Erklärvideo “Online-Betrug” – Nach nur fünf Minuten Phishing E-Mails nachweislich signifikant besser erkennen

Melanie Volkamer[1], Karen Renaud[2], Benjamin Reinheimer[1], Philipp Rack[1], Marco Ghiglieri[1], Nina Gerber[1], Peter Mayer[1] und Alexandra Kunz[1]

Kurzfassung:
Betrüger haben schon immer das Vertrauen von unvorsichtigen Personen ausgenutzt und versucht diese zu betrügen. Im Zeitalter der Computer wurden die Möglichkeiten der Betrüger erweitert und sie können nun jede beliebige Person, die im Besitz einer E-Mail Adresse ist, zu ihrem Ziel machen. Die Betrüger passen ihre Phishing-Nachrichten gezielt auf ihre Opfer an und verschleiern Täuschung und Betrug so gut wie möglich. Daraus folgernd wird die Sensibilisierung der Nutzer in Bezug auf das Thema Phishing und die erfolgreiche Erkennung dessen von immer größerer Wichtigkeit. Unsere bisher entwickelten Phishing Awareness-Programme adressieren bestehende Fehlannahmen und Missverständnisse bezüglich Phishing und können gezielt dabei helfen, die Erkennung solcher Nachrichten zu verbessern. Der größte Nachteil dieser Awareness-Programme stellt die dafür aufzuwendende Zeit dar. Deshalb haben wir ein Phishing Awareness Video entwickelt und evaluiert, welches in fünf Minuten über das Thema Phishing informiert. Nach dem Ansehen des Videos konnten Probanden in unserer Untersuchung Phishing-Nachrichten signifikant zuverlässiger erkennen (verglichen mit der Erkennung vor dem Ansehen des Videos). Diese Fähigkeit konnte auch nach einer achtwöchigen Pause in einer abschließenden Befragung nachgewiesen werden.

Stichworte: Phishing Awareness, Nutzerstudie, Retention-Studie

1. Einleitung

20 Jahre nach dem ersten Auftreten von Phishing ist dieses immer noch erfolgreich [1], [2], [3]. Phishing-Angriffe werden zunehmend durchdachter. Zu Beginn waren Phishing-Nachrichten aufgrund von fehlerhaften sprachlichen Formulierungen und Rechtschreibfehlern einfach zu identifizieren. Heutzutage sind Phisher wesentlich gewiefter, indem sie Nachrichten versenden, die gezielt entwickelt wurden um zu betrügen. Die Betrüger beschränken sich dabei nicht nur auf E-Mails sondern versenden die Nachrichten auch über Soziale Medien und Nachrichtendienste. Ein sehr gängiger Trick dabei ist, den Fokus auf einen in der Nachricht enthaltenen Link zu legen, dem ihre potentiellen Opfer folgen sollen, um entweder direkt Schadsoftware auf das verwendete Gerät herunterzuladen oder eine dem Original gleichende Webseite zu besuchen. Auf dieser Webseite sollen Nutzer dazu verleitet werden, persönliche Daten wie Login-Daten preiszugeben. Automatisierte Erkennungsmethoden stellen eine wirkungsvolle Vorgehensweise gegen Phishing dar, sind jedoch weit entfernt von einer 100%-igen Erkennungsrate [4], [5]. Um diese Lücke zu schließen, ist es notwendig, Internetnutzer darüber aufzuklären, wie sie Phishing-Nachrichten erkennen können.

Unsere Forschungsgruppe hat bereits zahlreiche Phishing Awareness-Programme entwickelt (darunter Apps, Flyer, Informationsmaterial, Präsentationen für Seminare)

[1] Karlsruher Institut für Technologie und Technische Universität Darmstadt
[2] Abertay University und University of South Africa

und mehrere wissenschaftliche Studien durchgeführt, um deren Effektivität zu belegen [6], [7], [8], [9], [10], [11], [12], [13], [14]. Die Untersuchungen zeigten, dass alle Formate die Erkennungsrate von Phishing signifikant erhöhen konnten. Einige Unternehmen kritisierten jedoch die im Durchschnitt benötigte Zeit von 25 bis 45 Minuten, die Mitarbeiter je nach Art der Intervention zur Durchsicht der Materialien aufwenden mussten. Um diesen Unternehmen nun zusätzlich ihren Wunsch nach einer möglichst zeiteffizienten Maßnahme zur Mitarbeiterschulung zu erfüllen, haben wir ein Video entwickelt, das Mitarbeitern innerhalb von fünf Minuten die Informationen vermittelt, die zur Erkennung einer Phishing-Nachricht besonders nötig sind. Das Video wurde, basierend auf Feedback von Personen mit verschiedenen fachlichen Hintergründen (Laien, Filmproduzenten, Psychologen und Sicherheitsexperten), iterativ entwickelt. An der Evaluation des Videos nahmen 89 Probanden teil, welche Phishing-Nachrichten signifikant öfter erkannten nachdem sie das Video sahen. Vielen von ihnen zeigten dieselbe Leistung nach einer achtwöchigen Pause und anschließender erneuten Befragung. Das Video[3] wurde unter der Creative Commons Lizenz CC BY-SA 4.0 veröffentlicht, um uneingeschränkte Nutzung zu gewährleisten.

2. Entwicklungsprozess

2.1 Identifikation des relevanten Inhalts

Das Video klärt Nutzer über gängige Techniken und Strategien auf, die Phisher verwenden. Darüber hinaus vermittelt es Wissen darüber, welche Konsequenzen Nutzer zu erwarten haben, wenn sie auf einen gefährlichen Link klicken. Beispielsweise könnte Schadsoftware auf ihr verwendetes Gerät heruntergeladen werden oder sie könnten auf eine echt aussehende Webseite weitergeleitet werden, die sie dazu auffordert, persönliche Daten preiszugeben. Finanzieller Verlust und/oder Identitätsdiebstahl könnten die Folge sein. Das Video adressiert außerdem in Literaturrecherchen identifizierte, bestehende Fehlannahmen und Missverständnisse in Bezug auf Phishing [15], [16], [17], [18], [19], wie z.B. dass lediglich wohlhabende Personen Ziel eines Phishing-Angriffs werden. Ganz im Gegenteil kann jeder Ziel eines Phishing-Angriffs werden, unabhängig davon wie bekannt oder wohlhabend eine Person ist oder welchen Status sie beispielsweise in einem Unternehmen besitzt.

Ziel des Videos ist die Steigerung der Fähigkeit, zwischen legitimen und Phishing-Nachrichten unterscheiden zu können. Lediglich durch die Untersuchung eines in der Nachricht enthaltenen Links können Nutzer verlässlich zwischen legitimen und Phishing-Nachrichten unterscheiden. Die folgenden Anweisungen und Erklärungen werden im Video thematisiert:

[3] Deutsches Phishing Video: https://www.youtube.com/watch?v=XeslAkZIuwY&t=9s
Englisches Phishing Video: https://www.youtube.com/watch?v=F4y2wzYpIKw

Anweisung 1: Ermitteln Sie das tatsächliche Ziel eines angezeigten Links:

Der erste Schritt in der Phishing-Erkennung ist das Erlangen von Wissen darüber, wie man das tatsächliche Ziel eines Links erkennt. Dieses kann entweder in einem Tooltip, in der Statuszeile oder in einem speziellen Dialogfenster angezeigt werden. Der angezeigte Tooltip kann jedoch auch gefälscht sein, um Nutzern ein falsches Gefühl von Sicherheit vorzuspielen. Darüber hinaus ist es wichtig, minimale Veränderungen bei Links zu erkennen. Manchmal ist das tatsächliche Ziel durch Schaltflächen, Bilder oder Texte wie „Klicke hier“ verschleiert.

Anweisung 2: Identifizieren Sie den sogenannten Wer-Bereich der URL:

Nachdem Nutzer die tatsächliche Ziel-URL identifiziert haben, sollten sie wissen, wie sie die Domain erkennen, welche wir als Wer-Bereich bezeichnen. Im Video beschrieben wir den Nutzern diesen als die letzten zwei durch Punkte getrennten Bereiche vor dem ersten alleinstehenden „/“ einer URL[5].

Außerdem erklärten wir ihnen, dass Phisher Nutzer hinters Licht führen wollen, indem sie den Unternehmensnamen an anderer Stelle als im Wer-Bereich der URL unterbringen. Dieser kann entweder vor oder nach dem Wer-Bereich platziert werden. Darüber hinaus sollten sich Nutzer nicht durch die Verwendung von HTTPS täuschen lassen. Im Folgenden werden beispielhafte Phishing-URLs gezeigt:

https://www.gmail.com.mail-nows.com/login

https://www.mail-nows.com/https://www.gmail.com/login.

Anweisung 3: Überprüfen Sie die Authentizität des Wer-Bereichs:

Nachdem der Wer-Bereich identifiziert wurde, ist der letzte Schritt die Verifizierung seiner Authentizität, indem dieser Zeichen für Zeichen überprüft wird. Das Video weist Nutzer daraufhin, dass Phisher oftmals (1) vertrauenswürdige Ausdrücke im Wer-Bereich verwenden (z.B. „shop-sicher.com“) oder (2) heimlich Zeichen austauschen. Beispielsweise tauschen sie „d“ durch „cl“ aus oder benutzen Tippfehler wie „mircosoft“.

2.2 Entwicklung des Videos

Gemeinsam mit einem professionellen Entwickler von Awareness-Videos entwickelten wir eine Geschichte, welche den Nutzern die relevanten Inhalte anschaulich und verständlich erklärt. Dabei wurde einfache Sprache benutzt und

[5] Die Studie wurde in Deutschland durchgeführt. Das heißt, der Fokus lag auf Domains bestehend aus zwei Ausdrücken, z.B. amazon.de und wir haben andere Konventionen wie z.B. in Groß-Britannien bestehend aus drei Ausdrücken nicht berücksichtigt, z.B. amazon.co.uk

auf die Verwendung von nicht-technischen Begriffen geachtet (z.B. die Verwendung von „Wer-Bereich“ statt des Begriffs „Domain“), damit der Inhalt auch Laien verständlich nähergebracht wird. Wichtige Aspekte bei der Überprüfung von Nachrichten (z.B. die Statuszeile) wurden mittels Screenshots hervorgehoben.

3. Evaluation – Methode

Der Fokus der Evaluation lag auf der Untersuchung der Effektivität des Videos, um signifikante Verbesserungen in Bezug auf die Erkennung von Phishing-Nachrichten aufzudecken. Für die Evaluation wurden die folgenden Hypothesen formuliert:

H1: Nutzer, die das Video gesehen haben, können die Legitimität von Nachrichten besser beurteilen, d.h. sie können zuverlässiger legitime Nachrichten und Phishing-Nachrichten identifizieren.

H2: Nutzer können acht Wochen nachdem sie das Video gesehen haben, die Legitimität von Nachrichten besser beurteilen, d.h. sie können zuverlässiger legitime Nachrichten und Phishing-Nachrichten identifizieren.

3.1 Studiendesign

Es wurde eine Onlinestudie mit Between-Subject-Design in zwei Phasen durchgeführt. Hypothese 1 wurde mit den Daten aus der ersten Phase untersucht und Hypothese 2 mit den Daten aus beiden Phasen.

Folgend werden die Aufgaben, welche die Probanden in der ersten Phase bearbeiteten, vorgestellt:

1. **Beurteilung von Nachrichten-Screenshots.** Den Probanden wurde die Aufgabe gestellt: „Entscheiden Sie für jeden Screenshot, ob dies ein Phish oder eine legitime Nachricht ist.“
2. **Ansehen des Videos.**
3. **Beurteilung von Nachrichten-Screenshots.** Als die Probanden aufgefordert wurden, die Nachrichten zu beurteilen, wurde die Frage gestellt: „Ist dies eine betrügerische Nachricht?“ Mögliche Antworten waren: „Ja, dies ist eine betrügerische Nachricht“ oder „Nein, dies ist keine betrügerische Nachricht“.
4. **Feedback zum Video.**
5. **Angabe von demographischen Daten.**
6. **Fragen nach Erlaubnis**, den/die Probanden/in für die Retention-Studie zu kontaktieren. Stimmten die Probanden zu, fragten wir nach den E-Mail Adressen und gaben jedem/r Probanden/in einen zufälligen Code, um ihre Ergebnisse aus den zwei Phasen anonym miteinander verknüpfen zu können.

Während der zweiten Phase (ungefähr acht Wochen später) wurden die Probanden für die Retention-Studie kontaktiert. In dieser wurden die Probanden erneut dazu aufgefordert, zwischen Phishing-Nachrichten und legitimen Nachrichten zu unterscheiden (lediglich Schritt 3 aus der ersten Phase). Dazu nutzten wir die Online-Plattform SoSciSurvey. Die Evaluation wurde als Quiz angelegt, mit dem Thema Sicherheit als Hauptaufgabe.

3.2 Material

Die Nachrichten-Screenshots wurden so gestaltet, dass eine Überprüfung nur anhand der tatsächlichen URL eines enthaltenen Links möglich ist. Bei allen Screenshots wurde die Maus so positioniert, dass die tatsächliche URL angezeigt wurde, abhängig von der vorhandenen Software entweder im Tooltip (mit Outlook) oder in der Statusleiste (mit Thunderbird oder einem Webbrowser). Die eine Hälfte der Nachrichten enthielt verdächtige Links, die andere Hälfte legitime Links[6]. Außerdem musste in Betracht gezogen werden, dass Probanden eine Nachricht als Phishing-Versuch einstufen könnten, weil sie den Sender nicht kennen oder kein Benutzerkonto bei diesem Anbieter besitzen. Deshalb wurde den Probanden ein Szenario vorgestellt, in welches sie sich hineinversetzen sollten. Sie nahmen dabei die Rolle von Max Müller ein, der ein Benutzerkonto bei allen in der Studie verwendeten Anbietern besitzt und dessen Kollege den Namen Jonas Schmidt trägt. Des Weiteren wurde ihnen mitgeteilt, dass es wichtig sei, zu entscheiden, ob eine Nachricht legitim ist oder nicht, weil die betrügerischen Nachrichten sie schädigen könnten und das Ignorieren echter Nachrichten negative Folgen haben könnte (zur Vermeidung, dass sie alle Nachrichten als Phishing-Nachrichten klassifizieren). Für jede Evaluationsphase wurden dieselben 16 Nachrichten verwendet (Pre, Post, Retention). Alle Nachrichten enthielten einen plausiblen Inhalt und wurden während der Auswertung in zufälliger Reihenfolge angezeigt.

Nachfolgend findet sich in Tabelle 1 eine Übersicht über die präsentierten Phishing-Nachrichten:

[6] Da wir als Evaluationsmethode ein Quiz nutzten, konnten wir das Verhältnis von Phishing-Nachrichten zu legitimen Nachrichten auf 50:50 anpassen, während dies unter realisitischen Bedingungen vermutlich nicht der Fall wäre.

Webadresse	Typ	Anweisung	Sender der Nachricht
https://162.179.34.56/login	TT	1+2	Service (DHL)
https://www.secure-documents-online.com/...	SB	1+2	Person (Kollege)
https://control-center.1uncl1.de/...	TT	1+3	Service (1 und 1)
https://www.volksbanknig.de/...	TT	1+3	Service (Volksbank)
https://www.google.com.best-photos.com/...	SB	1+2	Service (Google)
https://www.zehrukol.com/ebay.com/...	TT	1+2	Person (Kollege)
https://www.bahncard.bahm.de/...	SB	1+3	Service (DB)
https://www.cognstar.de/...	SB	1+3	Service (Congstar)

Tabelle 1: Überblick über die präsentierten Phishing-Nachrichten (SB = Statusbar; TT = Tooltip).

3.3 Rekrutierung und ethische Aspekte

Die Rekrutierung erfolgte über Online-Plattformen, Soziale Netzwerke, Flyer und persönliche Einladungen. Die Probanden erhielten keine Aufwandsentschädigung, jedoch motivierten wir sie zur Teilnahme, indem wir ihnen versprachen, dass sie im Rahmen der Studie gezeigt bekommen, wie sie vermeiden, Opfer von Betrug zu werden.

Die Anforderungen der Ethikkommission unserer Universität[7] in Bezug auf Studien, die Untersuchungen am Menschen beeinhalten, wurden eingehalten. Dies beinhaltete, dass die Daten der Personen anonym erhoben und gespeichert wurden. Die E-Mail Adressen, die die Probanden uns für die Teilnahme an der Retention-Studie zur Verfügung stellten, wurden getrennt von den Antworten der Probanden in einer separaten Datenbank gespeichert und konnten nicht mit den abgegebenen Antworten in Verbindung gebracht werden (mittels zufälliger Reihenfolge der Speicherung).

4. Evaluation – Ergebnisse

Unsere Stichprobe teilte sich in zwei Gruppen: Probanden, die lediglich an der ersten Phase teilnahmen (89: 39 weiblich/50 männlich, M=36,1 Jahre) und jene Probanden, die an beiden Phasen teilnahmen (22: 12 weiblich/10 männlich, M=38,09 Jahre). Es gab keine statistisch signifikanten Unterschiede zwischen den beiden Gruppen, weder in Bezug auf das Alter noch in Bezug auf das Geschlecht. Die Stichprobe wies dabei folgende Verteilung in Bezug auf den Bildungsgrad auf: Von den 89 Probanden in der ersten Phase besaßen 50 Probanden einen Universitäts- oder Hochschulabschluss und

[7] https://www.intern.tu-darmstadt.de/gremien/ethikkommisson/zustndigkeit/zustndigkeit.de.jsp

21 Probanden besaßen die Allgemeine Hochschulreife. Die entsprechenden Zahlen für die Probanden, die an beiden Phasen teilnahmen, sehen folgendermaßen aus: Zehn Probanden mit einem Universitäts- oder Hochschulabschluss und fünf Probanden mit der Allgemeinen Hochschulreife. Die deskriptiven Statistiken können in Tabelle 2 eingesehen werden.

	Pre	**Post**	**Retention**
Phish G1	65,5 (SD 28,6)	83,8 (SD 20,5)	
Phish G2	42,6 (SD 29,3)	86,9 (SD 18,3)	81,3 (SD 16,3)
Phish (Alle)	59,8 (SD 30,3)	84,55 (SD 20,0)	81,3 (SD 16,3)
Legitim G1	75,8 (SD 21,2)	87,7 (SD 17,3)	
Legitim G2	75,0 (SD 21,1)	88,1 (SD 17,9)	83,0 (SD 20,3)
Legitim (Alle)	75,6 (SD 21,1)	87,8 (SD 17,3)	83,0 (SD 20,3)

Tabelle 2: Überblick über die Erkennungsraten in % und ihre Standardabweichungen (SD) für alle Probanden (Alle), diejenigen, die nur an der ersten Phase teilnahmen (G1) und diejenigen, die an beiden Phasen teilnahmen (G2).

Die Leistungsveränderungen in Bezug auf die Erkennung von Phishing-Nachrichten und legitimen Nachrichten wurde in Abhängigkeit von korrekt erkannten Phishing-Nachrichten und legitimen Nachrichten gemessen. Der Unterschied in der Leistung vor und nach dem Ansehen des Videos (H1) wurde für beide Gruppen separat mittels einer ANOVA mit Messwiederholung durchgeführt. Die Leistung aus der Retention-Studie (H2) wurde ebenfalls mittels einer ANOVA mit Messwiederholung analysiert.

4.1 Erkennung von Phishing-Nachrichten

Pre-Post für alle Probanden: Zuerst stellen wir die Ergebnisse der ANOVA mit Messwiederholung dar. Der within-subject Faktor (Pre- und Post-Leistung) ist signifikant mit $p < 0{,}001$ und $\eta^2 = 0{,}526$, d.h. die Leistung in Bezug auf die Erkennung verändert sich signifikant. In Kombination mit den deskriptiven Daten (siehe Tabelle 2) zeigt sich, dass die Fähigkeit der Erkennung von Phishing-Nachrichten nach dem Ansehen des Videos signifikant ansteigt. Demnach kann H1 angenommen werden.

Probanden in der Retention-Studie: Die Ergebnisse der ANOVA mit Messwiederholung zeigen einen signifikanten Effekt in Bezug auf die Erkennung von bertrügerischen Nachrichten für Pre-, Post- und Retention-Leistung mit $p < 0{,}001$ und $\eta^2 = 0{,}636$. Ein post-hoc Test mit Bonferroni-Korrektur zeigt einen signifikanten Unterschied zwischen Pre- und Post-Test mit $p < 0{,}001$ und einen signifikanten Unterschied für Pre- und Retention-Leistung mit $p < 0{,}001$. Deshalb

können H1 und H2 für die Probanden, die an beiden Phasen teilnahmen, angenommen werden.

4.2 Erkennung von legitimen Nachrichten

Pre-Post für alle Probanden: Zuerst stellen wir die Ergebnisse der ANOVA mit Messwiederholung dar. Der within-subject Faktor (Pre-, Post-Leistung) ist signifikant mit $p < 0{,}001$ und $\eta^2 = 0{,}219$, d.h. die Fähigkeit in der Erkennung von legitimen Nachrichten verändert sich signifikant. In Kombination mit den deskriptiven Daten (siehe Tabelle 2) lässt sich erkennen, dass sich die Identifikationsrate nach dem Ansehen des Videos signifikant verbessert hat. Deshalb kann H1 angenommen werden.

Probanden in der Retention-Studie: Die ANOVA mit Messwiederholung zeigt einen signifikanten Effekt (Pre-, Post und Retention-Leistung) mit $p = 0{,}019$ und $\eta^2 = 0{,}173$. Ein post-hoc Test mit Bonferroni-Korrektur zeigt einen signifikanten Unterschied zwischen Pre- und Post-Leistung mit $p < 0{,}001$. Deshalb kann H2 angenommen werden.

5. Diskussion

Das fünfminütige Video konnte die Fähigkeit in der Erkennung von Phishing-Nachrichten und legitimen Nachrichten signifikant verbessern, ohne dabei eine Übervorsichtigkeit bei den Nutzern hervorzurufen.

Da Nutzer für gewöhnlich nicht auf einer täglichen Basis mit Phishing-Nachrichten konfrontiert werden, ist vor allem die Retention-Phase der Studie von speziellem Interesse. Das neu erworbene Wissen wird von den Nutzern demnach nicht regelmäßig angewendet, was begünstigt, dass dieses und somit die Ratschläge und Tipps aus dem Video in absehbarer Zeit wieder in Vergessenheit geraten.

Unsere Probanden verbesserten vor allem ihre Fähigkeit in der Erkennung von Phishing-Nachrichten, während die Erkennungsrate von legitimen Nachrichten gleich blieb.

Schwierigkeiten bei Phishing-Nachrichten traten vor allem in Bezug auf die Diskrepanz zwischen der im Text angezeigten URL und der tatsächlichen URL, welche in der Statuszeile eingeblendet wurde, auf. Positiv hervorzuheben ist, dass das Video in Bezug auf Instruktion 3 im Vergleich zu früheren Evaluationen die Leistung der Probanden deutlich verbessern konnte.

Der am häufigsten genannte Aspekt im Rahmen des Feedbacks der Probanden betrifft die Länge des Videos, welche als zu kurz angesehen wurde. Dies ist insofern interessant, als wir versucht haben, das Video so kurz wie möglich zu halten und dennoch eine hohe Effektivität zu erzielen. Darüber hinaus gibt es zwei interessante Punkte, die in Bezug auf die Weiterentwicklung des Videos relevant sind: (1) Den Fakt deutlicher hervorzuheben, dass lediglich die URL für die Beurteilung der Authentizität relevant ist. (2) Am Ende des Videos eine Zusammenfassung bereitzustellen, um das neu gewonnene Wissen nochmals zu festigen. Darüber hinaus wurden aber vor allem die

Einfachheit und Klarheit des Videos in Bezug auf den Inhalt des Videos gelobt als auch die allgemeine Verständlichkeit. Die genannten Aspekte wurden bei der Weiterentwicklung beachtet und adressiert und das überarbeitete Video dauert nun 5:09 Minuten und bietet mehr Zeit für Beispiele.

6. Limitationen

Fast die Hälfte der 89 Probanden gab uns ihre E-Mail Adresse, um sie bezüglich der Retention-Studie zu kontaktieren. Jedoch nahmen nur 22 Probanden auch tatsächlich an der Retention-Phase teil. Das bedeutet, dass diese Ergebnisse nicht für die Gesamtbevölkerung verallgemeinert werden können. Zusätzlich beeinträchtigt die eher homogene Zusammensetzung der Stichprobe in Bezug auf den Bildungsgrad die Repräsentativität der Studie. Da zudem bei der Rekrutierung bereits mitgeteilt wurde, dass Probanden durch die Teilnahme an der Studie lernen würden wie sie sich erfolgreich gegen Internet-Betrug wehren könnten, könnte dies vor allem die Nutzer angesprochen haben, die bereits interessiert an diesem Thema waren. In Bezug auf zukünftige Forschung sollten die Probanden demnach unter anderen demographischen Gesichtspunkten ausgewählt werden.

Da im Rahmen der Studie das Thema Sicherheit im Fokus stand und den Probanden als Hauptaufgabe gegeben wurde, sind die Ergebnisse demnach als „Best-Case-Szenario“ zu werten. Realistischere Erkennungsraten würden vermutlich schlechter ausfallen. Dennoch ist zu bemerken, dass Probanden vor dem Ansehen des Videos nicht in der Lage waren Phishing zu erkennen, obwohl ihnen dies als Hauptaufgabe gegeben wurde. Dies zeigt die Notwendigkeit von Awareness-Programmen auf.

Bedingt durch technische Einschränkungen seitens SoSciSurvey konnten die Probanden nicht mit der Maus über den Link fahren, um sich die tatsächliche URL anzeigen zu lassen. Diese wurde bereits mit auf dem präsentierten Screenshot angezeigt. Hier könnte argumentiert werden, dass die Probanden eventuell erst gar nicht über den Link gefahren wären, wenn ihnen dieser nicht bereits präsentiert worden wäre.

7. Related Work

Es existiert eine Vielzahl von Nutzerstudien, welche Einblicke in die mentalen Modelle von Nutzern in Bezug auf ihr Verhalten in der Phishing-Erkennung und die Effektivität entsprechender Methoden erlangen wollen. Dazu gehören beispielsweise spielerische Ansätze [20], [21, 7], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31]. Die Effektivität einiger dieser Ansätze wurde in Nutzerstudien überprüft.

Ein weiterer Ansatz nutzt den sogenannten „Teachable Moment“: Nutzern wird eine simulierte Phishing E-Mail mit einem verdächtig aussehenden Link zugeschickt. Klicken Nutzer auf den enthaltenen Link, werden diese zu einer Informationsseite weitergeleitet, welche entsprechende Informationen zum Thema Phishing bereithält. Ein solcher Ansatz wurde insbesondere von Caputo et al. [32] verwendet. Die Autoren

führten ebenfalls nach einem Zeitraum von 90 Tagen eine Retention-Studie zur Anti-Phishing-Schulung in einem Unternehmen durch. Die Ergebnisse der Studie zeigten jedoch keine signifikante Verbesserung. Ein ähnlicher Ansatz wurde in weiteren Forschungsarbeiten verwendet [33], [34], [35], die nach einer Woche ebenfalls Retention-Studien durchführten und deutliche Verbesserungen hinsichtlich der Verringerung der Anfälligkeit der Teilnehmer für Phishing E-Mails erzielten.

8. Fazit

Moderne Technologie ermöglicht es Betrügern, mit minimalen Kosten eine große Anzahl von Personen mithilfe von Phishing-Nachrichten anzugreifen. Da technische Methoden alleine nicht genügen, um 100% der Nachrichten zu erkennen, ist es wichtig zu wissen, wie Menschen diese erkennen können. Der hier vorliegende Beitrag stellt ein auf früheren Forschungen basierendes, kurzes, aber effektives Video vor, welches das Bewusstsein gegenüber Phishing wecken und stärken soll, ohne dabei gleichzeitig eine Übervorsichtigkeit zu entwickeln. Das fünfminütige Video wurde in einer Studie mit 89 Teilnehmern evaluiert. Darüber hinaus wurde nach acht Wochen eine Retention-Studie durchgeführt, an der 22 dieser 89 Teilnehmer teilnahmen. Die Ergebnisse der Studie zeigen, dass das Ansehen des Videos die Fähigkeit der Teilnehmer, zwischen legitimen und Phishing-Links zu unterscheiden, signifikant erhöhen kann und dass die Teilnehmer selbst nach acht Wochen Phishing-Links zuverlässiger erkennen konnten als zuvor.

Danksagungen

Diese Arbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Kompetenzzentrum für Angewandte Sicherheitstechnik (KASTEL) und im Zentrum für Forschung in Sicherheit und Datenschutz (CRISP) unterstützt. Zusätzlicher Dank geht an Alexander Lehmann für die Erstellung des Videos. Weitere Videos zu Sicherheit und Datenschutz finden Sie unter: https://www.youtube.com/user/alexanderlehmann.

Literaturverzeichnis

[1] Anti-Phishing Working Group, „Phishing Activity Trends Report, 4th Quarter 2016,“ 2016. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf. [Zugriff am 18 Mai 2018].

[2] Verizon, „Verizons,“ 2017. [Online]. Available: http://www.verizonenterprise.com/verizon-insights-lab/ dbir/2017/. [Zugriff am 18 Mai 2017].

[3] W. S. Technologies, „State of the Phish: Effectively Reducing Phishing and Malware Infections,“ 2016. [Online]. Available: http://pittsburgh.issa.org/ISSA\%20Pittsburgh\ %20Wombat\%20Security\%20May\%206\%202016.pdf . [Zugriff am 18 Mai 2017].

[4] O. Asudeh und M. Wright, „Poster: Phishing website detection with a multiphase framework to find visual similarity,“ *CCS 2016, ACM,* p. 1790–1792, 2016.

[5] X. Han, N. Kheir und D. Balzarotti, „Phisheye: Live monitoring of sandboxed phishing kits,“ *CCS 2016,* p. 1402–1413, 2016.

[6] G. Canova, M. Volkamer, C. Bergmann und R. Borza, „Nophish: An anti-phishing education app,“ *Security and Trust Management (STM),* p. 188–192, 2014.

[7] G. Canova, M. Volkamer, C. Bergmann, R. Borza, B. Reinheimer, S. Stockhardt und R. Tenberg, „Learn to spot phishing urls with the android nophish app,“ *IFIP World Conference on Information Security Education,* p. 87–100, 2015.

[8] G. Canova, M. Volkamer, C. Bergmann und B. Reinheimer, „Nophish app evaluation: lab and retention study,“ *USEC, Internet Society,* 2015.

[9] A. Kunz, M. Volkamer, S. Stockhardt, S. Palberg, T. Lottermann und E. Piegert, „Nophish: evaluation of a web application that teaches people being aware of phishing attacks,“ *Informatik,* 2016.

[10] S. Neumann, B. Reinheimer und M. Volkamer, „Don’t Be Deceived: The Message Might Be Fake,“ *International Conference on Trust and Privacy in Digital Business,* p. 199–214, 2017.

[11] S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, A. Kunz, P. Rack und D. Lehmann, „Teaching phishing-security: Which way is best?,“ *IFIP International Information Security and Privacy Conference,* p. 135–149, 2016.

[12] M. Volkamer, K. Renaud und P. Gerber, „Spot the phish by checking the pruned url,“ p. 372–385, 2016.

[13] M. Volkamer, K. Renaud und B. Reinheimer, „Torpedo: tooltip-powered phishing email detection,“ *IFIP International Information Security and Privacy Conference,* p. 161–175, 2016.

[14] M. Volkamer, K. Renaud, B. Reinheimer und A. Kunz, „User experiences of torpedo: Tooltip-powered phishing email detection,“ *Computers Security,* p. 100 – 113, 2017.

[15] X. Dong, J. Clark und J. Jacob, „Modelling user-phishing interaction,“ *Human System Interactions,* p. 627–632, 2008.

[16] J. Downs, M. Holbrook und L. Cranor, „Decision strategies and susceptibility to phishing,“ *SOUPS,* p. 79–90, 2006.

[17] T. Jagatic, N. Johnson, M. Jakobsson und F. Menczer, „Social phishing,“ *Communications of the ACM,* Bd. 50, Nr. 10, p. 94–100, 2007.

[18] M. Jakobsson, A. Tsow, A. Shah, E. Blevis und Y. Lim, „What instills trust? A qualitative study of phishing,“ *Financial Crypto,* p. 356–361, 2007.

[19] M. Kauer, T. Pfeiffer, M. Volkamer, H. Theuerling und R. Bruder, „It is not about the design — it is about the content! Making warnings more efficient by communicating risks appropriately,“ *Sicherheit,* Nr. 195, 2012.

[20] N. Arachchilage und M. Cole, „Design a mobile game for home computer users to prevent from “phishing attacks”,“ *i-Society 2011: International Conference on Information Society,* p. 485–489, 2011.

[21] M. Baslyman und S. Chiasson, „“Smells Phishy?”: An educational game about online phishing scams,“ *eCrime 2016: APWG Symposium on Electronic CrimeResearch*, p. 1–11, 2016.

[22] M. Hale und R. Gamble, „Toward increasing awareness of suspicious content through game play.,“ *SERVICES*, p. 113–120, 2014.

[23] M. Hale, R. Gamble und P. Gamble, „Cyberphishing: a game-based platform for phishing awareness testing,“ *Hawai'i International Conference on SystemSciences,* p. 5260–5269, 2015.

[24] S. Helser, „Fit: Identity theft education: Study of text-based versus game-based learning,“ *ISTAS 2015*, p. 1–4, 2015.

[25] M. Scott, G. Ghinea und N. Arachchilage, „Assessing the role of conceptual knowledge in an anti-phishing educational game,“ *ICALT*, p. 218–218, 2014.

[26] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong und E. Nunge, „Anti-phishing Phil: the design and evaluation of a game that teaches people not to fall for phish,“ *SOUPS*, p. 88–99, 2007.

[27] J. Sun, C. Kuo, H. Hou und L. Yu-Yan, „Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game,“ *Journal of Educational Technology & Society*, Bd. 20, Nr. 1, 2017.

[28] J. Sun und K. Yeh, „The effects of attention monitoring with EEG biofeedback on university students' attention and self-efficacy: The case of anti-phishing instructional materials,“ *Computers & Education*, p. 73–82, 2017.

[29] S. Tseng, K. Chen, T. Lee und J. Weng, „Automatic content generation for anti-phishing education game,“ *ICECE*, p. 6390–6394, 2011.

[30] Z. Wen, Y. Li, R. Wade, J. Huang und A. Wang, „What. hack: Learn phishing email defence the fun way,“ *CHI EA 201*, p. 234–237, 2017.

[31] C. Yang, S. Tseng, T. Lee, J. Weng und K. Chen, „Building an anti-phishing game to enhance network security literacy learning,“ *ICALT*, p. 121–123, 2012.

[32] D. Caputo, S. Pfleeger, J. Freeman und M. Johnson, „Going spear phishing: Exploring embedded training and awareness.,“ *IEEE S&P*, Bd. 12, Nr. 1, p. 28–38, 2014.

[33] K. Jansson und R. von Solms, „Phishing for phishing awareness,“ *Behaviour & Information Technology*, Bd. 32, Nr. 6, p. 584–593, 2013.

[34] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. Cranor und J. Hong, „Getting users to pay attention to anti-phishing education: evaluation of retention and transfer,“ *APWG: eCrime*, p. 70–81, 2007.

[35] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor und J. Hong, „Lessons from a real world evaluation of anti-phishing training,“ *APWG: eCrime*, p. 1–12, 2008.