Zürcher Hochschule für Angewandte Wissenschaften

Bachelor of Science in Wirtschaftsinformatik

Design und prototypische Implementierung einer multimedialen Lern-Plattform für Phishing Prävention im KMU-Umfeld

Bachelorarbeit

Autor

Jeremy Bolt

Matrikelnummer: 14670301

Mettlenstrasse 41

8330 Pfäffikon ZH

Betreuer

Dr. Peter Heinrich

ZHAW School of Management and Law

Gertrudstrasse 15

8401 Winterthur

Abgabedatum

Donnerstag, 24. Mai 2018

Wahrheitserklärung

„ Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig, ohne Mithilfe Dritter und nur unter Benützung der angegebenen Quellen verfasst habe und dass ich ohne schriftliche Zustimmung der Studiengangleitung keine Kopien dieser Arbeit an Dritte aushändigen werde.“

Gleichzeitig werden sämtliche Rechte am Werk an die Zürcher Hochschule für angewandte Wissenschaften (ZHAW) abgetreten. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Name des Studenten

Jeremy Bolt

Unterschrift des Studierenden

……

Management Summary

Phishing ist eine Art der Cyber-Attacke, bei welcher einem Opfer eine Nachricht versendet wird, die vortäuscht von einer vertrauenswürdigen Quelle oder Organisation zu stammen. Typischerweise versuchen Phishingmails die Opfer davon zu überzeugen, persönliche Informationen wie Benutzernamen, Passwörter, Kreditkarten-Informationen oder Bankdaten preiszugeben.

Phishing-Attacken können sowohl Privatpersonen sowie Unternehmen angreifen. Unternehmen setzen verschiedene Anti-Phishing-Massnahmen ein, wie Email-Filtering, Anti-Phishing Toolbars, Anti-Phishing Education sowie Phishing-Tests innerhalb der Organisation. Eine Lern-Plattform für Anti-Phishing Education wurde in dieser Arbeit designt und prototypisch in einem Schweizer KMU umgesetzt. Durch das Versenden von Phishingmails an die Mitarbeiter dieses KMUs wurde untersucht, ob eine Lern-Plattform die Anzahl an erfolgreichen Phishing-Attacken senken kann.

Die Lern-Plattform wird in der Form eines Quiz umgesetzt und vermittelt Wissensinhalte zu den möglichen Merkmalen eines Phishingmails oder einer Phishing-Webseite und wie man diese erkennen kann. Das Quiz ist von einer Hälfte der Mitarbeitenden absolviert worden, während die andere Hälfte kein Training erhielt. Vor dem Absolvieren des Quiz wurde durch ein Test-Phishingmail analysiert, wie viele Mitarbeitende auf eine Phishing-Attacke eingehen würden. Nach dem Quiz wurde innerhalb von 48 Stunden ein zweites und nach 7 Tagen ein drittes Phishingmail versendet, um den Effekt des Anti-Phishing Trainings zu ermitteln.

Das Resultat des ersten Phishingmails zeigte, dass 26.6% der Mitarbeitenden auf die Phishing-Attacke eingegangen sind. Diese überraschend hohe Anzahl an erfolgreichen Phishingmails rechtfertigte den Einsatz einer Lern-Plattform bei diesem KMU. Beim zweiten Phishingmail sind insgesamt 17.4% und im letzten 16.5% der Mitarbeitenden auf das Phishingmail eingegangen. Die Gruppe der Quiz-Teilnehmer erzielte dabei deutlich verbesserte Werte. In dieser Gruppe lag der erste Werte bei 20.5%, bei den darauf folgenden Phishingmails sind es noch 4.5% und 9.1%.

Die Ergebnisse des zweiten und dritten Phishingmails beweisen, dass der Einsatz dieser Lern-Plattform das Risiko einer erfolgreichen Phishing-Attacke senken kann. Die Resultate zeigen aber auch, dass das Risiko von erfolgreichen Phishing-Attacken nicht gänzlich durch den Einsatz dieser Lern-Plattform eliminiert werden kann.

Um dieses Risiko weiter zu senken, könnte das Quiz wiederholt durchgeführt werden. Die Wissensinhalte des Quiz könnten dabei immer tiefer auf die Thematik Phishing eingehen und so erweitertes Wissen vermitteln. Ein wiederholtes Anti-Phishing Training ist sinnvoll, da die Anzahl der erfolgreichen Phishing-Attacken vom zweiten zum dritten Phishingmail wieder angestiegen ist. Diese Lern-Plattform ist nur in digitaler Form umgesetzt worden, und könnte mit der Kombination einer herkömmlichen Schulung eine weitere Entwicklung und Verbesserungsmöglichkeit bieten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACT-R	Adaptive Control of Thought-Rational
APWG	Anti Phishing Working Group
CRT	Cognitive Reflection Test (Nyeste, 2011, p. 41)
DNS	Domain Name System
DST	Signal Detection Theory (Nyeste, 2011, p. 59)
fedpol	Bundesamt für Polizei
KA	Knowledge Acquisition von Schmidt and Bjork (1992)
KR	Knowledge Retention von Schmidt and Bjork (1992)
SMC Corp.	Sintered Metal Corporation (Mutterhaus SMC Schweiz AG)
SMC	SMC Schweiz AG
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

1 Einleitung

Täglich finden weltweit Cyber-Attacken in Form von Phishingmails statt. Beispiele für Cyber-Security Attacken gibt es unzählige. Ende 2017 wurde das Telekommunikationsunternehmen Swisscom Opfer einer Attacke und gab bekannt das über 800'000 Kunden von Swisscom von einem Datenleck betroffen waren.[1] Der wohl im Moment am meisten diskutierte Vorfall, ist der Cambridge Analytica Skandal (Facebook hat zugegeben, dass Daten von über 50 Millionen Nutzer unerlaubt weiterverwendet wurden).[2] Dieser, sowie viele weitere Beispiele zeigen, dass weder Privatpersonen noch Grossunternehmen Cyber-Security aussen vor lassen können.

Die Thematik Cyber-Security enthält viele Ansatzpunkte und Inhalte und wird daher oft in verschiedene Themenbereiche unterteilt. Ein Aspekt von Cyber Security ist die Gefahr von Phishing-Attacken. Im Jahr 2016 wurden 14'033 Verdachtsmeldungen für Cyber Kriminalität via Online Formular beim fedpol gemeldet. Davon sind 2328 Meldungen zum Thema Phishing eingegangen, was 16.6% entspricht.[3] Phishing ist in der Schweiz eine der meistverwendeten Methoden von Cyber Angriffen.

Im Rahmen dieser Arbeit wird untersucht, wie Mitarbeiter eines KMU zum Thema Phishing ausgebildet werden könnten. Ist eine Lern-Plattform eine möglicher Ansatz zur Ausbildung? Könnte eine Phishing Lern-Plattform das Risiko von erfolgreichen Phishing-Attacken vermindern? Im ersten Teil dieser Arbeit wird Phishing und mögliche Auswirkungen von Phishing-Attacken erläutert. In einem nächsten Schritt wird durch einen Literaturreview nach vorhandenen Lösungen und Ansätzen im Bereich einer Phishing Lern-Plattform gesucht.

Anschliessend wird ein Versuch mit den Mitarbeitenden eines Schweizer KMUs durchgeführt. Das KMU genannt SMC Schweiz AG (SMC), ist in den letzten zwei Jahren schon mehrmals Opfer von Phishing-Attacken geworden. Den Mitarbeitenden werden Phishingmails zugesendet um festzustellen, ob die Mitarbeitenden der SMC anfällig für Phishing-Attacken sind. Aufgrund der Ergebnisse aus diesem Versuch wird das Design einer Lern-Plattform erarbeitet. Diese wird ebenfalls Konzepte und Lösungen aus dem ersten Teil dieser Arbeit einschliessen. Den Mitarbeitenden wird diese Lern-Plattform als Prototyp zur Verfügung gestellt. Wiederum wird im letzten Schritt mit Phishingmails getestet, ob die vermittelten Inhalte zu einer Verbesserung im Erkennen von Phishing-Attacken führt. Das Design wird diskutiert und es werden

[1] ("Daten-Leck bei Swisscom: Was Kunden jetzt wissen müssen - Handelszeitung").

[2] ("If You Don't Fully Understand the Cambridge Analytica Scandal, Read This Simplified Version").

[3] ("Statistiken zum Jahresbericht fedpol 2016").

Empfehlungen verfasst, welche für zukünftige Verbesserungen oder Designs verwendet werden können. Nicht Teil dieser Arbeit, ist der Vergleich verschiedener Ansätze einer Lern-Plattform. Durch den Literaturreview werden verschiedene Ansätze präsentiert, jedoch nicht gegeneinander bewertet.

2 Phishing

Im folgenden Kapitel wird ein Überblick über die Thematik Phishing geschaffen. Was sind die Faktoren die Phishing mit sich bringt und wie wirken sich diese auf Mitarbeitende eines Unternehmens aus?

2.1 Begriff Phishing

Das Wort Phishing tauchte erstmals 1995-1996 auf und ist vom Begriff «Fishing» abgeleitet. Dabei wird sinngemäss ein «Haken» ausgeworfen und auf einen «Biss» gewartet.[4] Viele Autoren haben ihre eigene Definition geschaffen, welche erst mit der Studie von Lastdrager von 2014 erstmals zur folgenden Definition des Begriffes geführt hat: *«Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target.»*[5]

Jemand der eine Phishing-Attacke ausübt wird als «Phisher» bezeichnet.[6] Dabei handelt es sich meist um Personen einer kriminellen Organisation, die Phishing als Mittel zur persönlichen Bereicherung ausüben.[7]

2.1.1 Ziele von Phishing

Phishing kann in verschiedenen Intensitäten betrieben werden. Vom ganz einfachen Phishingmail, welches eine Aufforderung zum Öffnen eines Linkes enthält, bis hin zur gezielten Attacke auf ein bestimmtes Individuum, welches mit personifizierten Informationen fehlgeleitet wird. Die Evolution gilt nicht nur für Tiere und Pflanzen, sondern auch für unsere Technologie. Bestes Beispiel dafür ist die Panzerung welche den Träger vor Verletzungen schützen soll. Aufgrund dieser Panzerung, wurden Wege gefunden, welche die Panzerung durchbrechen können. Als Antwort darauf wurden wieder neue Panzerungen gefunden und der Kreis dreht sich immer weiter. Phishing-Attacken und die nachfolgenden Massnahmen dagegen bewegen sich im selben Kreis.[8] Phishing entwickelt sich demnach immer weiter und die Massnahmen und Vorkehrungen die unternommen werden um Phishing zu unterbinden werden ebenfalls weiter entwickelt. Beispiele für Phishing-Attacken gibt es viele und die Ziele die dabei

[4] Lastdrager (2014, pp. 1–2).
[5] Lastdrager (2014, p. 8).
[6] Bellovin (2004, p. 144).
[7] Emigh (2005, p. 6).
[8] Robila and Ragucci (2006, p. 237).

verfolgt werden variieren je nach Attacke und Ziel der Täterschaft welche die Attacke startet. Das Grundziel bleibt dabei immer gleich, an sensitive Informationen eines Opfers zu kommen, indem sich der «Phisher» als eine vertrauenserweckende Entität ausgibt.[9] Dabei zählt der menschliche Faktor zu einem der schwächsten in der Kette, welche durch Phishing angegriffen werden.[10] Welche Auswirkungen diese für Unternehmen und deren Mitarbeitenden haben können, wird im Kapitel 3.1.4 behandelt.

2.1.2 Arten von Phishing

Ein Phishingmail enthält normalerweise einen Text der beim Empfänger den Eindruck erwecken soll, dass dieses Email legitim ist. Zusätzlich zum Text enthält ein Phishingmail oft einen Link, den das Opfer öffnen soll. Mit dem Klick auf den Link wird man auf eine Phishing-Website weitergeleitet. Diese kann eine echte Website imitieren und das Opfer so davon überzeugen, zum Beispiel persönliche Informationen wie Benutzername und Passwort preiszugeben. In den folgenden Abschnitten werden weitere Variationen von Phishing-Attacken beschrieben.

2.1.3 Spear-Phishing

Mit Spear-Phishing sind Phishing-Attacken gemeint, welche sich auf ein bestimmtes Opfer fokussieren und dabei vorgeben von einer vertrauenswürdigen Quelle zu stammen. Dabei werden die Emails so aufbereitet, dass sie spezifisch auf das ausgewählte Opfer passen.[11] Spear Phishingmails unterscheiden sich von herkömmlichen Phishingmails vor allem indem sie viel gezielter erstellt und versendet werden. Zum Beispiel wird ein Email nicht an alle Mitarbeiter eines Unternehmens gesendet, sondern nur an einen kleinen Personenkreis. Dies im Namen eines Mitarbeiters, welcher diesem Personenkreis bekannt ist. Damit erwecken die «Phisher» den Eindruck, dass das Email legitim ist und damit ist die Wahrscheinlichkeit eines Erfolges höher.

2.1.4 Malware Phishing

Beim Malware Phishing wird im Gegensatz zum normalen Phishingmail kein Link im Email hinterlegt sondern ein Anhang angehängt. Bei diesem Anhang handelt es sich um eine Datei,

[9] Jagatic, Johnson, Jakobsson, and Menczer (2007, p. 94).
[10] Robila and Ragucci (2006, p. 237).
[11] Vijayan (2005).

die beim Öffnen durch das Opfer eine schädliche Software ausführt. Die Malware kann die Form von Ransomware annehmen, bei der Dateien so verschlüsselt werden, dass man sie nicht mehr öffnen kann. Gegen Bezahlung gibt der Phisher an, den Schlüssel zur Wiederherstellung der Dateien zu übergeben. Die Malware könnte auch andere Phishing-Ziele verfolgen, wie das Sammeln von Informationen und Zugangsdaten.[12]

2.1.5 DNS Phishing

Beim DNS[13] Phishing wird versucht den Lookup Prozess eines Domain Namen zu beeinflussen. Damit wird das Opfer beim Aufruf einer Webseite nicht auf diese, sondern auf die vom Phisher gewählte Adresse geleitet. Weil durch eine Manipulation des DNS Eintrages für diese Adresse ein anderes Ziel eingegeben wurde. Zum Beispiel zeigt der DNS Eintrag von «www.google.com» neu auf «www.phishers.com». Dabei hat der Phisher mehrere Möglichkeiten zu manipulieren. Das sogenannte Host-File eines Computers kann mit einem Eintrag erweitert werden, welches eine Adresse direkt mit einer Phishing-Webseite referenziert.[14] Eine weitere Möglichkeit ist, den gespeicherten DNS Cache eines Computers zu verändern oder den DNS Lookup Server auf einen korrupten DNS Server zu ändern.[15]

2.1.6 Social Engineering

Beim Social Engineering wird mit Hilfe von gesammelten Informationen versucht, ein Individuum oder eine Organisation zu beeinflussen. In Bereich Phishing werden persönliche Informationen benutzt um die Phishing-Attacke überzeugender wirken zu lassen. Wenn ein Email mit auf den Empfänger spezialisierten Inhalten ausgestattet ist, wird der Empfänger einfacher getäuscht. Solche Social-Phishing Attacken können bis zu vier Mal häufiger zum Erfolg führen als wenn blind attackiert wird.[16]

2.1.7 Anti-Phishing Massnahmen

Mit dem Aufkommen von Phishing als Cyber-Security Risiko, kamen auch Technologien und Massnahmen gegen diese Gefahr zur Anwendung, sei das nun für Privatpersonen oder

[12] W. Kim, Jeong, Kim, and So (2011, p. 677).
[13] Wikipedia (2018).
[14] Emigh (2005, p. 10).
[15] Emigh (2005, pp. 10–11).
[16] Gao, Wang, Hu, Huang, and Chen (2011, p. 59).

Unternehmungen. Purkait (2012) teilte die bestehenden Anti-Phishing Massnahmen in acht Kategorien ein um diese zu klassifizieren. Dabei gibt es den Ansatz, in dem versucht wird, die Phishingmails zu filtern bevor sie ihre Destination erreichen. Dabei werden die Emails in legitime und falsche Emails eingeteilt.[17] Diese Art von Filter ist auch bekannt unter dem Name Spam Filter und wird heute in fast allen Unternehmungen und von vielen Email-Dienstleistern eingesetzt. Wie ein Spam Filter filtert, dafür gibt es eine Vielzahl von Studien und Vorschläge. Ein Beispiel ist der Einsatz von Whitelists und Backlists auf denen Absender entweder zugelassen oder gesperrt werden können.[18] Eine weitere Kategorie nach Purkait (2012) ist das Anti-Phishing Training. Dabei wird argumentiert, dass ein Anti-Phishing Training eine bessere Strategie darstellt im Vergleich zum Versenden von Warnungen über Phishing.[19] Um den bestmöglichen Schutz vor Phishing zu gewährleisten ist jedoch eine Kombination verschiedener Methoden zu empfehlen. Solange der Anreiz zu Phishing besteht, werden immer neue Wege gefunden um an den Anti-Phishing Massnahmen vorbeizukommen.[20]

2.1.8 Abgrenzung Phishing

Phishing-Attacken sind ein Teil des Gefahrenkataloges welcher heute für Unternehmen sowie Private relevant ist. Der Cyber-Betrug, wie zum Beispiel falsche Immobilienanzeigen, fiktive Transportfirmen, falsche Unterstützungsanfragen, falsche Zahlungsbestätigungen, Vorschussbetrug, Romance-Scam sind ebenfalls Gefahren welche allgegenwärtig sind. Diese haben laut fedpol im Jahr 2016, 26.9% aller Meldungen zu Cyber-Phänomenen ausgemacht.[21] Weiter gibt es die Angriffe mit Software z.B. Malware oder Ransomware. Die Abgrenzung von Phishing zu diesen Methoden ist jedoch insofern schwierig, da auch bei Cyber-Attacken eine Kombination aus verschiedenen Methoden benutzt werden kann. Eine mögliche Variante wäre, eine schädliche Software (Malware) im Netz oder auf dem Computer eines Opfers zu platzieren. Dies kann durch das Verschaffen eines externen Zugriffes oder via einem Phishingmail mit angehängter Software gelingen. Grundsätzlich gilt, dass beim Phishing immer eine Aktion des Opfers notwendig ist, damit die Phishing-Attacke zum Erfolg führt. Bei anderen Arten von Cyber-Angriffen ist dies nicht notwendig.

[17] Purkait (2012, p. 390).
[18] Pfleeger and Bloom (2005, p. 43).
[19] Purkait (2012, pp. 400–401).
[20] Purkait (2012, p. 391).
[21] ("Statistiken zum Jahresbericht fedpol 2016," p. 2).

2.1.9 Aktuelles zu Phishing

Neben den Statistiken des fedpol zur Phishing-Kriminalität in der Schweiz gibt es die Organisation APWG, welche sich mit der Globalen Phishing Situation auseinandersetzt. Die APWG erstellt jedes Quartal einen Phishing-Report. In diesem Report wird die aktuelle Situation der letzten drei Monate aufgezeigt. Die Informationen erhält die APWG von Partner Organisationen und Unternehmen, welche die APWG unterstützen.[22] Im Q3 Report für das Jahr 2017 wurden der APWG 296'208 einzelne Phishing-Attacken rapportiert. Dies entspricht einer Zunahme von über 23’000 zum vorangegangen Quartal.[23] Wie in Abbildung 1 ersichtlich wurden im Q3 weltweit 6'431 neue Phishing-Websites gefunden, davon sind 85 Seiten in der

Country of hosting	July	Aug	Sept	Total
United States	1,392	1,686	1,082	**4,160**
Ireland	375	208	165	**748**
Brazil	148	239	175	**562**
France	19	60	87	**166**
Germany	21	68	57	**146**
Canada	44	68	33	**145**
Switzerland	0	77	8	**85**
Netherlands	12	34	22	**68**
United Kingdom	11	21	30	**62**
Czech Republic	19	25	13	**57**
Others (35 countries)	59	121	52	**232**
Total	**2,100**	**2,607**	**1,724**	**6,431**

Abbildung 1: Hosted Phishing-Websites Q3 2017 (Manning, 2018, p. 10)

Schweiz beheimatet. Die Schweiz ist bei den attackierten Ländern eingestuft, dies zeigt eine aktuelle Studie der KPMG von 2017 nach der 88% der befragten Schweizer Unternehmen in den letzten 12 Monaten, Ziel eines Cyber-Angriffes wurden.[24] Und trotzdem gibt es innerhalb der Schweiz Elemente, welche im Bereich von Cyber-Kriminalität in Form von Phishing aktiv sind, wie der Report von APWG zeigt.

[22] Manning (2018).
[23] Manning (2018).
[24] Arikan (2017).

2.1.10 Auswirkungen auf Unternehmen

Wie im vorherigen Abschnitt erläutert sind Schweizer Unternehmen immer aktiver von Phishing-Attacken und generell von der Cyber-Kriminalität betroffen. Doch was kann eine Phishing-Attacke für ein Unternehmen bedeuten und welche Auswirkungen bilden sich daraus? Von Phishing-Attacken sind nicht ausschließlich die großen Unternehmungen betroffen, sondern es werden ebenfalls KMUs Opfer von Cyber-Security Angriffen. Gerade im KMU-Umfeld fehlen oft die zeitlichen und finanziellen Ressourcen um sich mit allen Themen der Cyber-Security auseinanderzusetzen.[25] Phishing kann also alle Arten von Unternehmungen betreffen und ist deshalb für viele Unternehmen ein Thema, mit welchem man sich auseinandersetzen muss. Die Auswirkungen für ein Unternehmen können verschiedene Formen annehmen. Hinter Phishing-Attacken steht oft eine kriminelle Organisation, welche ein monetäres Ziel verfolgt. Alleine im Jahr 2007 werden die Kosten durch Phishing-Attacken in den USA auf 3.2 Milliarden US Dollar geschätzt.[26] Dies zeigt, dass eine erfolgreiche Phishing-Attacke oft ein finanzieller Verlust für das Unternehmen zu Folge hat. Das Abgreifen von Firmeninternen Daten mit «gephishten» Benutzernamen und Passwörtern, ist eine Möglichkeit mit der sich Firmen auseinandersetzen müssen. Weiter kann durch einen Angriff mit Phishing Ransomware, die Firma zu einer finanziellen Transaktion erpresst werden.

[25] Portmann and Hirschi (2018, p. 457).

[26] Kim, W. et al. (2011, p. 692).

3 Literatur Review «Phishing Education»

Um die grundlegende Literatur für das folgende Lernkonzept zu erhalten wird eine Literaturrecherche durchgeführt. Die Recherche soll vorhandene Konzepte und Praktiken zur «Phishing Education» aufzeigen. Die gefundene Literatur wird als Basis für das Lernkonzept benützt.

3.1.1 Ansatz - Vorgehen

Auf Google Schoolar erreicht der Suchbegriff «Phishing AND Education» ca. 21'800 Ergebnisse und die gegensätzliche Version von «Education AND Phishing» ca. 21'700. Um die grosse Anzahl von Ergebnissen bei den verwendeten Online Bibliotheken zu verfeinern, wird mit Hilfe eines Frameworks nach Jan vom Brocke et al. (2009)[27] die Suche eingegrenzt.

Die in Klammern gehaltenen Nummern im folgenden Abschnitt verweisen auf die Abbildung 1 mit den einzelnen «Characteristics». Der Fokus der verwendeten Literatur sollte auf vorhanden «Applications» sowie auf deren Ergebnisse liegen. Wir wollen bereits vorhandene Konzepte nutzen, welche im besten Fall bereits angewendet und wissenschaftlich untersucht oder ausprobiert wurden (1). Die Ergebnisse die wir finden, wollen wir wenn möglich in unsere Schulung einbinden, da der Fokus der Arbeit nicht ist ein von Grund auf neues Schulungskonzept zu entwickeln, sondern vorhandenes in einer als Beispiel Lern-Plattform zu Verfügung zu stellen (2). Strukturiert wird der Review nach den gefundenen Konzepten um so einen Überblick zu erhalten, welche Konzepte erarbeitet wurden (3). Die Literatur sollte neutral betrachtet werden, da unser Ziel die Integration von verschiedenen Quellen sein soll. Erst in einem zweiten Schritt soll eine Position vertreten werden, welches die gewählten Schulungsmethoden sind (4). Diese Arbeit soll einen Nutzen und mögliche Quelle für weitere Untersuchungen und praktische Beispiele bieten, deshalb könnte sich die Leserschaft aus Wirtschaftsvertretern oder zukünftigen Studenten ergeben (5). Und schlussendlich wird die Literaturrecherche nicht der zentrale Punkt dieser Arbeit sein, sondern soll einen Überblick über die vorhandene Literatur gewähren. Da im Bereich der Cyber-Security Schulungen viel an Literatur bereits vorhanden ist, wird sich dieser Review auf eine repräsentative Auswahl beschränken (6).

[27] Jan vom Brocke et al. (2009, p. 10).

Characteristics		Categories			
(1)	Focus	Research outcomes	Research methods	Theories	Applications
(2)	Goal	Integration	Criticism	Central issues	
(3)	Organisation	Historical	Conceptual	Methodological	
(4)	Perspective	Neutral representation		Espousal of position	
(5)	Audience	Specialised schoolars	General scholars	Practitioners/Politicians	General public
(6)	Coverage	Exhaustive	Exhaustive and selective	Representative	Central/Pivotal

Abbildung 2: Klassifizierung Characteristics nach Jan vom Brocke et al., 2009, p. 10

Um nun einen Suchstring zu erhalten welcher die angestrebte Literatur bietet, muss zuerst geklärt werden, was über das Thema bereits in Erfahrung gebracht wurde.[28] Im Kapitel 2 wurde das Thema Phishing bereits behandelt und Literatur zu diesem Thema ist vorhanden. Bei den Schulungskonzepten von Phishing als Teil von Cyber-Security gibt es verschiedene Ansätze. Um nur ein Beispiel zu zeigen, Cone, Irvine, Thompson, and Nguyen (2007) zeigten die Möglichkeit auf ein Videospiel zu benutzen um Spielern Cyber-Security Risiken näher zu bringen.[29] Die weitere Literatur wird durch den Literatur Review erarbeitet.

3.1.2 Suchbegriff

Aufgrund der vorhergehenden Erkenntnissen wird mit folgendem Suchbegriff nach Literatur gesucht welche für den Review betrachtet wird.

(Phishing AND Education) OR (Phishing AND Teaching)

Die Online Bibliotheken EBSCOhost, Web of Science und ACM Digital Library wurden mit dem Suchbegriff abgefüllt. Bei ProQuest gab es bei einer ersten Suche über 5000 Ergebnisse, deshalb wurde die Suche auf «Peer Reviewed» eingeschränkt, was zu 384 Literaturquellen führte, dies übersteigt jedoch die Möglichkeit zur einzelnen Überprüfung und deshalb wurden diese Suchergebnisse nicht miteinbezogen in den Literaturreview. Es wurden Suchergebnisse,

[28] Torraco (2016, p. 359).

[29] Cone et al. (2007).

welche unvollständige Informationen enthielten ausgesondert. Die gefundenen Titel wurden in Kategorien sortiert anhand des Quelltitels und des Abstracts. Die Kategorien sind «Human Factor», «Technology Approach» und «Weitere Themen».

Der «Human Factor», alle Quellen welche mit dem menschlichen Faktor in Sachen Phishing zu tun haben.[30] Der «Technology Approach», welcher alle Literatur zu Technischen Ansätzen und Lösungen beinhaltet. Zusätzlich wurde eine dritte Kategorie «Weitere Themen» für Quellen, welche zu keiner der oberen Kategorie passen erfasst. Nach dem kategorisieren und aussortieren der ersten Runde sind bei «Human Factor» noch 27 Quellen übrig. «Technology Approach» beinhaltet 50 Quellen und 5 Quellen sind nicht eindeutig zuteilbar oder behandeln weitere Themen und Aspekte. Um diese Auswahl an Quellen zu verfeinern werden die Abstracts der Titel gelesen und interessante für eine weitere Runde markiert.

Am Ende des Literatur Review blieben 12 Quellen übrig, die für diese Arbeit sicher verwendet werden können und weiterführendes Wissen über das Thema Phishing-Education vermitteln. Die Abbildung illustriert die Anzahl Suchergebnisse und die darauffolgende Selektion sowie die schlussendliche Auswahl von 12 Quellen.

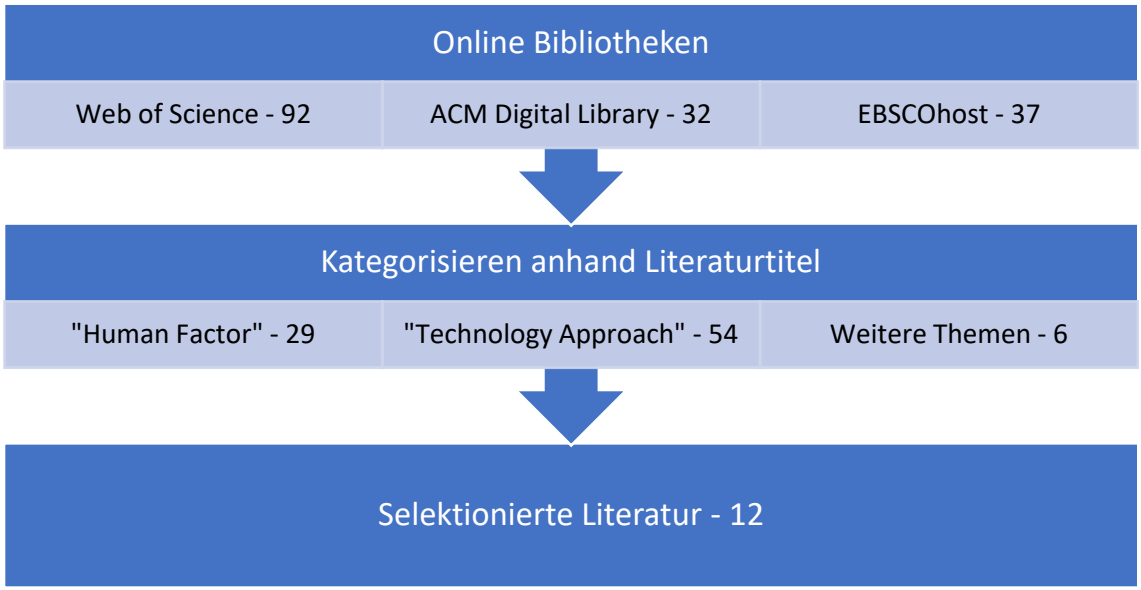


Abbildung 3: Eigene Darstellung Literaturreview

Im folgenden Abschnitt wird ein Überblick über die selektionierten Quellen (Anhang 12.1) gegeben und weshalb diese Quelle für den Literaturreview gewählt wurde.

[30] Robila and Ragucci (2006, p. 237).

3.1.3 Überblick Literaturreview

Der Literaturreview beinhaltet verschiedenen Methoden und Praxisbeispiele zur Phishing-Education und zusätzlich Literatur zum Thema der technischen Massnahmen gegen Phishing. Welche Themen in einem Phishing-Wissenstransfer enthalten sein könnten, wird durch die Arbeit von Emigh (2005) abgedeckt. Phishing-Technologien sowie Gegenmassnahmen werden erläutert. Emigh (2005) definiert Phishing dabei folgendermassen: *«Phishing is online identity theft in which confidential information is obtained from an individual.»* [31] Daraufhin werden die einzelnen Arten von Phishing-Attacken wie Keyloggers, Web Trojans und Man-in-the-middle analysiert und dazugehörige Gegenmassnahmen diskutiert. Der Fokus der Arbeit liegt auf den technologischen Aspekten von Anti-Phishing Massnahmen.[32]Welche Lern-Methodik die Beste ist, versuchen Hoepman et al. (2016) zu ermitteln. Dabei wurden in einer Studie die drei Methoden «text-based training», «computer-based training» und «instructor-based training» miteinander verglichen. Bewertet wurden die drei Ansätze in den Kategorien «effectiveness», «confidence», «user satisfaction» und «time efficiency». Die Studie hat ergeben, dass «instructor-based training» bei den drei Kriterien «confidence», «effectiveness» und «user satisfaction» das Feld anführt, jedoch bei «time efficiency» einen grossen Nachteil gegenüber den anderen beiden Methoden hat. Bei den ersten drei Kriterien schneidet «text-based training» leicht schlechter ab als «instructor-based training»; bei Anwendungsfällen, die zeitkritisch sind, ist es jedoch die schnellste Methode. Schlussendlich ist «computer-based training» bei allen vier Kategorien am schwächsten einzustufen. Hoepman et al. (2016) weisen darauf hin, dass die Methode aber das Erkennen von Phishing URLs erheblich verbessert hat. Ebenfalls erlaubt diese Methode das Lernen auf jeglichen digitalen Geräten und kann so durch die Benutzer jederzeit ausgeführt werden.[33] In die Kategorie von «computer-based training» ist die Arbeit von Perrault (2018) einzuteilen. Durch die Teilnahme an einem Online-Quiz sollen Studenten lernen, Phishingmails zu erkennen. Die Teilnehmer bestehen aus College Studenten, da diese oft Opfer von Phishing-Attacken werden.[34] Das Quiz besteht aus Bilder von Emails die entweder Phishingmails oder echte Emails darstellen. Die Studenten mussten wählen um welchem Typ es sich bei den gezeigten Bildern handelt. Das Ergebnis der Studie zeigt auf, dass vor allem die Selbsteinschätzung der Studenten beeinflusst wurde.[35] Zusätzlich bietet ein

[31] Emigh (2005) (2005, p. 1).
[32] Emigh (2005, p. 47).
[33] Hoepman et al. (2016, p. 148).
[34] Perrault (2018, p. 1155).
[35] Perrault (2018, p. 1163).

interaktives Quiz eine günstige und einfache Möglichkeit, College-Studenten zu schulen.[36] Sheng et al. (2007) und Cone et al. (2007) setzten ein Videospiel ein um Anti-Phishing Schulungen zu betreiben. Der Ansatz von Cone et al. (2007) basiert dabei auf einem Spiel namens CyberCIEGE, welches von der US Naval Postgraduate School im Jahr 2005 veröffentlich wurde. Der Fokus liegt bei diesem Spiel nicht auf Phishing sondern der Cyber-Security als ganzheitliches Thema. Das Ziel des Spieles ist es, den Benutzer mit interaktiven Inhalten im Bereich der Cyber-Security zu schulen. Das Spiel wurde nach der Entwicklung bereits in verschiedenen Organisationen eingesetzt und dient zur Weiterbildung und Unterstützung bei der Cyber-Security Schulung.[37] Dagegen verwenden Sheng et al. (2007) in ihrer Studie ein Spiel mit dem Namen «Anti-Phishing Phil», welches Benutzern Regeln und Tipps vermittelt, die sie vor Phishing-Attacken schützen sollen. Das Spiel wurde mit einem Versuch auf seine Effektivität gemessen. Dabei wurden Benutzer vor und nach dem Spielen von «Anti-Phishing Phil», auf ihre Fähigkeiten getestet, Phishing-Websites zu erkennen.[38] Das Spiel wurde mit vorhandenen Schulungsmethoden verglichen. Dabei wurde festgestellt, dass Benutzer, welche «Anti-Phishing Phil» gespielt haben, besser zwischen einer Phishing-Website und einer normalen Website unterscheiden konnten.[39] Die Studie kam zu Schluss, dass interaktive Spiele eine vielversprechende Möglichkeit sind, um Benutzern beizubringen, nicht auf Phishing-Attacken einzugehen.[40] Das Design eines Phishing Training-Systems wurde von Kumaraguru et al. (2007) vorgenommen. Dabei wurde dieses Trainings-System mit Interventionen während dem täglichen Umgang mit Emails gestaltet. Die Interventionen kamen in Form eines Comics mit Text und Grafiken und wurden beim Klick auf einen Link in einem Trainings-Email geöffnet, um dem Benutzer Hinweise zu vermitteln, worauf bei Phishing zu achten ist.[41] Kumaraguru et al. (2007) kommt zum Schluss, dass Training-Emails und Interventionen Benutzern helfen können, Phishing-Attacken zu identifizieren. Die Intervention, mit Comic stellte sich dabei als die effektivste Methode heraus. Zusätzlich wurden aufgrund der Resultate, Design-Prinzipien für Training-Systeme empfohlen.[42] Kumaraguru, Sheng, Acquisti, Cranor, and Hong (2010) vergleichen den Comic von Kumaraguru et al. (2007) und das Videospiel von Sheng et al. (2007) in einer Studie mit anderen Training-Systemen. Sie

[36] Perrault (2018, p. 1165).
[37] Cone et al. (2007, p. 63).
[38] Sheng et al. (2007, p. 88).
[39] Sheng et al. (2007, p. 97).
[40] Sheng et al. (2007, p. 98).
[41] Kumaraguru et al. (2007, p. 908).
[42] Kumaraguru et al. (2007, p. 913).

kommen zum Schluss, dass interaktives Anti-Phishing Training effektiver ist als das Versenden von Sicherheitshinweisen zu Phishing. Weiter steigert das Spielen des Anti-Phishing Phil Videospiels die Performance im Erkennen von Phishingmails und Webseiten. Die Inhalte welche gelernt wurden, konnten bis zu einer Woche beibehalten werden ohne einen signifikanten Performance-Verlust zu erleiden.[43] Von Nyeste (2011), wurden die beiden Training-System ebenfalls verglichen. Dabei sind die beiden Ansätze verschiedenen Tests (DST, CRT, Computer Experience[44]) unterzogen worden. Wie schon in den beiden vorangegangenen Studien von Sheng et al. (2007) und Kumaraguru et al. (2007) wurde dargelegt, dass die beiden Methoden wirksam die Anfälligkeit vor Phishing-Attacken senken können. Dies sowohl bei Studenten, wie auch bei Personen mit Erfahrung im Benutzen von Computern.[45] Ein System welches Training, Monitoring und Reporting ermöglichen, wurde von Lim, Park, and Lee (2016) entworfen. In einer Feld-Studie konnte erwiesen werden, dass dieses Trainings-System die «Click-Rate» von Links von 16% auf 12% senken konnte.[46]

Firmen setzen oft auf drei Schutz-Schichten im Bereich Phishing. Die erste Schicht besteht aus dem automatischen Erkennen und Entfernen von Phishingmails. Die Zweite aus einem Warnungs-Mechanismus welcher die Mitarbeiter vor verdächtigen Emails oder Webseiten warnt. Drittens, wird ein Verhaltens-Training durchgeführt welches den Mitarbeitenden das Erkennen von Phishingmails erleichtern soll.[47] Jensen et al. (2017) haben in der dritten Schicht eine Methode genannt «Mindfulness Techniques» angewendet und in einer Studie mit regelbasiertem Verhaltens-Training verglichen. Es konnte festgestellt werden, dass bei dem «Mindfulness» Verhaltens-Training ein kleinerer Anteil auf Phishingmails herein gefallen ist.[48]

Warum Personen auf Phishingmail reagieren, haben D. Kim and Hyun Kim (2013) analysiert. Dabei wurde ein «persuation mechanism framework» verwendet, um die für Phishingmails überzeugenden Inhalte und Darstellungen zu finden. Die Kriterien Inhalt und Struktur eines Phishingmails wurden betrachtet. Eine semantische Methode, um Textinhalte zu analysieren, wurden in der Studie zusätzlich angewendet.[49] Es wurde herausgefunden, dass erstens ein Zeitdruck in Phishingmails benutzt wird, um die Empfänger zu manipulieren und ihnen keine

[43] Nyeste (2011, p. 1).
[44] Nyeste (2011, pp. 40–41).
[45] Nyeste (2011, pp. 65–66).
[46] Lim et al. (2016, p. 1118).
[47] Jensen, Dinger, Wright, and Thatcher (2017, p. 599).
[48] Jensen et al. (2017, p. 617).
[49] Kim, D. and Hyun Kim (2013, pp. 838–839).

Zeit gelassen wird, die Emails genauer zu studieren. Zweitens werden oft logische und emotionale Anfragen benutzt, um die Erfolgsquote von Phishingmails zu erhöhen. Dies zeigt sich in Beispielen wie Security-Anfragen von Account-Informationen oder der Androhung von Konsequenzen, wenn der Aufforderung nicht Folge geleistet wird. Die Struktur soll beim Benutzer Bedenken aufkommen lassen und ihn somit zur Angabe von Account Informationen verleiten.[50] Durch Harrison, Svetieva, & Vishwanath (2016) wurden die individuellen Faktoren der Phishing-Empfänger analysiert. Dabei wurde festgestellt, dass Personen je nach Wissen und Erfahrung mit Phishingmails unterschiedlich auf Manipulationen reagieren. Eine generelle Aussage kann nur dahingehend gemacht werde, dass die Empfänglichkeit für Täuschung durch Phishingmails unterstützt wird durch einen «information processing style».[51]

3.1.4 Diskussion Literaturreview

Durch den Literaturreview konnten Ansätze für das Design der Lernplattform erarbeitet werden. Als Hilfestellung können von Nyeste (2011) und Kumaraguru et al. (2007) die angegeben Handlungsempfehlungen benutzt werden. Die verschiedenen Lern-Methoden (Comic, Quiz, «Mindfulness», Videospiel) sind alle online verfügbar. Die Analyse von Hoepman et al. (2016) hat gezeigt das das «computer-based learning» als Methode am schlechtesten abschneidet, jedoch Vorteile im Bereich der Verfügbarkeit, Zeit und Geld bringt. Auch ist die Tiefe des möglichen Wissenstransfers nicht zu vergleichen mit anderen Formen. Wenn die Lern-Plattform tiefgreifendes Phishing-Wissen vermitteln soll, könnte eine Kombination zweier Ansätze (zum Beispiel; computer-based + paper-based) durchaus Sinn ergeben. Wenn das Ziel der Lern-Plattform ist, die Anfälligkeit vor Phishing-Attacken zu senken, dann ist eines der genannten Beispiele der richtige Ansatz. Wobei hier das Quiz oder ein Videospiel, den schnellsten Lerneffekt hervorrufen könnten. Bei diesen ist die Interaktion der Teilnehmer nötig, was den Wissenstransfer beschleunigen kann. Weiter sollte die Lern-Plattform während der täglichen Arbeit angewendet werden können.[52] Ein Quiz welches direkte Beispiele von Phishingmails erläutert, könnte den täglichen Email Gebrauch sicherer gestalten. Ein Quiz, wäre anhand der Argumente aus der Diskussion zum Literaturreview ein mögliches Design der Lern-Plattform.

[50] Kim, D. and Hyun Kim (2013, p. 847).

[51] Harrison, Svetieva, and Vishwanath (2016, pp. 278–279).

[52] Kumaraguru et al. (2007, p. 913).

4 Phishing-System

Im folgenden Kapitel wird die Vorgehensweise sowie die technische Umsetzung des Phishing Versuches näher erläutert. Zuerst werden die Rahmenbedingungen für diesen Versuch dargestellt. Danach wird das Phishing-System konzeptionell und technisch erläutert. Die Umsetzung der prototypischen Lern-Plattform ist nicht Bestandteil dieses Kapitels.

4.1 SMC Schweiz AG

Die SMC Schweiz AG ist ein Tochterunternehmen der SMC Corporation, welche in der Automationsbrache tätig ist[53]. Mit weltweit ca. 18'000 Mitarbeitern zählt die SMC Corporation zu den weltweit grössten Unternehmungen im Bereich der Maschinen-Automation. Der Schweizer Ableger war das erste Tochterunternehmen im europäischen Raum und zählt mit seinen 120 Mitarbeitern als KMU. Da Produktion und Entwicklung hauptsächlich an den asiatischen Standorten der SMC Corporation zu finden sind, ist die Mehrheit der Belegschaft in der Schweiz im kaufmännischen Bereich angesiedelt.[54]

4.2 Phishing Vorfälle

Die SMC Schweiz AG wurde in den letzten Jahren Opfer von Phishing. Bei den vorgefallenen Phishing-Attacken handelte es sich um sogenannte Ransomware.[55] In einem Fall, wurden durch den Klick eines Mitarbeiters auf den Link in einem Phishingmail eine Ransomware-Applikation heruntergeladen und ausgeführt. Diese Applikation hat innerhalb von Sekunden alle für diesen Mitarbeiter zugänglichen Dateien verschlüsselt. In einem weiteren Vorfall wurde ebenfalls Ransomware eingesetzt, dabei wurde nicht auf einen Link geklickt sondern der Anhang eines Mails geöffnet. In beiden Fällen konnten die verschlüsselten Dateien wieder hergestellt werden. Aber aufgrund dieser beiden Vorfällen hat sich die SMC dazu entschlossen, an dieser Bachelorarbeit mitzuwirken und die Mitarbeiter an dem Versuch teilnehmen zu lassen.

[53] ("Corporate Summary／Corporate Principles").

[54] Corporation.

[55] Gavin O'Gorman and Geoff McDonald (2012).

4.3 Rahmenbedingungen

Folgende Rahmenbedingungen sind durch die SMC sowie die vorangegangene Studie der Literatur klar ersichtlich geworden.

4.3.1 SMC

Jedes E-Mail, das für diese Arbeit an Mitarbeiter der SMC gesendet wird, muss zuerst durch ein eingeweihtes Mitglied der Geschäftsleitung geprüft und freigeben werden. Die Daten, die erhoben werden, sind anonymisiert zu halten und es sollen keine Benutzer-Daten, zum Beispiel Nutzername und Passwort, gespeichert werden. Durch die SMC erlaubt wird aber die Möglichkeit, auszuwerten, ob ein Mitarbeiter nur das Mail geöffnet hat oder aber den Link geklickt sowie Daten eingeben hat.

4.3.2 Versuchsteilnehmer

Die Teilnehmer setzten sich aus den Mitarbeitenden der SMC zusammen. Dabei verfügen 112 Mitarbeitende über eine persönliche E-Mail Adresse. Die Teilnehmer wurden wie in Tabelle 1 ersichtlich, aufgeteilt. Um die Resultate des Versuches nicht zu beeinflussen ist nur eine Person der Geschäftsleitung sowie eine verantwortliche Person aus der IT-Abteilung über den geplanten Versand von Phishingmails informiert. Zusätzlich ist der Autor dieser Arbeit ebenfalls aufgeführt. Die Anzahl Teilnehmer pro Geschlecht in den Gruppen ist ebenfalls in der Tabelle 1 aufgelistet.

Gruppen	***Anzahl Teilnehmer***	***Männlich***	***Weiblich***
Involvierte Mitarbeiter	3	3	0
«Controlling» Gruppe	55	48	7
«Education» Gruppe	54	43	11
Total	**112**	**94**	**18**

Tabelle 1: Demographie Versuchsteilnehmer

Die Gruppe «Involvierte Mitarbeiter» besteht aus dem Autor, einem Mitglied der Geschäftsleitung sowie dem Verantwortlichen der IT-Abteilung der SMC. Diese Gruppe erhält keine Phishingmails, da sie über den Phishing-Versuch informiert ist. In die Gruppe «Controlling» wurden die ersten 55 Mitarbeiter nach Alphabet des Vornamens eingeteilt. In die

Gruppe «Education» wurden die 54 noch übrigen Mitarbeiter eingeteilt. Um nicht anhand von Vorkenntnissen des Autors über die Teilnehmer die Gruppenwahl zu beeinflussen, wurde die Methode mit dem Aufteilen nach Alphabet gewählt. An den beiden Teilnehmer-Gruppen «Education» und «Controlling» wird der Einfluss der Lern-Plattform beobachtet.

4.3.3 Ethik

Der ethische Aspekt eines Phishing-Versuches sollte durch den Autor abgeklärt werden, um möglichen ethischen Fragen und Vorfällen vorzubeugen. Um diese Voraussetzung zu untersuchen wird die Arbeit von Rasha Salah El-Din (2012) hinzugezogen.[56] Darin wird eine Roadmap vorgeschlagen, welche als Hilfestellung zur Klärung der ethischen Voraussetzungen dient. Diese Roadmap wird in diesem Versuch ebenfalls als Hilfestellung benutzt. Bei dem in dieser Arbeit angewendeten Versuch handelt es sich um eine «In-the-wild field-study»[57]. Ein solcher Versuch gibt vor, dass die Teilnehmer gezielt nicht informiert werden, um so das Verhalten der Teilnehmer nicht zu beeinflussen. Diese Art des Versuches ist die ethisch und rechtlich komplizierteste Form einer Phishing-Studie.[58] Zuerst müssen die verschiedenen ethischen Anspruchsgruppen angeschaut werden. Aus Sicht des Autors ist die Täuschung der Teilnehmer eine Voraussetzung, um zu verhindern, dass diese durch das Wissen der Versuchsteilnahme die Ergebnisse beeinflussen könnten. Die SMC als Unternehmung hat als firmeninternes Leitbild den Wert «Vertrauensvoll zusammenarbeiten». Die SMC möchte diesen Wert bewahren und deshalb ist die Täuschung der Mitarbeitenden so gering wie möglich zu halten. Die Täuschung, welche in einem Versuch angewendet wird, wurde durch die Arbeit von Rasha Salah El-Din folgend beurteilt: «*Although deception is a well-established research methodology in psychology, it is relatively new to security related research and accordingly provokes ethical debate. We argue that the use of deception in phishing research can be totally safe.*»[59]

In der Praxis bedeutet dies, dass die Mitarbeitenden von SMC während der Teilnahme nicht über die Phishingmails informiert werden. Nach dem Abschluss dieser Arbeit wird diese Information an alle nachgereicht.

[56] Rasha Salah El-Din (2012).
[57] Rasha Salah El-Din (2012, p. 2).
[58] Rasha Salah El-Din (2012, p. 1).
[59] Rasha Salah El-Din (2012, p. 4).

4.3.4 Technische Rahmenbedingungen

Die Technische Lösung, die für diesen Versuch benötigt wird, soll folgende Punkte umfassen;

- Emails an mehrere Empfänger gleichzeitig zu senden
- Ermöglicht Header und Body der Emails zu verändern
- Nachverfolgung der versendeten Emails (Angekommen, Email geöffnet, Link geöffnet und Daten eingegeben)
- Web-Server welcher die Phishing-Website enthält
- Technische Lösung innerhalb des SMC Netzwerkes

Die Bedingung, Emails an mehrere Empfänger zu versenden, ist aufgrund der beiden Teilnehmergruppen unbedingt nötig. Wenn die Emails manuell an jeden einzelnen Mitarbeiter gesendet werden müssten, bestände die Möglichkeit, dass sich die Mitarbeiter gegenseitig beeinflussen. Wenn Teilnehmer X von Abteilung A das Phishingmail vor dem Teilnehmer Y aus Abteilung A erhält, kann X Teilnehmer Y warnen, nicht auf das Email zu klicken. Da dieser Effekt nicht gemessen werden kann durch diesen Versuch, soll er möglichst vermieden werden. Wenn das Email bei allen Teilnehmern gleichzeitig eintrifft, kann eine Entscheidung ob das Mail legitim ist oder nicht, von jedem Teilnehmer einzeln getroffen werden. Trotzdem kann der Effekt der gegenseitigen Warnung nicht ganz ausgeschlossen werden, da davon auszugehen ist, dass Emails nicht von allen Teilnehmern sofort nach Erhalt geöffnet werden, aber eine Mehrheit innerhalb eines Tages auf Emails reagiert.[60] Der Inhalt des Email soll möglichst vertrauenswürdig erscheinen und deshalb soll der Header veränderbar sein, um dem Teilnehmer einen ihm bekannten Absender zu suggerieren. Ebenfalls muss der Body angepasst werden um den Text des Emails zu gestalten und einen Link auf die Phishing-Webseite im Email hinterlegen zu können. Die Nachverfolgung der versendeten Emails soll der zentrale Bestandteil dieses Phishing-Systems sein, da die Auswertung einerseits die Information für das Schulungskonzept liefert und andererseits die Effektivität des Schulungskonzeptes im Nachhinein testen soll. Der im Phishingmail enthaltene Link soll auf eine Phishing-Website führen, deshalb muss die Lösung das Hosting einer Website ermöglichen. Das ganze Phishing-System soll innerhalb des SMC Netzwerkes aufgebaut werden, um die Information wie Email-Adressen sowie Namen der Mitarbeiter, welche im Phishing-System vorhanden sind, zu schützen. In einem zweiten Schritt werden Emails, welche innerhalb des SMC Netzes versendet werden, nicht durch die Security Gateways von SMC geprüft. Das garantiert, dass die Emails

[60] Yoram M Kalman and Sheizaf Rafaeli (2005, p. 5).

bei den Mitarbeitern ankommen und nicht durch die vorhandenen Sicherheitsmassnahmen der SMC gefiltert werden.

4.3.5 Phishingmails Inhalt

Der Inhalt eines Phishingmails soll für die Teilnehmer plausibel sein. Es werden also keine «Prinz von Namibia» Emails versendet, sondern Inhalte, welche sich auf die SMC beziehen. Da man bei Phishing-Attacken von Social Engineering ausgehen kann, kann firmeninternes Wissen auch verwendet werden, welches zum Beispiel über die Social Media Kanäle der Firma oder über das Abfangen von nicht verschlüsselten Emails gesammelt werden kann.[61] Der genaue Inhalt der jeweils versendeten Mails wird in den Kapitel der Versuchsanalyse beschrieben.

4.3.6 Bewertung / Messung

Durch die Vorgaben der SMC wird klar definiert welche Ereignisse gemessen werden können bei den Phishingmails;

- Email geöffnet/gelesen
- Link im Email geöffnet
- Daten auf der Phishing-Website eingeben (Die eingegeben Daten dürfen nicht gespeichert werden)
- Anzahl Tickets welche bei der IT Abteilung geöffnet werden

Das erste Email, welches versendet wird, soll zeigen, wie die Mitarbeiter der SMC auf ein solches Mail reagieren. Es soll gemessen werden wie oft das Mail geöffnet und gelesen wurde sowie die Anzahl der Aufrufe des Links. Schlussendlich wird die Anzahl der Mitarbeiter gemessen werden, welche auf der Phishing-Website auch ihre persönlichen Daten hinterlegt haben. Ob das Lernkonzept eine Verbesserung in der Erkennung von Phishingmails gebracht hat, soll durch die nachfolgenden zwei Phishingmails gemessen werden. Alle innerhalb von 72 nach dem versenden der Phishingmails, geöffneten Mails zählen für die Auswertung. Nach 72 Stunden wir die Phishing-Webseite deaktiviert und somit werden danach geöffnete Emails nicht mehr gemessen. Durch die Aufteilung in eine «Education» und eine «Controlling» Group soll der Effekt beobachtet werden. Ebenfalls gemessen werden auch die Anzahl Tickets, die nach der Versenden eines Phishingmails geöffnet wurden. Die Messung der geöffneten IT Tickets wird durch das Ticketing System der SMC ermöglicht, dieses wird in dieser Arbeit nicht weiter

[61] Heartfield, Loukas, and Gan (2016).

beschrieben. Aus der Anzahl geöffneter Tickets könnten weitere Schulungsinhalte entstehen, in denen die Mitarbeiter instruiert werden, sich bei Verdacht in der IT Abteilung zu melden.

4.4 Phishing-System

Das Phishing-Versuchssystem wird in der Folge methodisch und technisch beschrieben und die Rahmenbedingungen werden angewendet.

4.4.1 System Konzept

Das Versuchssystem besteht aus einem Email-System, einem Phishing-System sowie einem Monitoring-System. Dabei wird das «Center System» von Lim et al.[62] als Basis genommen und anhand der Rahmenbedingungen in Kapitel 4.3 angepasst. So hat das «Center System» zusätzlich ein SMS-System, welches analog zu den Phishingmails auch SMS an die Teilnehmenden sendet. Aber dieses Phishing SMS-System kann bei unserem Versuch nicht berücksichtigt werden, weil nur wenige Teilnehmer über ein Unternehmensmobiltelefon verfügen. Ebenfalls wird das «Content System» nicht in den Versuch mit aufgenommen. Das «Content System» sammelt und speichert Informationen, die für die Teilnehmer des Versuches von Interesse sein könnten. Da der Autor die Unternehmung kenn, kann er auch bestens abschätzen, welche Informationen für die Mitarbeiter interessant sein könnten. Der Inhalt der versendeten Phishingmails wird durch den Autor anhand von Beispielen in verwandten Arbeiten kombiniert, mit Kenntnissen der verwendeten Arbeitsweise und Applikation der SMC. Parsons, McCormac, Pattinson, Butavicius, and Jerram haben die Phishingmails in Kategorien eingeteilt.[63] Die Emails, die für diesen Versuch versendet werden, sind aus der Kategorie «Risk or Loss», welche im Email jeweils einen Link zu einer Phishing-Website enthalten und dort zur Eingabe von persönlichen Informationen auffordern.[64] Diese Kategorie zählt nicht zu jenen Phishingmails, die durch Social Engineering für untrainierte Benutzer fast unmöglich zu erkennen sind.

[62] Lim et al. (2016, p. 1112).
[63] Parsons et al. (2015, p. 197).
[64] Parsons et al. (2015, p. 197).

4.4.2 Technische Umsetzung

Auf der Basis der ausgewählten Komponenten des «Center System» von Abschnitt 4.4.1 und den im Kapitel 4.3 genannten Rahmenbedingungen, wird im folgenden Abschnitt die Technische Lösung aufgezeigt und beschrieben.

4.4.3 Gophish

Nach einer Internetrecherche und dem Testen von verschiedenen Tools und Applikationen zum Thema Phishing, hat sich der Autor für die Opensource-Lösung Gophish entschieden. Dieses Phishing-System wurde extra für Organisationen entwickelt um Phishing-Tests durchzuführen und zu analysieren.[65] Diese Applikation erfüllt alle Rahmenbedingungen für diesen Versuch. Das Phishing-System ist auf einem Server innerhalb des SMC Netzwerkes gehostet. Die Daten, welche durch das Phishing-System enthalten sind so zu jedem Zeitpunkt innerhalb des Firmennetzwerkes vorhanden. Gophish kann auf einen built-in Web-Server Phishing-Websites hosten. Die Analyse der Log Files dieses Web Servers wird durch die Applikation direkt vorgenommen. Gophish ermöglicht es sogenannte «Phishing Kampagnen» zu erstellen. Diese

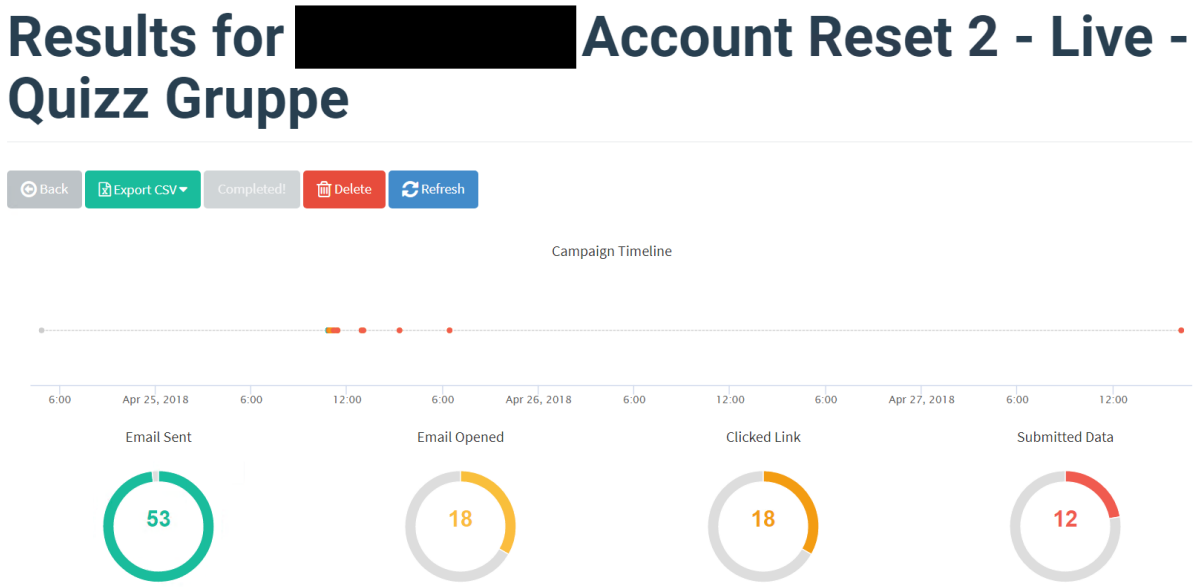


Abbildung 4: Beispiel Kampagne Gophish

[65] GoPhish (2012).

überwachen eine Phishing-Attacke vom Versand des Email bis hin zu den Ergebnissen, wie in Abbildung 4 ersichtlich. Um mit Gophish gezielte Phishing-Attacken durchzuführen ist kein tiefgründiges Wissen in den technischen Aspekten von Phishingmails und Webseiten nötig. Die Applikation kann durch ein einfaches Setup, mit minimaler Konfiguration, installiert und verwendet werden. Gophish ist deshalb gut geeignet, um einfache Phishing-Versuche in Unternehmen durchzuführen, auch wenn sie nicht die Ressourcen und Expertise haben um Phishing-Prävention aktiv zu betreiben.[66]

[66] Portmann and Hirschi (2018, p. 457).

5 Auswertung 1. Phishingmail

Das erste Phishingmail wurde an die beiden Gruppen «Education» und «Controlling» versendet. Im folgenden Kapitel werden die Resultate dieses ersten Versuches analysiert.

5.1 Inhalt Phishingmail

Das versendete Email besteht aus einem Text und einem Link zu einer Phishing-Website. Wie in Abbildung 5: Phishingmail 1 ersichtlich, ist der Absender des Emails die Adresse supportit@smc.ch. Bei der Domain smc.ch handelt es sich um die Email-Domain von SMC. Die Adresse supportit@smc.ch ist aber keine offizielle Adresse, die von der Firma genutzt wird. Die Applikation für welches der Aufruf «Account expired» galt, ist ein ERP-System welches durch die SMC eingesetzt wird und von jedem Teilnehmer genutzt wird

. Der Link im Email zeigt auf den Phishingmail Server.

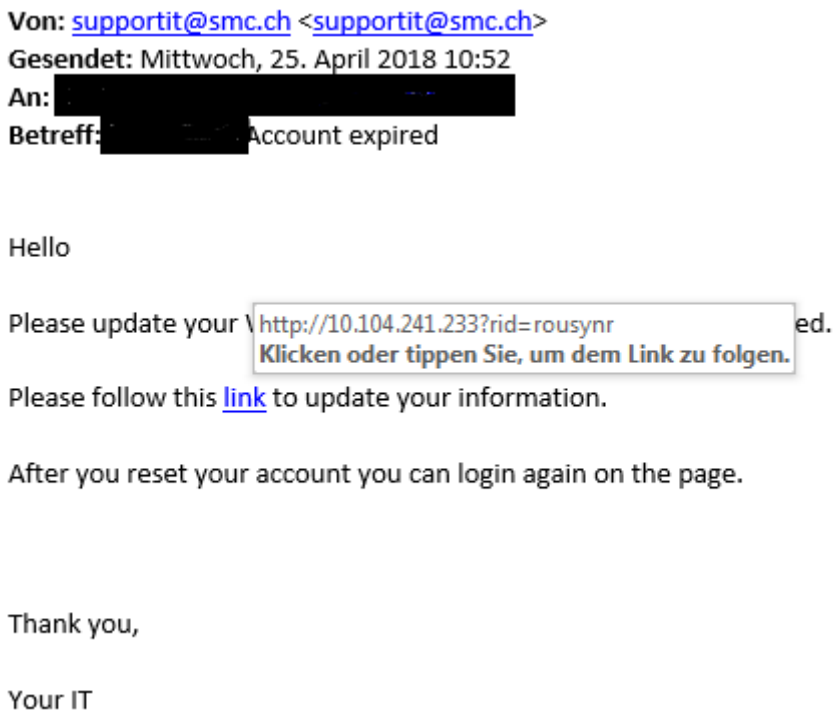


Abbildung 5: Phishingmail 1

5.2 Ergebnisse 1. Phishingmail

Von den 109 versendeten Emails an die Teilnehmer der beiden Gruppen «Education» und «Controlling» wurden 38 Emails innerhalb von 72 Stunden geöffnet. 34.86% der Teilnehmer haben das Email geöffnet und den Inhalt gelesen. Die restlichen 71 Empfänger haben das Email nicht geöffnet. Ob diese Empfänger das Email als Phishingmail identifiziert haben oder das Email gar nicht beachtet haben, ist nicht eruier bar. Es kann die Aussage gemacht werden, dass diese 71 nicht geöffneten Emails als nicht erfolgreiche Phishing-Attacken gezählt werden. Weiter ist von den 38 gelesenen Emails auch in allen 38 Emails auf den Link geklickt worden, was 34.86% der Teilnehmenden entspricht. Somit lässt sich klar sagen, dass das Email von diesen Empfängern bereits als vertrauenswürdig eingestuft wurde. 29 von 38 Teilnehmer haben auf der Phishing-Webseite die angeforderten Daten eingegeben. Somit führte es in 29 von 109 Fällen zum Erfolg der Phishing-Attacke aus Sicht eines «Phishers». Von den 38 geöffneten Links wurde in neun Fällen keine Daten eingegeben. In der IT-Abteilung der SMC wurden 11 Anfragen und Hinweise zu dem Phishingmail eingereicht. Im Laufe des Versuches wurden die Anfragen bei der IT-Abteilung vermehrt auch mündlich oder via Email eingereicht und nicht wie erwartet ausschliesslich via dem bekannten Ticketing System. Alle eingereichten Anfragen zu diesem Phishingmail wurden gezählt, unabhängig vom Medium der Übermittlung.

	Controlling	*Education*	***Total***
Number of Emails	55	54	**109**
Emails opened	20	18	**38**
Rate (%)	36,4%	33,3%	**34,9%**
Clicked Link	20	18	**38**
Rate (%)	36,4%	33,3%	**34,9%**
Submitted Data	17	12	**29**
Rate (%)	30,9%	22,2%	**26,6%**
Rate to click (%)	85,0%	66,7%	**76,3%**
Opened Tickets	3	8	**11**
Rate (%)	5,5%	14,8%	**10,1%**

Tabelle 2: Ergebnis 1. Phishingmail

5.3 Diskussion 1. Phishingmail

Wenn man das Email mit ähnlichen Versuchen vergleicht, war es aus Sicht des Autors kein ausgeklügeltes Phishingmail.[67] Es waren weder grafische Elemente noch eine persönliche Ansprache vorhanden. Trotzdem wurde nicht erwartet, das 34.9% das Email als genügend Vertrauenswürdig eingestuft haben, um den Link zu öffnen. Die Gründe für diesen hohen Wert, können durch diese Auswertung nicht festgestellt werden. Es kann angenommen werden, dass der Aufruf als zu wenig unseriös eingestuft wurde um kritische Gedanken hervorzurufen. Für das Design der Lern-Plattform ergeben sich aber Ansatzpunkte, welche verwendet werden können. Nicht alle Mitarbeitenden der Firma SMC sind über Phishingmails gleich sensibilisiert. Wenn man sich nicht bewusst ist, dass ein Phishingmail eine aktive Gefahr ist, können simple Phishing-Attacken zu Erfolg führen. Die «Awareness» (Bewusstsein) vor Phishing-Attacken zu erhöhen wird deshalb ein Ziel der Lern-Plattform sein. Beim «Submitted Data» Wert ist festzustellen, dass 76.3% die angefragten Daten eingegeben haben und den Unterschied zwischen der Phishing-Webseite und der originalen Website nicht erkannt haben. Ob die 23.7% der Mitarbeiter, welche keine Daten eingegeben haben, misstrauisch wurden bei der Frage nach den Zugangsdaten, ist nicht überprüfbar, jedoch kann man davon ausgehen. Die wenigen Nachfragen und Tickets die bei der IT-Abteilung eingegangen sind, zeigen ebenfalls eine Wissenslücke wie man sich im Zweifelsfall verhalten sollte. Zusammengefasst sieht man, dass ein Drittel der Teilnehmer der Attacke zum Opfer gefallen ist. Deshalb wird durch den prototypischen Einsatz einer Lern-Plattform bei der Hälfte der Teilnehmer eine verbesserte Wahrnehmung von Phishing-Attacken erwartet.

[67] Parsons et al. (2015, p. 198).

6 Design Lern-Plattform

In diesem Kapitel werden die Anforderungen und Ziele an die Lern-Plattform erfasst. Anschliessend wird ein Prototyp entworfen und im anschliessenden Kapitel 7 in der SMC implementiert.

6.1 Ziele der Lern-Plattform

Im Literaturreview in Abschnitt 3.1.4 sind bereits Ziele dieser Lern-Plattform ersichtlich geworden. Das übergeordnete Ziel dieser Lern-Plattform soll der Wissenstransfer im Bereich Phishing sein. Wie in Kapitel 2 erläutert, ist die Phishing-Thematik sehr umfassend. Deshalb ist das Ziel nicht auf den ganzen thematischen Inhalt von Phishing ausgelegt, sondern nur auf den Teil, welcher den Mitarbeitenden eines KMUs einfache und simple Möglichkeiten zum Erkennen von Phishingmails bietet. Dies wird auf die zwei folgenden Ziele aufgeteilt. Die «Awareness» zu erhöhen, dass es Phishing-Attacken gibt und diese auch stattfinden in einem KMU (Diskussion des ersten Phishingmails, Abschnitt 5.3). Das zweite Ziel ist das Bereitstellen von inhaltlichen Hilfestellungen zu Phishingmails. Im Literaturreview, wurden inhaltliche Punkte von Kumaraguru et al. (2007) und Jensen et al. (2017) erarbeitet, welche in das zweite Ziel integriert werden. Zusätzlich soll durch die Lern-Plattform klar werden, wie sich die Teilnehmer selbst einschätzen, eine Phishing-Attacke erkennen zu können oder nicht und es soll auch aufzeigen, wie hoch der aktuelle Wissensstand bei den Teilnehmern überhaupt ist. Damit können die Hilfestellungen im zweiten Ziel entsprechend dem Wissensstand angepasst werden, falls die Lern-Plattform in der SMC weiter verwendet wird. Wenn die Lern-Plattform eine Verbesserung im Erkennen von Phishing-Attacken ermöglicht, könnte diese auch zukünftig bei der SMC eingesetzt werden. Zusammengefasst soll die Lern-Plattform diese Ziele erfüllen:

1. Phishing «Awarness» vermitteln
2. Hinweise & Hilfestellungen im Umgang mit Phishingmails
3. Abfrage des aktuellen Wissenstandes der Teilnehmer (Zukunft)

6.1.1 Methodische Anforderungen der Lern-Plattform

Die inhaltlichen Ziele wurden festgelegt, folgend müssen diese durch Wissenstransfer vermittelt werden. In verschiedenen Quellen werden bereits Handlungsempfehlungen und Einschätzungen zu einzelnen Trainings-Methoden angegeben.[68] Diese Ansätze werden im Abschnitt 3.1.4 diskutiert und sollen für das Design wieder hinzugezogen werden. Eine wichtige Anforderung an die Lern-Plattform kommt aus dem Titel der Arbeit (multimedial) und bezieht sich auf die eingesetzten Medien. Das Design soll so aufgebaut sein, dass je nach Inhalt und Rahmenbedingungen verschiedene Medien genutzt werden können.

6.2 Design Prototyp

Die Basis für das Design der Lern-Plattform bieten «Instructional design principles», welche von Kumaraguru et al. (2010) zusammengefasst werden.[69] Der Autor entschied, die Lern-Plattform als Online Quiz aufzubauen. Dies erstens, weil im Literaturreview bereits ein ähnliches Quiz dargestellt wurde. Durch die Reaktionen auf das erste Phishingmail wurde klar, dass «Phishing Awareness» Inhalte weiterzugeben das Hauptziel der Lern-Plattform sein muss. In diesem Bereich bietet ein Quiz eine gute Plattform um Inhalte wiederzugeben.

Zweitens, weil die bei SMC vorhandene E-Learning-Plattform eine Quiz-Funktion anbietet. Durch ein Online Quiz können die Anforderungen und Ziele an die Lern-Plattform umgesetzt werden.

Learning-by-doing: ACT-R (Adaptive Control of Thought-Rational) wurde zur Modellierung des menschlichen Lern- und Erkenntnis-Vermögens entworfen. ACT-R stellt die Hypothese auf, dass Wissen und Fähigkeiten durch tatsächliches Ausüben von Tätigkeiten gefestigt werden. [70] Auf der Lern-Plattform wollen wir diese Hypothese nutzen und das Prinzip umsetzten. Wenn Wissen vermittelt wird, wird durch nachfolgendes Abfragen das Wissen in die Praxis umgesetzt. Das so Erlernte kann damit auch in die alltägliche Praxis miteinbezogen werden. Wenn man beispielsweise Wissen über das Erkennen von Phishingmails vermittelt und anschliessend durch ein Beispiel-Email testet, festigt sich das Wissen besser. Durch den Link mit dem Beispiel, kann das Erlernte ebenfalls im alltäglichen Umgang mit Emails angewendet werden.

---

[68] Kumaraguru et al. (2010, p. 6), Kumaraguru et al. (2007, p. 913), Hoepman et al. (2016, p. 145).

[69] Kumaraguru et al. (2010, pp. 5–7).

[70] Anderson (2014).

Immediate Feedback: Mathan and Koedinger (2003) haben bewiesen, dass sofortiges Feedback während des Wissenstransfers zu effizientem Lernen und zur Reduktion von unproduktivem Trödeln führen kann. Auch dieses Prinzip wird in das Design aufgenommen, indem nach jedem praktischen Beispiel die relevanten Wissenselemente hervorgehoben werden. Auch wenn die Antwort auf eine Frage korrekt sein sollte, werden trotzdem in jedem Fall die Wissenselemente erläutert. Damit können eventuelle zufällig richtig beantwortete Fragen oder unvollständiges Wissen ergänzt werden. Durch ein direktes Feedback wird angezeigt, ob eine Antwort richtig oder falsch ist.

Contiguity: Im Vergleich zu isolierten Anwendungen von Text und Bildern wird der Lerneffekt verbessert, wenn Text und Bilder im Online-Learning aufeinander folgen.[71] Im Online-Learning sind Texte von Phishingmails und Phishing-Webseiten zu sehen. Der Informations-Text dazu, ist ersichtlich, sobald eine Antwort gegeben wurde. Dadurch wird eine Verbindung zwischen Text und Bild hergestellt.

Personalization: Dieses Prinzip basiert darauf, dass Teilnehmer Lerninhalte einfacher erlernen, wenn ein persönlicher Bezug hergestellt werden kann. Studien suggerieren, dass Personalpronomen wie «ich», «du» und «wir» das Lernen verbessern können.[72] Die Texte sprechen die Teilnehmer immer via dem Personalpronomen «du» an. Damit soll sich der Teilnehmer direkt angesprochen fühlen und sich so mit der gestellten Frage auseinandersetzten.

Prinzip	***Anwendung***
Learning-by-doing	Das vermittelte Wissen wird durch Praxis-Beispiele abgefragt
Immediate Feedback	Sofortiges Feedback durch richtiges oder falsches Antworten
Contiguity	Auf Bilder folgt Informations-Text zur Erläuterung
Personalization	Das Personalpronomen «du» wird in allen Texten verwendet

Tabelle 3: Anwendung «Instructional design principles» am Design der Lern-Plattform

6.2.1 Didaktisches Szenario

Es gibt verschiedene Arten, wie man eine virtuelle Lern-Plattform einsetzen kann. Sie kann begleitend und ergänzend wirken und somit weitere Lern-Konzepte unterstützen. Oder die Lern-Plattform ist integriert in ein Konzept, welches sowohl eine nicht virtuelle Lern-

[71] Moreno and Mayer (1999).

[72] R. E. Mayer (2001).

Umgebung sowie eine virtuelle Lern-Plattform beinhaltet. In einem weiteren Ansatz von Schulmeister (2005) ist die Lern-Plattform ausschliesslich virtuell vorhanden.[73]Auch Mason (1998) kategorisiert Lern-Plattformen nach dem Grad des virtuellen Anteils an der Plattform.[74] Die vollständig virtuelle Lern-Plattform wird in dieser Arbeit gewählt, weil die SMC bereits eine Lern-Plattform einsetzt, welche auf einer virtuellen Lösung basiert. Um eine möglichst hohe Anzahl Teilnehmer zu erreichen, wird eine Integration in die vorhandene Lösung angestrebt.

6.2.2 Messung Lernfortschritt

Nach Schmidt and Bjork (1992) kann der Lernfortschritt mit der Methode «Knowledge Acquisition» (KA) und «Knowledge Retention» (KR) gemessen werden. Bei der KA soll erlerntes Wissen benutzt werden um Entscheidungen zu treffen und richtig zu handeln. Dies wird überprüft mit den Beispielfragen zu Phishing. Dabei wird bei jeder Frage das Gelernte in einer der folgenden Fragen wieder abgefragt und somit überprüft. KR könnte innerhalb der Lernplattform überprüft werden, in dem man das Online Quiz nach einer gewissen Zeitspanne in einer angepassten Form erneut durchführt. In diesem Fall wird KR anhand der im Nachhinein versendeten Phishingmails gemessen.

6.2.3 Aufbau Quizfragen

Im Online-Quiz gibt es drei Typen von möglichen Fragen.

- Single-Choice Fragen
- Multiple-Choice Fragen
- Informationsfenster

Bei den Single-Choice Fragen gibt es eine mögliche Antwort («Ja», «Nein»), bei den Multiple-Choice Fragen deren zwei. Bei den Informationsfenstern gibt es keine Antwortmöglichkeiten, da bei diesen Informationen, Instruktionen und Wissensinhalte wiedergegeben werden.

6.2.4 Fragenkatalog Quiz

Als erstes werden die Teilnehmer gefragt, ob ihnen der Begriff und die Bedeutung von Phishing etwas sagt. Gleich darauf wird plakativ nachgefragt, «Was ist Phishing?». Dabei wird eine Multiple-Choice Auswahl an Antworten gegeben. Die Frage 2 wird gestellt, unbeachtet ob in

[73] Schulmeister (2005, p. 4).
[74] Mason (1998, pp. 6–7).

Frage 1 ein «Ja» als Antwort gegeben wurde. Die Teilnehmer, denen Phishing ein Begriff ist, können damit selber überprüfen, ob sie richtig liegen. Für die Teilnehmer, welchen Phishing kein Begriff ist, bietet die Frage die Möglichkeit zu erfahren was Phishing ist. Mit der Frage 3 soll das erwartete Verhalten der Teilnehmer überprüft werden. Bei Frage 4 können in einem kurzem Video die wichtigsten Anhaltspunkte und Informationen veranschaulicht werden. Hier gibt es auch die Möglichkeit ein Merkblatt oder eine andere Form von Lerninhalt zu präsentieren. Die Lösung mit einem Video wurde gewählt, um das Wissen einfach und schnell verfügbar zu machen. Die Frage 5 und 6 zeigen Beispiele von Emails und Webseiten in Form von Bildern. Die Teilnehmer müssen durch Beobachtung des Bildes entscheiden, ob es sich um ein Phishing Inhalt handelt oder nicht. Die Frage 5 wird zehnmal gestellt, Frage 6 insgesamt fünfmal beide jedes Mal mit anderen Inhalten. Nach der Auswahl der Antwort wird nach dem Prinzip «*Contiguity*» ein Hilfetext eingeblendet, welcher die Merkmale und Eigenschaften des gezeigten Bildes erklärt. Zum Abschluss wird mit Frage 7 nachgefragt, wie sich die Teilnehmer nach dem Quiz selber einschätzen. Bei Frage 7 gibt es wie bei Frage 1 die Möglichkeit mit «Ja» und «Nein» zu antworten.

Nr.	*Inhalt*	*Typ*
1	Weisst du was Phishing ist?	Multiple-Choice
2	Was ist Phishing?	Multiple-Choice
3	Was machst du wenn du dir nicht sicher bist ob es ein Phishingmail ist oder nicht?	Multiple-Choice
4	Phishing – Eine kurze Erklärung	Informationsfenster (Video)
5	Phishingmail oder echtes Email? (10-mal)	Single-Choice
6	Phishing Webseite oder nicht? (5-mal)	Single-Choice
7	Fühlst du dich in der Lage nach diesem Quiz Phishingmails und Webseiten zu erkennen?	Single-Choice

Tabelle 4: Fragenkatalog Quiz

6.2.5 Inhalt Fragen 4, 5 und 6

Bei der Frage 4 wurde ein Video gezeigt, welches Phishing als Begriff erklärt und die Ziele sowie Motive näher bringt.[75] Das Video wurde durch den Autor ausgewählt aufgrund der Video-Länge (1:34 Minuten) und des Inhaltes. Für die Frage 5 wurden Bilder von Phishingmails aus einem Online Phishing-Quiz verwendet.[76] Zusätzlich wurden Bilder aus einer Internetrecherche benutzt, um fehlende Phishingmail-Beispiele zu ergänzen. Für Frage 6 wurde ein Online Phishing-Webseite Quiz von OpenDNS als Quelle der Bilder verwendet.[77]

6.2.6 Weiterentwicklung Lern-Plattform

Die Lern-Plattform wird in dieser Arbeit in Form eines Online Quiz entwickelt und implementiert. Das Konzept dieser Lern-Plattform könnte auch auf weitere Medien und Methoden adaptiert werden. Ebenso ist eine Kombination von zwei oder mehreren Ansätzen (Quiz, Videospiel, Comic) möglich. Zu beachten sind die jeweiligen Vorgaben, die durch die Teilnehmer-Umgebung gegeben ist. Weiter ist eine Verbindung der Lern-Plattform mit dem Phishing-System möglich. Nach jedem Training via Quiz könnte der Wissenstand durch den aktiven Test mit Phishingmails getestet werden. Was in dieser Arbeit zur Bewertung der Lern-Plattform dient, könnte in einem produktiven System auch als Methode zu weiterem Training genutzt werden. Eine weitere Entwicklungsmöglichkeit, ist das Verwenden von dynamischen Inhalten wie von Cone et al. (2007) in einem Videospiel eingesetzt. Dabei wird der gezeigte Wissensinhalt anhand der vorgegangenen Spielweise angepasst, was in einem Quiz durch dynamische Fragen, welche die Reihenfolge ändern erreicht werden könnte.

[75] ("Was ist Phishing?").

[76] ("Phishing IQ Test | SonicWall").

[77] ("Take the OpenDNS Phishing Quiz," 2018).

7 Implementierung Prototyp

Die SMC setzt auf eine E-Learning Applikation welche für verschiedene Themenbereiche verwendet wird. Das Online-Quiz wurde auf dieser E-Learning Plattform implementiert und den Teilnehmern der «Education» Gruppe zur Verfügung gestellt.

7.1 Praktische Umsetzung

Die Fragen werden auf der E-Learning Plattform hinzugefügt und nach folgend wird pro Fragentyp ein Beispiel gemacht.

7.1.1 Single Choice-Frage

Bei den Single-Choice Fragen zeigt das Quiz jeweils an, ob die Antwort richtig oder falsch war. Zusätzlich wird aufgrund des Designs, sogleich die Erklärung zum jeweiligen Phishingmail angezeigt. Bei den Fragen 5 und 6 wurden die Bilder aufgrund der Anzeigegrösse auf ein vorangehendes Informationsfenster kopiert. Auf dieser haben die Teilnehmer die Möglichkeit, dass Bild zu vergrössern und alle Details zu sehen. Es ist eine technische Anforderung der E-Learning Plattform, dass jede Multiple-Choice und Single-Choice Frage einen Countdown hat. Da diese Zeitspanne zur Erkennung eines Phishingmails nicht ausreichend ist, wird vor jeder solchen Frage das Beispielbild in einem Informationsfenster dargestellt. Der Countdown auf der nachfolgenden Single-Choice Frage ist auf 40 Sekunden gesetzt.

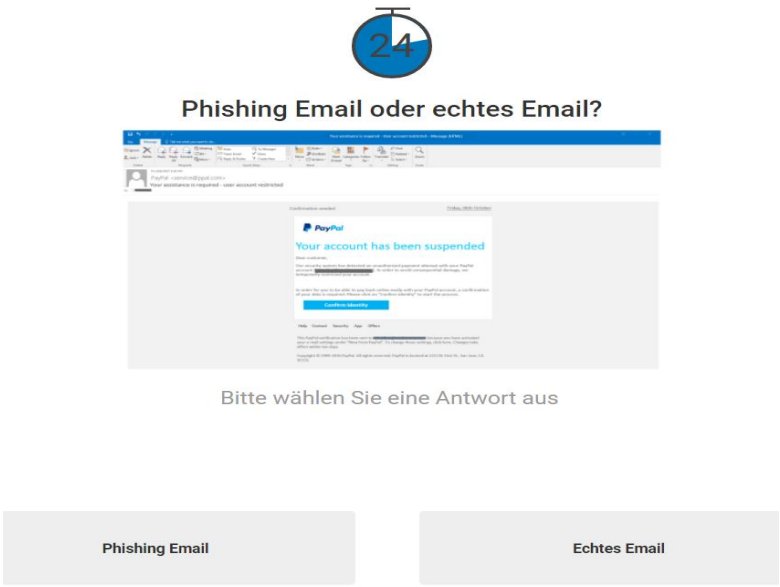


Abbildung 6: Phishingmail Single-Choice

7.1.2 Multiple-Choice Fragen

Bei diesem Fragentyp gibt es vier Antwortmöglichkeiten, bei Frage 1 gibt es nur deren zwei. Die erste Frage, wird nicht mir richtig oder falsch bewertet, da diese lediglich aufzeigen soll, ob die Teilnehmer wissen was Phishing ist. Zur zweiten Frage gibt es zwei und zur dritten Frage eine korrekte Antwort. Bei den Multiple-Choice Fragen ist ein Countdown von 30 Sekunden implementiert.

Abbildung 7: Multiple-Choice Frage 2

7.1.3 Informationsfenster

Das Informationsfenster zeigt bei Frage 2 ein Video, welches direkt abgespielt werden kann. Bei den Informationsfenstern, welche jeweils vor jeder Frage 5 und 6 dargestellt werden, wird das Phishing-Beispiel als Bild angezeigt. Durch einen Klick auf das Bild kann dieses vergrössert werden, damit alle Details ersichtlich sind.

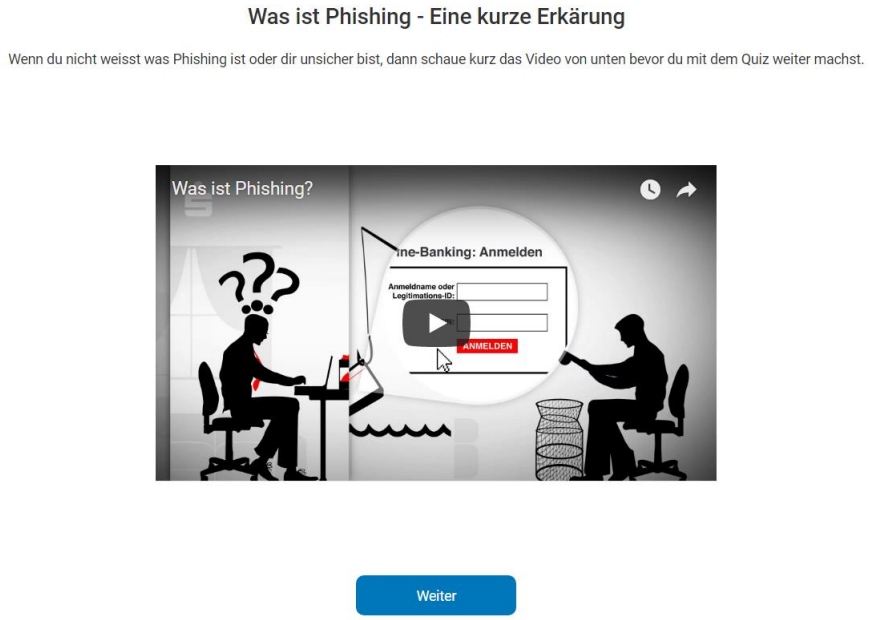


Abbildung 8: Informationsfenster Frage 4

8 Evaluation Prototyp

Die Teilnahme am Online Quiz und die Auswertung der erreichten Antworten wird als Erstes dargestellt. Danach wird der verwendete Prototyp durch das Versenden von zwei weiteren Phishingmails bewertet.

8.1 Auswertung Online Quiz

Am Quiz haben von den 54 eingeladenen Teilnehmern der Phishing-Gruppe «Education» 44 Personen das Quiz absolviert. Dies entspricht einer Teilnahmequote von 81.5%. Informationsfenster wie beispielweise Frage 4, werden nicht ausgewertet da diese keine Antwortmöglichkeiten bieten. Eine detaillierte Tabelle befindet sich im Anhang 12.3.

Frage 1: Bei der Frage «Weisst du was Phishing ist?» haben 23% der Teilnehmer dies mit «Ja» beantwortet. Die restlichen 77% gaben an, dass sie nicht wissen was Phishing ist.

Frage 2: Was Phishing bedeutet, wurde von 64% korrekt beantwortet. Die korrekten Antworten waren: «Eine Möglichkeit illegal an persönliche Information zu gelangen» und «Ein Versuch, jemanden zu täuschen mit der Angabe von falschen Informationen».

Frage 3: In Frage 3 haben nur 27% angegeben, dass sie bei einer Unsicherheit den IT-Support kontaktieren würden. Die restlichen wählten aus, dass sie das Email löschen oder einen Arbeitskollegen um Rat fragen, wenn eine Unsicherheit bezüglich der Echtheit eines Emails bestünde.

Frage 5: Bei den Phishingmails wurde durchschnittlich von 73% erkannt, ob es sich um ein Phishingmail oder ein echtes Email handelte. Beim ersten Beispiel, welches ein echtes Email war, haben 73% ein Phishingmail vermutet. Beim letzten Beispiel, welches ein Phishingmail darstellte, wurde dies von 95% korrekt erkannt.

Frage 6: Bei den Phishing-Webseiten, haben 56% der Teilnehmer korrekt erkannt, ob es sich um Phishing-Webseiten handelte oder nicht. Das erste Beispiel, welches eine echte Webseite darstellte, wurde wie bei Frage 5 mehrheitlich falsch beantwortet. Insgesamt 82% der Teilnehmer haben diese als Phishing-Webseite interpretiert.

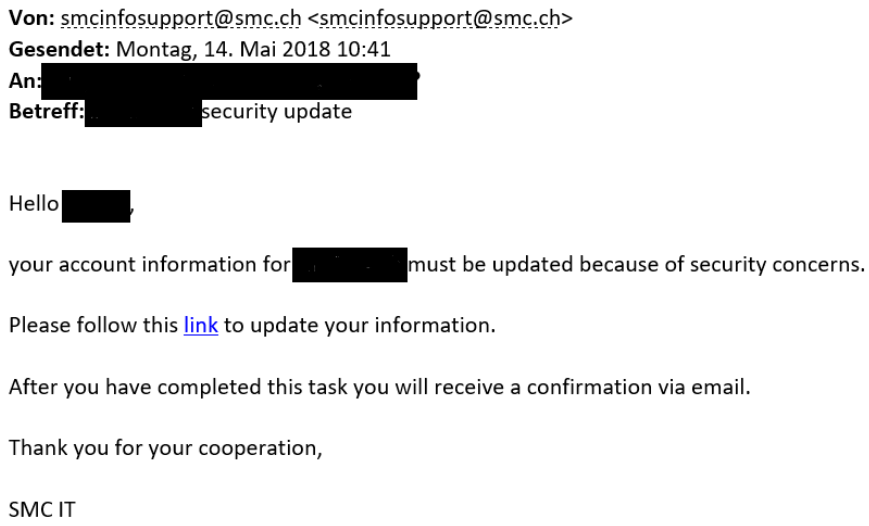
Frage 7: Nach dem Absolvieren des Quiz, fühlten sich 73% in der Lage, zukünftige Phishing-Attacken zu erkennen. Dagegen denken 27% der Teilnehmer, sie würden eine Phishing-Attacke nicht als solche erkennen.

8.2 Auswertung 2. Phishingmail

Das zweite Phishingmail wurde an die beiden Gruppen «Education» und «Controlling» versendet. Dieses wurde am 09.05.2018 versendet, 48 Stunden nachdem das Online-Quiz den Teilnehmer der «Education» Gruppe zur Verfügung gestellt wurde.

8.2.1 Inhalt

Das zweite Phishingmail ist identisch aufgebaut wie das erste Phishingmail von Abschnitt 5.1. Der Absender des Emails ist wiederum frei erfunden und entspricht keiner offiziellen Unternehmens Email Adresse. Die Teilnehmer werden wiederum aufgefordert Ihre Account Informationen für ein Webbasiertes Tool anzugeben. Diesmal wird als Grund «Security concerns» genannt, diese werden jedoch weder spezifiziert noch begründet. In der Email-Ansprache wird der Vornamen des Empfängers benützt um das Email legitimer wirken zu lassen. Eine ähnliches Email-Design wurde verwendet, um die Resultate mit dem ersten Phishingmail vergleichen zu können.



Von: smcinfosupport@smc.ch <smcinfosupport@smc.ch>
Gesendet: Montag, 14. Mai 2018 10:41
An: [redacted]
Betreff: [redacted] security update

Hello [redacted],

your account information for [redacted] must be updated because of security concerns.

Please follow this link to update your information.

After you have completed this task you will receive a confirmation via email.

Thank you for your cooperation,

SMC IT

Abbildung 9: Phishingmail 2

8.2.2 Ergebnisse 2. Phishingmail

Von den 109 versendeten Emails an die Teilnehmer der beiden Gruppen «Education» und «Controlling» wurden 26 Emails innerhalb von 72 Stunden geöffnet. In 19 von 26 Fällen wurden auf der Phishing-Webseite Daten eingegeben, dies entspricht einem Anteil von 73.1%. Im Vergleich mit dem ersten Phishingmail, ist die gesamte Anzahl an geöffneten Emails und geklickten Links um 12 Teilnehmer gesunken. Auf den ersten Blick, weist dies darauf hin, dass sich die Fähigkeit Phishingmails zu erkennen bei beiden Gruppen verbessert hat. Weil aber nicht 100% der «Education» Gruppe auf der Lern-Plattform ein Training absolviert haben, wird dieser Wert im Abschnitt 8.3.3 erläutert. Die «Rate to click» (Prozent der eingegeben Daten zu der Anzahl geöffneten Links) ist beinahe gleich geblieben im Vergleich zum ersten Phishingmail. Die Anzahl an geöffneten Tickets und Anfragen bei der IT-Abteilung ist ebenfalls ähnlich zum ersten Phishingmail (11 Tickets zu 13 Tickets).

	Controlling	*Education*	***Total***
Number of Emails	55	54	**109**
Emails opened	15	11	**26**
Rate (%)	27,3%	20,4%	**23,9%**
Clicked Link	15	11	**26**
Rate (%)	27,3%	20,4%	**23,9%**
Submitted Data	10	9	**19**
Rate (%)	18,2%	16,7%	**17,4%**
Rate to click (%)	66,7%	81,8%	**73,1%**
Opened Tickets	5	8	**13**
Rate (%)	9,1%	14,8%	**11,9%**

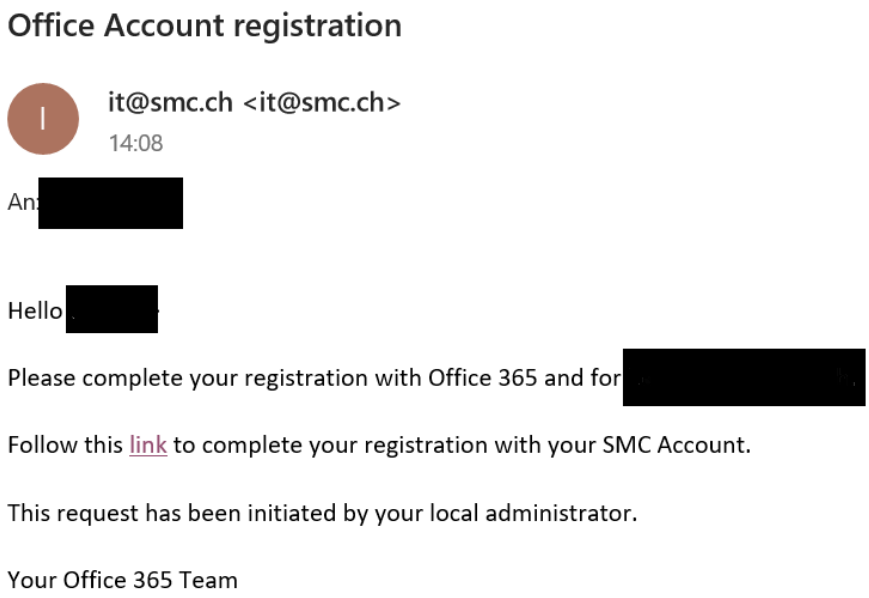
Tabelle 5: Ergebnis 2. Phishingmail

8.3 Auswertung 3. Phishingmail

Das dritte Phishingmail wurde an die beiden Gruppen «Education» und «Controlling» versendet. Dieses Mail wurde 7 Tage nach der Freigabe des Online-Quiz, am 14.05.2018 versendet.

8.3.1 Inhalt

Der Inhalt des dritten Phishingmails ist wiederum ähnlich aufgebaut wie die beiden Ersten. Die persönliche Ansprache mit Vornamen aus Phishingmail 2 wird beibehalten. Zusätzlich wurde die Email-Adresse des Empfängers eingefügt, um einen weiteren Grad der Personalisierung zu erhalten. Unterschiedlich ist, dass es nicht um einen «Account reset» oder «expired», sondern um eine «Account registration» geht. Es wird suggeriert, dass der Aufruf durch den «local administrator» angefordert wurde. Damit wird versucht die Echtheit mit einem Autoritätsargument zu stützen und so den Teilnehmer zu täuschen. Wiederum wie bei den anderen Phishingmails, ist der Absender keine offizielle SMC Adresse.


Office Account registration

it@smc.ch <it@smc.ch>

14:08

An: [redacted]

Hello [redacted]

Please complete your registration with Office 365 and for [redacted]

Follow this link to complete your registration with your SMC Account.

This request has been initiated by your local administrator.

Your Office 365 Team

Abbildung 10: Phishingmail 3

8.3.2 Ergebnisse 3. Phishingmail

Nach dem Versenden des dritten und letzten Phishingmail an alle 109 Teilnehmer haben 24 Teilnehmer das Email geöffnet und den Link geklickt. Von diesen 24 haben 18 auch ihre Benutzerinformationen auf der Phishing-Webseite angegeben. Total haben 75% der geöffneten Emails zum Phishing-Erfolg geführt. Die Anzahl an geöffneten Tickets lag bei 14. Im ersten Phishingmail hatten noch 29 Teilnehmer Daten eingegeben, beim zweiten Phishingmail waren es 19 Teilnehmer und im letzten Phishingmail sind es 18 Teilnehmer. Die Rate ist nach dem Einsatz der Lern-Plattform gesunken. Ebenfalls beim dritten Phishingmail werden die Ergebnisse im folgenden Abschnitt, bei einer Teilnehmerquote von 81.5% dargestellt.

	Controlling	*Education*	***Total***
Number of Emails	55	54	**109**
Emails opened	16	8	**24**
Rate (%)	29,1%	14,8%	**22,0%**
Clicked Link	16	8	**24**
Rate (%)	29,1%	14,8%	**22,0%**
Submitted Data	12	6	**18**
Rate (%)	21,8%	11,1%	**16,5%**
Rate to click (%)	75,0%	75,0%	**75,0%**
Opened Tickets	6	8	**14**
Rate (%)	10,9%	14,8%	**12,8%**

Tabelle 6: Ergebnis 3. Phishingmail

8.3.3 Teilnehmerquote Quiz von 81.5%

Bei einer Teilnehmerquote in der «Education» Gruppe von 81.5% haben zehn Teilnehmer nicht am Quiz teilgenommen. Um den Unterschied von vor und nach dem Quiz zu beobachten, wurden diese zehn Teilnehmer von den Resultaten der Gruppe «Education» ausgeschlossen. Um dies über alle drei Phishingmails zu vergleichen, werden diese zehn Teilnehmer von allen drei Ergebnissen der «Education» Gruppe entfernt. Beim ersten Phishingmail haben von diesen zehn Teilnehmern drei den Link geöffnet und Daten eingegeben. Nach Abzug dieser drei Teilnehmer, wurden im ersten Phishingmail 15 Emails gelesen und der entsprechende Link geklickt. Von diesen 15 sind in neun Fällen Account-Informationen eingegeben worden. Im zweiten Phishingmail sind es nach dem Abzug noch vier Phishingmails, bei welchen der Link geöffnet wurde. Beim dritten Phishingmail sind es nun insgesamt sechs Emails, bei denen der Link geöffnet wurde. Daten eingegeben, haben beim Zweiten Phishingmail, zwei Teilnehmer und beim dritten sind es vier Teilnehmer.

«Education» bei 81.5% Teilnehmer	*Phishingmail 1*	*Phishingmail 2*	*Phishingmail 3*
Number of Emails	44	44	44
Emails opened	15	4	6
Rate (%)	34,1%	9,1%	13,6%
Clicked Link	15	4	6
Rate (%)	34,1%	9,1%	13,6%
Submitted Data	9	2	4
Rate (%)	20,5%	4,5%	9,1%
Rate to click (%)	60,0%	50,0%	66,7%

Tabelle 7: Ergebnisse bei 81.5% Teilnahmequote

8.4 Diskussion der Ergebnisse

Die Lern-Plattform wurde prototypisch umgesetzt und das Training in Form eines Quiz absolviert. Ein Phishingmail wurde vor dem Training und zwei nach dem Training versendet. Im folgenden Abschnitt werden die Ergebnisse dieser Arbeit diskutiert und Schlussfolgerungen gezogen.

8.4.1 Lern-Plattform

Das Phishing nicht allen Teilnehmern ein Begriff ist, wurde mit dem tiefen «Ja» Wert von 23% von Frage 1 klar. Diese Annahme wurde durch das Ergebnis des ersten Phishingmails bekräftigt. Von der Frage 2 hingegen wurde diese Annahme nicht unterstützt. Eine Mehrheit von 64% hat korrekt geantwortet, was aber den vier Antwortmöglichkeiten zuzuschreiben sein könnte. Wenn ein Teilnehmer von vier möglichen Antworten die zwei plausibleren auswählt, muss nicht unbedingt Wissen über Phishing vorhanden sein und trotzdem kann die Frage 2 korrekt beantwortet werden. Nur 27% der Teilnehmer wussten, was im Falle von Unsicherheit bei einem Phishingmail zu tun ist. Hier wird argumentiert, dass Mitarbeiter im täglichen Mailverkehr eher einen Kollegen oder eine Kollegin um Hilfe fragen, als bei der IT-Abteilung ein Ticket zu eröffnen. Aus Sicht des Autors ist es klar, dass hier der Zeitfaktor eine Rolle spielt. Sicherheitstechnisch ist es ein Risiko, wenn das fragliche Email nicht durch die IT-Abteilung überprüft wird. Wie hoch die Anzahl an korrekten Antworten bei den Fragen 5 und 6 ist, ist insofern interessant, da man einen generellen Überblick über das vorhandene Wissen erhält. Ein sofortiger Lern-Effekt entsteht bei diesen Fragen durch das Anzeigen des Informationstextes, unabhängig davon ob eine Frage korrekt oder falsch ist. 73% der Teilnehmer fühlen sich in der Lage, Phishingmails zu erkennen. Das würde bedeuten, dass die Anzahl an erfolgreichen Phishingmails gegenüber dem ersten Phishingmail sinken müsste. Dies

trifft zu, da die Phishingmails zwei und drei eine tiefere Anzahl an erfolgreichen Phishingmails erzielen als das Erste. Die Mehrheit der Teilnehmer haben sich selber gut eingeschätzt. Ein anderes Bild zeigt das Experiment von Perrault (2018), bei welchem ausgesagt wird, dass sich Teilnehmer vor dem Quiz in der Lage fühlten Phishingmails zu erkennen und durch die Ergebnisse des Quiz diese Meinung änderten.[78] In dieser Arbeit ist das Gegenteil der Fall; viele der Mitarbeiter wissen vor dem Quiz, nicht was Phishing ist, fühlen sich jedoch in der Lage, nach dem Quiz Phishingmails zu erkennen. Man könnte hier argumentieren, dass die versendeten Phishingmails simpler zu erkennen waren als die von Perrault (2018) verwendeten.

8.4.2 Phishingmails

Der Inhalt ist bei allen drei versendeten Phishingmails ähnlich gestaltet, der Empfänger wird jeweils aufgefordert, seine Benutzerinformationen auf einer Webseite zu aktualisieren oder einzugeben. Bereits nach dem ersten Phishingmail wurde klar, dass bei der SMC ein Bedarf für Anti-Phishing Training besteht, 34.9% der versendeten Emails wurden geöffnet und der darin enthaltene Link zur Phishing-Webseite angeklickt. Das zweite Phishingmail wurde wieder an dieselben Teilnehmer versendet. Diesmal haben 23.9% der Teilnehmer das Email geöffnet und auf den Link geklickt. Der Anteil der geöffneten Emails im Vergleich zum ersten Phishingmail ist um 11% gesunken. Eine Reduktion des Wertes war ein Ziel der Lern-Plattform, jedoch ist dieser noch zu hoch. Nach dem dritten Phishingmail zeichnete sich ein ähnliches Bild ab wie beim Zweiten. Es wurden 22% der Phishingmails geöffnet und davon in 75% der Fälle Daten eingegeben. Dies zeigt, dass Phishing ein ernsthaftes Problem für die SMC darstellt.

Anhand des Versuches wurde nicht nur das Risiko von einer erfolgreichen Phishing-Attacke bei der SMC, sondern auch der Einfluss einer Lern-Plattform darauf evaluiert. Um diesen Einfluss zu messen, werden die beiden Gruppen «Education» und «Controlling» verglichen. Beim Vergleich der Teilnehmer der Gruppe «Education bei 81.5% Teilnehmerquote» und der Gruppe «Controlling» wird klar, dass durch die Teilnahme am Quiz die Anzahl an erfolgreichen Phishingmails gesenkt werden konnte. Wobei die Anzahl der erfolgreichen Phishingmails bei der Gruppe «Controlling» unerwartet gesunken ist. Von den ursprünglichen 36.4% an geöffneten Phishingmails ist die Anzahl auf 27.3% und 29.1% gesunken, dies könnte jedoch dem Effekt der Wiedererkennung zuzuweisen sein. Da die drei Phishingmails eine gewissen inhaltliche Ähnlichkeit aufweisen, könnte es sein dass bei dem einen oder anderen Teilnehmer

[78] Perrault (2018, p. 1163).

der Eindruck entstanden ist, dass es sich um kein legitimes Email handelt. Die Zunahme von 27.3% auf 29.1% vom zweiten zum dritten Phishingmail könnte mit dem Einfluss der verstrichenen Zeit auf den Wiedererkennungswert zusammenhängen.

In der Gruppe «Education» kann ganz klar festgestellt werden, dass der Anteil an geöffneten Phishingmails, geklickten Links und eingegebenen Daten im Vergleich vom 1. Phishingmails zum 2. und 3. Phishingmail gesunken ist.

8.4.3 Eröffnete Tickets

Mit der Frage 3 wurde aufgezeigt das nur eine Minderheit der Mitarbeiter sich bei der IT-Abteilung meldet bei einer Unsicherheit im Umgang mit Emails. Dieses Resultat durch alle drei Phishingmails bestätigt. Bei allen drei Phishingmails liegt die Anzahl an geöffneten Tickets zwischen 11 und 14 über beide Gruppen zusammengefasst. Man hätte aufgrund der Teilnahme am Quiz bei der Gruppe «Education» eine höhere Anzahl an Tickets erwarten können dadurch, dass mit Frage 3 eine Hilfestellung dazu vermittelt wird. Die Anzahl hielt sich jedoch konstant bei 8 Tickets und Anfragen pro versendetem Phishingmail. Weshalb sich hier die Anzahl nicht erhöht hat ist nicht klar zu definieren. Eine mögliche Erklärung ist der Zeitverlust welcher durch die Anfrage bei der IT-Abteilung anfällt. Festzustellen ist, dass die Hilfestellung aus Frage 3 keinen Einfluss auf die Mitarbeitenden gehabt hat.

9 Fazit

In dieser Arbeit wurde ein Quiz designt und in einem Schweizer KMU prototypisch implementiert. Der Effekt dieses Quiz auf die Fähigkeit der Mitarbeiter eine Phishing-Attacke zu erkennen wurde mit dem Versenden von Phishingmails getestet. Das Quiz wurde anhand eines Literaturreviews und den Ergebnissen aus einem ersten versendenten Phishingmail designt. Das Ziel des Quiz war es, die «Phishing Awareness» zu steigern, damit die Mitarbeiter Phishing-Attacken erkennen können und nicht mehr darauf eingehen. Um diesen Effekt zu messen wurden die Teilnehmer in die Gruppe «Education» und «Controlling» eingeteilt. Die «Education» Gruppe absolvierte das Quiz, die «Controlling» Gruppe dagegen erhielt kein Anti-Phishing Training. Die Teilnahme am Quiz hat die Anzahl an erfolgreichen Phishingmails innerhalb der «Education» Gruppe gesenkt. Es zeigte sich, dass nach einer Zeitspanne von sieben Tagen die Anzahl an erfolgreichen Phishingmails wieder leicht anstieg. Dies lässt vermuten, dass die «Phishing Awareness» nur für einen begrenzten Zeitraum anhält und danach wieder abnimmt.

Im Vergleich mit der Gruppe «Controlling» ist die Anzahl an erfolgreichen Phishingmails kleiner und daher lässt sich hier eine positive Wirkung der Lern-Plattform feststellen. Das Vermitteln von «Phishing Awareness» bietet einem Schweizer KMU die Möglichkeit das Risiko vor erfolgreichen Phishing-Attacken zu senken. Der Einsatz einer Lern-Plattform implementiert durch ein Quiz, verbessert die Chance eine Phishing-Attacke abzuwehren. Dieses Resultat ist insofern allgemeingültig, dass der Einsatz eines Anti-Phishing Quiz eine Verbesserung der «Phishing Awareness» bringen kann. Die Anzahl an erfolgreichen Phishingmails wird jedoch von KMU zu KMU unterschiedlich gross sein, da jedes KMU individuelle Voraussetzungen mitbringt. Die tatsächliche Verbesserungsquote, die durch ein Quiz erzielt wird, ist daher nicht eindeutig auf einen Wert festzulegen.

10 Handlungsempfehlungen

Mit Hilfe der Lern-Plattform konnte eine Verbesserung der «Phishing Awareness» erreicht werden, welche anhand der eingesetzten Phishingmails bewiesen werden konnte. Wie gut die Lern-Plattform jedoch im Vergleich mit einer anderen Form des Wissenstransfers abschneidet ist nicht geklärt. Ob beispielsweise ein Video-Spiel [79], ein Comic [80] oder «instructor-based training» [81] ein besseres Ergebnis erzielen würde, könnte überprüft werden. Dabei könnten anstelle der Gruppen «Education» und «Controlling», die Teilnehmer auf verschiedene Lernmethoden aufgeteilt werden. Für alle Lernmethoden stellen dieselben Phishingmails die Basis, damit ein adäquater Vergleich gewährleistet ist.

Der ähnliche Inhalt der verwendeten Phishingmails könnte der Grund für die nicht geplante Verbesserung bei der Kontrollgruppe gewesen sein. Um dies zu verhindern könnten sich bei zukünftigen Phishingmails die Inhalte stärker voneinander unterscheiden. Damit wird den Teilnehmern der Kontrollgruppe das unbewusste Misstrauen genommen, da die Phishingmails keine gemeinsamen Merkmale beinhalten. Die verwendete Lern-Plattform könnte weiter mit einer herkömmlichen Lernmethode kombiniert werden um ein verbessertes Ergebnisse erzielen zu können. Weiter Informationen zur Weiterentwicklung der Lern-Plattform befinden sich im Abschnitt 6.2.6.

[79] Cone et al. (2007).

[80] Kumaraguru et al. (2010).

[81] Hoepman et al. (2016).

11 References

Anderson, J. R. (2014). *Rules of the Mind*: Taylor & Francis. Retrieved from https://books.google.ch/books?id=1KOYAgAAQBAJ

Arikan, C. (2017). Cyberkriminalität in der Schweiz: Starke Zunahme und neue Bedrohungen durch künstliche Intelligenz | KPMG | CH. Retrieved from https://home.kpmg.com/ch/de/home/medien/medienmitteilungen/2017/05/cyber-crime-in-switzerland.html

Bellovin, S. M. (2004). Spamming, Phishing, Authentication, and Privacy. *Communications of the ACM*, *47*(12), 144. https://doi.org/10.1145/1035134.1035159

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Corporate Summary／Corporate Principles. Retrieved from http://www.smcworld.com/about/en-jp/

Corporation, S. M.C. Unternehmen: SMC Schweiz AG. Retrieved from https://www.smc.eu/portal_ssl/webpages/00_local/ch/DE/about_us/unternehmen.jsp

Daten-Leck bei Swisscom: Was Kunden jetzt wissen müssen - Handelszeitung. Retrieved from https://www.handelszeitung.ch/unternehmen/daten-leck-bei-swisscom-was-kunden-jetzt-wissen-mussen

Emigh, A. (2005). Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. *ITTC Report on Online Identity Theft Technology and Countermeasures*.

Gao, H., Wang, J., Hu, J., Huang, T., & Chen, Y. (2011). Security Issues in Online Social Networks. *IEEE Security & Privacy*, 56–63.

Gavin O'Gorman, & Geoff McDonald. (2012). Ransomware: A Growing Menace. Retrieved from http://www.01net.it/whitepaper_library/Symantec_Ransomware_Growing_Menace.pdf

GoPhish. (2012). Introduction · Gophish User Guide. Retrieved from https://gophish.gitbooks.io/user-guide/content/

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, *40*(2), 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Heartfield, R., Loukas, G., & Gan, D. (2016). You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. *IEEE ACCESS*, *4*. https://doi.org/10.1109/ACCESS.2016.2616285

Hoepman, J.-H., Katzenbeisser, S., Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P.,. . . Lehmann, D. (Eds.) 2016. *Teaching Phishing-Security: Which Way is Best?: ICT Systems Security and Privacy Protection*: Springer International Publishing.

If You Don't Fully Understand the Cambridge Analytica Scandal, Read This Simplified Version. Retrieved from https://www.inc.com/alyssa-satara/if-you-dont-fully-understand-cambridge-analytica-scandal-read-this-simplified-version.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

Jan vom Brocke, Alexander Simons, Bjoern Niehaves, Kai Reimer, Anne Cleven, & Ralf Plattfaut. (2009). RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS. Retrieved from https://pdfs.semanticscholar.org/c5f5/7551155b188d6ebc1ac21acc33735666d3dd.pdf

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Kim, D., & Hyun Kim, J. (2013). Understanding persuasive elements in phishing e-mails. *Online Information Review*, *37*(6), 835–850. https://doi.org/10.1108/OIR-03-2012-0037

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

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 *CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, VOLS 1 AND 2* (pp. 905–914).

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). https://doi.org/10.1145/1754393.1754396

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 308. https://doi.org/10.1186/s40163-014-0009-y

Lim, I.-k., Park, Y.-G., & Lee, J.-K. (2016). Design of Security Training System for Individual Users. *WIRELESS PERSONAL COMMUNICATIONS*, *90*(3), 1105–1120. https://doi.org/10.1007/s11277-016-3380-z

Manning, R. (2018). APWG Phishing Activity Trends Report. *APWG*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf

Mason, R. (1998). Models of Online Courses. *ALN Magazine*. Retrieved from http://www.johnsilverio.com/EDUI6704-7804/Assignment1AReadings/ModelsOfOnlineClass.pdf

Mathan, S., & Koedinger, K. R. (2003). Recasting the Feedback Debate: Benefits of Tutoring Error Detection and Correction Skills. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.8448&rep=rep1&type=pdf

Mayer, R. E. (2001). Multimedia learning. 2001.

Moreno, R., & Mayer, R. E. (1999). Cognitive principles of multimedia learning: The role of modality and contiguity. *Journal of Educational Psychology*, *91*(2), 358–368. https://doi.org/10.1037//0022-0663.91.2.358

Nyeste, P. G. (2011). Training Users to Counteract Phishing. *ProQuest Dissertations and Theses*. (3463721), 108.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194–206. https://doi.org/10.1016/j.cose.2015.02.008

Perrault, E. K. (2018). Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioral Intentions About Phishing. *JOURNAL of EDUCATIONAL COMPUTING RESEARCH*, *55*(8), 1154–1167. https://doi.org/10.1177/0735633117699232

Pfleeger, S. L., & Bloom, G. (2005). Canning Spam: Proposed Solutions to Unwanted Email. *IEEE Security and Privacy Magazine*, *3*(2), 40–47. https://doi.org/10.1109/MSP.2005.38

Phishing IQ Test | SonicWall. Retrieved from https://www.sonicwall.com/en-us/phishing-iq-test-landing

Portmann, A., & Hirschi, O. (2018). Cybersecurity in Schweizer Unternehmen. In T. K. Birrer, M. Rupp, & M. Spillmann (Eds.), *Corporate Treasury Management: Konzepte für die Unternehmenspraxis* (pp. 456–473). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-18567-1_20

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, *20*(5), 382–420. https://doi.org/10.1108/09685221211286548

Rasha Salah El-Din. (2012). To Deceive or Not to Deceive!: Ethical Questions in Phishing Research. *University of York*.

Robila, S. A., & Ragucci, J. W. (2006). Don't be a phish: Steps in user education. *ACM SIGCSE Bulletin*, *38*(3), 237–241. https://doi.org/10.1145/1140123.1140187

Schmidt, R. A., & Bjork, R. A. (1992). New Conceptualizations of Practice: Common Principles in Three Paradigms Suggest New Concepts for Training. Retrieved from http://hp-research.com/sites/default/files/publications/Schmidt%20%26%20Bjork%20(PS,%201992)_0.pdf

Schulmeister, R. (Ed.). (2005). *Lernplattformen: Optimierung der Ausbildung oder didaktischer Rückschritt? ; Web-based Training 2005* (1. Aufl.). Dübendorf: Empa-Akademie. Retrieved from http://rolf.schulmeister.com/pdfs/Lernplattformen.pdf

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 : *SOUPS '07, Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 88–99). New York, NY, USA: ACM. https://doi.org/10.1145/1280680.1280692

Statistiken zum Jahresbericht fedpol 2016. Retrieved from https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2016-stat-d.pdf

Take the OpenDNS Phishing Quiz: What is Phishing? (2018). Retrieved from https://www.opendns.com/phishing-quiz/

Torraco, R. J. (2016). Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, *4*(3), 356–367. https://doi.org/10.1177/1534484305278283

Vijayan, J. (2005). Training Needed to Halt 'Spear-Phishing' Attacks. *Computerworld*, *39*(34), 6.

Was ist Phishing? Retrieved from https://www.youtube.com/watch?v=LY30sfl4nhQ

Wikipedia. (2018). Domain Name System. Retrieved from https://de.wikipedia.org/w/index.php?oldid=176294949

Yoram M Kalman, & Sheizaf Rafaeli. (2005). Email Chronemics: Unobtrusive Profiling of Response Times: Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Retrieved from http://ieeexplore.ieee.org/servlet/opac?punumber=9518

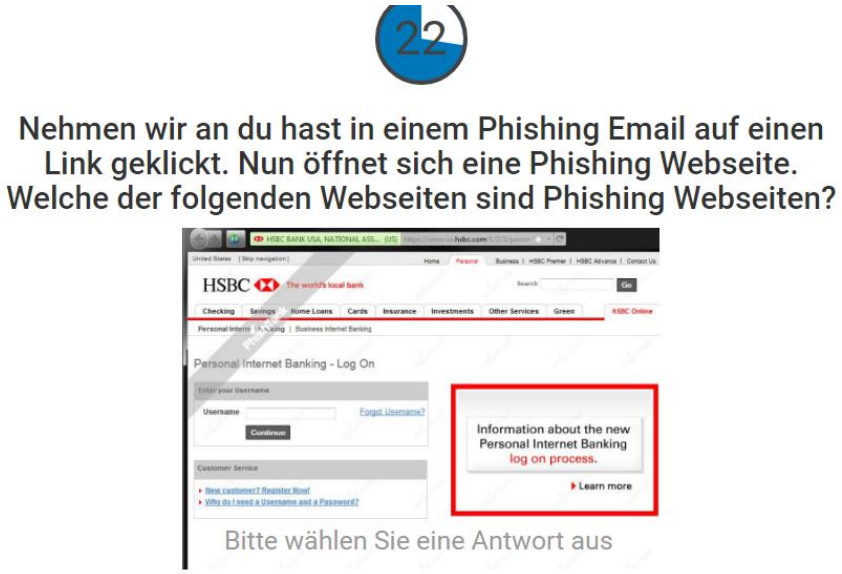
12 Anhang

12.1 Literaturreview

Titel	Autoren	Jahr
A video game for cyber security training and awareness	Cone, Benjamin D.; Irvine, Cynthia E.; Thompson, Michael F.; Nguyen, Thuy D.	2007
Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures	Emigh, Aaron	2005
Individual processing of Phishingmails	Harrison, Brynne; Svetieva, Elena; Vishwanath, Arun	2016
Teaching Phishing-Security: Which Way is Best?	Hoepman, Jaap-Henk; Katzenbeisser, Stefan; Stockhardt, Simon; Reinheimer, Benjamin; Volkamer, Melanie; Mayer, Peter; Kunz, Alexandra; Rack, Philipp; Lehmann, Daniel	2016
Training to Mitigate Phishing Attacks Using Mindfulness Techniques	Jensen, Matthew L.; Dinger, Michael; Wright, Ryan T.; Thatcher, Jason Bennett	2017
Understanding persuasive elements in phishing e-mails	Kim, Daejoong; Hyun Kim, Jang	2013
Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System	Kumaraguru, Ponnurangam; Rhee, Yong; Acquisti, Alessandro; Cranor, Lorrie Faith; Hong, Jason; Nunge, Elizabeth	2007
Teaching Johnny Not to Fall for Phish	Kumaraguru, Ponnurangam; Sheng, Steve; Acquisti, Alessandro; Cranor, Lorrie Faith; Hong, Jason	2010
Design of Security Training System for Individual Users	Lim, Il-kwon; Park, Young-Gil; Lee, Jae-Kwang	2016
Training Users to Counteract Phishing	Nyeste, Patrick Gabor	2011
Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioral Intentions About Phishing	Perrault, Evan K.	2018
Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish	Sheng, Steve; Magnien, Bryant; Kumaraguru, Ponnurangam; Acquisti, Alessandro; Cranor, Lorrie Faith; Hong, Jason; Nunge, Elizabeth	2007

12.2 Quiz Anhang

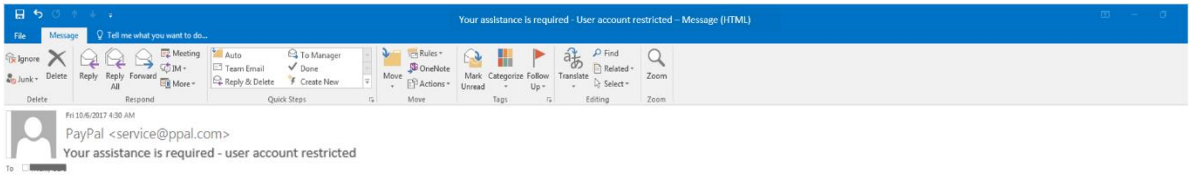
Weiter Beispielfragen aus dem Online-Quiz und Beispiel von verwendeten Ressourcen zum Online-Quiz.

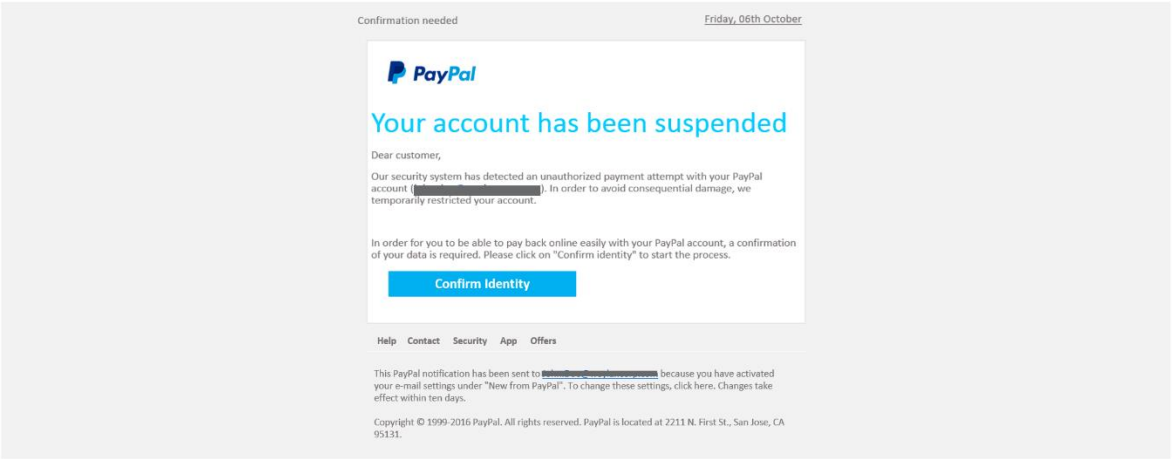


Phishing Webseite

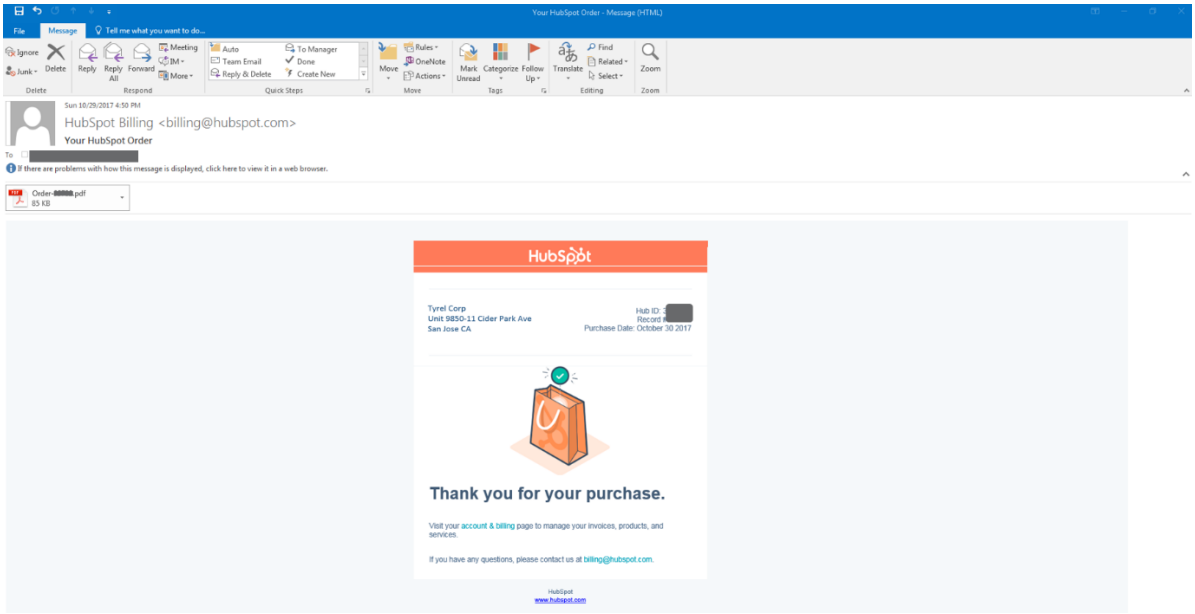
Echtes Webseite

Phishingmail:

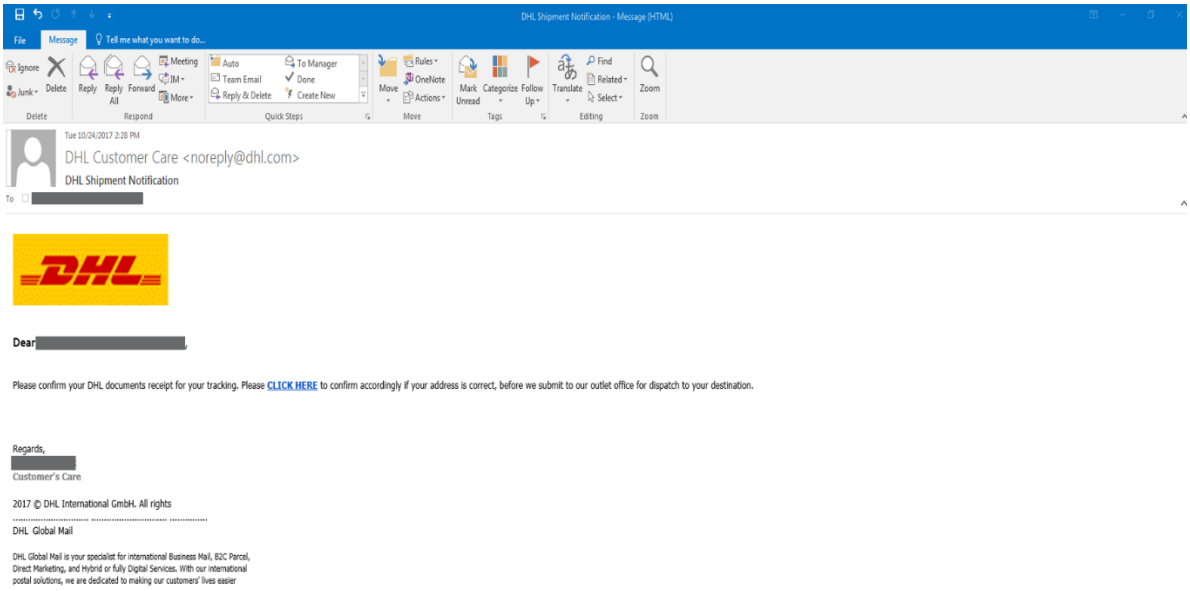




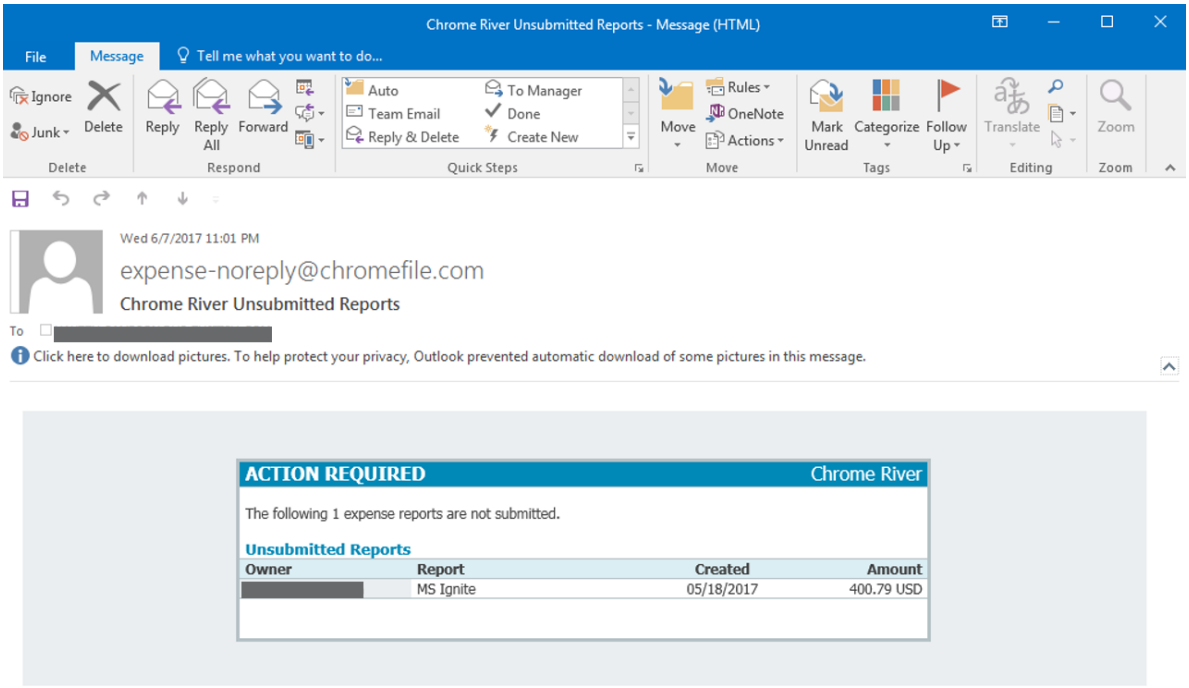
Legitimes Mail:



Phishingmail:



Phishingmail:



12.3 Auswertung Quiz

Berechnung Quizz		2										**Prozent**			
	Fragenkatalog	Anz. Teilnehmer	Option 0	Option 1	Option 2	Option 3	Is Correct	Is Wrong	Correct Answer Index			Ja	Nein	Is Corret	Is Wrong
Frage 1	1	44	10	34	[redacted]				0,1		0 = JA, 1 = Nein	**23%**	**77%**		
Frage 2	2	44	40	6	4	32	28	16	0,3					**64%**	**36%**
Frage 3	3	44	28	14	34	4	12	32	2					**27%**	**73%**
Frage 4	5	44	12	32	[redacted]		12	32	0		Echtes Mail			27%	73%
Frage 5	5	44	38	6	[redacted]		38	6	0		Phishing Mail			86%	14%
Frage 6	5	44	28	16	[redacted]		28	16	0		Phishing Mail			64%	36%
Frage 7	5	44	38	6	[redacted]		38	6	0		Phishing Mail			86%	14%
Frage 8	5	44	28	16	[redacted]		28	16	0		Echtes Mail			64%	36%
Frage 9	5	44	28	16	[redacted]		28	16	0		Phishing Mail			64%	36%
Frage 10	5	44	38	6	[redacted]		38	6	0		Phishing Mail			86%	14%
Frage 11	5	44	34	10	[redacted]		34	10	0		Phishing Mail			77%	23%
Frage 12	5	44	34	10	[redacted]		34	10	0		Phishing Mail			77%	23%
Frage 13	5	44	42	2	[redacted]		42	2	0		Phishing Mail			95%	5%
Durchschnitt		**440**	**320**	**120**	[redacted]		**320**	**120**						**73%**	**27%**
Frage 14	6	44	8	36	[redacted]		8	36	0		Echte Webseite			18%	82%
Frage 15	6	44	32	12	[redacted]		32	12	0		Phishing Webseite			73%	27%
Frage 16	6	44	28	16	[redacted]		28	16	0		Phishing Webseite			64%	36%
Frage 17	6	44	24	20	[redacted]		24	20	0		Phishing Webseite			55%	45%
Frage 18	6	44	28	16	[redacted]		28	16	0		Phishing Webseite			64%	36%
Frage 19	6	44	28	16	[redacted]		28	16	0		Phishing Webseite			64%	36%
Durchschnitt		**264**	**148**	**116**	[redacted]		**148**	**116**						**56%**	**44%**
Frage 20	7	44	32	12	[redacted]				0,1		0 = JA, 1 = Nein	**73%**	**27%**		
Wissensfrage															
Phishing Email															
Phishing Webseite															