netidee PROJEKTE

Phishingtraining

Endbericht | Call 15 | Projekt ID 5126

Lizenz CC-BY-SA

Inhalt

1 Einleitung

Das Internet ist in der heutigen Zeit nicht mehr aus unserem Alltag wegzudenken. Vor allem für die heutigen Kinder und Jugendlichen ist es leicht einen Zugang zu dieser Technologie zu finden (Turner, 2015). Sie sind es schon gewohnt durch diverse Technologien miteinander zu kommunizieren und zu interagieren. In Übereinstimmung mit anderen Studien konnten die ForscherInnen Riedl et. al. (2016) feststellen, dass das Internet, vor allem soziale Netzwerke, Jugendlichen hilft sich mit Peers auseinanderzusetzen, aber es auch in Bezug auf Schule und weitere Ausbildungen eine wichtige Rolle spielt (vgl. Glüer, 2018). Allerdings erwähnt das Forscherteam (Riedl, et al., 2016) auch ausdrücklich die Notwendigkeit für Jugendliche Medienkompetenzen zu erlernen, um einen verantwortungsbewussten Umgang mit dem Internet zu lernen. Insbesondere da das Internet auch neue Möglichkeiten für Betrüger und Hacker ermöglicht. So zeigt sich, dass eines der häufigsten Sicherheitsprobleme in der Altersgruppe von 16- bis 24-jährigen der Erhalt von Phishing Mails ist (28,25%; Statistik Austria, 2019).

Im Rahmen des netidee-Projekts **Phishingtraining** haben wir als interdisziplinäres Team an der Universität Wien Technik mit Psychologie verbunden und eine Plattform geschaffen, um die Resistenz von Jugendlichen gegen Phishing-Angriffe zu trainieren und dauerhaft zu verbessern. In einer Pilotstudie mit zwei Schulklassen konnten erste Ergebnisse zur Wirksamkeit des Konzepts gewonnen werden, die in zukünftige Phishingtrainings einfließen werden.

2 Projektbeschreibung

Phishing, eine Untergruppe von Social Engingeering, ist ein bis heute ungelöstes Problem. Studien haben gezeigt, dass dieses nicht durch klassische Awareness-Programme erfolgreich bekämpft werden kann. Diese haben zum Ziel Menschen gegen äußere Beeinflussungen zu immunisieren (Weßelmann, 2008). Menschen lernen durch ein sogenanntes *rule-based training* Regeln, wie sie beispielsweise Hinweise in Phishingnachrichten entdecken und schließlich die Nachricht als Phishing klassifizieren können (Stafford, 2020). Laut Weßelmann (2008) ist jedoch eine Immunisierung in dieser Art nicht effektiv möglich, da Social Engineering sich z.B. auch in der Erziehung oder bei Verhandlungstechniken wiederfindet und eine Immunisierung somit soziale Interaktionen, effektives Zusammenarbeiten, aber auch die

persönliche Weiterentwicklung behindern würde. Zudem gibt Weßelmann (2008) an, dass der Mensch als Variable bei diesen Awareness-Trainings nicht mit einkalkuliert wird. Würde jeder Mensch beim Erhalt einer Phishingnachricht überlegt handeln, also die Nachricht genau betrachten, die Absenderadresse überprüfen, etc., würden wesentlich weniger Menschen Opfer einer Social-Engineering-Attacke werden. Jedoch würden externe Faktoren wie etwa Zeitmangel dazu führen, dass sich Menschen nur auf Heuristiken verlassen würden. Bei Phishing wird beispielsweise bewusst Zeit- oder Autoritätsdruck erzeugt. Das löst ein Verhalten aus, das dazu führt, dass der Phishing-Link angeklickt wird (vgl. (Hoss, 2015).

Kahnemann (2011) hat in seinen Forschungen zwei Systeme postuliert: System 1, welches automatisch funktioniert und schnell agiert. Dort sind Heuristiken verankert, da es keiner großen Mühe Bedarf ein Verhalten zu zeigen, das wir regelmäßig an den Tag legen. System 2 wiederum denkt logisch und versteht komplexe Abläufe. Allerdings erfordert es Konzentration und Anstrengung, sich auf ein bestimmtes Ereignis zu konzentrieren.
Bei der Einschätzung, ob es sich um eine Phishingnachricht handelt, sollte System 2 aktiv sein, da Konzentration und Anstrengungsbereitschaft erforderlich sind, um herauszufinden, ob es sich tatsächlich um eine Phishingnachricht handelt. Durch spezifische Faktoren (z.B. vermittelte Autorität oder Zeitdruck) übernimmt diese Aufgabe aber oft System 1 und führt damit zu Fehlentscheidungen (Klicken auf den Link). **Das Ziel des Projektes war also, beim Erhalt einer Phishingnachricht System 2 zu aktivieren.**
Da laut Studien besonders die Gruppe der 18- bis 25-jährigen Zielgruppe für Phishing-Attacken ist (vgl. (Jampen, Gür, Sutter, & Tellenbach, 2020), war das vorliegende Projekt vorerst auf 14- bis 18-jährige ausgelegt. Damit kann eine Intervention gesetzt werden, bevor die Jugendlichen zur Zielscheibe von Phishing-Attacken werden. Zudem bietet die neuro-psychologische Entwicklung dieser Altersgruppe einen Vorteil, um Resilienz gegenüber Phishing zu steigern, da in diesem Alter die Kapazität des Arbeitsgedächtnisses und damit einhergehend auch das Faktenwissen der Jugendlichen leicht erweitert werden kann (Lindberg & Hasselhorn, 2018).

Das Gesamtkonzept des Phishintrainings erfolgte in mehreren Phasen. In der **Aufklärungsphase** wird ein einstündiges Awareness-Training zum Thema Phishing durchgeführt und die Plattform des Phishingtrainings vorgestellt. Dabei erhalten SchülerInnen umfassende Informationen zum Thema Phishing (z.B. wie Phishingnachrichten aussehen, mögliche Konsequenzen beim Klicken eines Phishing-Links) und es werden basierend auf Kleins Recognition-Primed Decision Model (RPDM; Klein, 1993) Lösungsansätze erarbeitet und anhand von realistischen Beispielen erprobt. Die Jugendlichen sollen, indem sie auf bestimmte Punkte achteten (Erkennen kritischer Hinweise, Formen, Erwartungen, Stecken von plausiblen Zielen, Setzen einer geeigneten Handlung) die Situation, dass es sich um eine Phishingnachricht handelt, wiedererkennen und die Handlungsoptionen (nicht auf den Link klicken, E-Mail löschen) evaluieren und mental simulieren. Im Anschluss an das Awareness-Training erhalten die Jugendlichen per E-Mail einen

Link zur Registrierung für die Plattform.
In der ersten Phase des aktiven Trainings, der **Trainingsphase**, bekommen die Jugendlichen innerhalb eines Monats acht Phishingnachrichten zu zufälligen Zeitpunkten. Die hohe Frequenz dient dazu das Gelernte häufig anzuwenden und somit schneller zu einer Gewohnheit zu formen, also zu einer automatischen Handlungsweise, welche wiederum in System 1 verankert ist (vgl. Betsch & Haberstroh, 2005). Ziel ist es also, dass die Inhalte und Reaktionen, die zunächst im System 2 gespeichert werden, automatisiert werden, um dann Teil von System 1 zu werden. Die versendeten Phishingnachrichten variierten in Schwierigkeitsgraden (vier verschiedene Schwierigkeitsstufen abhängig von der Anzahl an kritischen Hinweisen) und wurden über verschiedene Kanäle (E-Mail, SMS, Social Media) versandt. Beim Klicken auf den Link in einer Phishingnachricht werden die Jugendlichen auf eine Webseite weitergeleitet, wo sie direkt Feedback darüber erhalten, dass sie gephisht wurden und eine Kurzfassung der Lerninhalte aus dem Awareness-Training präsentiert bekommen (= „embedded training“, wird in vielen Studien als effektives Tool zur Sensibilisierung verwendet; vgl. Canfield, Fischhoff, & Davis, 2016; Jampen, Gür, Sutter, & Tellenbach, 2020). Zusätzlich wird abgefragt, wo sich die Jugendlichen gerade befinden, und was sie gemacht haben, um aufzudecken, in welchen Situationen Jugendliche besonders gefährdet für Phishing bzw. unaufmerksame Reaktionen sind. Am Ende der Phase bekommen die Jugendlichen schließlich individuelles, schriftliches Feedback zu ihren Reaktionen in dieser Phase.
In der darauffolgenden **Testphase** werden die Intervalle in welchen die Phishingnachrichten verschickt wurden verlängert, sodass sie nur fünf Nachrichten in einem Zeitraum von drei Monaten erhalten.
Schließlich erfolgte nach einer Pause von einem Monat, in welchem keine Nachrichten verschickt werden, der Versand einer letzten Phishingnachricht (**Abschlussphase**) um einen längerfristigen Lerneffekt, nach Pausieren der laufenden Wiederholung des Gelernten festzustellen.
Abschließend erfolgt erneut Feedback an die Jugendlichen sowie der Versand eines Feedbackfragebogens an sie, um das Konzept weiter zu verbessern.

Im Sommersemster 2021 wurde eine erste Version des Phishingtrainings mit zwei Schulklassen durchgeführt. Von 104 verschickten Phishingnachrichten in der Trainingsphase wurden 55,77% geöffnet (am häufigsten Schwierigkeitsgrad 3) und in 4,81% der Fälle der darin enthaltene Link angeklickt (am häufigsten Schwierigkeitsgrad 4). Insgesamt haben alle Jugendlichen zumindest zwei Mal eine Phishingnachricht geöffnet, wobei vier Schüler*innen auf den Link in der Nachricht geklickt haben. In der Testphase wurden von 57 Phishing Nachrichten 50,88% geöffnet und vier Mal (=7,02%) ein Link angeklickt. In der Abschlussphase haben sieben von zwölf der Jugendlichen die Nachricht geöffnet, wobei einmal der Link angeklickt wurde. Nach der Durchführung wurden die SchülerInnen um Feedback zur Studie gebeten. Dabei haben die SchülerInnen angegeben, dass sie das Projekt als wenig aufwändig einschätzen. Das Awareness-Training wurde als informativ eingestuft und es konnten neue Inhalte mitgenommen werden. Zwar haben sie die

Phishingnachrichten als „eher leicht“ bis „sehr leicht“ eingestuft, gaben dennoch an, das Gefühl zu haben nach dem Training solche Nachrichten besser erkennen zu können und dass das Projekt ihr Denken und Handeln beim Öffnen von Nachrichten beeinflusst habe. Alle SchülerInnen würden bei einem ähnlichen Projekt erneut teilnehmen.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 – *Detailplanung und Formales am Projektstart*

Arbeitspaket 1 wurde im Dezember 2020 mit der Abgabe und Abnahme des Detailprojektplans, dem ersten Blogeintrag sowie dem ersten Förderratenabruf abgeschlossen.

3.2 Arbeitspaket 2 – *Entwicklung des psychologischen Konzepts*

Die Aufgabe dieses Arbeitspakets war die Entwicklung eines psychologischen Konzepts für ein effektives Training gegen Phishing. Nach einer ausführlichen Literaturrecherche zu bisherigen Studien und Statistiken zum Thema Phishing und Awareness wurde das Konzept erstellt. Es wurde bewusst so gestaltet, dass es für Laien verständlich ist und von LehrerInnen als Wissensgrundlage für die zukünftig geplante selbstständige Durchführung des Phishingtrainings genutzt werden kann. Es beschreibt die Relevanz des Themas, die bisherigen Lösungsversuche für die Problematik von Phishing und schließlich das entwickelte Training. Das finale Dokument wurde nun mit den Ergebnissen der aktuellen Studie ergänzt und öffentlich zugänglich gemacht.

3.3 Arbeitspaket 3 – *Implementierung der Webapplikation*

In diesem Arbeitspaket wurde die Webplattform zum Erstellen und Verwalten von Phishing-Kampagnen geplant und implementiert. Die Ziele der Plattform und die erforderlichen Features wurden in Workshops mit dem gesamten Team festgelegt. Die wesentlichen Features umfassen:

- Phishing-Kampagnen anlegen und verwalten
- Benutzerverwaltung
- Metadateneingabe für personalisierte Nachrichten (z.B. Social Media Accounts,
- Telefonanbieter, Adresse)
- Verwaltung von Phishing-Templates
- Fragebogen nach Klick auf Phishing-Links

Als Technologiestack wurde .NET Core als etabliertes Framework für Webapplikationen mit einem breiten Ökosystem gewählt, in Kombination mit einer SQL-basierten Datenbank. Da die Applikation im Kern mit externen Systemen kommuniziert (z.B. via E-Mails, SMS) sind sowohl die Entwicklungsumgebung als auch das Deployment eine Herausforderung. Um eine möglichst stabile Umgebung zu schaffen, wurde auf Docker-Container gesetzt und die Plattform auf der IT-Infrastruktur der Universität Wien gehostet.

Um glaubhafte Phishingnachrichten zu erzeugen, mussten außerdem passende Domains gekauft werden und der Mailserver entsprechend konfiguriert werden. Weiters wurde mit CM.com ein passendes Gateway für den Versand von SMS über die Plattform ausgewählt und integriert.

Der Code der Plattform wurde auf Github veröffentlicht.

3.4 Arbeitspaket 4 – *Implementierung der Phishingengine*

Die Phishing-Plattform ermöglicht es, komplette Phishing-Kampagnen automatisiert mit Teilnehmerinnen durchzuspielen. Die im Rahmen des Projekts implementierte Plattform unterstützt Phishing-Templates (Plaintext oder HTML), die Platzhalter für Metadaten vorsehen (z.B. Vorname, Geburtsdatum). In Templates kann die Zieldomäne (für Links) definiert werden, Absendernamen, ein Zeitfenster (z.B. zwischen 30.12. und 1.1. für Neujahrs-Phishingmails), ob es sich um Gruppenmails handelt, sowie Informationen zu Schwierigkeitsgrad und Auswirkungen. Es wird auch der Kanal gewählt, über den die Nachrichten gesendet werden (E-Mail oder SMS). Beim Klick auf einen Link in den Phishingnachrichten wird die Teilnehmerin oder der Teilnehmer auf einen Feedback-Fragebogen weitergeleitet. Zusätzlich werden Bilder aus den HTML Templates dynamisch vom Server nachgeladen. Damit kann der Zeitpunkt des Öffnens der E-Mail festgestellt und automatisiert in der Plattform abgespeichert werden. Als Auswertungsexport können .csv-Files in Kampagnen erzeugt werden.
Das Gesamtkonzept und die Strategie, Nachrichten für die einzelnen TeilnehmerInnen zu erzeugen, war eine herausfordernde Aufgabe. Letztendlich haben wir die Template-Engine im Laufe des Projekts mehrmals erweitert, um benötigte Funktionalitäten zu ergänzen.
Es wurde viel Zeit investiert, um die Templates und die Konfiguration des Mailservers so zu gestalten, dass unsere Phishingnachrichten nicht unmittelbar von E-Mail Providern wie Google und GMX als Spam klassifiziert werden. Dies konnte am Ende für alle Templates erreicht werden.

3.5 Arbeitspaket 5 – *Betreuung der Schulklassen*

Dieses Arbeitspaket beinhaltet die Betreuung der Schulklassen. Direkt nach dem Abschluss der Detailplanung wurde mit mehreren Schulen Kontakt aufgenommen, um das von uns geplante Phishingtraining anzubieten. Entgegen unseren Erwartungen bekamen wir nur sehr begrenzt Rückmeldungen, trotz mehrmaliger Kontaktaufnahme. Wir führen dies auf die schwierige Situation in den Schulen zum damaligen Zeitpunkt, aufgrund von wechselnden Phasen von Präsenz-, Online- und Hybrid-Unterricht, zurück. Es gelang uns dennoch, zwei Klassen an zwei Schulen von der Teilnahme zu überzeugen und somit die Projektauflagen zu erfüllen. Mit diesen wurde ein Online-Termin vereinbart, ein Awarenesstraining durchgeführt und anschließend die Studie erklärt. Alle SchülerInnen, die an der Studie teilnehmen wollten, mussten eine unterzeichnete Einverständniserklärung an uns schicken und bekamen den Link zur Registrierung auf der Phishing-Plattform retour. Schließlich wurden mehrmals Erinnerungen zur Registrierung und der Angabe von Meta-Daten (für personalisierte Nachrichten) an die

SchülerInnen geschickt, bevor das Training mit der Trainingsphase begonnen hat. Die finale Anzahl der Teilnehmer an der Studie war leider geringer als gehofften und geplant, weshalb eine deskriptive Auswertung der Daten erfolgte.

3.6 Arbeitspaket 6 – *Psychologische Abschlussevaluierung des Konzepts*

Das Arbeitspaket 6 dient der Evaluierung des Konzepts durch die Auswertung der Ergebnisse sowie einer Rückmeldung durch die TeilnehmerInnen. Nachdem ein Analyseplan erstellt wurde, wurde nach Ende der Datenerhebung die Datenaufbereitung und anschließend die Auswertung der Daten durchgeführt und im Konzept schriftlich für Laien aufbereitet ergänzt. Die Rohdaten wurden zur Nachvollziehbarkeit auf dem OpenData-Portal veröffentlicht. Implikationen für die weitere Nutzung und Verbesserung des Phishingtrainings wurden ebenfalls abgeleitet und im Konzept ergänzt.

3.7 Arbeitspaket 7 – *Dokumentation und Formales am Projektende*

Dieses Arbeitspaket beinhaltet die abschließende Prüfung und Dokumentation des Projekts. Es wurde ein letzter Blogeintrag verfasst. Der Projektendbericht, Zusammenfassung, Anwender_innen-Dokumentation (für Lehrer_innen) und Entwickler_innen-Dokumentation wurde erstellt und an netidee übermittelt sowie auf die Projektwebsite hochgeladen. Die Endabrechnung inkl. aller Originalbelege wurde dokumentiert und an netidee übermittelt. Die Projektwebsite wurde aktualisiert und alle Ergebnisse unter Angaben der Lizenzen der Öffentlichkeit zur Verfügung gestellt. Das Projekt wurde somit vollständig dokumentiert abgeschlossen.

4 Umsetzung Förderauflagen

In der Fördervereinbarung wurden vier Förderauflagen festgelegt.

Bereits mit dem Zwischenbereicht erfüllt:

Auflage 1: Vor Förderabschluss Detaillierung Projektergebnis *Die Detailierung des konkreten Projektergebnisses wurde via E-Mail vor Projektstart durchgeführt.*

Auflage 2: Vor Förderabschluss klären, ob Antragsteller Uni oder genannten Personen selbst sind *Das Projekt wurde als Universität Wien beantragt und ebendort durchgeführt.*

Auflage 3: Konkrete Pilotcases mit Schulen durchführen & dokumentieren
Die Plattform wird mit Schülerinnen und Schülern von zwei niederösterreichischen Schulen im Rahmen von konkreten Pilotcases durchgeführt. Diese wurden bereits gestartet und laufen bis zum Sommer.

Wird mit dem Endbericht zeitgleich erfüllt:

Auflage 4: Veröffentlichung psychologisches Konzept iSv open source

Das Konzept wurde auf der Projektwebseite veröffentlicht.

5 Liste Projektendergebnisse

1	***Projektzwischenbericht***	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
2	***Projektendbericht***	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
3	***Entwickler_innen-DOKUMENTATION*** *Anleitung für die Installation und den Betrieb der Plattform auf einem eigenen Server (README.md)*	*GPL 3.0*	*https://github.com/sschritt/phishingtraining*
4	***Anwender_innen-DOKUMENTATION*** *Dokumentation für LehrerInnen (bzw. Admins eines Phishingtrainings)*	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
5	***Veröffentlichungsfähiger Einseiter***	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
6	***Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit*** *(Teil des Endberichtes)*	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
7	***Webapplikation "Phishingtraining"*** *Vollständige Codebasis der Webapplikation in einem Github-Respository*	*GPL 3.0*	*https://github.com/sschritt/phishingtraining*
8	***Phishingengine*** *(Teil von Projektergebnis 7)*	*GPL 3.0*	*https://github.com/sschritt/phishingtraining*
9	***Daten-Projektergebnisse als Open Data*** *Anonymisierte Ergebnisse der Evaluierung mit Schulklassen*	*CC-BY Sharelike-3.0 AT*	*https://www.opendataportal.at*

10	***Psychologisches Konzept*** *inkl. Studiendesign und -ergebnisse der Evaluierung mit Schulklassen*	*CC-BY Sharelike-3.0 AT*	*https://netidee.at/phishingtraining*
11	***Projektwebseite***	*GPL 3.0*	*https://sschritt.github.io/phishingtraining/*

6 Verwertung der Projektergebnisse in der Praxis

Angaben zur Verwertung der Projektergebnisse in der Praxis

Auch wenn die Aussagekraft aufgrund der geringen Teilnehmeranzahl begrenzt ist, kann insgesamt ein Lernerfolg nach der Trainingsphase angenommen werden. Da sich insgesamt jedoch nur eine kleine Verbesserung zwischen Trainings- und Testphase gezeigt hat, kann davon ausgegangen werden, dass wie bereits in vorausgehender Literatur angegeben, reine Awareness-Trainings bei Phishing nicht ausreichend sind. Stattdessen muss ein kontinuierliches Training stattfinden, wie es durch die Trainingsphase in unserem Konzept umgesetzt wird. Möglicherweise wäre das Training daher noch erfolgreicher, wenn diese Phase länger andauern würde. Um diese Annahmen zu prüfen und um noch mehr Daten bzw. mehr Studienteilnehmer zu bekommen und die Ergebnisse zu stärken, sind wir mit Schulen in Kontakt und hatten geplant im Herbst 2021 noch weitere Trainings zu starten. Aufgrund der andauernden Corona-Situation haben wir diese Phishingtrainings jedoch in Rücksprache mit den Schulen wieder verschoben. Gemeinsam mit der Saferinternet.at-Initiative planen wir allerdings noch im Verlauf des Schuljahres weitere Trainings umzusetzen, um die vorläufigen Ergebnisse zu untermauern und das Konzept abhängig von den Ergebnissen in dieser oder abgeänderter Form auch weiterhin für Schulen anzubieten. Weiters wird die Phishingplattform im Rahmen von weiteren Kooperationsprojekten (z.B. mit der Arbeiterkammer NÖ) genutzt (siehe 7 Öffentlichkeitsarbeit/Vernetzung).

7 Öffentlichkeitsarbeit/ Vernetzung

Beschreibung der im Rahmen Ihres netidee-Projektes bereits erfolgten bzw. noch geplanten Öffentlichkeitsarbeit oder Vernetzung

Es bestehen Kooperationen, in welchen das Phishingtraining zum Einsatz kommen wird. Einerseits soll die Plattform gemeinsam mit Saferinternet.at genutzt werden, zum anderen öffnen wir im März 2022 die Plattform in Kooperation mit der Arbeiterkammer Niederösterreich als Trainingsangebot für ArbeitnehmerInnen für eine weitere Zielgruppe, um auch im Erwachsenenbereich das Bewusstsein für und die Resilienz vor Phishing zu stärken.

8 Eigene Projektwebsite

Es wurde eine Projektwebseite über Github Pages unter https://sschritt.github.io/phishingtraining angelegt. Die Plattform selbst wird nicht-öffentlich auf Systemen der Universität Wien bzw. der Kooperationspartner gehostet. Über die AKNÖ wird ab März 2022 eine öffentlich verfügbare Version des Phishingtrainings verfügbar sein.

9 Geplante Aktivitäten nach netidee-Projektende

Wie unter Punkt 6 angegeben ist es geplant, regelmäßige Trainings an Schulen durchzuführen und die Plattform über Kooperationspartnern auch anderen Zielgruppen zur Verfügung zu stellen.

10 Anregungen für Weiterentwicklungen durch Dritte

Die modulare Phishingengine unterstützt aktuell E-Mail und SMS-Versand. Eine Automatisierung des Versands von Instagram-Nachrichten wurde evaluiert, aufgrund fehlender APIs und den im Widerspruch dazu stehenden Nutzungsbedingungen von Instagram wurde dies jedoch für die erste Kampagne nicht umgesetzt. Dennoch wäre die vermehrte Einbindung von Social Media im Hinblick auf die Zielgruppe von SchülerInnen erstrebenswert.

Referenzen

Betsch, T., & Haberstroh, S. (2005). *The Routines of Decision Making.* Psychology Press.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *The Journal of the Human Factors and Ergonomics Society*, S. 1158-1172.

Glüer, M. (2018). Digitaler Medienkonsum. In A. L. (eds), *Entwicklungspsychologie des Jugendalters* (S. 197-222). Berlin, Heidelberg: Springer.

Hoffmann, J. (2017). Erwerb willkürlichen, zielgerichteten Verhaltens beim Menschen. In Springer-Lehrbuch, *Lern- und Gedächtnispsychologie.* Berlin, Heidelberg: Springer.

Hoss, D. (2015). Social Engineering – unterschätzte Bedrohung für die Informationssicherheit. *Wirtschaftsinformatik & Management*, S. 54-60.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric computing and information sciences*, S. 1-41.

Kahnemann, D. (2011). *Schnelles Denken, langsames Denken.* Penguin Verlag.

Klein, G. A. (1993). *Decision making in action: Models and methods.* Ablex Publishing.

Lindberg, S., & Hasselhorn, M. (2018). Kognitive Entwicklung. In L. A. (eds), *Entwicklungspsychologie des Jugendalters* (S. 51-73). Berlin, Heidelberg: Springer.

Riedl, D., Stöckl, A., Nussbaumer, C., Rumpold, G., Sevecke, K., & Fuchs, M. (2016). Nutzungsmuster von Internet und Computerspielen. *Neuropsychiatrie*, S. 181-190.

Stafford, C. D. (2020). *Weakest Link: Assessing factors that influence susceptibility to falling victim to phishing attacks and methods to mitigate.* Utica College Masterarbeit.

Statistik Austria. (2019). *Ausgewählte Sicherheitsprobleme, die bei der privaten Internetnutzung in den letzten zwölf Monaten.*

Turner, A. (2015). Generation Z: Technology and Social Interest. *The Journal of Individual Psychology*.

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering. *Datenschutz und Datensicherheit*, S. 601-604.