universität wien

Psychologisches Konzept

netidee Phishingtraining

Dr. Esther Seidl | Alexandra Kaiser, MSc.

Einleitung

Das Internet ist in der heutigen Zeit nicht mehr aus unserem Alltag wegzudenken. Vor allem für die heutigen Kinder und Jugendlichen, die sogenannte Generation Z (Jahrgänge von 1993 bis 2005), 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. Die Benutzung eines Smartphones ist selbstverständlich und der Alltag der Jugendlichen damit digitalisiert worden (Glüer, 2018).

Im Jahr 2020 haben bereits 99,6% der europäischen 16- bis 24-jährigen zumindest in den letzten drei Monaten das Internet genutzt (Statistik Austria, 2020). In einer Studie, die Tiroler Jugendliche im Alter zwischen 11 und 18 Jahren zu ihrer Internetnutzung befragte, geben die Proband*innen an, das Internet am häufigsten für das Ansehen von Videos zu nutzen und, um in sozialen Netzwerken präsent zu sein (Riedl, Stöckl, Nussbaumer, Runpold, Sevecke & Fuchs, 2016). Die beliebtesten sozialen Netzwerke der österreichischen Jugendlichen sind 2020 WhatsApp und Youtube, dicht gefolgt von Instagram, Snapchat und Facebook (Saferinternet, 2020).

In Übereinstimmung mit anderen Studien konnten die Forscher*innen 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.

Das Internet eröffnet auch neue Möglichkeiten für Betrüger und Hacker. So zeigt sich, dass eines der häufigsten Sicherheitsprobleme in der Altersgruppe von 16- bis 24-jährigen der Erhalt von betrügerischen E-Mails, auch Phishing Mails genannt ist (28,25%; Statistik Austria, 2019).

Phishing

Phishing wird dazu genutzt unbefugt Daten oder Informationen zu erwerben oder Individuen dazu zu bewegen gegen Vorschriften zu verstoßen (Hoss, 2015). Ziel von Phishing ist es an sensible Informationen via E-Mails bzw. Nachrichten auf sozialen Netzwerken zu kommen, die der Adressat durch das Klicken auf einen Link bzw. das Öffnen einer schädlichen Datei an den Absender (unfreiwillig) freigibt (Stirnimann, 2018). Eine besondere Form von Phishing wird als Spear-Phishing bezeichnet. Hier wird die E-Mail personalisiert und Detailinformationen des Adressaten sind enthalten.
Studien zeigten, dass das Umfeld in dem Personen Phishingnachrichten erhalten ausschlaggebend für die Entscheidung sein kann, wie auf die Mail reagiert wird (Gassmann, Benenson, & Landwirth, 2019). Wenn eine Phishing-Mail über Facebook gesendet wird, ein Netzwerk in dem mit Freunden und Bekannten kommuniziert wird, liegt die Wahrscheinlichkeit doppelt so hoch, dass auf die Phishing-Mail reagiert wird, sofern sie der normalen Kommunikationsart entspricht (vgl. (Gassmann, Benenson, & Landwirth, 2019). Anhand dieses Beispiels kann sehr gut erkannt werden, wie leicht ausführbar und daher, wie gefährlich, Spear-Phishing sein kann.

Generell wird Phishing als eine Untergruppe des Begriffs Social Engineering gesehen (Hoss, 2015). Unter Social Engineering werden Techniken verstanden, die zur Beeinflussung von Menschen verwendet werden. Die Ziele von Social Engineering und Phishing sind ident, sodass mittels dieser Techniken versucht wird, an wertvolle Daten oder Informationen zu gelangen, oder Individuen dazu zu bringen gegen Regeln zu verstoßen. Dabei kann es vorkommen, dass die sogenannten Social Engineers eine bestimmte Identität oder den Gesamtkontext vortäuschen, um an ihr Ziel zu kommen. Ein Beispiel im Kontext des Phishings wäre, wenn der Social Engineer die Identität des Firmen CEOs annimmt und in seiner Phishingnachricht Mitarbeiter*innen dazu auffordert auf einen Link zu klicken, um sich für einen Mitarbeiter*innen Tag anzumelden. Andere Methoden, mit denen es gelingt, das Ziel der Beeinflussung zu erreichen, wären beispielsweise das Erzeugen eines Zeit- oder Autoritätsdruck, oder auch Sympathie.

Zielgruppe

Viele Studien berichten davon, dass gerade die Gruppe der 18- bis 25-jährigen die Zielgruppe für Phishing-Attacken ist (vgl. (Jampen, Gür, Sutter, & Tellenbach, 2020), weshalb das vorliegende Konzept auf 14- bis 18-jährige ausgelegt ist. Somit kann eine Intervention gesetzt werden, bevor die Jugendlichen zur Zielscheibe der Phishing-Attacken werden.

Die neuro-psychologische Entwicklung dieser Altersgruppe bietet außerdem Vorteile die Resilienz gegenüber Phishingnachrichten zu steigern. In dieser Zeit kann die Kapazität des Arbeitsgedächtnisses und damit einhergehend auch das Faktenwissen der Jugendlichen leicht erweitert werden (Lindberg & Hasselhorn, 2018). Mit anderen Worten fällt es Jugendlichen in diesem Alterszeitraum leichter neue Informationen aufzunehmen

und diese mit Übungen umzusetzen, sodass sich daraus eine Verhaltensweise bzw. in weiterer Folge eine Gewohnheit, entwickeln kann.

Awarenesstrainings als Lösung für das Phishingproblem?

Um Individuen für das Thema Phishing und in dem Zusammenhang Social Engineering zu sensibilisieren, werden häufig Awarenesstrainings durchgeführt (vgl. Jampen, Gür, Sutter, & Tellenbach, 2020). Bei den klassischen Awareness-Maßnahmen ist das Ziel die Individuen gegen äußere Beeinflussungen zu immunisieren (Weßelmann, 2008). Die Individuen lernen durch ein Training, *rule-based training*, Regeln, wie sie beispielsweise Hinweise in Phishingnachrichten entdecken und schließlich die Nachricht als Phishing Mail ausmachen können (Stafford, 2020). Durch wiederholende Übungen, beispielsweise E-Mails, die sie an die Regeln erinnern, soll das gezeigte Verhalten automatisiert und damit das Risiko, ein Phishing Opfer zu werden, reduziert werden.

Laut Weßelmann (2008) kann diese Immunisierung allerdings nicht funktionieren, da Social Engineering sich auch in der Erziehung, bei Verhandlungstechniken, aber auch in der alltäglichen Kommunikation wiederfindet. Social Engineering wird auch benutzt, um Menschen in ihren Berufen zu beraten bzw. Mitarbeiter*innen zu motivieren. Würden nun die Menschen gegen alle äußeren Beeinflussungen immunisiert werden, wären soziale Interaktionen, effektives Zusammenarbeiten, aber auch die persönliche Weiterentwicklung nicht möglich.

Ein weiterer Grund, warum Weßelmann (2008) denkt, dass Awarenesstrainings alleine nicht funktionieren können ist, dass der Mensch als Variable nicht mit einkalkuliert wird. Würde jedes Individuum beim Erhalt einer Phishing-Mail überlegt handeln, also die E-Mail genau betrachten, die Absenderadresse überprüfen, etc., würden wesentlich weniger Menschen Opfer einer Social-Engineering Attacke werden. Das Problem dabei ist, dass oft Informationen fehlen oder Zeitmangel herrscht, weshalb sich auf das Bauchgefühl, in der Fachsprache Heuristik genannt, verlassen wird.

Heuristiken, System 1 und System 2

Heurisiken sind jenes Wissen, auf das man beinahe automatisch zurückgreift (Kahnemann, 2011). Es wurde gelernt, wenn das Ziel X erreicht werden soll, muss das Verhalten Y gezeigt werden, um zum gewünschten Ergebnis zu kommen (Hoffmann, 2017).

Bei Phishingnachrichten werden 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 zu Heuristiken zwei Systeme ausgemacht, die Aufschluss über das Denkverhalten geben sollen. System 1 funktioniert automatisch

und agiert schnell. In diesem System verankert sind Heuristiken, da es keiner großen Mühe Bedarf ein Verhalten zu zeigen, dass 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 Entscheidung, ob ein Individuum eine Nachricht als Phishingnachricht einstuft, ist System 2 gefragt, da Konzentration und Anstrengungsbereitschaft erforderlich sind, um herauszufinden, ob es sich tatsächlich um eine Phishingnachricht handelt. Durch spezifische Faktoren übernimmt diese Aufgabe aber oft System 1 und führt damit zu Fehlentscheidungen (Klicken auf den Link).

Daher stellt sich die Frage, wie beim Erhalt einer Phishing-Mail System 2 aktiviert werden kann.

Das Trainings-Konzept

Um System 2 im Kontext von Phishingnachrichten zu aktivieren, wurde das vorliegende Konzept gestaltet, welches in vier Phasen unterteilt ist, die nachfolgend genauer beschrieben werden.

Alle vier Phasen durchläuft die gleiche Stichprobe, Jugendlichen im Alter von 14 bis 18 Jahren, die alle Oberstufenklassen in Niederösterreich besuchen.

Eine Übersicht über die Phasen des Trainings-Konzepts ist in Abbildung 1 dargestellt.

Abbildung 1. Grafische Darstellung des Ablaufs eines Phishingtrainings

Aufklärungsphase

In den einzelnen Schulklassen sollen zunächst klassische Awareness-Maßnahmen besprochen werden. Im Rahmen eines interaktiven (Online-)Vortrags während einer Schulstunde erhalten die Schüler*innen Informationen, wie Phishingnachrichten aussehen, werden, werden über mögliche Konsequenzen beim Klicken eines Phishing-Links aufgeklärt und Lösungsansätze werden erarbeitet. Anschließend soll anhand von realistischen Beispielen von Phishingnachrichten der Lösungsansatz gemeinsam mit den Schüler*innen erprobt werden.

Der Lösungsansatz orientiert sich an Kleins Recognition-Primed Decision Model (RPDM; 1993; Klein, 1993)

Zunächst sollen die Jugendlichen die Situation „Erhalt einer Phishing-Mail“ wiedererkennen, in dem sie auf folgende vier Punkte achten:

1. Das Erkennen der kritischen Hinweise (z.B. Aufforderungen zum Folgen eines Links und zur Eingabe wichtiger/vertraulicher Daten, Öffnen von Anhängen, namenlose Anrede, schlechte Rechtschreibung und Grammatik, Nachrichten in Fremdsprachen, Vorwand von (sicherheits-) technischen Gründen, hohe Dringlichkeit, Drohungen, Nachrichten von unbekannten Firmen)
2. Das Formen der Erwartung (“Durch die kritischen Hinweise, die ich schon einmal gesehen habe, ist es sehr wahrscheinlich, dass wieder das gleiche Ergebnis eintritt.”)
3. Das Stecken von plausiblen Zielen (“Ich will nicht gephisht werden.”)
4. Das Setzen einer geeigneten Handlung (“Um das bekannte Ergebnis zu erzielen, muss ich x machen.”)

Darauffolgend sollen die Jugendlichen die Handlungsoption (nicht auf den Link klicken, E-Mail löschen) evaluieren und anschließend mental simulieren. Sie überlegen also, was passieren könnte, wenn sie die Mail löschen bzw. nicht auf den Link klicken. Schlussendlich kommt es zu der Ausführung der Option.

Zusätzlich bekommen die Jugendlichen ein Handout ausgeteilt auf dem die kritischen Hinweise, wie Phishingnachrichten erkannt werden können, und der Lösungsansatz zusammengefasst werden.

Nach dem Awarenesstraining werden die Interessent*innen gebeten den Forscher*innen eine E-Mail zukommen zu lassen, in der sich die bereits unterschriebene Einverständniserklärung befinden soll. Damit kann sicher gegangen werden, dass die Schüler*innen freiwillig an der Studie teilnehmen.

Anschließend bekommen die Jugendlichen per E-Mail einen Link zur Registrierung für die Phishing Projekt Webseite zugeschickt. Anhand eines beigefügten Dokuments wird den Teilnehmer*innen erklärt, wie sie sich für die einzelnen Phasen anmelden und welche Informationen sie preisgeben können.

Trainingsphase

Das aus dem Awarenesstraining Gelernte sollen die Jugendlichen anschließend in einer Trainingsphase umsetzen und vertiefen (vgl. Jensen, Dinger, Wright, & Thatcher, 2017). Je öfter sie das Gelernte anwenden, desto schneller wird es zu einer Gewohnheit, zu einer automatischen Handlungsweise, die wiederum in System 1 verankert ist (vgl. Betsch & Haberstroh, 2005). Ziel ist es also, dass die Inhalte und Reaktionen, die zunächst im System 2 aktiviert werden in weiterer Folge automatisiert werden, um dann Teil von System 1 zu werden.

Dazu erhalten die Jugendlichen innerhalb eines Monats 8 Phishingnachrichten, die in ihren Schwierigkeitsgraden (leicht, mittel, schwer, sehr schwer) variieren werden. Der Schwierigkeitsgrad ist davon abhängig, wie viele kritische Hinweise in der Phishingnachricht verwendet werden. Außerdem werden die Phishingnachrichten von verschiedenen Kanälen (6x E-Mail; 1x Social Media: Instagram; 1 SMS), verschiedenen Absendern (bekannt, unbekannt) und in verschiedenen Formaten (6x belohnend, 2x bestrafend) versandt werden. Zudem variiert der Zeitpunkt, wann die Schüler*innen die Phishingnachrichten erhalten. Insgesamt stehen 11 Phishingnachrichten (9x E-Mail; 1x Social Media: Instagram; 1 SMS) zur Verfügung, wobei hier 8 Phishingnachrichten in randomisierter Reihenfolge und zu zufälligen Zeitpunkten in einem vorgegebenen Zeitraum an die Jugendlichen verschickt werden. Dies soll gewährleisten, dass nicht alle Teilnehmer*innen genau dieselben Nachrichten zur gleichen Zeit erhalten, falls die Jugendlichen untereinander die Nachrichten vergleichen.

Sollten die Schüler*innen auf den verschickten Link in der Phishingnachricht klicken, werden sie auf eine Webseite weitergeleitet. Dort erhalten sie direkt Feedback darüber, dass sie gephisht wurden und bekommen eine Kurzfassung der Lerninhalte aus dem Awarenesstraining präsentiert (z.B. auf welche kritischen Hinweise sie in der Nachricht hätten achten sollen, welche möglichen Konsequenzen nun drohen würden, etc.). Diese Art von Feedback im Zusammenhang mit Phishingnachrichten wird *embedded training* genannt und in vielen Studien als effektives Tool zur Sensibilisierung verwendet (vgl. Canfield, Fischhoff, & Davis, 2016; Jampen, Gür, Sutter, & Tellenbach, 2020). Zusätzlich wird mit wenigen Fragen erhoben, 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 Schluss des Monats bekommen alle Teilnehmer*innen ein individuelles Feedback, wie oft sie auf einen Phishing Link geklickt haben. Dies soll einerseits gewährleisten, dass jeder, auch Schüler*innen die eventuell nie auf einen Link geklickt haben, Feedback bekommen, und andererseits die Jugendlichen dazu motivieren noch genauer auf mögliche Phishingnachrichten zu achten.

Testphase

Nach dem Abschluss der Trainingsphase findet 3 Monate lang eine Testphase statt, bei der die Jugendlichen nur mehr gelegentlich, insgesamt bis zu 5-mal, eine Phishingnachricht bekommen (3x Mail, 1x Social Media, 1 SMS). Auch diese werden in ihrer Schwierigkeit, in den Kanälen, Absendern und Formaten über die Jugendlichen hinweg variieren. Auch die Umgebungsfaktoren werden in dieser Phase weiterhin erhoben.

Abschlussphase

Nach einer Pause von einem Monat nach Abschluss der Testphase, wird in der letzten Phase an die Schüler*innen nur mehr eine Nachricht verschickt (1x Mail). Dies soll dazu dienen, einen längerfristigen Lerneffekt festzustellen.

Abschließen wird noch einmal individuelles Feedback gegeben.

Studie

Beschreibung der Stichprobe

Das Phishing Training konnte an zwei niederösterreichischen Schulen durchgeführt werden, wobei bei der ersten Schule Schüler*innen des Wahlfachs Informatik und bei der zweiten Schule Schüler*innen des Informatikzweigs teilnahmen. Die teilnehmenden Jugendlichen waren 17-18 Jahre alt. COVID-bedingt musste das Awarenesstraining online im Rahmen einer Schulstunde stattfinden.

An der ersten Schule konnten 2 Schüler*innen für die Trainingsphase und 1 Schüler*in für die Testphase gewonnen werden. An der Trainings- und Testphase in der zweiten Schule nahmen 11 Schüler*innen teil.

Die Proband*innen bekamen nach der Trainingsphase ein individuelles Feedback und nach der Abschlussphase einen Überblick über die Ergebnisse aller Teilnehmenden während Trainings-, Test- und Abschlussphase per E-Mail.

Beschreibung der Phishingnachrichten

In der Trainingsphase wurden acht von elf Phishingnachrichten randomisiert an die Teilnehmer*innen versandt, wobei sicher gegangen wurde, dass die Instagram Nachricht und die SMS (sofern die Proband*innen diese Daten angegeben haben) definitiv verschickt wurden.

Es gibt vier Schwierigkeitsgrade (leicht, mittel, schwer, sehr schwer), die davon abhängig sind, wie viele kritische Hinweise in der Phishingnachricht enthalten sind.
Die inhaltlichen Bereiche der Phishingnachrichten sind Gewinnspiele, Information, Account-Verifizierung und Einteilung für ein Referatsthema in der Schule

In der folgenden Tabelle sind Beispiele für den Inhalt der verwendeten Phishingnachrichten pro Schwierigkeitsgrad detailliert dargestellt. Eine beispielhafte Darstellung eines Phishingtemplates ist in Abbildung 2 zu sehen.

Channel	Absender	Betreff	Bekannt/ Unbekannt	Belohnend/ Bestrafend	Schwierigkeit
E-Mail	Online-Versandhändler	Jetzt Gutschein sichern! 25€ Rabatt bei nächster Bestellung	bekannt	Belohnend (25 Euro Gutschein)	sehr schwer
E-Mail	yogaforyou	Schluss mit Verspannung! Gratis Yoga Übungen	unbekannt	Belohnend (gratis Übungen)	schwer
E-Mail	{ClassTeacher}	Referatsthema	bekannt	Bestrafend (Schlechte Note)	mittel
E-Mail	Fitnessstudio	Mitgliedsbeitrag	bekannt	Bestrafend (Mitgliedsbeitrag)	leicht

Tabelle 1: Beispiele von verwendeten Phishingnachrichten in der Trainingsphase

Bei {ClassTeacher} konnte der Name des Klassenlehrers individuell für die Schule durch das System eingefügt werden.

In der Testphase wurden fünf Phishingnachrichten an die Jugendlichen verschickt. Es wurde das Schwierigkeitsniveau an die Schüler*innen angepasst, da wenige Phishingnachrichten in der Trainingsphase geöffnet bzw. der Link angeklickt wurde, sodass es nur drei Schwierigkeitsgrade (mittel, schwer, sehr schwer) gab.

Die inhaltlichen Themen der Phishingnachrichten waren Informationen und Angebote.

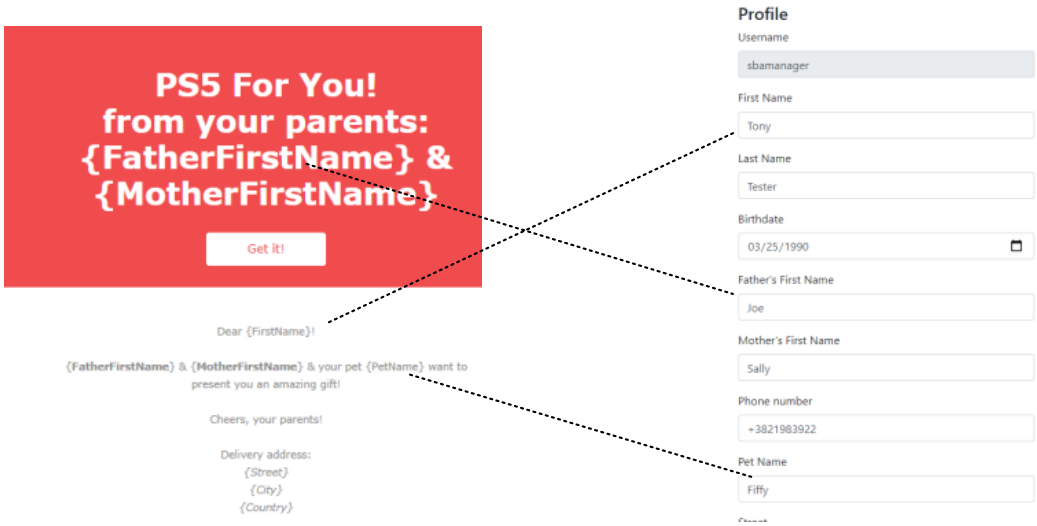

Abbildung 2. Beispiel für das Template “PS5”

In der folgenden Tabelle sind Beispiele für die verwendeten Phishingnachrichten pro Schwierigkeitsgrad detailliert dargestellt.

Channel	Absender	Betreff	Bekannt/ Unbekannt	Belohnend/ Bestrafend	Schwierigkeit
E-Mail	{InformaticsTeacher}	Wichtiges Update	bekannt	belohnend	sehr schwer
SMS	CoV-Testservice	SARS-CoV-2 Testergebnis	bekannt	belohnend	schwer
E-Mail	Online-Reiseagentur	Angebote für Urlaube	bekannt	belohnend	mittel

Tabelle 2: Beispiele von verwendeten Phishingnachrichten in der Testphase

Bei {InformaticsTeacher} konnte der Name des Klassenlehrers individuell für die Schule durch das System eingefügt werden.

Ergebnisse der Studie

Trainingsphase

In der Trainingsphase wurden 13 Proband*innen in einem Zeitraum von einem Monat 104 Phishingnachrichten geschickt. Davon wurden 55,77% geöffnet und 4,81% haben den darin enthaltenen Link angeklickt. Anhand der geöffneten Phishingnachrichten misst das 8,62%

Es gab vier verschiedene Schwierigkeitsgrade (leicht, mittel, schwer, sehr schwer), wobei die Phishingnachrichten mit Schwierigkeitsgrad 3 (schwer), am häufigsten geöffnet wurden (50%, siehe Grafik 1) und der Link in den Phishingnachrichten mit Schwierigkeitsgrad 4 (sehr schwer) am öftesten angeklickt wurde.

Insgesamt haben alle Teilnehmer*innen zumindest zwei Mal eine Phishingnachricht geöffnet (siehe Grafik 2), wobei nur vier Schüler*innen auf den Link in der Nachricht geklickt haben.

Testphase

In der Testphase wurden 57 Phishingnachrichten in einem Zeitraum von drei Monaten an 12 Jugendliche geschickt. Davon wurden 50,88% geöffnet und vier Mal (=7,02%) ein Link angeklickt.

Da bereits in der Trainingsphase wenige Proband*innen die Phishingnachrichten geöffnet bzw. auf den Link geklickt haben, wurde das Schwierigkeitsniveau an die Phishing Kompetenz der Schüler*innen angepasst, sodass es nur 3 Schwierigkeitsgrade (mittel, schwer, sehr schwer) gab. In Grafik 3 ist zu erkennen, dass die meisten Jugendlichen Phishingnachrichten mit dem Schwierigkeitsgrad 4 geöffnet haben (58%).

Abschlussphase

In der Abschlussphase wurde den 12 Proband*innen nach einem Monat Pause eine letzte Phishingnachricht geschickt, die dem Schwierigkeitsgrad 2 zugeordnet werden kann. Sieben von zwölf der Teilnehmer*innen haben die Nachricht geöffnet. Eine Person hat den Link angeklickt.

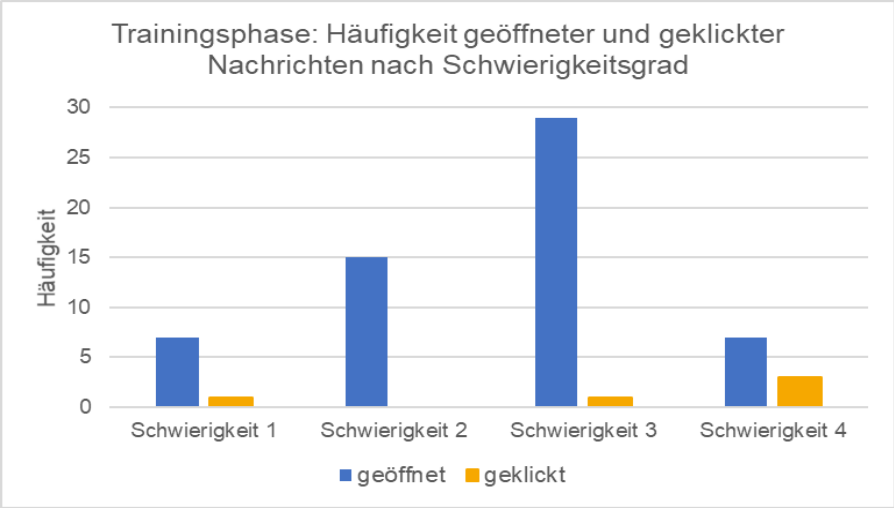

Abbildung 3: Darstellung der geöffneten und angeklickten Phishingnachrichten anhand von Schwierigkeitsgraden in der Trainingsphase

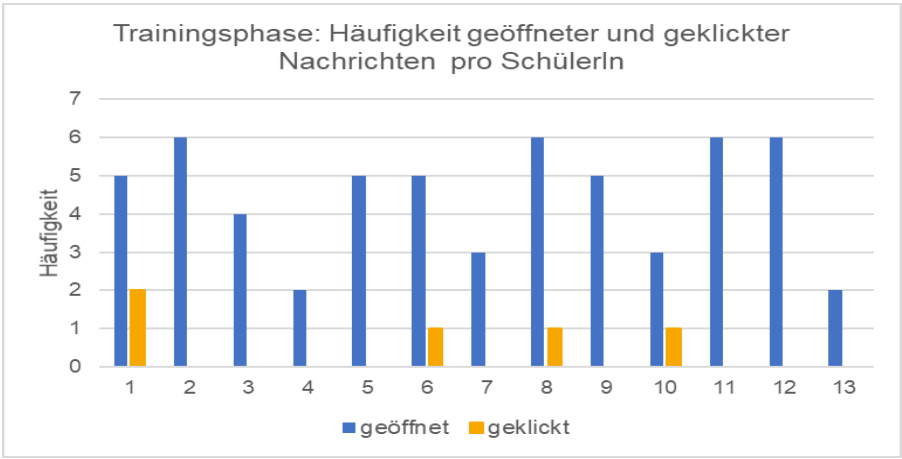

Abbildung 4: Darstellung der geöffneten und geklickten Phishingnachrichten pro SchülerInnen in der Trainingsphase

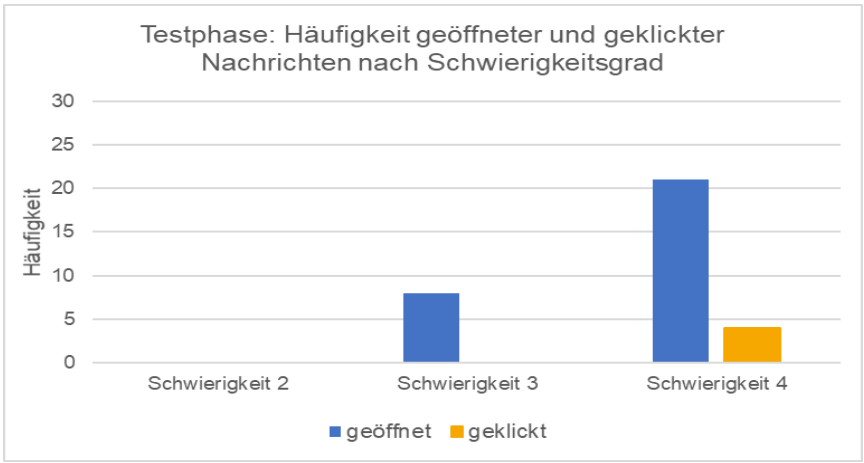

Abbildung 5: Darstellung der geöffneten und angeklickten Phishingnachrichten anhand von Schwierigkeitsgraden in der Testphase

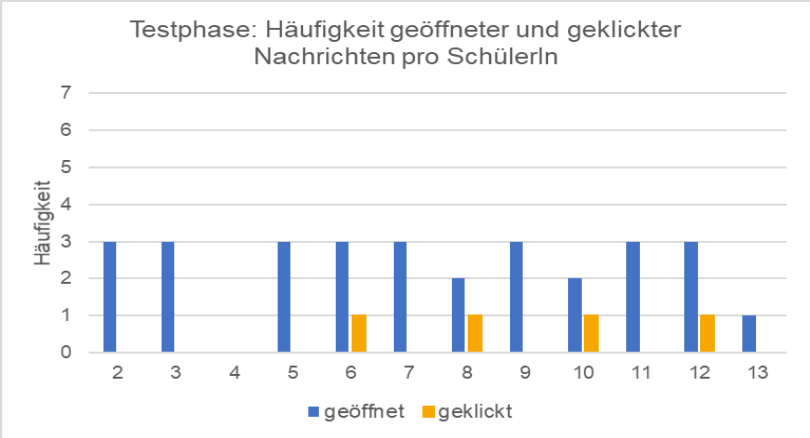

Abbildung 6: Darstellung der geöffneten und geklickten Phishingnachrichten pro SchülerInnen in der Testphase

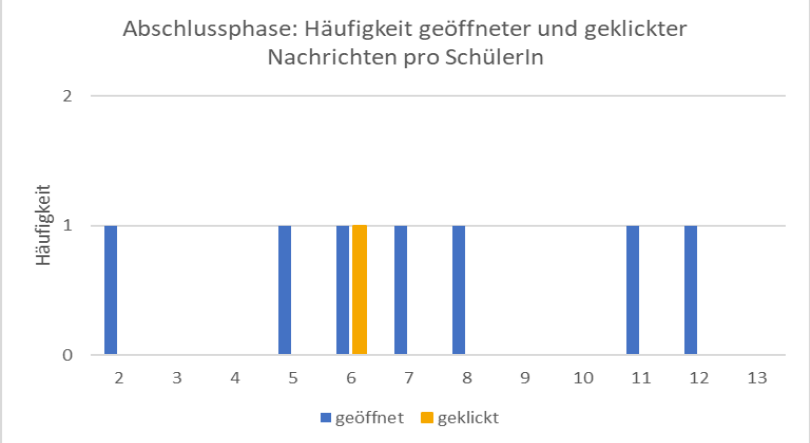

Abbildung 7: Darstellung der geöffneten und geklickten Phishingnachrichten pro SchülerInnen in der Abschlussphase

Bei Betrachtung nach Nachrichtentyp zeigt sich ein deutlicher Unterschied zwischen SMS und E-Mail Nachrichten: bei SMS wurden 4 von 22 (18,18%) Links angeklickt im Vergleich zu 6 von 116 (=5,17%) bei E-Mailnachrichten. Dies kann ein Hinweis darauf sein, dass das Bewusstsein für Phishing-Nachrichten im SMS-Kontext deutlich geringer ist als bei E-Mail Nachrichten. Bei Social Media Nachrichten wurde niemals ein Link angeklickt, was damit zusammenhängen kann, dass die SchülerInnen Nachrichten dann als potenzielle Gefahr erkennen, wenn sie, wie im Studiensetting, von fremden Accounts versendet werden.

Da insgesamt (von allen Jugendlichen in allen Studienphasen) nur drei Angaben zu den Umgebungsfaktoren vorliegen wurden diese nicht ausgewertet.

Feedback der SchülerInnen zur Studie

Nach der Durchführung wurden die SchülerInnen um Feedback zur Studie gebeten. Dabei haben die SchülerInnen angegeben, dass sie das Projekt als wenig aufwändig einschätzen. Sie empfanden sich nach der Aufklärung über das Projekt informiert, lediglich die Erklärungen zum Anmeldeprozess könnten noch verbessert werden - hier gaben die SchülerInnen an, dies als “eher verständlich” bis “wenig verständlich” empfunden zu haben. Dies könnte möglicherweise auf das Online-Setting zurückgeführt werden, da hier die Möglichkeiten, es den SchülerInnen direkt zu demonstrieren eingeschränkter waren, als es bei einem Präsenztermin möglich gewesen wäre. Das Awareness-Training wurde als informativ eingestuft und es konnten neue Inhalte von den SchülerInnen daraus 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.

Diskussion

Das hier beschriebene Projekt kann als ein Pilotprojekt betrachtet werden, da für aussagekräftige Ergebnisse mehr Proband*innen notwendig sind. Die geringe Probandenanzahl ist auf die Corona-Pandemie und die unklare Situation in den Schulen zurückzuführen. Mit dauernd wechselnden Anforderungen, die an die Schulen in dieser Krisenzeit gestellt werden (Home-Schooling, Präsenz, Hybrid, Wechsel innerhalb von einer Woche ohne Vorlaufzeit, etc.) waren nur wenige Schulen zu einer Kooperation bzw. Teilnahme an der Studie bereit.

Zur Stichprobe muss ergänzt werden, dass alle Teilnehmer*innen ein vertieftes Wissen im Schulfach Informatik aufweisen, was bedeuten könnte, dass sie bereits mehr theoretische und praktische Kenntnisse zum Thema Phishing besitzen und dadurch Phishingnachrichten eher als diese erkennen können. Allerdings hat selbst diese informierte Stichprobe i ca. 50% der Fälle die Nachrichten geöffnet und in der Trainingsphase auch 5% der Links geklickt.

Je nachdem wie bereitwillig die Schüler*innen mit der Eingabe ihrer Daten waren (E-Mailadresse, Wohnadresse, Handynummer, Instagram-Account, etc.), desto mehr Phishingnachrichten konnten auf unterschiedlichen Kanälen an die Jugendlichen versandt werden. Wenn Schüler*innen beispielsweise ihre Handynummer nicht bekannt gegeben haben, so bekamen sie sowohl in der Trainings- als auch in der Testphase eine Phishingnachricht (die per SMS) weniger als die anderen Teilnehmer*innen.

COVID bedingt fanden die theoretische Einführung des Phishingtrainings (Awarenesstraining) sowie die Rückmeldung online statt, sodass nur begrenzt auf die

Schüler*innen eingegangen werden konnte, was möglicherweise auch die geringe Anzahl an Teilnehmer*innen erklärt.

Auch wenn die Aussagekraft aufgrund der geringen Teilnehmeranzahl begrenzt ist, kann insgesamt ein geringer Lernerfolg nach der Trainingsphase vermutet werden. Eindeutig zu sehen ist, dass die SchülerInnen in der Testphase im Vergleich zur Trainingsphase keine Nachrichten des Schwierigkeitsgrades 2 mehr öffnen. Da sich insgesamt nur eine minimale Verbesserung zwischen Trainings und Testphase zeigt, kann aber davon ausgegangen werden, dass wie bereits in vorausgehender Literatur angegeben, reine Awareness Trainings nicht ausreichend sind, um Personen darin zu schulen, welche Nachrichten bedrohlich sein könnten, sondern dass es ein kontinuierliches Training dafür brauchen könnte, wie es durch die Trainingsphase in unserem Konzept umgesetzt wird. Möglicherweise wäre das Training daher noch erfolgreicher, wenn diese Phase länger andauern würde. Zudem hat sich gezeigt, dass die SchülerInnen im Verhältnis bei SMS-Nachrichten deutlich häufiger auf Links klicken als bei E-Mail-Nachrichten, was für ein geringeres Bewusstsein für Phishing im SMS-Kontext sprechen kann. 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 planen (abhängig von der Corona-Situation) dieses Schuljahr noch weitere Trainings umzusetzen.

Literaturverzeichnis

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.

Gassmann, F., Benenson, Z., & Landwirth, R. (2019). Kommunikation als Gefahr. *Österreichische Zeitschrift für Soziologie*, S. 135-155.

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.

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*, S. 597-626.

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.

Saferinternet. (2020). *Jugend-Internet-Monitor.* Verfügbar unter: https://www.saferinternet.at/services/jugend-internet-monitor/.

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.*

Statistik Austria. (2020). *Internetnutzerinnen oder Internetnutzer 2002 bis 2020.*

Stirnimann, S. (2018). Social Engineering als Modus Operandi. In *Der Mensch als Risikofaktor in der Wirtschaftskriminalität* (S. 127-157). Gabler, Wiesbaden: Springer.

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.

Abbildungsverzeichnis

Tabellenverzeichnis