Lukas Aldag, Benjamin Berens, Milan Burgdorf, Andreas Lorenz, Marie-Claire Thiery, Melanie Volkamer

NoPhish-Challenge-Karten

Evaluation in der Praxis

Phishing-Angriffe stellen nach wie vor eine große Bedrohung im privaten wie auch im Unternehmenskontext dar. Neben einer Verbesserung der technischen Schutzmaßnahmen setzen viele Unternehmen auch auf die Sensibilisierung der Mitarbeitenden für Phishing-Angriffe und deren Erkennung. Dabei stellt sich die Frage, wie man eine erste Ansprache von Mitarbeitenden konzipieren kann, um deren Aufmerksamkeit auf das Thema Phishing zu lenken und mit ihnen ins Gespräch zu kommen. Der vorliegende Beitrag stellt dafür entwickelte NoPhish-Challenge-Karten bzw. -Poster vor und fasst die Ergebnisse einer Evaluation deren Einsatzes im Rahmen einer Vor-Ort-Security-Awareness-Kampagne an einer Hochschule zusammen.

1 Einleitung

Phishing ist eine Form von Cyber-Angriffen, bei der Kriminelle gefälschte E-Mail-Nachrichten verwenden, um Menschen zu täuschen und somit an sensible Informationen zu gelangen oder Schadsoftware zu verbreiten, z B. um dann die Opfer erpressen zu können [4, 5]. Im Jahr 2020 waren jede und jeder vierte schon einmal von Cyber-Kriminalität betroffen [2]. Zudem sind 28% der Internetkriminalität auf Phishing zurückzuführen [1]. Diese

Vorfälle können zu Betriebsstörungen oder ausfällen führen und in der Folge für Unternehmen extrem kostspielig sein.

Um die Aufmerksamkeit auf die Wichtigkeit des Themas Phishing zu lenken und die Kompetenz von Mitarbeitenden bzgl. der Erkennung von Phishing Nachrichten zu steigern, organisieren viele Unternehmen Awareness-Veranstaltungen an zentralen Orten des Unternehmens, wie bspw. den Kantinen. Für die Ausgestaltung gibt es viele Möglichkeiten.

Im Rahmen unserer Forschung setzen wir zunächst darauf, mit den Adressaten der Security-Awareness-Maßnahmen bzw. konkret der Phishing-Awareness-Maßnahmen ins Gespräch zu kommen. Hierdurch sollen die Angesprochenen für die Problematik sensibilisiert und für die eigentliche Maßnahme motiviert werden.

Eine einfache Ansprache wie „Wissen Sie, was Phishing ist?“ führt dazu, dass viele Angesprochene einfach „klar“ antworten und weiter gehen. Auch eine offenere Ansprache wie „Ich würde mich gerne mit Ihnen über Phishing unterhalten“ ist wenig erfolgreich. Viele der Angesprochenen glauben, dass sie bereits wissen, was Phishing ist, oder erwarten, dass ihnen bereits bekanntes Wissen vermittelt werden soll (z. B. mit Links und Anhängen vorsichtig zu sein). Entsprechend wenig erfolgreich sind diese Formen der Ansprache bei vielen Mitarbeitenden oder Studierenden.

Wir entwickelten daher so genannte Challenge-Karten. Diese zeigen auf Vorder- und Rückseite je eine E-Mail: eine legitime und eine Phishing-E-Mail. Die Idee ist, die Adressaten zu fragen, ob sie sagen können, welche der beiden E-Mails die Phishing-E-Mail ist und angeben können, an welchen Merkmalen dies sichtbar wird. Nur wer weiß, worauf es bei der Erkennung von Phishing ankommt, wird die Lösung schnell finden. Den anderen kann auf diese Art und Weise an der E-Mail selbst erklärt werden, worauf zu achten ist (z. B., dass es wichtig ist, die URL zu prüfen, wo diese zu finden ist und welcher Teil der URL wichtig ist).

Im Rahmen unserer Forschung haben wir diesen Ansatz mit zwei unterschiedlichen Challenge-Karten anlässlich des „Safer Internet Days“ in der Mensa des Karlsruher Institut für Technologie (KIT) evaluiert. Dabei waren die E-Mails der einen Karte im Stil einer offiziellen E-Mail des KIT gehalten, die der anderen Karte stammten von einem (ausgedachten) Paketdienst.

2 Challenge-Karte

Die grundsätzliche Idee der Challenge-Karte ist, die Adressaten mit der Aufgabe „herauszufordern“, die Phishing-E-Mail zu erkennen und so auf eine spielerische Weise das Interesse an dem Thema Phishing zu wecken. Dabei sind die E-Mails auf der Vorder- und der Rückseite der Karte bis auf den Absender oder die URL hinter dem Link identisch. Es wird also ein Clone-Phishing-Angriff simuliert.

Hierbei steht der Realismus etwas im Hintergrund, da ein direkter Vergleich von betrügerischen und legitimen E-Mails in der Realität oft nicht möglich ist. Die Erfahrung von Vergangen Veranstaltungen lehrte uns, dass vielen Nutzerinnen und Nutzern die Erkennung schwer fällt, wenn die Phishing-E-Mail sich nicht am falschen Design oder Fehlern im Text erkennen lässt, da sie (noch) nicht wissen, wie sie Phishing-E-Mails effektiv erkennen.

Generell sind unterschiedliche Gestaltungen der Challenge-Karten möglich: Verschiedene E-Mail-Clients, verschiedene Inhalte, verschiedene Absendertypen (intern oder extern aus Sicht des Unternehmens) jeweils kombiniert mit verschiedenen Angriffsvarianten.

Zwei dieser Ausprägungen wurden für die Evaluation am KIT verwendet: einmal der ausgedachte Paketdienst und einmal die an jenem Tag (Safer Internet Day) verschickte E-Mail des Informationssicherheitsbeauftragten. Aus marken- und urheberrechtlichen Gründen wurde als Absender kein reales Paketdienst-Unternehmen verwendet. Abb. 1 zeigt eine E-Mail der Karte mit dem ausgedachten Paketservice. Abb. 2[1] zeigt eine E-Mail der zweiten Karte mit KIT-Bezug.

Ein Vorteil des fiktiven Beispiels ist, dass es jederzeit verwendet werden kann und nicht für jede Durchführung der Maßnahme angepasst werden muss. Somit ist der Herstellungsaufwand für die Nutzung fiktiver Beispiele geringer.

Abbildung 1 | Fiktiver Paketdienst

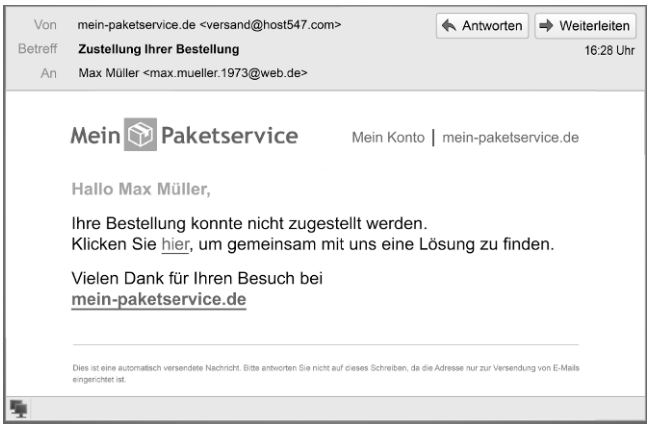
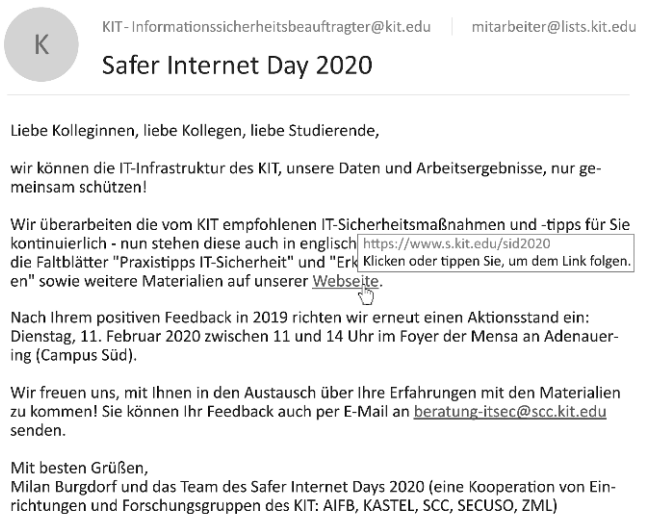


Abbildung 2 | KIT-Kontext



1 Es wurde diskutiert, ob die originale E-Mail in Veröffentlichungen verwendet werden darf oder ob man dadurch potentiellen Angreifern die perfekte Vorlage gibt. Zum einen sollte Sicherheit aber nicht auf dem „Security by Obscurity“ Prinzip beruhen und zum anderen stehen die Informationen zum Informationssicherheitsbeauftragten öffentlich sichtbar auf den Webseiten des KIT. Mit der Information alleine (die auch einfacher zu finden sind als die Challenge-Karten) könnten Angreifer die gleiche Art von Angriff umsetzen.

Für die Beispiele wurden zwei unterschiedliche E-Mail-Clients verwendet: für das KIT-Kontext-Beispiel Outlook und für das fiktive Beispiel Thunderbird. Zum einen werden die URL und der Absender in den E-Mail-Clients unterschiedlich dargestellt, zum anderen war nicht bekannt, welche E-Mail-Clients die Adressaten in der Mensa nutzen, da hier vor allem Studierende und Mitarbeitende des KITs angesprochen wurden.

In der E-Mail des fiktiven Dienstes wurde für die Phishing-E-Mail die Absender-Adresse geändert. So wurde als Name des Absenders in beiden Fällen „mein-paketservice.de" angezeigt, direkt dahinter jedoch die tatsächliche E-Mail-Adresse des Absenders („versand@mein-paketservice.de" oder „versand@host547.com"). In der E-Mail mit KIT-Kontext wurde für die Phishing-E-Mail die Zieladresse geändert. Dadurch sieht man lediglich das Wort „Webseite", aber nicht den dahinter liegenden Link. Ein Mauszeiger befindet sich auf dem Link, wodurch eine Toolbox mit den tatsächlichen Links angezeigt wird. Je nach Beispiel erscheint entweder die Domain des KIT („kit.edu/") oder aber die der Angreifer („kit.edu.mppls.com/"). Weitere Beispiele für Challenge-Karten, die in der Evaluation nicht verwendet wurden, sind auf der SECUSO@KIT-Webseite verfügbar.[2]

3 Studiendesign

Die Security-Awareness-Veranstaltung „Safer Internet Day" für KIT-Angehörige wurde genutzt, um den Einsatz der Challenge-Karten als Phishing-Awareness-Maßnahme zu evaluieren. Die Studie wurde von zwei Studienleitenden in der Mensa des KIT durchgeführt. Geplant und durchgeführt wurde die Maßnahme außerdem durch den Informationssicherheitsbeauftragten sowie Mitarbeitende von Hochschulrechenzentrum[3], KASTEL[4] und SECUSO[5]. Während die Studienleitenden Teilnehmende für die Studie ansprachen, klärten die weiteren Mitwirkenden mit Awareness-Materialien über das Thema Phishing und die Meldepflicht von IT-Sicherheitsvorfällen auf. Es gab Informationsstände mit Postern und Monitoren, an denen Awareness-Videos gezeigt wurden. Die Unterstützenden nutzten die Challenge-Karten auch über die Evaluation hinaus, um die Besucherinnen und Besucher der Mensa auf das Thema Phishing aufmerksam zu machen. Im Folgenden wird vorgestellt, wie die Karten eingesetzt wurden, um deren Einfluss auf die Motivation, sich mit dem Thema Phishing auseinander zu setzen, zu evaluieren. Der Ablauf war strukturiert und beinhaltete eine informierte Einwilligung der Teilnehmenden, die es uns ermöglicht, über die Ergebnisse zu berichten.

3.1 Studienumfrage

Die Besucherinnen und Besucher wurden in der KIT-Mensa angesprochen, ob sie bereit wären, entweder als Einzelpersonen oder als kleinere Gruppen von bis zu drei Personen an der Studie teilzunehmen. Die Teilnehmenden in kleinen Gruppen wurden gebeten, die Challenge-Karte einzeln zu bewerten. Dazu wurde der Ablauf der Studie kurz dargelegt und erklärt, dass die Daten anonym erhoben werden. Den Teilnehmenden wurde mitgeteilt, dass sie die Teilnahme jederzeit abbrechen können und in diesem Fall die erhobenen Daten gelöscht würden. Ebenso durften die Teilnehmenden jederzeit Fragen zu der Studie stellen. Zum Erheben der Daten nutzten die Studienleitenden jeweils ein Klemmbrett mit dem Fragebogen sowie die Challenge-Karten. Die Daten wurden in Form von Strichlisten oder kurzen Notizen gesammelt, damit die Teilnehmenden nicht zu lange aufgehalten wurden.

Im Rahmen der Studie wurden den Teilnehmenden vier Fragen gestellt: Zunächst sollten die auf den Karten dargestellten E-Mail-Nachrichten auf ihre Legitimität bewertet werden. Hierbei wurden die Teilnehmenden zwei unterschiedlichen Gruppen zugeordnet: Sie erhielten entweder die Challenge-Karte mit den E-Mails im KIT-Kontext oder die mit denen des fiktiven Paketdienstes. Die Zuteilung erfolgte durch die Studienleitenden.

Anschließend wurde erhoben, wie motiviert die Teilnehmenden sind, sich „weiter mit dem Thema Phishing bzw. Phishing-Nachrichten zu beschäftigen". Dies wurde mit einer fünfstufigen Skala erhoben, bei der 1 für eine geringe und 5 für eine sehr hohe Motivation stand.

Für die abschließenden Fragen wurden den Studienteilnehmenden beide Varianten der Challenge-Karte vorgelegt (vgl. Abb. 1 und Abb. 2). Die vorletzte Frage befasste sich damit, ob ein realistisches Beispiel mehr oder weniger zu der Motivation beiträgt,

2 https://secuso.aifb.kit.edu/Poster_Phishing_BetrNachrichten.php

3 Das Steinbruch Centre for Computing ist das Informationstechnologie-Zentrum des Karlsruher Instituts für Technologie (KIT) https://www.scc.kit.edu/

4 Das Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL) https://www.kastel.kit.edu/

5 Forschungsgruppe Security, Usability and Society (SECUSO) am Karlsruher Institut für Technologie (KIT) https://secuso.aifb.kit.edu/

sich mit dem Thema Phishing auseinander zu setzen. Unabhängig davon, ob die Befragten angegeben hatten, ein Realitätsbezug des Beispiels würde sie mehr oder weniger motivieren sich mit dem Thema auseinanderzusetzen, wurden die Befragten gebeten, die Gründe ihrer Einstellung zu erläutern. Auf Grund der Gegebenheiten in der Mensa und des Zeitdrucks der Teilnehmenden wurden die diesbezüglichen Antworten kurz und prägnant notiert. Vergleichbare Gründe wurden in Form einer Strichliste zusammengefasst.

3.2 Studienteilnehmende

Die Teilnehmenden waren primär Studierende und vereinzelt Mitarbeitende des KIT, die sich im Rahmen des „Safer Internet Days" in der Mensa eingefunden hatten. Insgesamt wurden 73 Teilnehmende befragt: 30 zu der Challenge-Karte in Abbildung 1 und 43 zu der Karte in Abbildung 2.

4 Ergebnisse

Die Auswertung der Ergebnisse zeigt, dass fast 50% der Befragten, die eine Ja- oder Nein-Antwort gaben, die Darstellung der fiktiven Nachricht korrekt eingeschätzt hatten. Das Ergebnis ist nicht besser als zufälliges Raten, da es nur zwei Antwortmöglichkeiten gab (legitim oder Phishing-E-Mail). Das zeigt, wie wichtig es ist, für dieses Thema zu sensibilisieren.

Neun von 30 Befragten, die die E-Mail mit dem fiktiven Dienst bewertet haben, haben die Nachricht falsch identifiziert und sieben gaben an, die Antwort nicht zu wissen. Die Bewertung der Nachricht mit KIT-Kontext war weniger offensichtlich: 28 der Befragten konnten kein Urteil über die Nachricht treffen, neun der 43 Befragten konnten die E-Mail richtig identifizieren und fünf urteilten falsch.

Ihre Motivation sich nach dem vorgelegten Beispiel weiterhin mit dem Thema Phishing bzw. Phishing-Nachrichten zu beschäftigen, bewerteten die Befragten der fiktiven Nachricht auf einer Skala von eins (für „gering") bis fünf (für „sehr hoch") mit einem durchschnittlichen Wert von 3,1. Das Ergebnis für die reale Nachricht fiel mit einem Mittelwert von 2,6 ein wenig geringer aus. Insgesamt lag der Durchschnitt aller Befragten bei 2,8. Beide Gruppen weisen einen Median von drei auf; damit ist mindestens die Hälfte der Angaben drei oder höher.

Die Bedeutung des Realitätsbezugs eines Beispiels bewerteten 48 der 73 Befragten mit „Ja". Der prozentuale Anteil der „Ja"-Antworten war dabei bei den Personen höher (77%), die zum fiktiven Dienst befragt wurden, als bei jenen, denen eine Nachricht mit realem Bezug vorlag (58%). Vier der 73 Teilnehmenden gaben keine Antwort.

Die für diese Einschätzung angegebenen Gründe waren unterschiedlicher Art. Elf Teilnehmende gaben an, ein konkretes Beispiel sei von Vorteil, da es realistischer sei. Sechs hingegen waren der Ansicht, eine Phishing-E-Mail sei unabhängig von ihrem Realitätsbezug eine Phishing-E-Mail, und eine abstrakte Nachricht sei besser auf andere Szenarien übertragbar. Zudem wurde angemerkt, dass eine Nachricht je nach verwendetem E-Mail-Client anders dargestellt wird, somit sei ein konkretes Hineinversetzen in das Szenario selbst im Fall einer realistischen Nachricht nicht zwangsläufig für alle Adressaten realistisch.

Darüber hinaus wurde mehrfach das Feedback geäußert, dass eine Nachricht mit weniger Text verwendet werden sollte, da viele durch den langen Text abgelenkt wurden und darin den Fehler vermuteten. Aus den Gesprächen ergab sich, dass einige Teilnehmende die E-Mail, die wir als Basis für die Challenge-Karte mit KIT-Bezug verwendet hatten, gar nicht kannten.

Eine weitere Erkenntnis aus der Studie war, dass die Ansprache der Befragten mittels der Challenge-Karten leichter gelang. Im Jahr zuvor war diese Kampagne ebenfalls durchgeführt worden, jedoch noch nicht durchgehend mit Challenge-Karten. Durch die Verwendung der Challenge-Karten waren die Angesprochenen meist interessierter und Personen, die danebenstanden, hatten mehr Interesse und hörten zu. So war es für die Studienleitenden einfacher, weitere Personen anzusprechen.

5 Diskussion

Eine Mehrheit der Teilnehmenden bevorzugt Beispiele mit einem Realitätsbezug, was bei der Erstellung der Beispiele allerdings einen Mehraufwand bedeutet. Es stellt sich also die Frage, ob der Mehrwert durch die Verwendung eines realen Inhalts den dafür erforderlichen Aufwand rechtfertigt. Aus den offenen Antworten lässt sich ableiten, dass es ggf. wenig Mehrgewinn gibt, wenn durch die Heterogenität der Teilnehmenden deren Wahrnehmung des Realitätsbezugs sehr unterschiedlich ausfällt, wenn also, wie im vorliegenden Fall, nicht alle den gleichen E-Mail-Client in der gleichen Konfiguration nutzen und nicht sichergestellt werden kann, dass die meisten Teilnehmenden diese E-Mail bereits kennen. Zumindest sollte die E-Mail möglichst in dem E-Mail-Client und in der Konfiguration abgebildet werden, die die angesprochene Teilnehmerin oder der angesprochene Teilnehmer auch nutzt. Dies wird im Unternehmenskontext einfacher sein als an einer Universität, wo die Adressaten (insbesondere Studierende) unterschiedliche E-Mail-Clients nutzen.

Die Ergebnisse zeigen, dass der Realitätsbezug einer Challenge-Karte nach dem Betrachten einer fiktiven Nachricht bedeutender eingeschätzt wurde als nach der Betrachtung einer an die Zielgruppe angepassten Nachricht. Eine Erklärung für dieses Ergebnis könnte der sogenannte „Self-Serving Bias“ liefern [3]: Laut Forsyth neigen Menschen dazu, bei einer schlechten Performance äußeren Einflussfaktoren die Schuld zu geben. In diesem Fall hätten Teilnehmende, die die fiktive Nachricht erhalten haben, die realitätsbezogene Nachricht vielleicht besser erkennen können, wenn sie diese im Kontext ihres gewohnten Umfeldes erhalten hätten (in diesem Fall der KIT-Kontext). Diese „Ausrede“ gilt weniger für die andere Gruppe und daher fällt hier die Zustimmung etwas geringer aus.

Allgemein war die Motivation zur weiteren Beschäftigung mit Phishing mit einem Durchschnitt von 2,8 nicht sehr hoch. Allerdings liegt uns kein Vergleichswert einer Kontrollgruppe vor, und es ist uns leider nicht bekannt, wie hoch die Motivation generell ist, sich mit dem Thema Phishing auseinander zu setzen.

Eine mögliche Erklärung für dieses Ergebnis könnte auch die Formulierung der eigentlichen Frage sein. Vielleicht haben Teilnehmende die Frage so verstanden, wie hoch ihre Motivation ist, sich unmittelbar mit dem Thema weiter zu beschäftigen. Da viele Teilnehmenden sich in der Mittagspause befanden, könnte dies zu einer geringeren Motivation geführt haben. Daher sollte bei einer zukünftigen Erhebung deutlich gemacht werden, dass es um die generelle Motivation geht, und ein anderer Befragungszeitpunkt gewählt werden, an dem Teilnehmende weniger Zeitdruck haben. Außerdem wäre die Erhebung einer Kontrollgruppe interessant, um das Ergebnis in Relation setzen zu können. Auch ein Vergleich der Motivation vor und nach der Beschäftigung mit der Challenge-Karte wäre interessant.

Die Anregung, weniger Text in den Beispielen zu verwenden, sollte für das zukünftige Design der E-Mails für die Challenge-Karten berücksichtigt werden. Zwar kann argumentiert werden, dass man sich nicht vom Text beeinflussen lassen sollte. De facto ist das aber bei vielen der Fall, die wenig Erfahrung mit Phishing haben. Außerdem dauert die Challenge unnötig lang, wenn lange Texte verwendet werden, da die Teilnehmenden meist den Text in Ruhe lesen, um Hinweise zu finden. Dies könnte einen negativen Einfluss auf die anschließende Motivation haben, sich weiter mit dem Thema Phishing zu beschäftigten.

Für eine zukünftige Studie wäre es interessant, die Daten abhängig von den Antworten in weitere Kategorien aufzuteilen. Wie motiviert waren die Teilnehmenden, die die Nachricht richtig eingeschätzt haben, im Vergleich mit denjenigen, die sie nicht richtig eingeschätzt haben? Des Weiteren könnte nach einem bestimmten Zeitraum erfragt werden, ob die Teilnehmenden sich weiter informiert haben.

6 Fazit

Die Challenge-Karten haben – unabhängig davon, ob der Inhalt an den Kontext angepasst ist oder nicht – einen positiven Einfluss auf das Interesse der Teilnehmenden, sich mit dem Thema Phishing zu beschäftigen. Zudem fällt es den Studienleitenden leichter, mit den Teilnehmenden ins Gespräch zu kommen. Die Studie hat aber auch gezeigt, dass es wichtig ist, die Beispiel-E-Mail möglichst realitätsnah zu gestalten. Außerdem sollte die E-Mail möglichst wenig Text beinhalten.

Als Future Work bleibt die Untersuchung dieses Ansatzes in anderen Kontexten, z. B. in Form von Challenge-Postern, die an zentralen Orten aufgehängt werden und die die Adressatinnen und Adressaten selbst bspw. über QR-Codes auflösen können. Im Rahmen der Auflösung wird dann jeweils erläutert, woran erkannt werden kann, ob die E-Mail ungefährlich oder eine Phishing-E-Mail ist.

Danksagung

Diese Arbeit wurde unterstützt durch Finanzierungen der Helmholtz-Gemeinschaft (HGF), Unterthema Engineering Secure Systems (ESS).

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2019*.

[2] Bundesamt für Sicherheit in der Informationstechnik. 2020. *Digitalbarometer 2020: Trotz Gefahren, jeder Zehnte ohne Schutz im Netz*. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Digitalbarometer_090919.html. Accessed 22 January 2021.

[3] Donelson R. Forsyth. 2008. *Self-Serving Bias*. JEPSON School of Leadership Studies, University of Richmond.

[4] Garera, S., Provos, N., Chew, M., and Rubin, A. D. 2007. *A framework for detection and measurement of phishing attacks*. *DOI*=10.1145/1314389.1314391.

[5] Hong, J. 2012. *The state of phishing attacks*. Communications of the ACM, 55(1), 74.