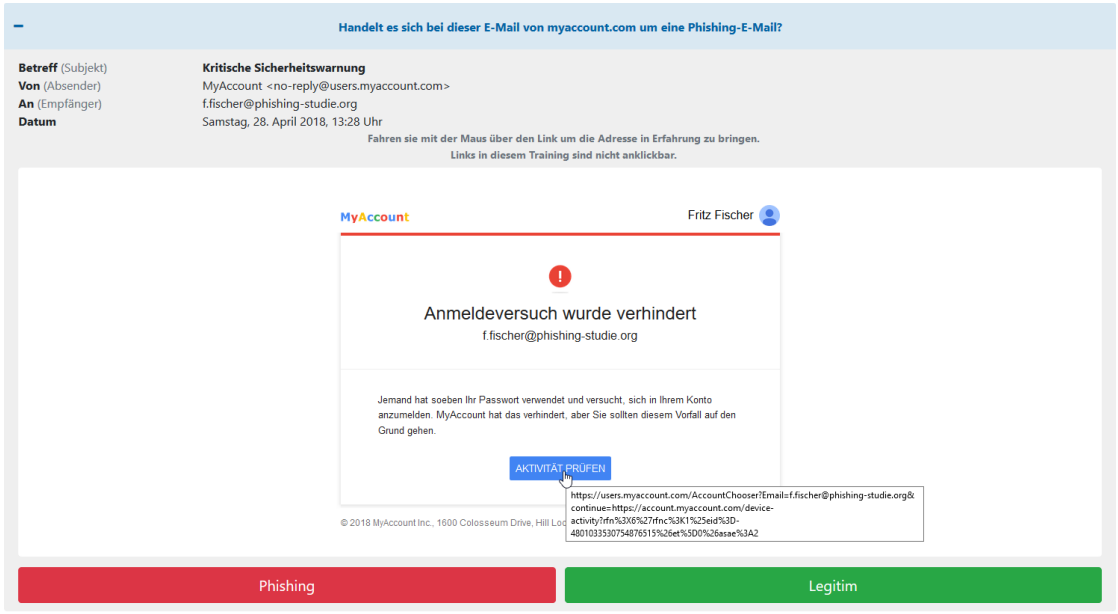


Abbildung A.12: Phishing-Studie-Applikation - Training - MyAccount - ungelöst

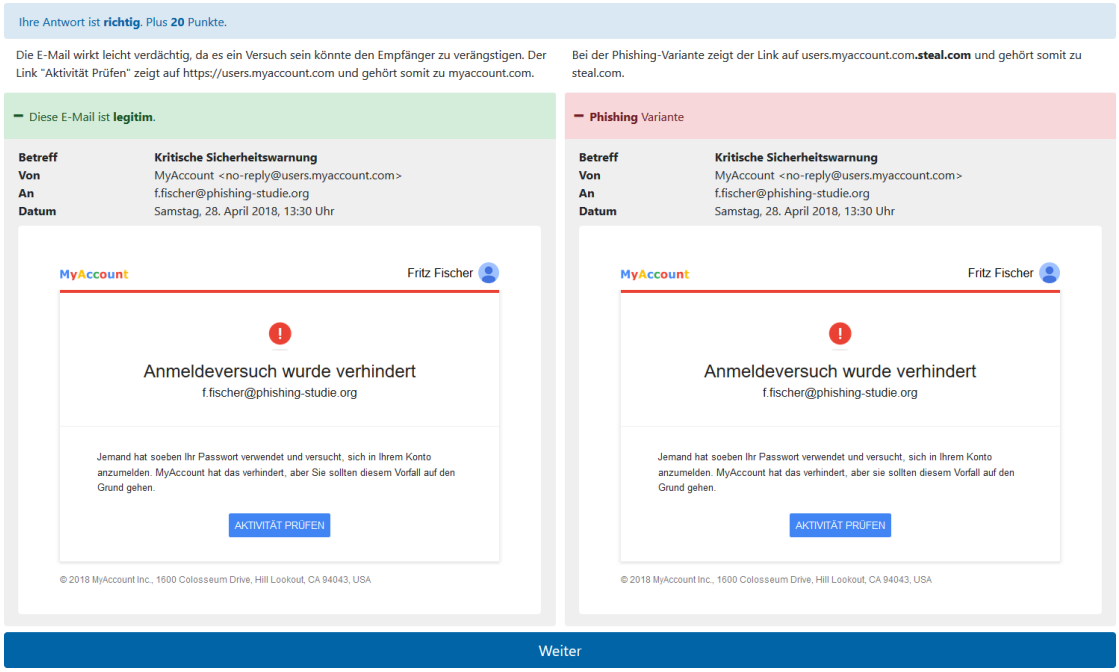


Abbildung A.13: Phishing-Studie-Applikation - Training - MyAccount - gelöst

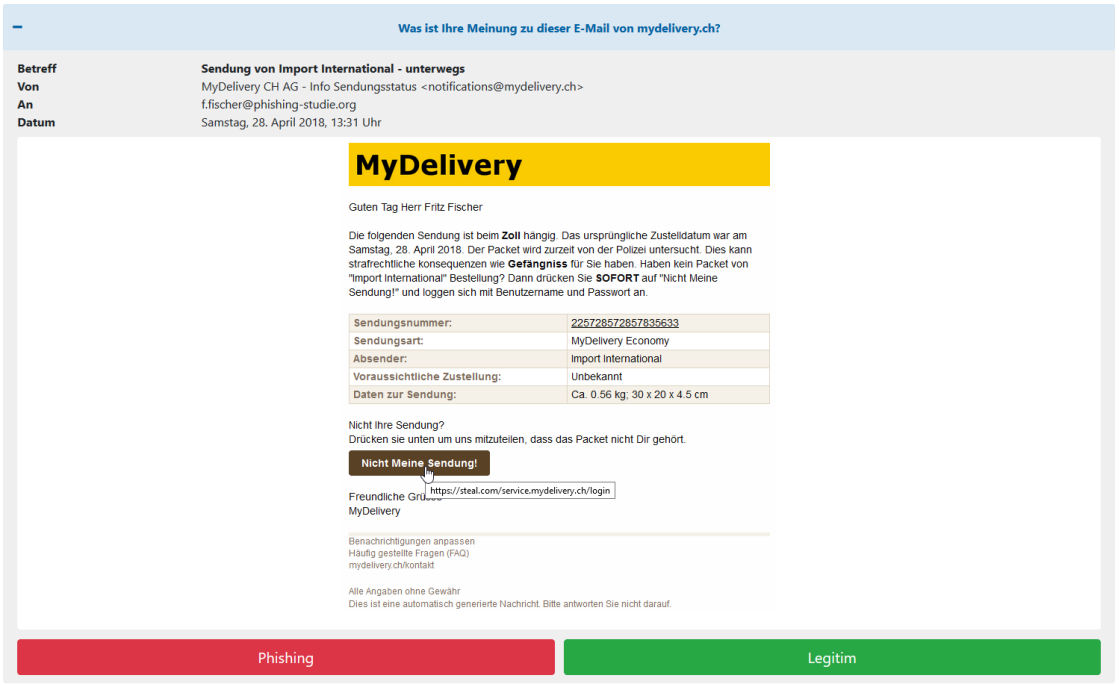


Abbildung A.14: Phishing-Studie-Applikation - Training - MyDelivery - ungelöst

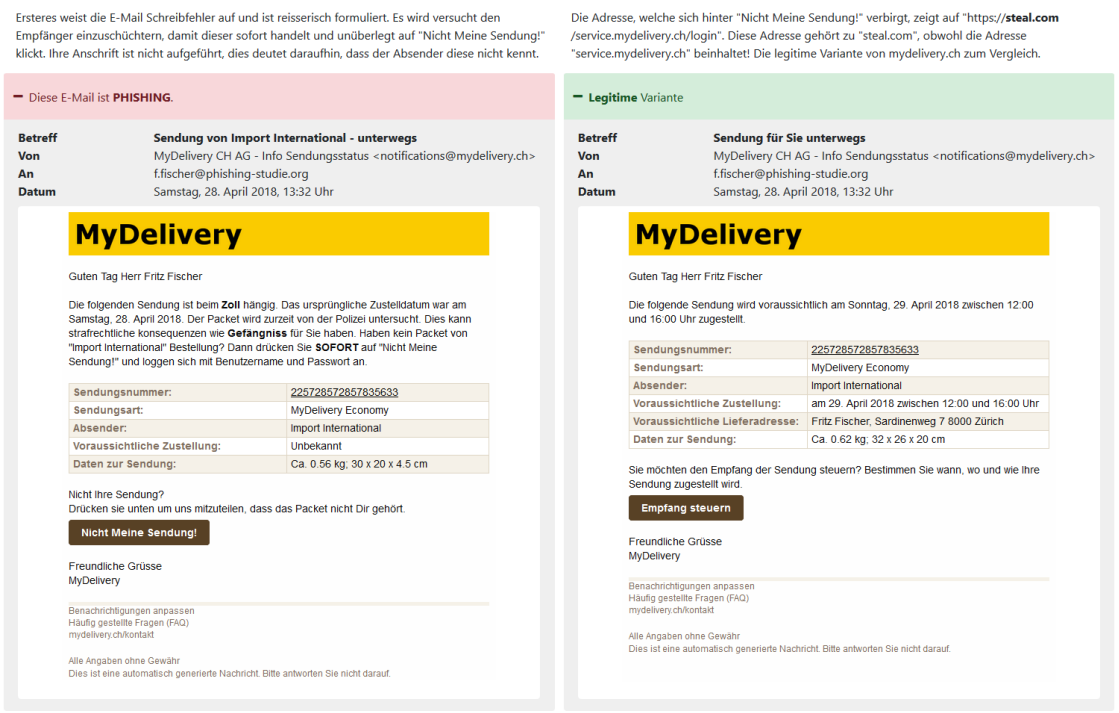


Abbildung A.15: Phishing-Studie-Applikation - Training - MyDelivery - gelöst

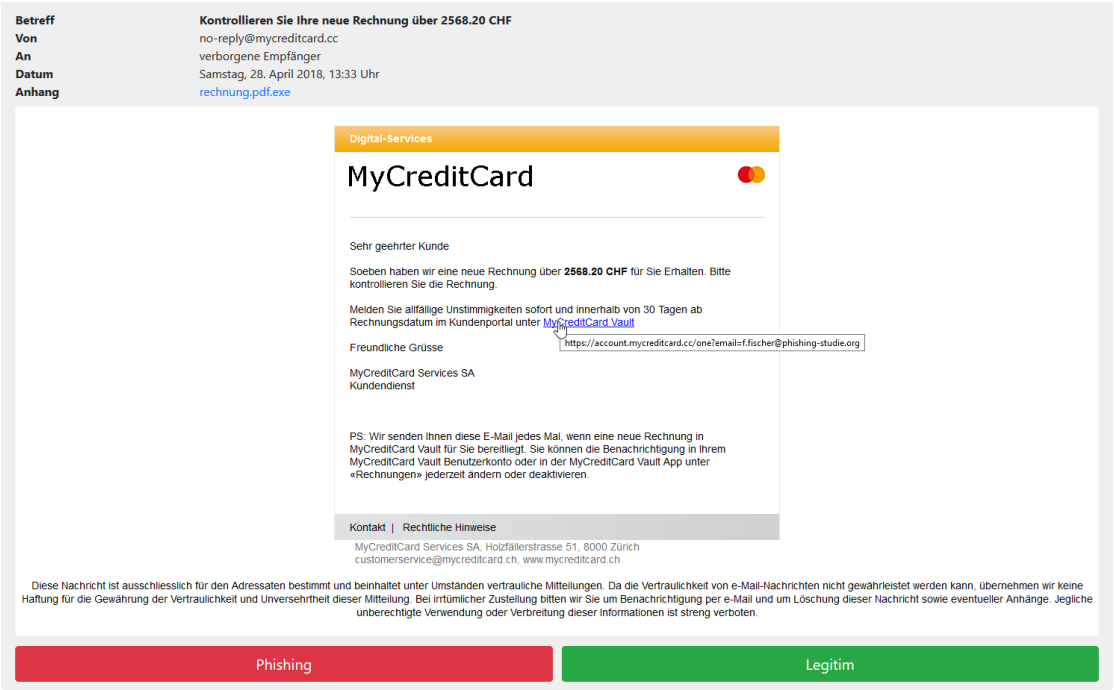


Abbildung A.16: Phishing-Studie-Applikation - Training - MyCreditCard - ungelöst

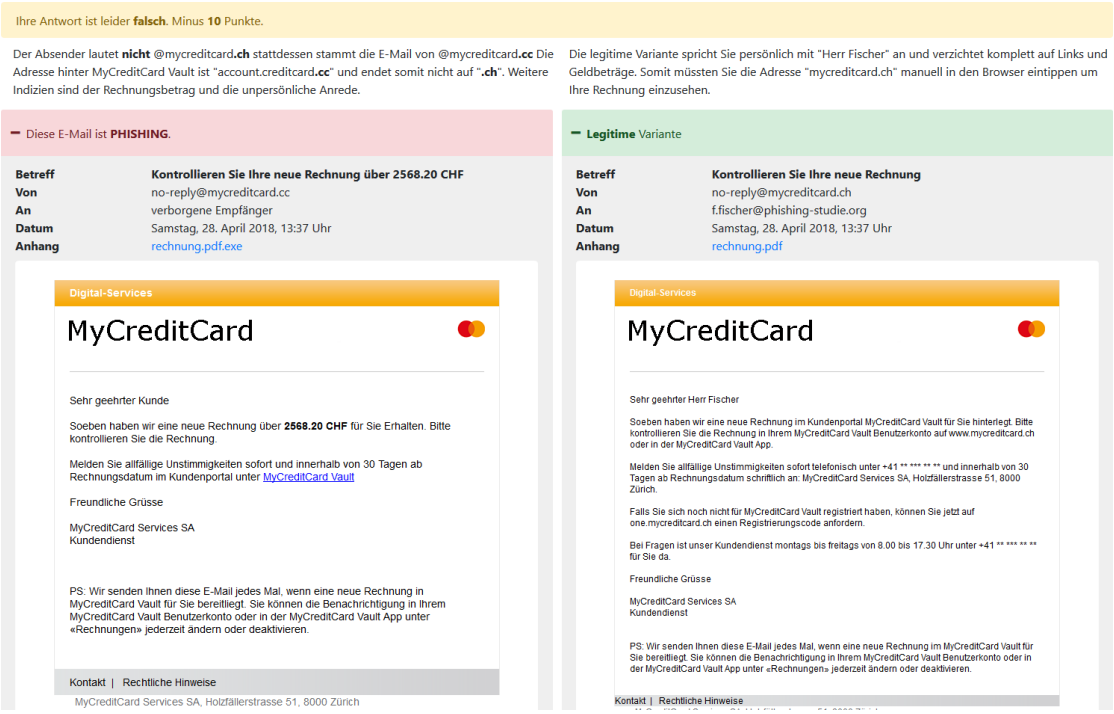


Abbildung A.17: Phishing-Studie-Applikation - Training - MyCreditCard - gelöst

Abbildung A.18: Phishing-Studie-Applikation - Training - Malware-Anhang

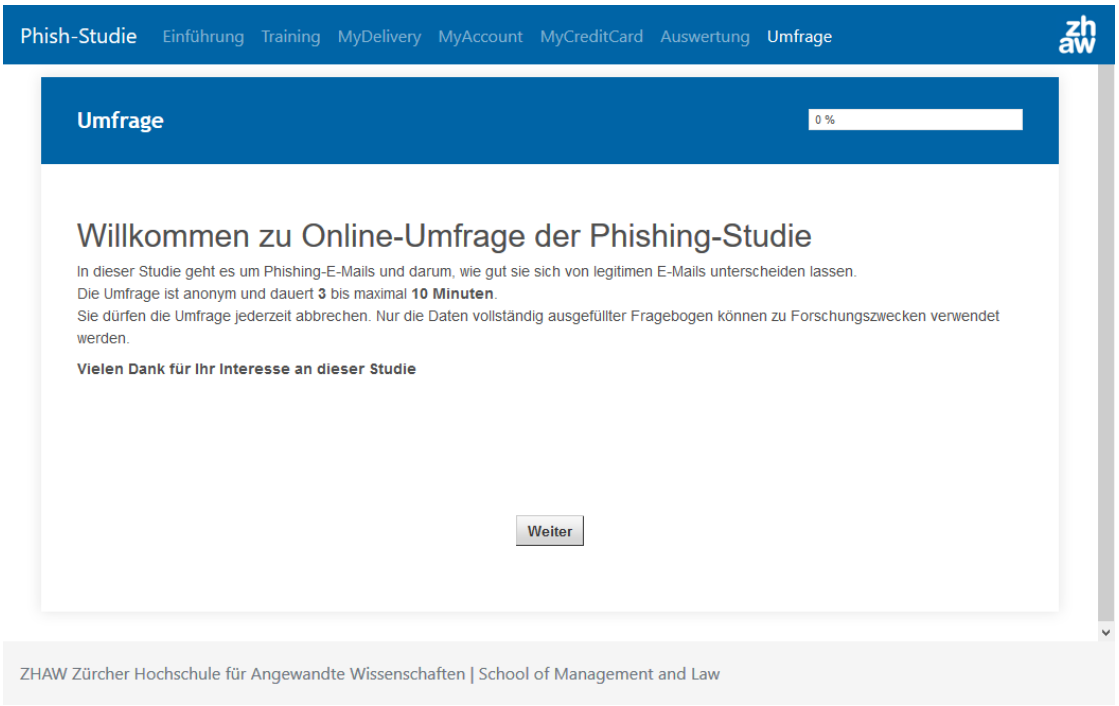


Abbildung A.19: Phishing-Studie-Applikation - Umfrage

A.2 Die Online-Umfrage

Abbildung A.20: Umfrage - Willkommen

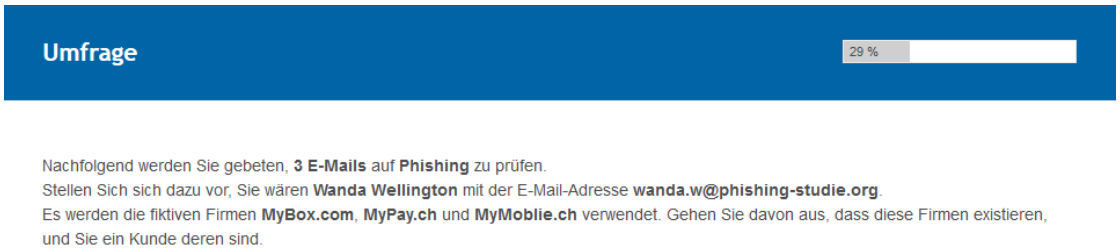


Abbildung A.21: Umfrage - Intermezzo

Abbildung A.22: Umfrage - Abschluss

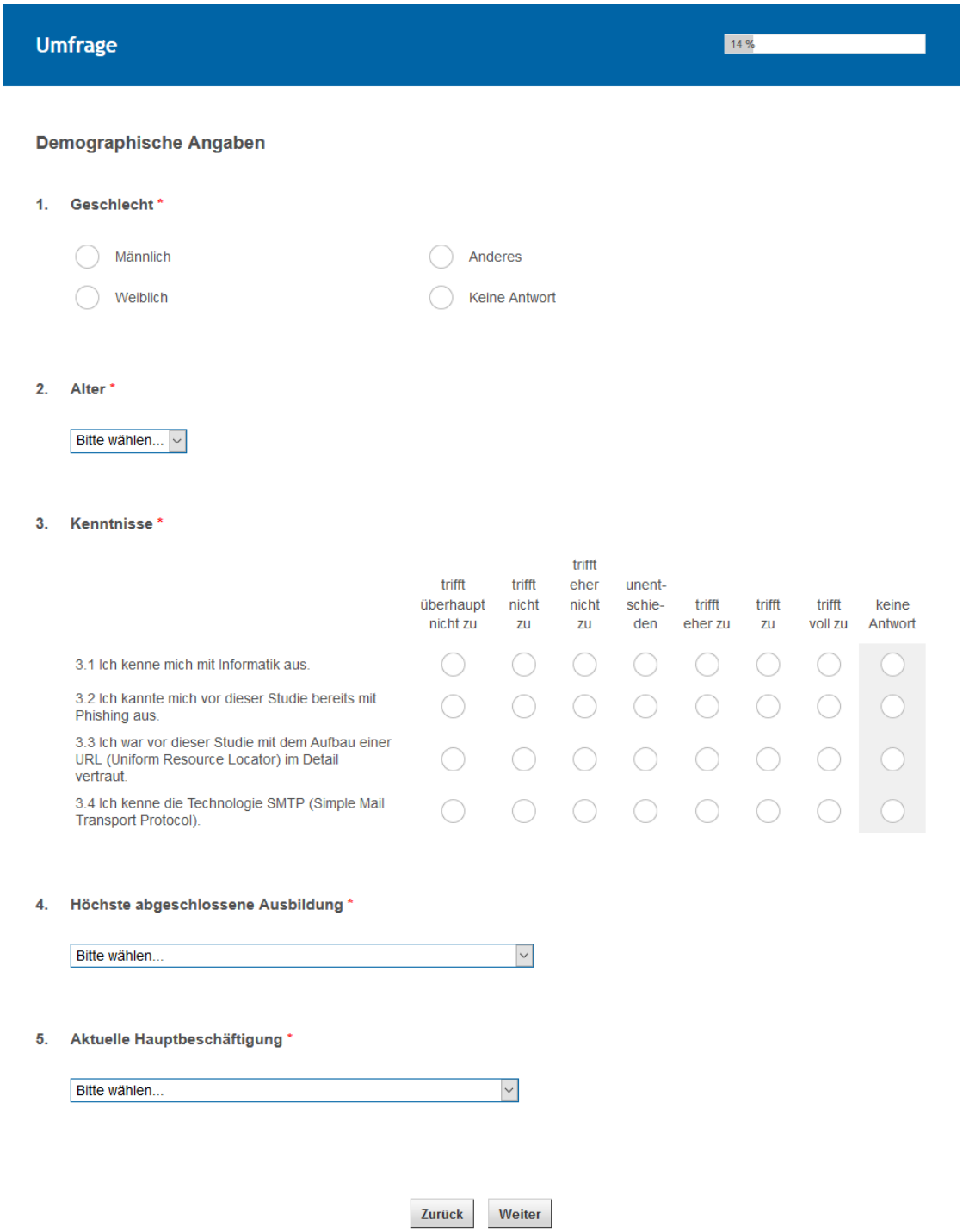


Abbildung A.23: Umfrage - Demografische Angaben

E-Mail von MyMobile

Gehen Sie davon aus, dass Sie **MyMobile.ch** kennen und Kunde dieser fiktiven Firma sind.
Hinweis: Ihre E-Mail lautet "wanda.w@phishing-studie.org"

M. Bitte betrachten Sie diese E-Mail genau und beantworten Sie die unten stehenden Fragen.

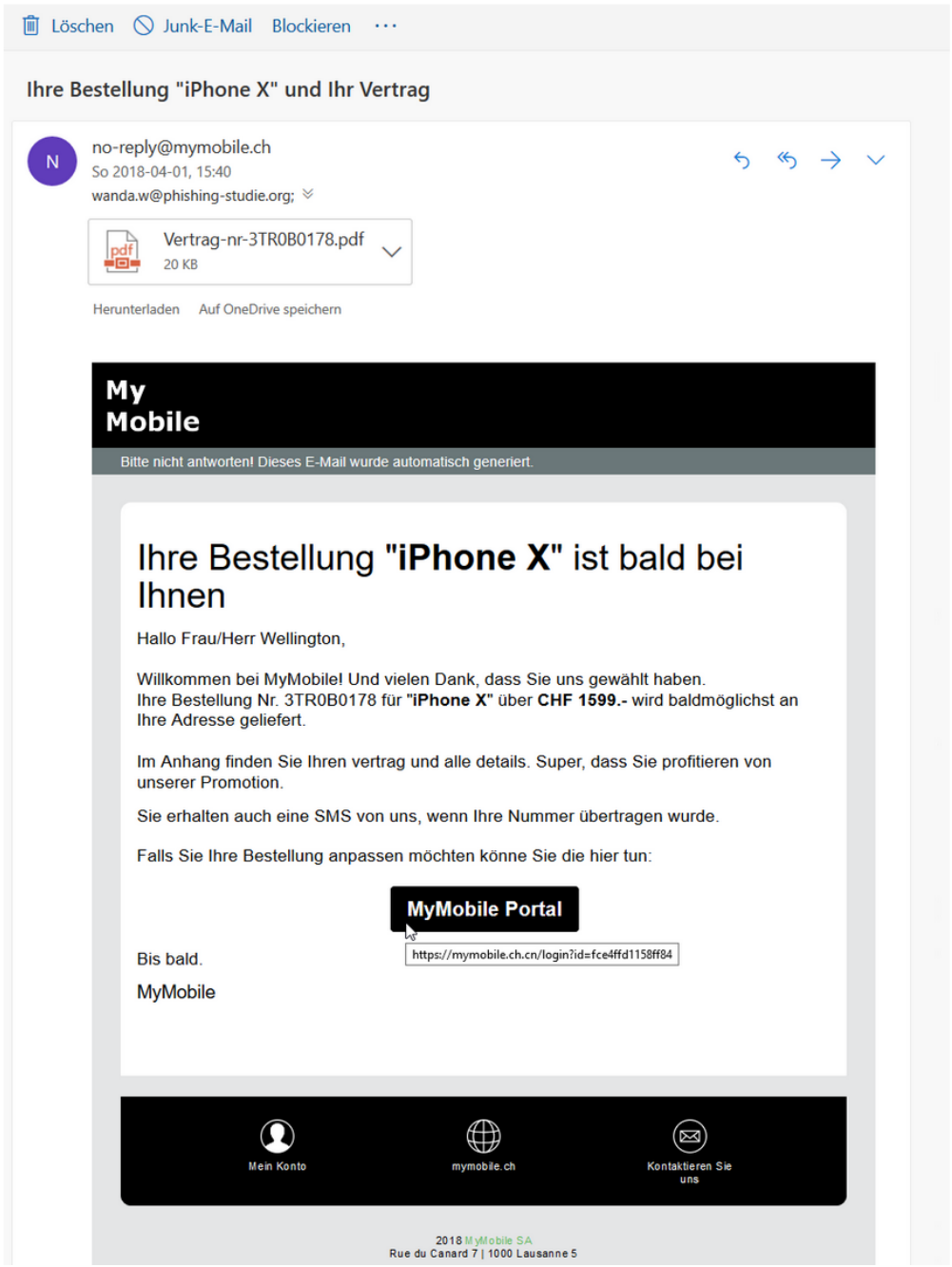


Abbildung A.24: Umfrage - Fall - MyMobile I

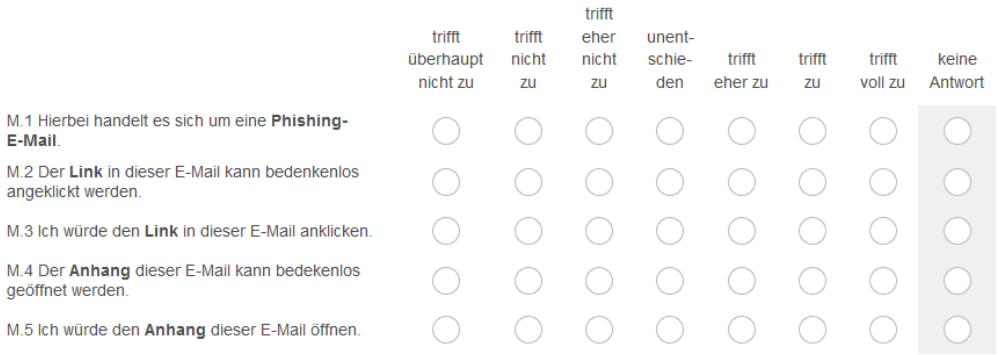


Abbildung A.25: Umfrage - Fall - MyMobile II

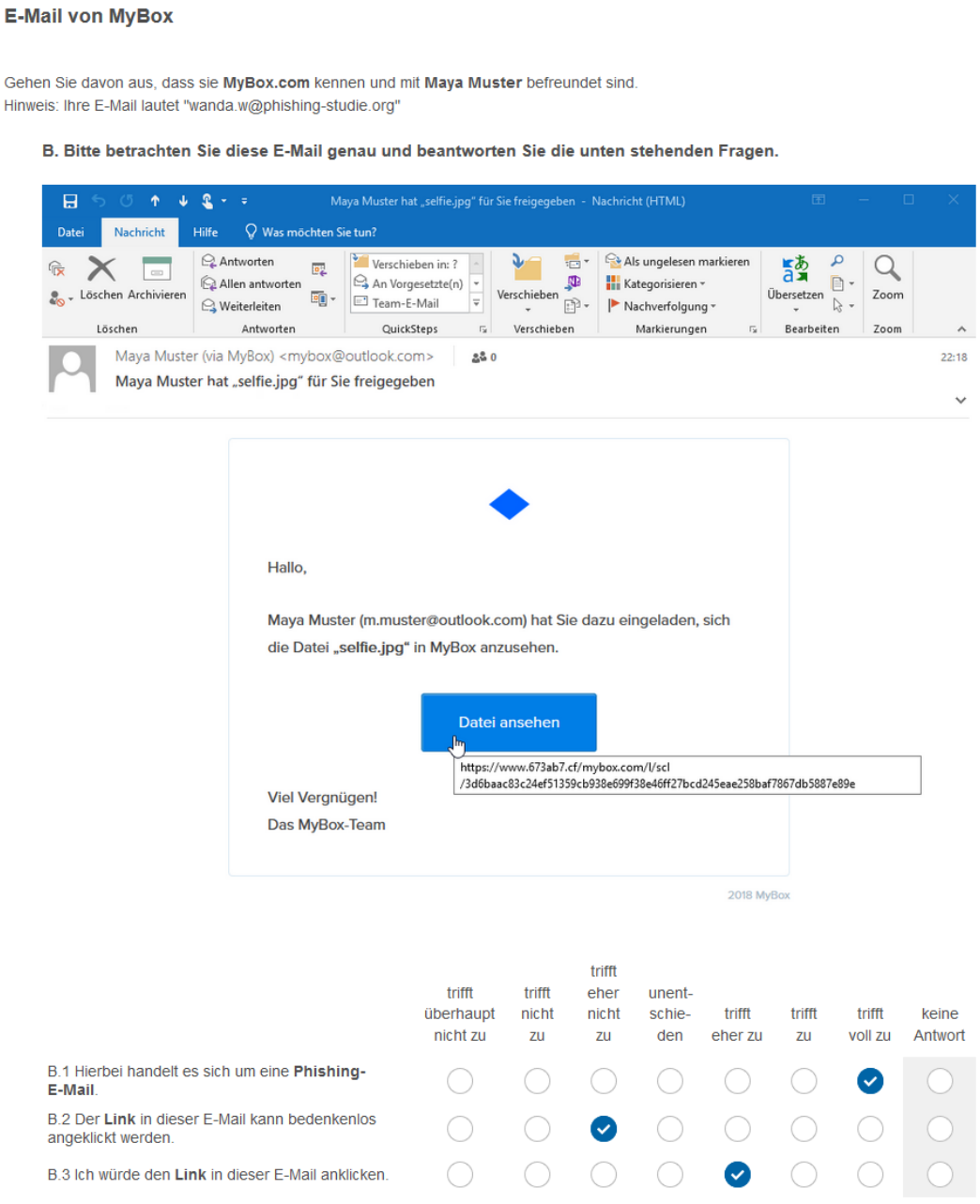
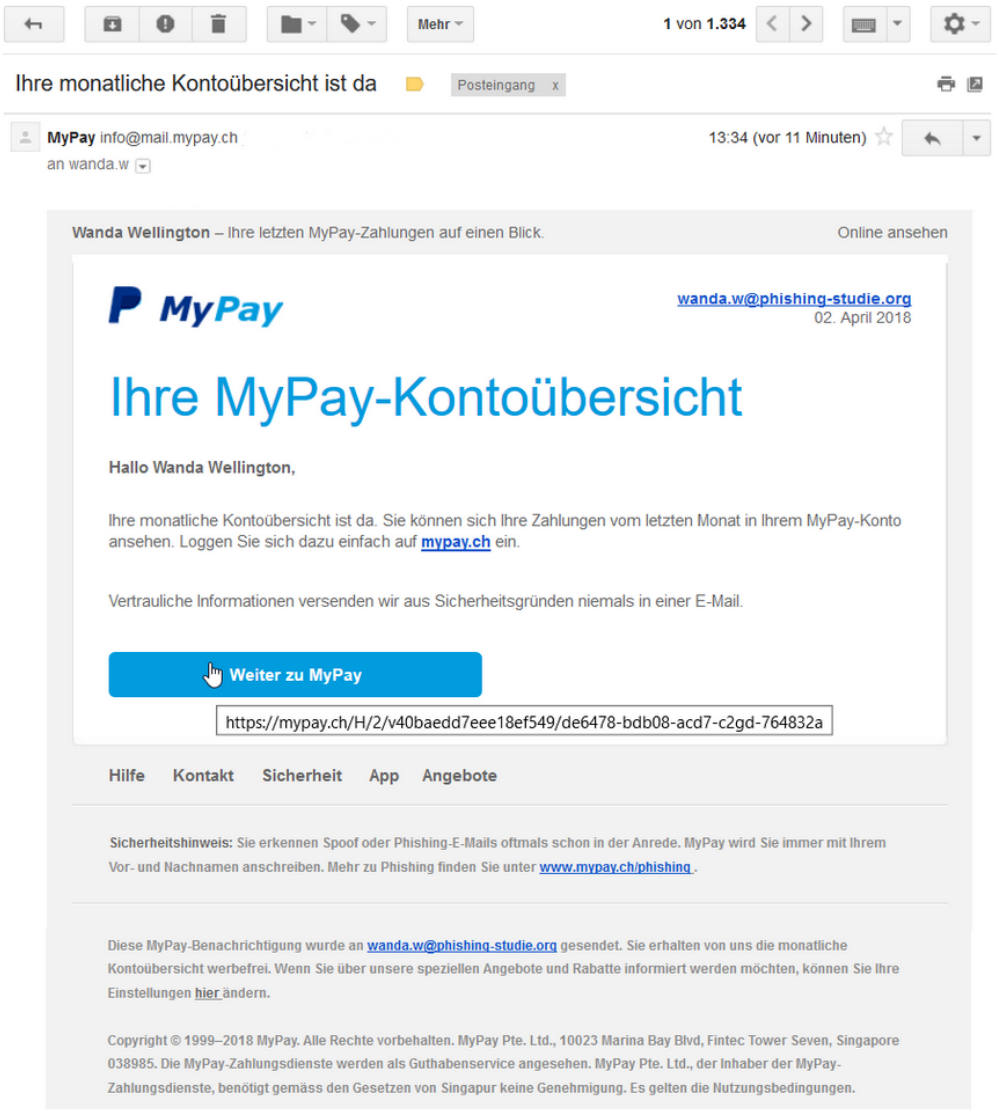


Abbildung A.26: Umfrage - Fall - MyBox

E-Mail von MyPay

Gehen Sie davon aus, dass Sie **MyPay.ch** kennen und Kunde dieser fiktiven Firma sind.
Hinweis: Ihre E-Mail lautet "wanda.w@phishing-studie.org"

P. Bitte betrachten Sie diese E-Mail genau und beantworten Sie die unten stehenden Fragen.



	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	unent-schie-den	trifft eher zu	trifft zu	trifft voll zu	keine Antwort
P.1 Hierbei handelt es sich um eine **Phishing-E-Mail**.	○	○	○	○	○	○	○	○
P.2 Der **Link** in dieser E-Mail kann bedenkenlos angeklickt werden.	○	○	○	○	○	○	○	○
P.3 Ich würde den **Link** in dieser E-Mail anklicken.	○	○	○	○	○	○	○	○

Abbildung A.27: Umfrage - Fall - MyPay

A.3 Diagramme

A.3.1 Pilot-Studie

A.3.1.1 Stichprobe

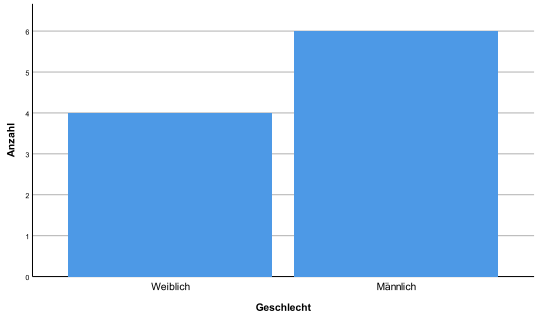


Abbildung A.28: Pilot-Studie - Histogramm - Geschlechterverteilung

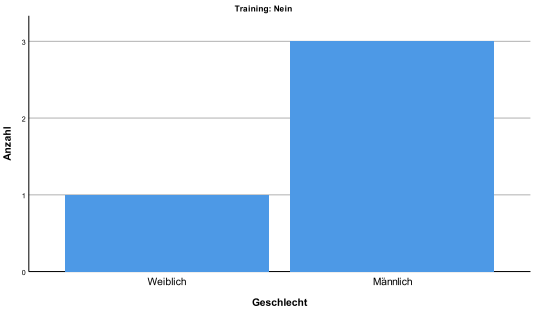


Abbildung A.29: Pilot-Studie - Histogramm - Geschlechterverteilung der Kontrollgruppe

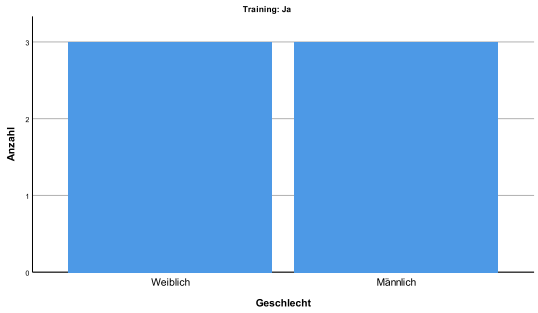


Abbildung A.30: Pilot-Studie - Histogramm - Geschlechterverteilung der Experimentalgruppe

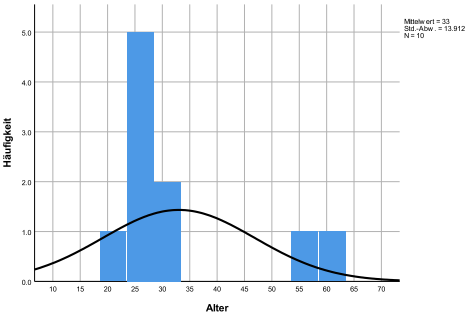


Abbildung A.31: Pilot-Studie - Histogramm - Altersverteilung

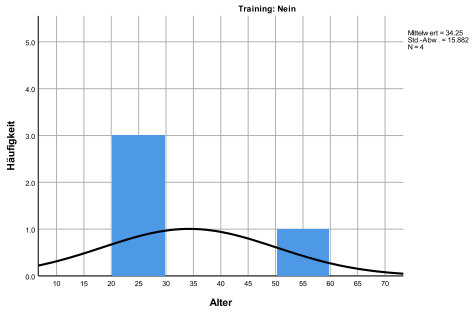


Abbildung A.32: Pilot-Studie - Histogramm - Altersverteilung der Kontrollgruppe

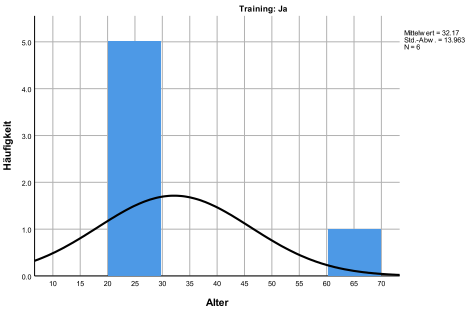


Abbildung A.33: Pilot-Studie - Histogramm - Altersverteilung der Experimentalgruppe

A.3.1.2 Deskriptive Statistik

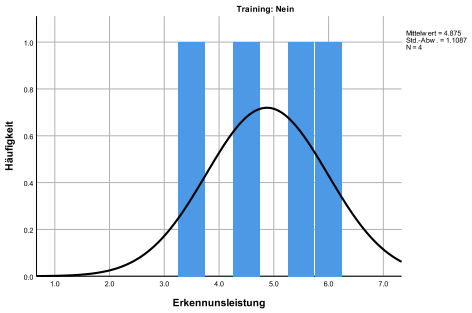


Abbildung A.34: Pilot-Studie - Histogramm der EKL der Kontrollgruppe

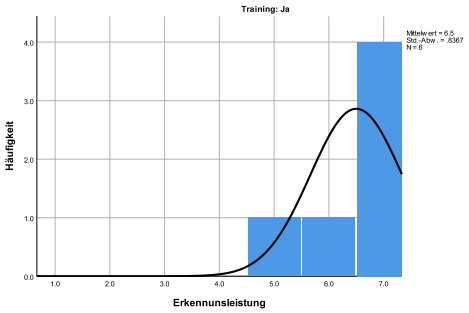


Abbildung A.35: Pilot-Studie - Histogramm der EKL der Experimentalgruppe

A.3.2 Hauptstudie

A.3.2.1 Stichprobe

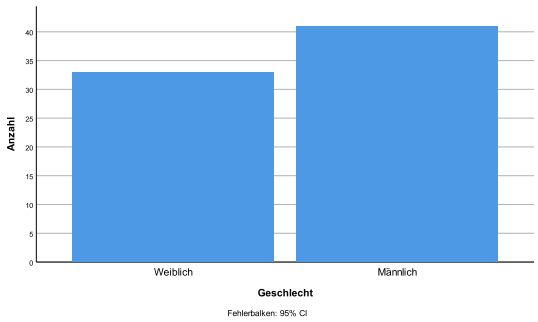


Abbildung A.36: Studie - Histogramm - Geschlechterverteilung

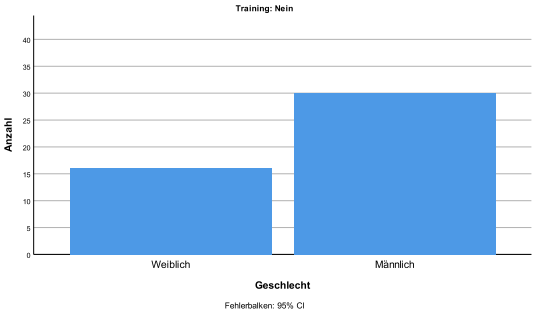


Abbildung A.37: Studie - Histogramm - Geschlechterverteilung der Kontrollgruppe

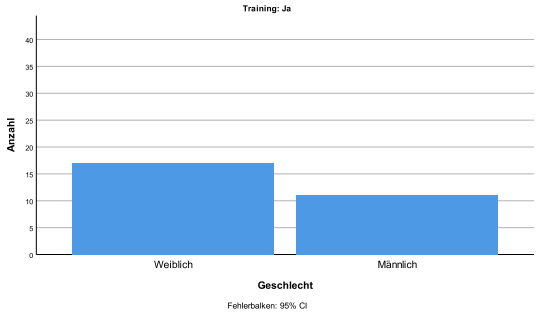


Abbildung A.38: Studie - Histogramm - Geschlechterverteilung der Experimentalgruppe

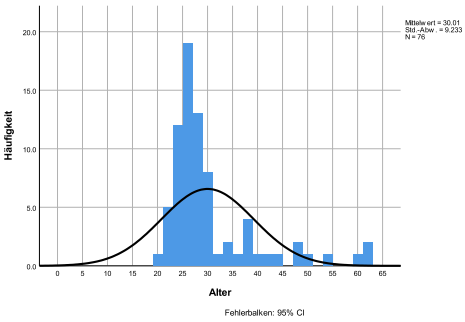


Abbildung A.39: Studie - Histogramm - Altersverteilung

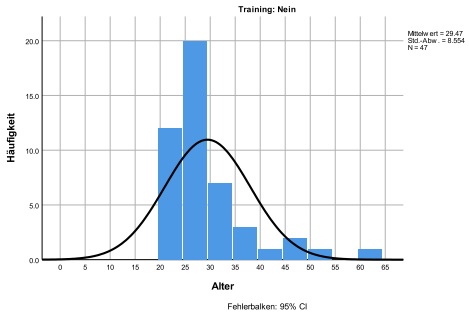


Abbildung A.40: Studie - Histogramm - Altersverteilung der Kontrollgruppe

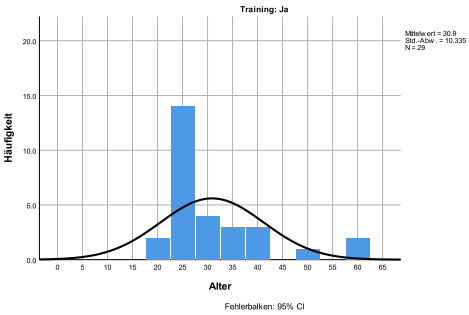


Abbildung A.41: Studie - Histogramm - Altersverteilung der Experimentalgruppe

A.3.2.2 Deskriptive Statistik

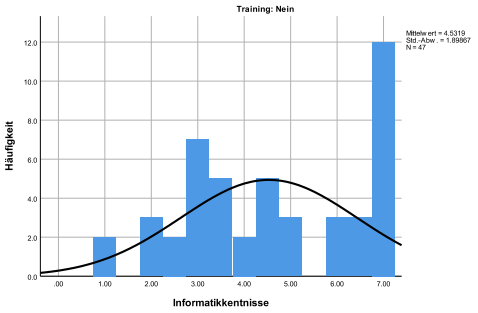


Abbildung A.42: Studie - Histogramm ITK Kontrollgruppe

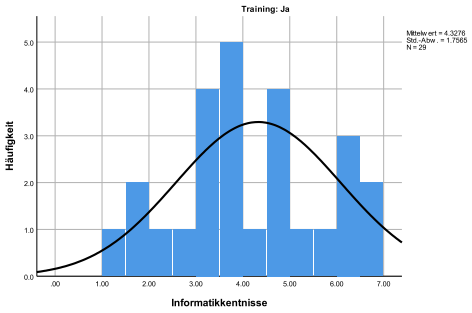


Abbildung A.43: Studie - Histogramm ITK Experimentalgruppe

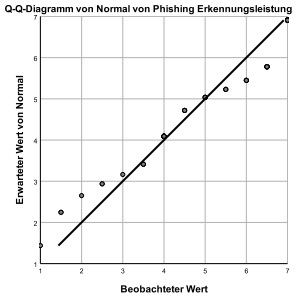


Abbildung A.44: Studie - Quantil-Quantil-Diagramm der EKL

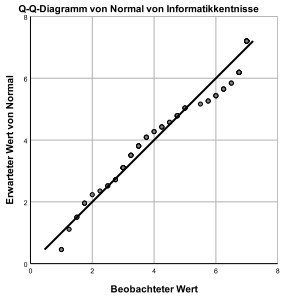


Abbildung A.45: Studie - Quantil-Quantil-Diagramm der ITK

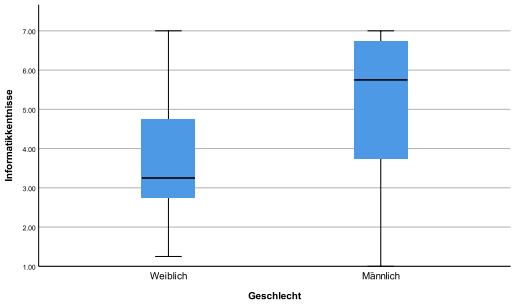


Abbildung A.46: Studie - Box-Plot der ITK nach Geschlecht

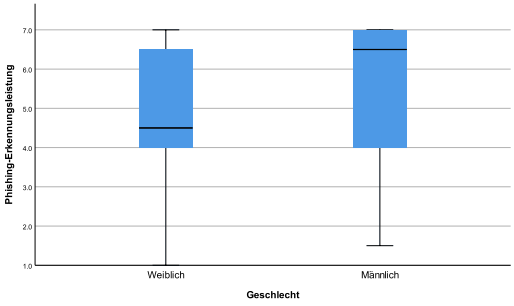


Abbildung A.47: Studie - Box-Plot der EKL nach Geschlecht

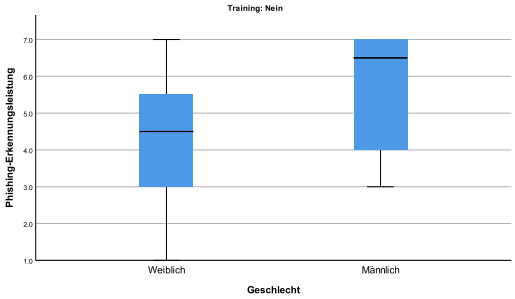


Abbildung A.48: Studie - Box-Plot der EKL nach Geschlecht in der Kontrollgruppe

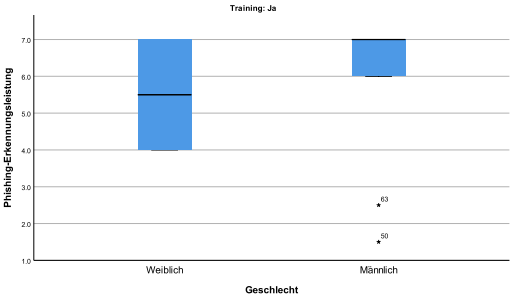


Abbildung A.49: Studie - Box-Plot der EKL nach Geschlecht in der Experimentalgruppe

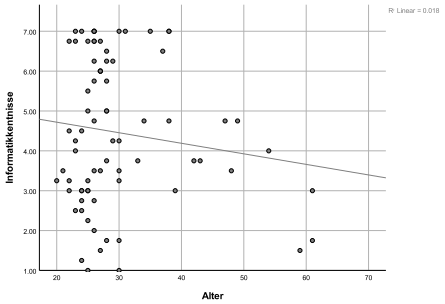


Abbildung A.50: Studie - Streudiagramm der ITK nach Alter

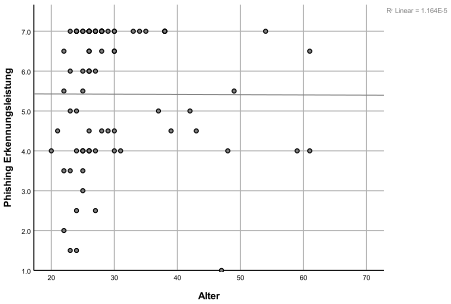


Abbildung A.51: Studie - Streudiagramm der EKL nach Alter

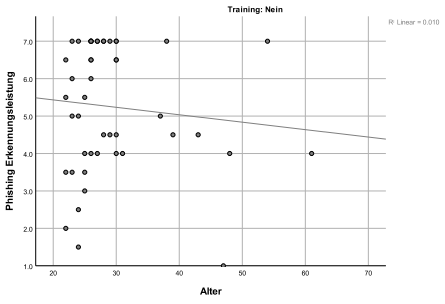


Abbildung A.52: Studie - Streudiagramm der EKL nach Alter in der Kontrollgruppe

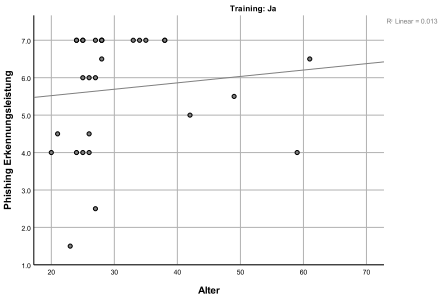


Abbildung A.53: Studie - Streudiagramm der EKL nach Alter in der Experimentalgruppe

A.3.3 Auswertung pro Fall

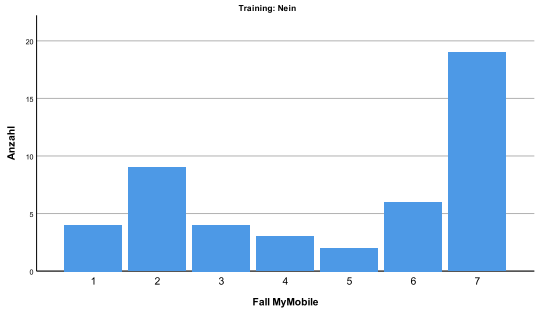


Abbildung A.54: Auswertung - Fall MyMobile - Kontrollgruppe

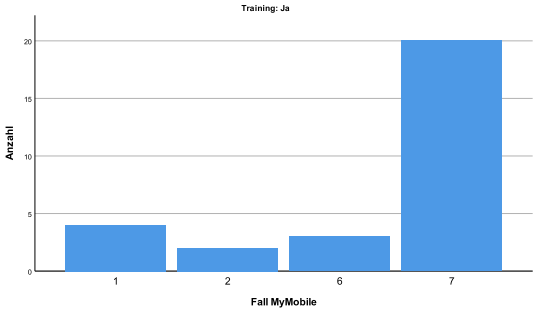


Abbildung A.55: Auswertung - Fall MyMobile - Experimentalgruppe

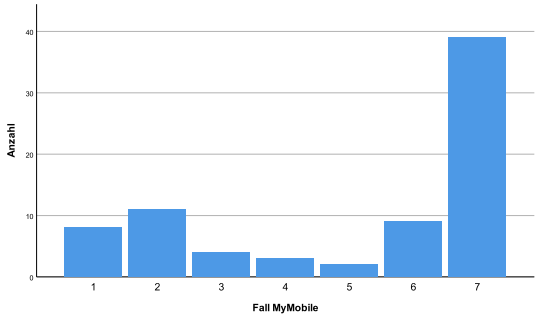


Abbildung A.56: Auswertung - Fall MyMobile

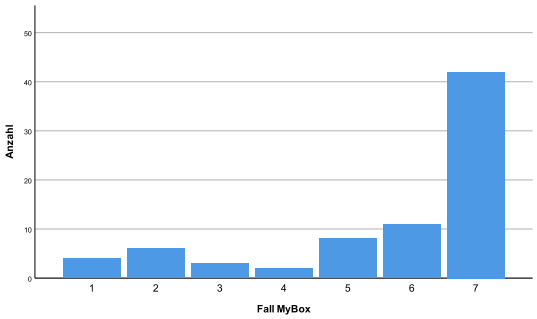


Abbildung A.57: Auswertung - Fall MyBox

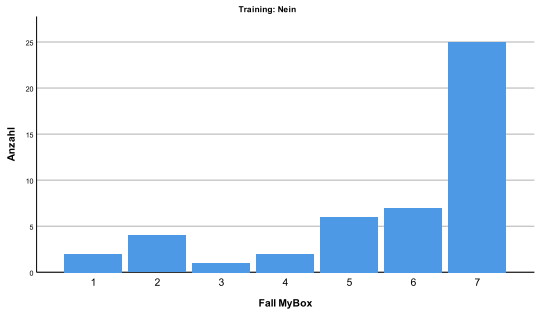


Abbildung A.58: Auswertung - Fall MyBox - Kontrollgruppe

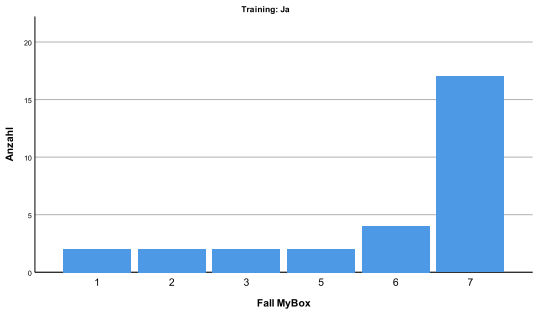


Abbildung A.59: Auswertung - Fall MyBox - Experimentalgruppe

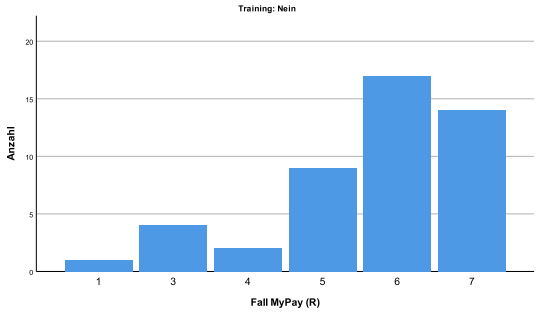


Abbildung A.60: Auswertung - Fall MyPay - Kontrollgruppe

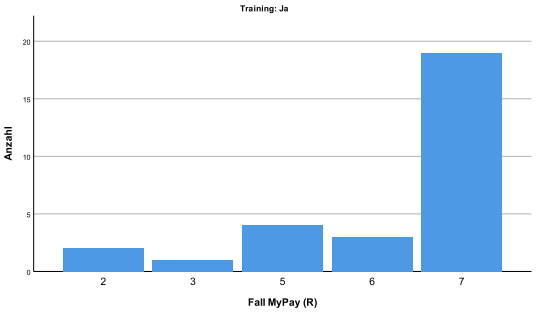


Abbildung A.61: Auswertung - Fall MyPay - Experimentalgruppe

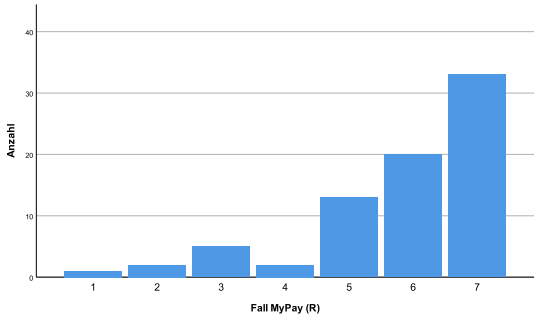


Abbildung A.62: Auswertung - Fall MyPay

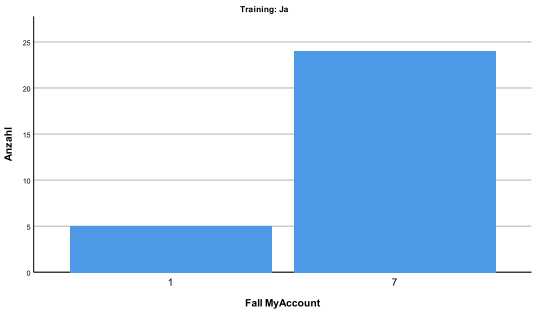


Abbildung A.63: Auswertung - Fall MyAccount - Experimentalgruppe

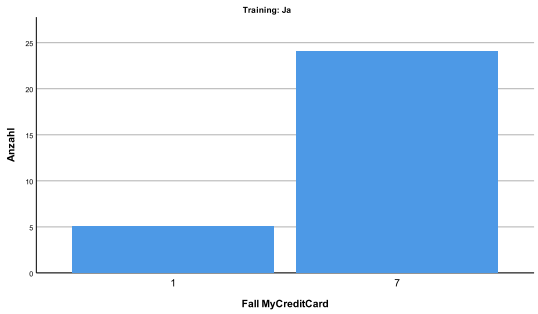


Abbildung A.64: Auswertung - Fall MyCreditCard - Experimentalgruppe

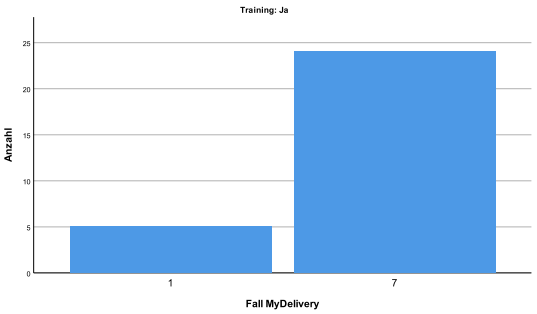


Abbildung A.65: Auswertung - Fall MyDelivery - Experimentalgruppe

A.4 Inhalt des Datenträgers

Den gedruckten Exemplaren dieser Arbeit liegt ein Datenträger bei, auf welchem die Masterthesis in digitaler Form gespeichert ist. Die Thesis liegt im Verzeichnis *Masterthesis* als PDF-Datei und im Unterverzeichnis *Latex* im LaTeX-Format vor, welches ins PDF-Format übersetzt werden kann. Auf dem Datenträger sind ebenfalls die ausgewerteten *Daten* der Pilot- und Hauptstudie im SPSS- und Excel-Format vorhanden. Die verwendeten Quellen liegen im BibLaTex-Format und als HTML-Report vor, ebenfalls ist die referenzierte *Literatur* soweit als möglich im PDF-Format beigelegt. Der gesamte *Quellcode* der *Phishing-Studie-Applikation* ist auf dem Datenträger archiviert. Zusätzlich ist eine Ubuntu 18.4 LTS Installation als virtuelle Maschine (VM) im VM-Ware-Format mit einer Ruby und Datenbankinstallation verfügbar, um die App mit geringem Aufwand auszuführen. Das Passwort für den Benutzer der VM lautet ‘phisher’ ohne Anführungszeichen. Auf dem Desktop der VM ist ein Shell-Skript gespeichert, welches im Terminal ausgeführt werden kann. Das Shell-Skript startet die App und öffnet die Startseite der App im Firefox-Browser. Auf der beiliegenden DVD wurde die VM aus Platzgründen gepackt und muss vorgängig extrahiert werden. Ausserdem funktioniert eine VM auf einem schreibgeschützten Speichermedium nur eingeschränkt. Falls dieser Arbeit ebenfalls eine SD-Karte beiliegt, ist darauf die bereits entpackte VM vorhanden. Aus Archivierungsgründen ist die *Software* um PDFs anzuzeigen, LaTeX zu übersetzen und die VM zu verwenden ebenfalls abgelegt. Die Software ist unter Windows 10 Build 1803 lauffähig. Folgend eine Auflistung der wichtigsten Dateien und Verzeichnisse des Datenträgers.

```
Datenträger
├── Masterthesis
│   ├── Masterthesis.pdf
│   └── Latex
│       ├── bibliography
│       ├── content
│       ├── image
│       ├── matter
│       ├── style
│       └── thesis.tex
├── Daten
│   ├── Pilot-Studie
│   │   ├── pilot-studie-spss.sav
│   │   └── pilot-studie-umfrage.xlsx
│   └── Studie
│       ├── phishing-studie-spss.sav
│       ├── phishing-studie-training-und-umfrage.xlsx
│       └── phishing-studie-umfrage.xlsx
├── Literatur
│   ├── files
│   ├── report.html
│   └── sources.bib
├── Phishing-Studie-Applikation
│   ├── Quellcode
│   └── Virtual-Machine[.7z]
└── Software
    ├── 7-Zip
    ├── Adobe Acrobat Reader
    ├── MiKTeX
    ├── TeXstudio
    └── VMware Player
```

Literaturverzeichnis

Aaron, G. (2010). The State of Phishing. *Computer Fraud & Security*, *2010* (6), 5-8. https://doi.org/10.1016/S1361-3723(10)70065-8

Abraham, S. & Chengalur-Smith, I. (2010). An Overview of Social Engineering Malware: Trends, Tactics, and Implications. *Technology in Society*, *32* (3), 183-196. https://doi.org/10.1016/j.techsoc.2010.07.001

Aburrous, M., Hossain, M. A., Dahal, K. & Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Cognitive Computation*, *2* (3), 242-253. https://doi.org/10.1007/S12559-010-9042-7

Ajzen, I. & Fishbein, M. (1977). Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin*, *84* (5), 888-918. https://doi.org/10.1037/0033-2909.84.5.888

Ajzen, I. & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviour*. Prentice-Hall.

AlamgirKhan, A. (2013). Preventing Phishing Attacks Using One Time Password and User Machine Identification. *International Journal of Computer Applications*, *68* (3), 7-11. https://doi.org/10.5120/11557-6839

Aleroud, A. & Zhou, L. (2017). Phishing Environments, Techniques, and Countermeasures: A Survey. *Computers & Security*, *68* (5), 45. https://doi.org/10.1016/j.cose.2017.04.006

Allen, I. E. & Seaman, C. A. (2007). Likert Scales and Data Analyses. *Quality Progress*, *40* (7), 64-65.

Anderson, J. R. (1976). *Language, Memory, and Thought*. Psychology Press.

APWG. (o. J.). *Welcome to APWG & CMU's Phishing Education Landing Page.* Abgerufen von http://phish-education.apwg.org/r/

APWG. (2016). *Global Phishing Survey: Trends and Domain Name Use in 2016.* Abgerufen von https://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

APWG. (2017a). *Phishing Activity Trends Report, 1st Half 2017.* Abgerufen von http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf

APWG. (2017b). *Phishing Activity Trends Report 3rd Quarter 2017.* Abgerufen von http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf

APWG. (2018a). *About the APWG.* Abgerufen von https://www.antiphishing.org/about-APWG/

APWG. (2018b). *Unifying the Global Response to Cybercrime | APWG.* Abgerufen von https://www.antiphishing.org/

APWG & SISA. (2018). *Stop.Think.Connect.* Abgerufen von https://www.stopthinkconnect.ch/en/phishing.html

Arachchilage, N. A. G. & Cole, M. (2011). Design a Mobile Game for Home Computer Users to Prevent from "phishing Attacks". In *International Conference on Information Society* (S. 485-489). London, England.

Arachchilage, N. A. G. & Hameed, M. A. (2017). Integrating Self-Efficacy into a Gamified Approach to Thwart Phishing Attacks. *Computing Research Repository*, *abs/1706.07748*.

Arachchilage, N. A. G. & Love, S. (2013). A Game Design Framework for Avoiding Phishing Attacks. *Computers in Human Behavior*, *29* (3), 706-714. https://doi.org/10.1016/j.chb.2012.12.018

Arachchilage, N. A. G. & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior*, *38* (Supplement C), 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S. & Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior*, *60* (Supplement C), 185-197. https://doi.org/10.1016/j.chb.2016.02.065

Atkins, B. & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, *1* (3), 10.

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84* (2), 191-215. https://doi.org/10.1037/0033-295X.84.2.191

Banu, M. N. & Banu, S. M. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies*, *4* (6), 783-786.

Barth, A. (2011). *Http State Management Mechanism* (RFC Nr. 6256). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/pdf/rfc6265.pdf

Benenson, Z., Gassmann, F. & Landwirth, R. (2017). Unpacking Spear Phishing Susceptibility. In M. Brenner et al. (Hrsg.), *Financial Cryptography and Data Security* (S. 610-627). Springer International Publishing.

Benesty, J., Chen, J., Huang, Y. & Cohen, I. (2009). Pearson Correlation Coefficient. In *Noise Reduction in Speech Processing* (S. 1-4). Berlin, Deutschland: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-00296-0_5

Beobachter. (2017). *Phishing: Immer raffiniertere Betrugsversuche.* Abgerufen von https://www.beobachter.ch/konsum/konsumentenschutz/phishing-immer-raffiniertere-betrugsversuche

Bin, S., Qiaoyan, W. & Xiaoying, L. (2010). A DNS Based Anti-Phishing Approach. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (Bd. 2, S. 262-265). https://doi.org/10.1109/NSWCTC.2010.196

Brewer, R. (2016). Ransomware Attacks: Detection, Prevention and Cure. *Network Security*, *2016* (9), 5-9. https://doi.org/10.1016/S1353-4858(16)30086-1

Brown, M. B. & Forsythe, A. B. (1974). Robust Tests for the Equality of Variances. *Journal of the American Statistical Association*, *69* (346), 364-367. https://doi.org/10.2307/2285659

Browner, W. S., Newman, T. B. & Hulley, S. B. (2007). Estimating Sample Size and Power: Applications and Examples. *Designing clinical research*, *3*, 367.

BSI. (2008). *IT-Grundschutz-Vorgehensweise* (BSI-Standard 100-2). Bonn, Deutschland: Autor. Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile

BSI. (2016). *Die Lage der IT-Sicherheit in Deutschland 2016.* Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/%0020Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34* (3), 523-548.

Chandrasekaran, M., Narayanan, K. & Upadhyaya, S. J. (2006). Phishing E-Mail Detection Based on Structural Properties. In *NYS Cyber Security Conference* (S. 7). New York, NY.

Chaudhary, G. K. (2014). Development Review on Phishing: A Computer Security Threat. *International journal of advance research in computer science and management studies*, *2* (8), 55-64.

Chaudhry, J. A., Chaudhry, S. A. & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. *International Journal of Security and its Applications*, *10* (1), 247-256. https://doi.org/10.14257/ijsia.2016.10.1.23

Chen, C. C., Shaw, R. S. & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal*, *24* (1), 1-14.

Chen, X., Bose, I., Leung, A. C. M. & Guo, C. (2011). Assessing the Severity of Phishing Attacks: A Hybrid Data Mining Approach. *Enterprise Risk and Security Management: Data, Text and Web Mining*, *50* (4), 662-672. https://doi.org/10.1016/j.dss.2010.08.020

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, *112* (1), 155.

Cook, T. D., Campbell, D. T. & Shadish, W. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Houghton Mifflin Bo-

ston.

Cortina, J. M. (1993). What Is Coefficient Alpha? An Examination of Theory and Applications. *Journal of applied psychology*, *78* (1), 98.

Cranor, L. F., Egelman, S., Hong, J. I. & Zhang, Y. (2007). Phinding Phish: An Evaluation of Anti-Phishing Toolbars. In *NDSS* (S. 20). Pittsburgh, PA: Carnegie Mellon University.

Credit Suisse. (2015). *Important Security Factor – Your Awareness.* Abgerufen von https://www.credit-suisse.com/ch/en/privatkunden/online-und-mobile-banking/sicherheit/sicherheitsfaktor.html

Davis, F. D. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results* (Dissertation). Massachusetts Institute of Technology.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13* (3), 319-340. https://doi.org/10.2307/249008

Denning, T., Lerner, A., Shostack, A. & Kohno, T. (2013). Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the 2013 ACM SIGSAC conference on computer and communications security* (S. 915-928). Berlin, Deutschland: ACM. https://doi.org/10.1145/2508859.2516753

De Vaus, D. (2013). *Surveys in Social Research.* Routledge.

De Winter, J. & Dodou, D. (2010). Five-Point Likert Items: T Test Versus Mann–Whitney–Wilcoxon. *Practical Assessment, Research and Evaluation*, *15*, 17.

Dhamija, R., Tygar, J. D. & Hearst, M. (2006). Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (S. 581–590). Montreal, Kanada: ACM. https://doi.org/10.1145/1124772.1124861

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P. & Kaiser, S. (2012). Guidelines for Choosing Between Multi-Item and Single-Item Scales for Construct Measurement: A Predictive Validity Perspective. *Journal of the Academy of Mar-*

keting Science, *40* (3), 434-449. https://doi.org/10.1007/s11747-011-0300-3

Dodge, R. C., Carver, C. & Ferguson, A. J. (2007). Phishing for User Security Awareness. *Computers & Security*, *26* (1), 73-80. https://doi.org/10.1016/j.cose.2006.10.009

Döring, N. & Bortz, J. (2016). *Forschungsmethoden und Evaluation*. Heidelberg: Springer.

Downs, J. S., Holbrook, M. & Cranor, L. F. (2007). Behavioral Response to Phishing Risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (S. 37-44). Pittsburgh, PA: ACM. https://doi.org/10.1145/1299015.1299019

Downs, J. S., Holbrook, M. B. & Cranor, L. F. (2006). Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (S. 79–90). Pittsburgh, PA: ACM. https://doi.org/10.1145/1143120.1143131

Dunlop, M., Groat, S. & Shelly, D. (2010). Goldphish: Using Images for Content-Based Phishing Analysis. In *2010 Fifth International Conference on Internet Monitoring and Protection* (S. 123-128). https://doi.org/10.1109/ICIMP.2010.24

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2018). *Datenschutz und Forschung im Allgemeinen.* Abgerufen von https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/statistik--register-und-forschung/forschung/datenschutz-und-forschung-im-allgemeinen.html

Eifler, S. (2014). Experiment. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 195-209). Wiesbaden, Deutschland: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0_11

Eisinga, R., Te Grotenhuis, M. & Pelzer, B. (2013). The Reliability of a Two-Item Scale: Pearson, Cronbach, or Spearman-Brown? *International Journal of Public Health*, *58* (4), 637-642. https://doi.org/10.1007/s00038-012-0416-3

Emily Schechter. (2018a). *Evolving Chrome's Security Indicators.* Abgerufen von https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

Emily Schechter. (2018b). *A Secure Web Is Here to Stay.* Abgerufen von https://

security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

European Union. (o. J.). *Guidance on Upcoming New Data Protection Rules Across the EU - EUR-Lex.* Abgerufen von https://eur-lex.europa.eu/content/news/guidance-for-general-data-protection-regulation-application.html

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, *L119*, 1-88. Abgerufen von http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Evans, N. J. (2009). *Information Technology Social Engineering: An Academic Definition and Study of Social Engineering - Analyzing the Human Firewall* (Dissertation). Iowa State University, Ann Arbor, MI.

FBI IC3. (2014). *Internet Crime Complaint Center (IC3) | Business E-Mail Compromise: The 3.1 Billion Dollar Scam.* Abgerufen von https://www.ic3.gov/media/2016/160614.aspx

FBI IC3. (2016). *Internet Crime Report 2016.* Abgerufen von https://pdf.ic3.gov/2016_IC3Report.pdf

Fennema, E. & Sherman, J. A. (1976). Fennema-Sherman Mathematics Attitudes Scales: Instruments Designed to Measure Attitudes toward the Learning of Mathematics by Females and Males. *Journal for Research in Mathematics Education*, *7* (5), 324-326. https://doi.org/10.2307/748467

Fishbein, M. & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*.

Fisher, R. A. (1925). *Statistical Methods for Research Workers*. Genesis Publishing Pvt Ltd.

Fisher, R. A. (1926). Introduction to “the Arrangement of Field Experiments”. *The journal of the Ministry of Agriculture*, *33*, 503-13.

Fisher, R. A. (1935). The Design of Experiments. *Oliver and Boyd, Edinburgh*.

Ford, J. (1983). How Random Is a Coin Toss? *Physics Today*, *36*, 40-47.

Free Software Foundation. (2007a). *Gnu Affero General Public License.* Abgerufen von https://www.gnu.org/licenses/agpl-3.0.en.html

Free Software Foundation. (2007b). *Gnu General Public License.* Abgerufen von https://www.gnu.org/licenses/gpl.html

Free Software Foundation. (2015). *Why the Affero GPL.* Abgerufen von https://www.gnu.org/licenses/why-affero-gpl.en.html

Geer, D. (2005). Security Technologies Go Phishing. *Computer*, *38* (6), 18-21. https://doi.org/10.1109/MC.2005.201

Georgiev, M. (2015). *U.S. Patent No. 9083733 - Anti-Phishing Domain Advisor and Method Thereof.* Washington, DC: U.S. Patent and Trademark Office.

Goodman, J. T., Rehfuss, P. S., Rounthwaite, R. L., Mishra, M., Hulten, G. J., Kenneth G. Richards, ... Roderic C. Deyo (2005). *U.S. Patent No. 7634810 - Phishing Detection, Prevention, and Notification.* Washington, DC: U.S. Patent and Trademark Office.

Goodman, S. (2008). A Dirty Dozen: Twelve p-Value Misconceptions. *Seminars in Hematology*, *45* (3), 135-140. https://doi.org/10.1053/j.seminhematol.2008.04.003

Google. (2018). *Helping G Suite Customers Stay Secure with New Proactive Phishing Protections and Management Controls.* Abgerufen von https://www.blog.google/products/g-suite/helping-g-suite-customers-stay-secure-new-proactive-phishing-protections-and-management-controls/

GovCERT. (2018). *GovCERT.ch - Phishing Statistic.* Abgerufen von https://www.govcert.admin.ch/statistics/phishing/#

Gupta, D. S., Tanbeer, S. K. & Mohandas, R. (2017). *U.S. Patent No. 9621566 - System and Method for Detecting Phishing Webpages.* Washington, DC: U.S. Patent and Trademark Office.

Gupta, S., Singhal, A. & Kapoor, A. (2016). A Literature Survey on Social Engineering Attacks: Phishing Attack. In *2016 International Conference on Computing, Communication and Automation* (S. 537-540). Greater Noida, Indien: IEEE. https://doi.org/10.1109/CCAA.2016.7813778

Hansen, T., Kucherawy, M. & Crocker, D. (2011). *DomainKeys Identified Mail (DKIM) Signatures* (RFC Nr. 6376). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/html/rfc6376

Hardy, S., Crete-Nishihata, M., Kleemola, K., Senft, A., Sonne, B., Wiseman, G., … Deibert, R. J. (2014). Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware. In *USENIX Security Symposium* (S. 527-541).

Harrington, S., Anderson, C. & Agarwal, R. (2006). Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions. In (S. 21).

Herley, C. & Florêncio, D. (2008). A profitless endeavor: Phishing as tragedy of the commons. In *Proceedings of the 2008 New Security Paradigms Workshop* (S. 59-70). Lake Tahoe, CA: ACM.

Hochschule Luzern. (2018a). *Phishing-Test.* Abgerufen von https://www.ebas.ch/de/ihr-sicherheitsbeitrag/phishing/phishing-test

Hochschule Luzern. (2018b). *Phishing und wie Sie sich davor schützen.* Abgerufen von https://www.ebankingabersicher.ch/de/ihr-sicherheitsbeitrag/phishing

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, *55* (1), 74–81. https://doi.org/10.1145/2063176.2063197

Huang, H., Tan, J. & Liu, L. (2009). Countermeasure Techniques for Deceptive Phishing Attack. In *2009 International Conference on New Trends in Information and Service Science* (S. 636-641). https://doi.org/10.1109/NISS.2009.80

IBM SPSS Statistics for Windows. (2017). Armonk, NY: IBM Corp. Abgerufen von https://www.ibm.com/products/spss-statistics

Internet Security Research Group. (2018). *Let's Encrypt Stats - Let's Encrypt - Free Ssl/Tls Certificates.* Abgerufen von https://letsencrypt.org/stats/

ISACA. (2012). *COBIT 5.* ISA.

ISACA. (2013). *IT-Risikomanagement – leicht gemacht mit COBIT* (Bericht). Kelkheim, Deutschland: ISACA Germany Chapter. Abgerufen von https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/

2012-isaca-leitfaden-it-risikomanagement_0.pdf

ISO/IEC. (2013). *Information Technology - Security Techniques - Information Security Management Systems - Requirements* (ISO/IEC Norm 27001:2013). Winterthur, Schweiz: SNV Schweizerische Normen-Vereinigung. Abgerufen von https://www.iso.org/standard/54534.html

Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, *50* (10), 94–100. https://doi.org/10.1145/1290958.1290968

Jakobsson, M. & Ratkiewicz, J. (2006). Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Query Features. In *Proceedings of the 15th International Conference on World Wide Web* (S. 513–522). Edinburgh, Schottland: ACM. https://doi.org/10.1145/1135777.1135853

Johnston, L. W. (1970). Student's t-Test. *Journal of Quality Technology*, *2* (4), 243-245. https://doi.org/10.1080/00224065.1970.11980443

Kahveci, M. (2010). Students' Perceptions to Use Technology for Learning: Measurement Integrity of the Modified Fennema-Sherman Attitudes Scales. *Turkish Online Journal of Educational Technology*, *9* (1), 185-201.

Kaspersky Lab. (2015). *10 Tips to Protect Yourself from Phishing.* Abgerufen von https://www.kaspersky.com/blog/phishing-ten-tips/10550/

Kaspersky Lab. (2018). *Financial Cyber-Threats in 2017.* Autor. Abgerufen von https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07162608/Kaspersky_Lab_financial_cyberthreats_in_2017.pdf

Kirda, E. & Kruegel, C. (2005). Protecting Users Against Phishing Attacks with Antiphish. In *29th Annual International Computer Software and Applications Conference* (Bd. 1, S. 517-524 Vol. 2). https://doi.org/10.1109/COMPSAC.2005.126

Kitterman, S. (2014). *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1* (RFC Nr. 7208). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/html/rfc7208

Kitterman, S. (2018). *Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)* (RFC Nr. 8301). IETF Internet Engineering Task Force.

Abgerufen von https://tools.ietf.org/html/rfc8301

Klein, A. & Golan, Z. (2006). *U.S. Patent No. 8266295 - System and Method for Detecting and Mitigating DNS Spoofing Trojans.* Washington, DC: U.S. Patent and Trademark Office.

Konsumenteninfo AG. (2018). *Aktuelle Fälle von Phishing.* Abgerufen von https://www.ktipp.ch/service/warnlisten/detail/w/aktuelle-faelle-von-phishing/

Krebs, D. & Menold, N. (2014). Gütekriterien quantitativer Sozialforschung. In *Handbuch Methoden der empirischen Sozialforschung* (S. 425-438). Berlin, Deutschland: Springer.

Kucherawy, M. & Zwicky, E. (2015). *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* (RFC Nr. 7489). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/html/rfc8301

Kühl, S. (2009). Experiment. In S. Kühl, P. Strodtholz & A. Taffertshofer (Hrsg.), *Handbuch Methoden der Organisationsforschung: Quantitative und Qualitative Methoden* (S. 534-557). Wiesbaden, Deutschland: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_26

Kühnel, S. & Dingelstedt, A. (2014). Kausalität. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 1017-1028). Wiesbaden, Deutschland: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0_80

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (S. 3:1–3:12). Mountain View, CA: ACM. https://doi.org/10.1145/1572532.1572536

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (S. 905–914). San Jose, CA: ACM.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F. & Hong, J. (2007). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of

Retention and Transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (S. 70–81). Pittsburgh, PA: ACM.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2008). Lessons from a Real World Evaluation of Anti-Phishing Training. In *2008 eCrime Researchers Summit* (S. 1-12). Carnegie Mellon University. https://doi.org/10.1109/ECRIME.2008.4696970

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*, *10* (2), 7:1–7:31. https://doi.org/10.1145/1754393.1754396

Lastdrager, E. (2014). Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature. *Crime Science*, *3* (1), 9. https://doi.org/10.1186/s40163-014-0009-y

Lastdrager, E., Gallardo, I. C., Hartel, P. & Junger, M. (2017). How Effective is Anti-Phishing Training for Children? In *Thirteenth Symposium on Usable Privacy and Security* (S. 229–239). Santa Clara, CA: USENIX Association.

Li, F., Lai, A. & Ddl, D. (2011). Evidence of Advanced Persistent Threat: A Case Study of Malware for Political Espionage. In *2011 6th International Conference on Malicious and Unwanted Software* (S. 102-109). https://doi.org/10.1109/MALWARE.2011.6112333

Liang, H. & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33* (1), 71-90. https://doi.org/10.2307/20650279

Liang, H. & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11* (7), 394.

Likert, R. (1932). A Technique for the Measurement of Attitudes. *Archives of psychology*.

Lim, T.-S. & Loh, W.-Y. (1996). A Comparison of Tests of Equality of Variances. *Computational Statistics & Data Analysis*, *22* (3), 287-301. https://doi.org/10.1016/0167-9473(95)00054-2

Lin, L. I.-K. (1989). A Concordance Correlation Coefficient to Evaluate Reproducibili-

ty. *Biometrics*, *45* (1), 255-268. https://doi.org/10.2307/2532051

Linstone, H. A. (1985). The Delphi Technique. In V. T. Covello, J. L. Mumpower, P. J. M. Stallen & V. R. R. Uppuluri (Hrsg.), *Environmental Impact Assessment, Technology Assessment, and Risk Analysis* (S. 621-649). Springer Berlin Heidelberg.

Long, R. M. (2013). *Using Phishing to Test Social Engineering Awareness of Financial Employees* (Masterarbeit). Eastern Washington University, Washington, WA.

Mann, H. B. & Whitney, D. R. (1947). On a Test of Whether one of Two Random Variables Is Stochastically Larger than the Other. *The Annals of Mathematical Statistics*, *18* (1), 50-60.

Mansfield-Devine, S. (2016). The Imitation Game: How Business Email Compromise Scams Are Robbing Organisations. *Computer Fraud & Security*, *2016* (11), 5-10. https://doi.org/10.1016/S1361-3723(16)30089-6

Matsumoto, M. & Nishimura, T. (1998). Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator. *ACM Transactions on Modeling and Computer Simulation*, *8* (1), 3-30.

McCall, T. (2007). *Gartner Survey Shows Phishing Attacks Escalated in 2007; More Than $3 Billion Lost to These Attacks.* Abgerufen von https://www.gartner.com/newsroom/id/565125

McCoy, C. & Fowler, R. T. (2004). "You Are the Key to Security": Establishing a Successful Security Awareness Program. In *Proceedings of the 32nd annual ACM SIGUCCS conference on User services* (S. 346-349). Baltimore, MD: ACM.

McKnight, P. E. & Najab, J. (2010). Mann-Whitney U Test. *Corsini Encyclopedia of Psychology*. https://doi.org/10.1002/9780470479216.corpsy0524

MELANI. (o. J.). *Melde- und Analysestelle Informationssicherung MELANI.* Abgerufen von https://www.melani.admin.ch/melani/de/home.html

MELANI. (2015a). *Antiphishing.ch.* Abgerufen von https://www.antiphishing.ch/en/

MELANI. (2015b). *Meldeportal gegen Phishing.* Abgerufen von https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/meldeportal_gegen_phishing.html

MELANI. (2017a). *Semi-Annual Report 2017/1*. Abgerufen von https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2017-1.html

MELANI. (2017b). *Verschlüsselungstrojaner*. Abgerufen von https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html

Misra, G., Arachchilage, N. A. G. & Berkovsky, S. (2017). Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. *CoRR*, *abs/1710.06064*.

Moore, T. & Clayton, R. (2007). An Empirical Analysis of the Current State of Phishing Attack and Defence. In *Workshop on the Economics of Information Security* (S. 20). Pittsburgh, PA: Carnegie Mellon University.

Muscanell, N. L., Guadagno, R. E. & Murphy, S. (2014). Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Social and Personality Psychology Compass*, *8* (7), 388–396. https://doi.org/10.1111/spc3.12115

Netsafe. (2017). *Time for some R&R and R&D*. Abgerufen von https://www.rescam.org

Ollmann, G. (2004). *The Phishing Guide*. IBM.

Parmar, B. (2012, Januar). Protecting Against Spear-Phishing. *Computer Fraud & Security*, *2012* (1), 8-11. https://doi.org/10.1016/S1361-3723(12)70007-6

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2015). The Design of Phishing Studies: Challenges for Researchers. *Computers & Security*, *52* (Supplement C), 194-206. https://doi.org/10.1016/J.COSE.2015.02.008

PhishLabs. (2018). *Phishing and Threat Intelligence Report 2017*. Abgerufen von https://pages.phishlabs.com/rs/130-BFB-942/images/2017%0020PhishLabs%0020Phishing%0020and%0020Threat%0020Intelligence%0020Report.pdf

Polizei Schweiz. (2018). *Kanton Zürich ZH - Achtung vor neuer Phishing-Variante*. Abgerufen von https://www.polizei-schweiz.ch/kanton-zuerich-zh-achtung-vor-neuer-phishing-variante/

Posten, H. O., Rasch, D. & Tiku, M. L. (1984). Robustness of the Two-Sample t-

Test. In *Robustness of Statistical Methods and Nonparametric Statistics* (S. 92-99). Dordrecht, Niederlande: Springer Netherlands. https://doi.org/10.1007/978-94-009-6528-7_23

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34* (4), 757-778. https://doi.org/10.2307/25750704

Purkait, S. (2013). Phishing Counter Measures and Their Effectiveness – Literature Review. *Information Management & Computer Security*, *20* (5), 382–420. https://doi.org/10.1108/09685221211286548

Rajalingam, M., Alomari, S. A. & Sumari, P. (2012). Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages. *International Journal of Computer Science and Security*, *6* (1), 1.

Ramanathan, V. & Wechsler, H. (2013). Phishing Detection and Impersonated Entity Discovery Using Conditional Random Field and Latent Dirichlet Allocation. *Computers & Security*, *34* (Supplement C), 123-139. https://doi.org/10.1016/J.COSE.2012.12.002

Rampillon, U. & Zimmermann, G. (1997). *Strategien und Techniken beim Erwerb fremder Sprachen*. Hueber Verlag.

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. In P. Stavroulakis & M. Stamp (Hrsg.), *Handbook of Information and Communication Security* (S. 433-448). Berlin, Deutschland: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04117-4_23

Rescorla, E. & Dierks, T. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2* (RFC Nr. 5246). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/html/rfc5246

Rice, M. E. & Harris, G. T. (2005). Comparing Effect Sizes in Follow-Up Studies: ROC Area, Cohen's d, and r. *Law and Human Behavior*, *29* (5), 615-620. https://doi.org/10.1007/s10979-005-6832-7

Rice, W. R. (1989). Analyzing Tables of Statistical Tests. *Evolution*, *43* (1), 223-225. https://doi.org/10.2307/2409177

Richardson, R. & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13* (1), 10-21, 101.

Ropohl, G. (1986). *Die unvollkommene Technik.* Suhrkamp.

Rosiello, A. P. E., Kirda, E., Kruegel, . & Ferrandi, F. (2007). A Layout-Similarity-Based Approach for Detecting Phishing Pages. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007* (S. 454-463). https://doi.org/10.1109/SECCOM.2007.4550367

Rowe, G. & Wright, G. (2001). Expert Opinions in Forecasting: The Role of the Delphi Technique. In J. S. Armstrong (Hrsg.), *Principles of Forecasting: A Handbook for Researchers and Practitioners* (S. 125-144). Boston, MA: Springer US. https://doi.org/10.1007/978-0-306-47630-3_7

Ruxton, G. D. (2006). The Unequal Variance t-Test Is an Underused Alternative to Student's t-Test and the Mann–Whitney U Test. *Behavioral Ecology*, *17* (4), 688-690. https://doi.org/10.1093/beheco/ark016

Rydell, J., M'Raihi, D., Pei, M. & Machani, S. (2011). *TOTP: Time-based One-time Password Algorithm* (RFC Nr. 6238). IETF Internet Engineering Task Force. Abgerufen von https://tools.ietf.org/html/rfc6238

Schneier, B. (2005). Two-Factor Authentication: Too Little, Too Late. *Commun. ACM*, *48* (4), 136.

Schweizerische Kriminalprävention. (2018). *Phishing.* Abgerufen von https://www.skppsc.ch/de/themen/internet/phishing/

Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, *27* (3), 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. & Downs, J. (2010). Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (S. 373-382). Atlanta, Georgia, USA: ACM. https://doi.org/10.1145/1753326.1753383

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd symposium on Usable Privacy and Security* (S. 88-99). Pittsburgh, PA: ACM.

Sheng, X. (2009). *A Policy Analysis of Phishing Countermeasures* (Dissertation). Carnegie Mellon University, Pittsburgh, PA.

Siadati, H., Jafarikhah, S. & Jakobsson, M. (2016). Traditional Countermeasures to Unwanted Email. In M. Jakobsson (Hrsg.), *Understanding Social Engineering Based Scams* (S. 51-62). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4939-6457-4_5

Siadati, H., Nguyen, T. & Memon, N. (2017). X-Platform Phishing: Abusing Trust for Targeted Attacks Short Paper. In M. Brenner et al. (Hrsg.), *Financial Cryptography and Data Security* (S. 587-596). Cham, Schweiz: Springer International Publishing. https://doi.org/10.1007/978-3-319-70278-0_37

SRF. (2018). *Neue Phishing-Methode - Wegen Betrugsfällen: Post schränkt Umleitung von Paketen ein.* Abgerufen von https://www.srf.ch/sendungen/kassensturz-espresso/wegen-betrugsfaellen-post-schraenkt-umleitung-von-paketen-ein-2

Stein, P. (2014). Forschungsdesigns für die quantitative Sozialforschung. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 135-151). Wiesbaden, Deutschland: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0_7

Stigler, S. (2008). Fisher and the 5% Level. *CHANCE*, *21* (4), 12-12. https://doi.org/10.1080/09332480.2008.10722926

Straka, G. A. & Macke, G. (2002). *Lern-lehr-theoretische Didaktik*. Münster, Deutschland: Waxmann Verlag.

Student. (1908). The Probable Error of a Mean. *Biometrika*, *6* (1), 1-25. https://doi.org/10.2307/2331554

Symantec. (2016). *Billion-dollar scams: The numbers behind BEC fraud.* Abgerufen von http://www.symantec.com/connect/blogs/billion-dollar-scams-numbers-behind-bec-fraud

Symantec. (2017). *Internet Security Threat Report 2017.* Abgerufen von https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

Tenberg, R. (2006). *Didaktik lernfeldstrukturierten Unterrichts: Theorie und Praxis beruflichen Lernens und Lehrens*. Julius Klinkhardt.

UBS. (2018). *Phishing.* Abgerufen von https://www.ubs.com/global/en/phishing.html

Ulevitch, D. (o. J.). *PhishTank | Join the fight against phishing.* Abgerufen von https://www.phishtank.com/

UMBC. (2018). *Ponnurangam Kumaraguru.* Abgerufen von https://ebiquity.umbc.edu/person/html/Ponnurangam/Kumaraguru/?pub=on

Universität Zürich. (2018). *t-Test für unabhängige Stichproben.* Abgerufen von http://www.methodenberatung.uzh.ch/de/datenanalyse/unterschiede/%0020zentral/ttestunabh.html

Van Teijlingen, E. & Hundley, V. (2002). The Importance of Pilot Studies. *Nursing Standard*, *16* (40), 33-36. https://doi.org/10.7748/ns2002.06.16.40.33.c3214

Venkatesh, Morris, Davis & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27* (3), 425. https://doi.org/10.2307/30036540

Venkatesh, V. & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46* (2), 186-204. https://doi.org/10.1287/MNSC.46.2.186.11926

Wagner, P. & Hering, L. (2014). Online-Befragung. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 661-673). Wiesbaden, Deutschland: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0_48

Wasserstein, R. L. & Lazar, N. A. (2016). The ASA's Statement on p-Values: Context, Process, and Purpose. *The American Statistician*, *70* (2), 129-133. https://doi.org/10.1080/00031305.2016.1154108

Welch, B. L. (1947). The Generalization of 'Student's' Problem when Several Different Population Variances are Involved. *Biometrika*, *34* (1/2), 28. https://doi.org/

10.2307/2332510

Wen, Z. A., Li, Y., Wade, R., Huang, J. & Wang, A. (2017). What.Hack: Learn Phishing Email Defence the Fun Way. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (S. 234-237). Denver, Colorado, USA: ACM. https://doi.org/10.1145/3027063.3048412

Whittaker, C., Ryner, B. & Nazif, M. (2010). Large-Scale Automatic Classification of Phishing Pages. In *NDSS* (Bd. 10, S. 14).

Whitten, A. & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium* (Bd. 348, S. 679–702).

Williams, N. & Li, S. (2017). Simulating Human Detection of Phishing Websites: An Investigation into the Applicability of the ACT-R Cognitive Behaviour Architecture Model. In *2017 3rd IEEE International Conference on Cybernetics* (S. 1-8). Exeter, England: IEEE. https://doi.org/10.1109/CYBConf.2017.7985810

Wilson, M. & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST SP 800-50). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50

Wisz, M. S., Hijmans, R. J., Li, J., Peterson, A. T., Graham, C. H. & Guisan, A. (2008). Effects of Sample Size on the Performance of Species Distribution Models. *Diversity and Distributions*, *14* (5), 763-773. https://doi.org/10.1111/j.1472-4642.2008.00482.x

Wolfram Alpha. (2018). *Wolfram|alpha: Making the World's Knowledge Computable.* Abgerufen von www.wolframalpha.com/

Wright, M. A. (1998). The Need for Information Security Education. *Computer Fraud & Security*, *1998* (8), 14-17. https://doi.org/10.1016/S1361-3723(98)80019-5

Wright, R. T. & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27* (1), 273-303. https://doi.org/10.2753/MIS0742-1222270111

Wu, M., Miller, R. C. & Garfinkel, S. L. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? In *Proceedings of the SIGCHI Conference on Human Factors*

in Computing Systems (S. 601-610). Montreal, Kanada: ACM.

Xue, F. & Zhu, B. B. (2015). *U.S. Patent No. 9178901 - Malicious Uniform Resource Locator Detection.* Washington, DC: U.S. Patent and Trademark Office.

Yates, F. (1964). Sir Ronald Fisher and the Design of Experiments. *Biometrics*, *20* (2), 307-321. https://doi.org/10.2307/2528399

Zhu, B. B., Choi, H., KR, Lee, H. & KR. (2013). *U.S. Patent No. 8521667 - Detection and Categorization of Malicious URLs.* Washington, DC: U.S. Patent and Trademark Office.

Zimmerman, D. W. (1987). Comparative Power of Student t Test and Mann-Whitney U Test for Unequal Sample Sizes and Variances. *The Journal of Experimental Education*, *55* (3), 171-174. https://doi.org/10.1080/00220973.1987.10806451

Zollinger, M. & Monsorno, A. (2015). *Mobile Malware* (Unveröffentlichte Bachelorarbeit). ZHAW, Winterthur, Schweiz.

Züricher Kantonalbank. (2018). *Vorsicht Phishing E-Mails | zkb.ch.* Abgerufen von https://www.zkb.ch/de/gs/lp/vorsicht-phishing-mails.html

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst habe.

Ort, Datum	**Winterthur, 25. Mai 2018**
Unterschrift	

Moritz Zollinger

Digitally signed by Moritz Zollinger
DN: cn=Moritz Zollinger, o=ZHAW, ou=SML,
email=mo.zollinger@gmail.com, c=CH
Date: 2018.05.25 05:00:03 +02'00'