Praktische Bachelorarbeit 2025
Digital Ideation Hochschule Luzern

Lass dich nicht angeln!

Nutzerzentrierter Ansatz für Cybersicherheit

Valérie Schneider
valerieschneider@proton.me

Vivien von Burg
vivien.vonburg@outlook.ch

Danksagung
Unsere Mentor:innen:
Angie Born, Stefan Fraefel, Susanne Hofer

Fachpersonen:
Céline Neubig, Cornelia Puhze, Dr. Katja Dörlemann (SWITCH)
Christoph von Burg, Thomas Halmer, Timotheus Bruderer (Swiss Life)
Prof. Oliver Hirschi (eBanking – aber sicher!)
Prof. Dr. Kristin Weber (Autorin: Mensch und Informationssicherheit)

Helfer:innen:
Fischer Lui (Hotel-Restaurant Eierhals Royal)
Louie Wolf (Unterwasser Synchronsprecher)
Valentin Küng (Holzwerkstatt Verantwortlicher HSLU DFK)
Alle Studierende, die an Interviews und Testings teilgenommen haben

Auch ein Dank gilt unsere Freunde und Familie für die kontinuierliche Unterstützung!

00 Erklärung zum Dokument

Da unsere Arbeit den Fokus auf UX-Research legt, haben wir einen UX-Report verfasst, der unsere Vorgehensweise, Erkenntnisse und deren Einfluss auf die Umsetzung detailliert dokumentiert.

Um den Leser:innen einen schnellen Überblick zu ermöglichen, beginnt jedes Kapitel mit einer kurzen Zusammenfassung, die die zentralen Inhalte und Ergebnisse auf den Punkt bringt.

Für ein grundlegendes Verständnis der Arbeit reicht es, die Zusammenfassungen zu lesen. Wer sich jedoch vertieft mit den einzelnen Aspekten auseinandersetzen möchte, findet in den vollständigen Kapiteln weiterführende Erklärungen, Abbildungen und Tabellen.

Index

01 Einleitung

Zusammenfassung

Diese Bachelorarbeit befasst sich mit der Frage, wie Studierende wirksam für die Gefahr von Phishing sensibilisiert werden können. Im Fokus steht dabei ein nutzerzentrierter Ansatz, der den Menschen und seine Verhaltensweisen ins Zentrum stellt. Die zunehmende Komplexität von Phishing-Angriffen macht deutlich, dass rein technische Schutzmassnahmen nicht ausreichen. Es braucht ein tieferes Verständnis der psychologischen Mechanismen und ein gestärktes Bewusstsein bei den Nutzenden. Unsere Arbeit orientiert sich an der ISO-Norm 9241-210 für Human-Centered Design, wobei dieser UX-Report den gesamten Research- und Konzeptionsprozess dokumentiert. Ziel ist es, zu zeigen, wie fundierte Nutzerforschung zu wirksamen, gestalterischen Lösungen in der digitalen Sicherheit beitragen kann.

Da sich unser Projekt iterativ entlang des Human-Centered-Design-Prozesses entwickelte, war das Endprodukt zu Beginn noch offen. Unser Schwerpunkt lag auf User Research, weshalb wir zentrale Arbeitsschritte bewusst gemeinsam ausführten, um Erkenntnisse kontinuierlich abzustimmen und Entscheidungen kollaborativ zu treffen. Nur kleinere Aufgaben wurden zur Effizienzsteigerung aufgeteilt. Dieses Vorgehen ermöglichte eine enge, reflektierte Zusammenarbeit über alle Projektphasen hinweg.

In dieser praktischen Bachelorarbeit setzen wir uns mit einer der aktuell drängendsten Herausforderungen im Bereich der digitalen Sicherheit auseinander: Phishing. Die Arbeit entstand im Rahmen des Studiengangs Digital Ideation an der Hochschule Luzern. Als Studierende mit Schwerpunkt auf User Experience Design und einem besonderen Interesse an nutzerzentrierter Forschung verfolgen wir das Ziel, Lösungen zu entwickeln, die den Menschen ins Zentrum stellen – besonders dann, wenn es um komplexe und schwer zugängliche Themen wie Informationssicherheit geht.

Phishing zählt zu den zentralen Bedrohungen im Bereich der Informationssicherheit, da es auf den sogenannten Faktor Mensch zielt. Durch den gezielten Einsatz von Social Engineering versuchen Angreifer:innen, das Vertrauen ihrer Opfer zu erschleichen und sie zur Preisgabe sensibler Daten wie Passwörter, Bankinformationen oder persönlicher Angaben zu bewegen. Die Angriffe erfolgen entweder massenhaft, etwa über täuschend echte E-Mails, oder gezielt über sogenannte Spear-Phishing-Attacken. (Bundesamt für Sicherheit in der Informationstechnik, 2022, S. 12, 27; Yasin et al., 2025, S. 1)

Die Auseinandersetzung mit der Frage, wie potenzielle Opfer vor Phishing-Angriffen geschützt werden können, ist ein wachsendes Forschungsfeld (Vishwanath et al., 2011, S. 576). Dabei werden zwei Ansätze verfolgt:

Zum einen der Informatikansatz, der sich auf die Entwicklung effizienterer technischer Lösungen konzentriert. Systeme zur automatischen Erkennung von Phishing-Angriffen sollen so verbesserter werden, dass diese Angriffsversuche entweder gar nicht erst von den Nutzenden gesehen werden oder sie durch Warnmeldungen darauf aufmerksam gemacht werden. (Vishwanath et al., 2011, S. 576)

Der zweite Ansatz, der aus dem Bereich der Sozialwissenschaft stammt, untersucht die psychologischen Abläufe eines Phishing-Angriffes. Dabei steht das Opfer im Fokus, um zu verstehen, warum es auf Phishing-Angriffe reagiert (Vishwanath et al., 2011, S. 577).

Die zunehmende Zahl neu registrierter Phishing-Webseiten sowie die wachsende Komplexität der Angriffsformen (vgl. Anti-Phishing Working Group, 2024; BSI, 2022) verdeutlichen, dass technische Massnahmen allein nicht ausreichen. Es braucht ein stärkeres Bewusstsein auf individueller Ebene, insbesondere bei jungen Menschen, die sich täglich online bewegen, dabei aber oft geringe Gewohnheit, niedrige Salienz und wenig Verhaltensabsicht im Umgang mit digitaler Sicherheit zeigen. Vor diesem Hintergrund beschäftigt sich unsere Arbeit mit folgender Forschungsfrage:

Wie können wir durch Human-Centered Design Studierende, die aktiv im Internet unterwegs sind und geringe Gewohn-

Der vorliegende UX-Report dokumentiert unseren Designprozess, unsere Methoden, die gewonnenen Erkenntnisse sowie die daraus abgeleiteten Konzepte. Ziel ist es, aufzuzeigen, wie fundierte Nutzerforschung nicht nur zum besseren Verständnis einer komplexen Problematik beiträgt, sondern auch als Grundlage für wirksame, kreative Lösungen dient.

heit, Salienz und Verhaltensabsicht besitzen, effektiv für das Thema Phishing sensibilisieren und ihre digitale Selbstbestimmung fördern?

Unsere Herangehensweise orientiert sich an der ISO-Norm 9241-210 für Human-Centered Design. Diese Methodik stellt die Bedürfnisse, Kontexte und Erfahrungen der Nutzer:innen konsequent ins Zentrum des Designprozesses. Dabei legen wir den Fokus insbesondere auf den Research-Prozess – von der Zielgruppendefinition über den Desk und Field Research bis hin zur Ideenfindung und iterativen Konzeptentwicklung. Auch wenn die praktische Umsetzung nicht im Zentrum dieses Dokuments steht, fliessen wichtige gestalterische und konzeptionelle Entscheidungen dennoch mit ein, um den Transfer von Forschung zu Gestaltung nachvollziehbar darzustellen.

01.1 Zusammenarbeit

Da sich unsere Bachelorarbeit am Human-Centered-Design-Prozess gemäss ISO 9241-210 orientiert und dieser einen nutzerzentrierten Ansatz vorsieht, bei dem das Endprodukt iterativ und auf Basis der Pains, Gains und Needs der Zielgruppe entwickelt wird, war zu Beginn des Projekts nicht klar definiert, wie das finale Produkt aussehen würde. Zudem lag unser beider Interessensschwerpunkt im Bereich User Research. Diese Kombination aus methodischem Vorgehen und thematischem Fokus war ausschlaggebend dafür, dass wir auf eine klassische Arbeitsteilung verzichteten. Stattdessen entschieden wir uns bewusst dafür, sämtliche zentralen Schritte im Projekt gemeinsam zu erarbeiten. So konnten wir in jeder Phase gemeinsam reflektieren, Entscheidungen abstimmen und auf neue Erkenntnisse reagieren.

Zur Effizienzsteigerung teilten wir lediglich kleinere Aufgaben auf, wie etwa die Auswertung einzelner Interviewabschnitte, die Gestaltung von Visualisierungen oder das Aufbereiten von Dokumentationen. In allen wesentlichen Arbeitsschritten waren wir jedoch gleichberechtigt involviert.

02 Zielgruppe

Zusammenfassung

Zu Beginn wurde die Zielgruppe auf internetaktive Personen im Alter von 40 bis 65 Jahren festgelegt, basierend auf statistischen Auswertungen zu gemeldeten Phishing-Fällen. Eine vertiefte Analyse sowie Rückmeldungen nach unserer Pitch-Präsentation zeigten jedoch, dass diese Altersgruppe nicht ideal geeignet ist. Studien wie jene von Vishwanath et al. (2011) machen deutlich, dass nicht das Alter oder die Internetaffinität, sondern Faktoren wie kognitive Involviertheit, Routineverhalten und technisches Engagement entscheidend für die Anfälligkeit gegenüber Phishing sind – Eigenschaften, die bei jüngeren Nutzer:innen oft stärker ausgeprägt sind.

Nach detaillierter Analyse theoretischer Einflussfaktoren sowie einer Bewertungsmatrix (siehe Tabelle 3) entschieden wir uns für die Zielgruppe der Studierenden. Sie gelten als besonders beeinflussbar, da sie häufig wenig Erfahrung mit Informationssicherheits-Trainings haben, kurz vor dem Berufseinstieg stehen und in Bezug auf Achtsamkeit, Salienz und Verhaltensabsicht Schwächen zeigen. Ausgeschlossen wurden Studierende mit Vorerfahrung oder besonderem Interesse im Bereich IT und Informationssicherheit, um die Relevanz der Sensibilisierung sicherzustellen.

Die ursprüngliche Zielgruppe des Projekts wurde auf Personen im Alter von 40 bis 65 Jahren festgelegt, die regelmässig im Internet aktiv sind. Die erste Definition wurde durch die Polizeiliche Kriminalstatistik 2023 (BFS 2024) erstellt (siehe Tabelle 1). Die Auswertung der gemeldeten Phishingangriffe zeigt deutlich, dass die meisten Betroffenen Personen im Alter von 40 bis 49 Jahren sind. Es folgen Personen im Alter von 50 bis 59 und 60 bis 69 Jahren. Bei dieser Statistik ist jedoch zu beachten, dass nur die gemeldeten Phishingangriffe berücksichtigt werden. Daher ist von einer hohen Dunkelziffer auszugehen. (BFS 2024)

Tabelle 1: Digitale Kriminalität: Modi Operandi der digitalen Kriminalität und geschädigten Personen (Schweiz im Jahr 2023)

Altersgruppen	10–14	15–17	18–19	20–24	25–29	30–34	35–39	40–49	50–59	60–69	70+
Anzahl Meldungen	4	56	79	195	200	251	259	449	391	308	234

Quelle: BFS - Polizeiliche Kriminalstatistik (PKS)

Die Studie von ProSenectute bestätigt diese Annahme (siehe Tabelle 2). Im Rahmen der Studie wurden Personen ab 55 Jahren zum Thema Finanzmissbrauch befragt. Es wurde festgestellt, dass rund 50 % der 65- bis 74-Jährigen und mehr als die Hälfte der 55- bis 64-Jährigen bereits Opfer von Cyberkriminalität geworden sind. In der Altersgruppe der 65- bis 74-Jährigen waren 7 % und in der Gruppe der 55- bis 65-Jährigen 8,5 % der Betroffenen bereits von Cyberkriminalität betroffen. In der vorliegenden Studie wird Phishing als eine der am häufigsten auftretenden Formen der Cyberkriminalität benannt. Da die Umfrage jedoch ausschliesslich Personen im Alter von 55 Jahren und darüber abdeckt, sind die Ergebnisse nur bedingt generalisierbar (Beaudet-Labrecque et al., 2023).

Tabelle 2: Studie von ProSenectute Schweiz: Finanzmissbrauchsopfer in der Schweizer Bevölkerung 55+ in den letzten fünf Jahren (2023)

Studie von Pro Senectute Schweiz: Finanzmissbrauchsopfer
in der Schweizer Bevölkerung 55+ in den letzten fünf Jahren (2023)

Altersgruppen	Ziel von Cyberkriminalität	Opfer von Cyberkriminalität
55 – 64	61,1%	8,5%
65 – 74	51,2%	7,0%
75 – 84	43,1%	4,4%
85+	20,0%	1,6%
Total (55+)	52,3%	6,9%

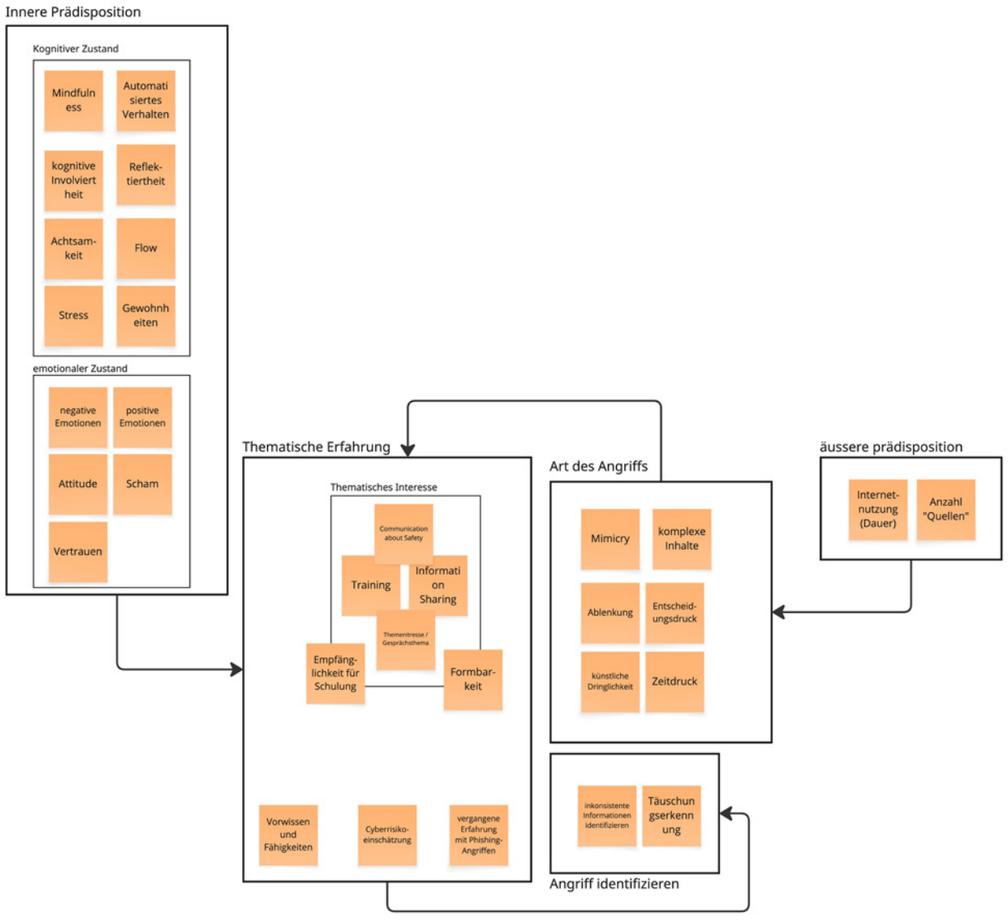
Quelle: *Tabelle 3. (Beaudet-Labrecque et al. 2023)*

Die Auswertung der Meldungen zu Phishing zeigt, dass die meisten Meldungen von Personen im Alter von 40 bis 69 Jahren eingegangen sind. Dies lässt den Schluss zu, dass diese Altersgruppe eine gewisse Empfänglichkeit und Betroffenheit aufweist (BFS 2024). Gemäss der Studie von ProSenectute ist statistisch gesehen etwa jede zweite Person in dieser Altersspanne bereits Opfer von Cyberkriminalität

geworden (Beaudet-Labrecque et al., 2023). Nach Auswertung der Erkenntnisse aus beiden Quellen haben wir die Zielgruppe definiert, um sicherzustellen, dass wir die relevante und geeignete Personengruppe abdecken. Im Anschluss an die Pitch-Präsentation wurde angemerkt, dass die Zielgruppe möglicherweise nicht korrekt gewählt wurde. Es wurde betont, dass wahrscheinlich jüngere Personen stärker von Phishing betroffen sind.

In unseren individuellen Theoriearbeiten wurde schnell deutlich, dass eine Anpassung der Zielgruppe erforderlich ist. Die Studie von Vishwanath et al. (2011) analysiert die Ursachen von Phishing-Anfälligkeit und kommt zu dem Schluss, dass nicht die Internetaffinität, sondern die kognitive Involviertheit entscheidend für die Phishing-Anfälligkeit ist. Personen mit hoher technischer Affinität zeigen häufig ein stärkeres Engagement, was zu einer höheren Wahrscheinlichkeit führt, Opfer von Phishing zu werden, da sie mehr E-Mails erhalten und beantworten (Vishwanath et al., 2011, S. 585). Routineverhalten, wie beispielsweise das regelmässige Öffnen von E-Mails, reduziert die kognitive Involviertheit und verringert die Wahrscheinlichkeit der Täuschungserkennung (Vishwanath et al., 2011, S. 585; 2018, S. 1159).

Abbildung 1: Zusammenhänge der Faktoren Phishingawareness



Aufgrund der Tatsache, dass insbesondere jüngere Personen eine hohe technische Affinität und ein stärkeres Engagement aufweisen, haben wir uns dazu entschlossen, eine jüngere Zielgruppe zu definieren. Zuvor haben wir jedoch noch weitere Faktoren untersucht.

Wir haben die Faktoren zu Phishingawareness, die uns aus der Theoriearbeit bekannt waren, zusammengetragen und in einer übersichtlichen Darstellung präsentiert (siehe Abb. 1), um die Abhängigkeiten zwischen den einzelnen Faktoren aufzuzeigen. Aus diesen erstellten wir eine Tabelle mit den relevanten Einschlussfaktoren, die bei der Bestimmung der Zielgruppe helfen soll (siehe Tabelle 3).

Nach dieser Analyse haben wir uns für zwei Zielgruppen entschieden, die wir als relevant und geeignet erachten: junge Erwachsene (14 bis 20 Jahre) und Studierende. Für beide Zielgruppen haben wir die Tabelle nach unserer Einschätzung individuell ausgefüllt. Wir haben uns bei der Analyse insbesondere auf die Spalten «Veränderbarkeit/Einfluss», «Risiko-Einschätzung» und «Innere Prädisposition (kognitiver Zustand und emotionaler Zustand)» sowie «Cyberhygiene (äussere Prädisposition)» konzentriert.

Tabelle 3: Bewertungsmatrix relevante Einschlussfaktoren

Definition	**Veränderbarkeit / Einfluss *****	**Messbarkeit ***	**Persönliche Relevanz *.5** (psychologisch / individuell)	**Systematische Relevanz *.5** (Umfeld / Exposition)	**Risiko-Einschätzung *****	**Intrinsische Motivation**	**Extrinsische Motivation**
Innere Prädisposition (kognitiver und emotionaler Zustand)	Wieviel Einfluss haben wir auf die Absichten und die innere Einstellung?	Wie könnte der Einfluss den wir auf die Absichten und die Einstellung haben gemessen werden?	Wie persönlich relevant ist für die Personen, dass sie bspw. automatisiertes Verhalten aufzeigen?	Wie relevant ist die innere Prädisposition der Person, um eine Auswirkung auf das Umfeld zu haben?	Welche Gewichtung glauben wir hat die innere Prädisposition auf das Cyberrisiko bezogen?	Wie stark ist die intrinsische Motivation in Bezug auf die Verbesserung der innere Prädisposition?	Wie stark ist die extrinsische Motivation in Bezug auf die Verbesserung der innere Prädisposition?
Thematische Erfahrung (Thematisches Interesse)	Wieviel Einfluss haben wir auf das Interesse fürs Thema?	Wie könnte die thematische Erfahrung gemessen werden?	Wie persönlich relevant ist für die Personen, dass sie über thematisches Wissen verfügt?	Wie relevant ist das thematische Wissen für das Umfeld der Person?	Welche Gewichtung glauben wir hat die thematische Erfahrung auf das Cyberrisiko?	Wie stark ist die intrinsische Motivation in Bezug auf das erlernen des thematischen Wissens?	Wie stark ist die extrinsische Motivation in Bezug auf die Verbesserung des thematischen Wissens?
Art des Angriffes	Wieviel Einfluss haben wir auf die Art des Angriffes?	Wie gut können Angriffsarten gemessen werden?	Welcher Einfluss hat die Angriffsart auf die Psychologie und welche persönliche Relevanz entsteht daraus?	Wie relevant ist das Wissen über die Angriffsart für das Umfeld der Person?	Welche Gewichtung glauben wir hat das wissen über die Angriffsart auf das Cyberrisiko?	Wie stark ist die intrinsische Motivation in Bezug auf das Wissen über die Angriffsarten?	Wie stark ist die extrinsische Motivation in Bezug auf das Wissen über die Angriffsarten?
Angriff identifizieren	Wieviel Einfluss haben wir darauf, dass ein Angriff identifiziert wird?	Wie gut können können wir die Verbesserung der Identifizierung messen?	Welcher Einfluss hat die Identifizierung des Angriffes auf die persönliche Relevanz?	Wie relevant ist die Angriffsidentifizierung für das Umfeld der Person?	Welche Gewichtung glauben wir, hat die Angriffsidentifizierung auf das Cyberrisiko?	Wie stark ist die intrinsische Motivation in Bezug auf die Identifizierung des Angriffs?	Wie stark ist die extrinsische Motivation in Bezug auf die Identifizierung des Angriffs?
Medienkonsum (Äussere Prädisposition)	Wieviel Einfluss haben wir auf das Medienkonsumverhalten?	Wie gut können können wir das Medienkonsumverhalten messen?	Wie persönlich relevant ist das Medienkonsumverhalten?	Wie systematisch relevant ist das Medienkonsumverhalten der Person auf das Umfeld?	Welche Gewichtung glauben wir, hat das Medienkonsumverhalten auf das Cyberrisiko?	Wie stark ist die intrinsische Motivation in Bezug auf das Medienkonsumverhalten?	Wie stark ist die extrinsische Motivation in Bezug auf das Medienkonsumverhalten?
Cyberhygiene (Äussere Prädisposition)	Wieviel Einfluss haben wir auf die Cyberhygiene?	Wie gut können können wir die Cyberhygiene messen?	Wie persönlich relevant ist die Cyberhygiene?	Wie systematisch relevant ist die Cyberhygiene der Person auf das Umfeld?	Welche Gewichtung glauben wir, hat die Cyberhygiene auf das Cyberrisiko?	Wie stark ist die intrinsische Motivation in Bezug auf die Cyberhygiene?	Wie stark ist die extrinsische Motivation in Bezug auf die Cyberhygiene?

Nach sorgfältiger Analyse und Bewertung der relevanten Faktoren haben wir uns dazu entschieden, den Fokus auf die Zielgruppe der Studierenden zu legen. Wir sind zu dem Schluss gekommen, dass diese Zielgruppe sowohl in Bezug auf Veränderbarkeit als auch auf den potenziellen Einfluss, den wir auf sie ausüben könnten, als besonders relevant erscheint.

Achtsamkeit beschreibt die geistige Beschäftigung von Menschen mit Sicherheit oder Misserfolg. Sie sind sehr sensibel für Misserfolge und immer auf der Suche nach dem, was schiefgehen könnte, um die Dinge sicherer zu machen.

Im Kontext von Information Security Awareness bezeichnet Salienz die Neigung, in einer potenziellen Risikosituation an informationssicherheitskonformes Verhalten zu denken.

Verhaltensabsicht beschreibt den Zustand, in dem die Nutzenden die Absicht haben, sich entsprechend ihrem Wissen zu verhalten.

Gleichzeitig haben wir aus unserem Desk Research die folgenden drei Faktoren herausgefiltert, die im Buch «Mensch und Informationssicherheit» von Kristin Weber (2024) als besonders wichtig erachtet werden, um den Menschen in Bezug auf Phishing anzusprechen: Achtsamkeit, Salienz und Verhaltensabsicht. Daraus formulierten wir unsere neue Zielgruppe: Studierende die aktiv im Internet unterwegs sind und geringe Gewohnheit, Salienz und Verhaltensabsicht in Bezug auf Phishing aufzeigen. Diese Zielgruppe der Studierenden steht kurz vor dem Eintritt in die Arbeitswelt, hatten bisher minimalen Kontakt zu Corporate Training und sind somit besonders relevant und beeinflussbar.

Folgende Personen gehören nicht zu unserer Zielgruppe:

- Studierende der Informatik und angrenzender Fachrichtungen.
- Studierende, die derzeit oder zuvor in Bereichen gearbeitet haben, in denen Compliance-Trainings erforderlich waren.
- Studierende, die sich vertieft für Informatik und Informationssicherheit interessieren oder in diesem Bereich arbeiten oder arbeiten möchten.

03 Desk Research

Zusammenfassung

Da unser Projekt einen nutzerzentrierten Ansatz verfolgt und ein tiefes Verständnis für den Themenkontext sowie bestehende Lösungsmuster voraussetzt, führten wir zu Beginn einen systematischen Desk Research durch. Dieser umfasste Literatur, Studien, Podcasts, Keynotes sowie Gespräche mit Expert:innen von Swiss Life und «eBanking – aber sicher» (EBAS). Die Erkenntnisse wurden systematisch aufbereitet und in fünf zentrale Themenfelder gegliedert: Soziologische Aspekte und der Mensch, Zielgruppenorientierung, Emotionen, Awareness sowie Arten der Sensibilisierung.

Deutlich wurde, dass Informationssicherheit ein sozio-technisches Thema ist, bei dem der Mensch nicht als Schwachstelle, sondern als Teil der Lösung betrachtet werden sollte. Effektive Awareness-Massnahmen müssen alltagsnah, niedrigschwellig und emotional sicher sein. Formate wie Gamification, Storytelling, Peer-Effekte und reale Anwendungsbeispiele fördern die Wirksamkeit. Dabei spielt nicht nur Wissen, sondern vor allem Verhaltensabsicht, Gewohnheit und Salienz eine zentrale Rolle.

Emotionen, Motivation und soziale Einbettung sind Schlüssel zur Verhaltensänderung. Sicherheitsverhalten soll nicht durch Angst, sondern durch Zugehörigkeit und Selbstwirksamkeit gefördert werden. Gleichzeitig wurde vor schlecht umgesetzten Phishing-Tests gewarnt, da sie Vertrauen gefährden können. Stattdessen sollten zielgruppenspezifische, ganzheitliche Trainings entwickelt werden.

Die gewonnenen Erkenntnisse bildeten die konzeptionelle Grundlage für die Interviewstruktur mit Studierenden.

Um fundierte inhaltliche Grundlagen für unser Projekt zu schaffen und ein vertieftes Verständnis für bestehende Herausforderungen, Lösungsansätze und Perspektiven im Bereich der Informationssicherheit, insbesondere im Kontext von Phishing, zu erlangen, führten wir einen Desk Research durch. Dieses Kapitel fasst sowohl die Auswertung von Literatur, Studien, Podcasts und Keynotes als auch Erkenntnisse aus Gesprächen mit Expert:innen der Swiss Life sowie von «eBanking – aber sicher» (EBAS) zusammen.

Für den Desk Research haben wir eine Vielzahl von Quellen analysiert, darunter das Buch «Mensch und Informationssicherheit» von Kristin Weber, Interviews im Rahmen der Security Awareness Insider Podcasts sowie wissenschaftliche Arbeiten und Keynotes.

Die Inhalte der untersuchten Quellen wurden systematisch aufbereitet. Wir haben zentrale Aussagen extrahiert, farblich nach Quelle codiert und sie im Rahmen eines Affinity Diagramms nach thematischer Ähnlichkeit gruppiert (siehe Abb. 2). Aus den genannten Aspekten resultieren fünf übergeordnete Themenfelder. Soziologische Aspekte und der Mensch, Zielgruppenorientierung, Emotionen, Awareness sowie Arten der Sensibilisierung.

Abbildung 2: Affinity Diagramm Quellen

Unsere Untersuchung zeigt deutlich, dass Informationssicherheit weit mehr ist als nur Technik – sie ist ein komplexes, soziotechnisches Thema, in dem der Mensch eine aktive Rolle spielt. In der Vergangenheit wurde der Mensch oft als das schwächste Glied in der Kette betrachtet. Ein Paradigmenwechsel, wie er von Kristin Weber in «Mensch und Informationssicherheit» beschrieben wird, stellt jedoch zunehmend den Menschen als Teil der Lösung in den Mittelpunkt. Zentrale Erkenntnisse dieses Ansatzes betonen, dass das Sicherheitsverhalten nicht allein durch Wissen bestimmt wird, sondern durch ein Zusammenspiel von Verhaltensabsicht, Salienz, Gewohnheit und Usability. Sicherheitsmassnahmen müssen daher einfach anwendbar, kontextsensibel und niedrigschwellig sein und gleichzeitig die tatsächliche Lebens- und Arbeitsrealität der Nutzer:innen abbilden. Anstelle der Suche nach Schuldigen bei Fehlern liegt der Fokus heute auf dem gemeinsamen Lernen aus diesen. Ziel ist es, Optimierungspotenziale zu identifizieren und zu analysieren, wie Systeme menschliche Stärken besser nutzen können, anstatt Schwächen zu bestrafen. (Quelle: Mensch und Informationssicherheit – Kristin Weber)

Diese Sichtweise wurde durch unseren Austausch mit der Swiss Life bekräftigt. Dort werden interaktive Formate wie Workshops, Gamification und Perspektivenwechsel (vom Opfer zum Angreifer) genutzt, um das Bewusstsein für das Thema zu fördern. Besonders wichtig sind dabei emotionale Sicherheit, also der Verzicht auf Schuldzuweisungen, die Möglichkeit zur freiwilligen Teilnahme und der gezielte Einsatz von Peer-Effekten. Mitarbeitende, die sich regelmässig beteiligen, tragen durch ihr Intresse das Wissen zum Thema weiter an ihre Kolleg:innen und wirken dadurch als Multiplikator:innen im Unternehmen. Es hat sich als besonders effektiv herausgestellt, den Fokus auf reale, firmenspezifische Beispiele zu legen. Diese schaffen Nähe und Verständnis und können so die Hemmschwelle zum Handeln senken. (Quelle: Gespräch mit Swiss Life)

Auch EBAS verfolgt einen praxisorientierten Ansatz. Mithilfe von Phishing-Tests, spielerischen Formaten wie Ransomware-Games und verständlichen Schulungen wird ein konkreter, emotionaler und wiederholter Zugang geschaffen. Der Fokus liegt darauf, die Thematik greifbar zu machen, statt sie abstrakt zu behandeln. (Quelle: Gespräch mit Oliver Hirschi / EBAS)

Ein weiteres zentrales Thema, das sich durch viele Quellen zog, war die Rolle von Emotionen. Johannes Büchs betont, dass Storytelling als Methode hilft, Nähe zu schaffen und sich mit den dargestellten Situationen zu identifizieren – gerade weil Figuren auch Fehler machen dürfen. Diese emotionale Verbindung wirkt identitätsstiftend und senkt die Barrieren für eine Verhaltensänderung. (Quelle: Johannes Büchs / Security Awareness Insider)

Abbildung 3: Unser Besuch bei der Swiss Life in Zürich.

Katja Dörlemann und Marcus Beyer betonen, dass Informationssicherheit emotional positiv besetzt werden muss – nicht nur durch «Awareness» im Sinne von Warnung, sondern auch durch Education und Training, die Selbstwirksamkeit fördern. (Quelle: Katja Dörlemann & Marcus Beyer / Security Awareness Insider)

Laut Dr. Katharina Bernecker fördern darüber hinaus positive Zielbilder wie das Gefühl, Teil einer Bewegung zu sein oder die eigene digitale Sicherheit selbst in der Hand zu haben, das gewünschte Verhalten. (Quelle: Dr. Katharina Bernecker / Security Awareness Insider)

Ein weiterer Aspekt ist die Motivation. Dr. Katharina Bernecker zufolge ist es entscheidend, positives Verhalten einfach (Nudging) oder unterhaltsam (Gamification) zu gestalten. Besonders bei jüngeren Zielgruppen wirkt der Hinweis auf bestehende Trends in der eigenen Peer-Group motivierend. Sicherheit sollte demnach nicht mit Angst, sondern mit Selbstwirksamkeit und Zugehörigkeit assoziiert werden. (Quelle: Dr. Katharina Bernecker / Security Awareness Insider)

Dr. Melanie Volkamer warnt gleichzeitig vor der unreflektierten Nutzung von Phishing-Simulationen. Schlechte Umsetzungen können dem Vertrauen schaden. Sie plädiert stattdessen für präventive, ganzheitlich konzipierte Schulungen, die allgemeine Erkennungsmerkmale und sichere Verhaltensweisen vermitteln und sich nicht nur auf einzelne Angriffsbeispiele fokussieren. (Quelle: Dr. Melanie Volkamer / Security Awareness Insider)

Ein durchgängiger Befund des Desk Research ist die Individualität der Zielgruppen. Das Sicherheitsverhalten ist hoch kontextabhängig. Tom Hofmann spricht in diesem Zusammenhang von einem Wicked Problem, also einem schwer nachvollziehbaren und mit klassischen Ingenieurmethoden nicht lösbaren Problem. (Quelle: Tom Hofmann / Security Awareness Insider)

Auf Basis dieser Erkenntnisse haben wir zentrale Themen und Fragestellungen abgeleitet, die uns bei der Konzeption der Interviews mit den Studierenden geleitet haben. Dabei bildeten Aspekte wie Salienz, Gewohnheiten und Verhaltensintentionen, der Einfluss positiver Emotionen, die Bedeutung von motivierenden Zielbildern und Peer-Groups sowie der Einsatz von Storytelling und sozial eingebetteter Kommunikation die inhaltliche Grundlage. Diese Themen haben wir gezielt in unsere Interviewstruktur integriert, um herauszufinden, wie sich Awareness-Massnahmen im konkreten Lebens- und Studienalltag unserer Zielgruppe verankern lassen. So konnten wir die theoretischen Erkenntnisse aus der Literaturrecherche gezielt mit den praktischen Erfahrungen und Sichtweisen der Zielgruppe verknüpfen und auf ihre Relevanz und Umsetzbarkeit hin überprüfen.

Im Zusammenhang mit dem Desk Research möchten wir uns herzlich bei allen Fachpersonen bedanken, die sich die Zeit genommen haben, mit uns über das Thema Phishing und unsere Bachelorarbeit zu sprechen. Wir haben den offenen Austausch und die unterstützende Haltung aller Gesprächspartner:innen sehr geschätzt und es war eine grosse Freude, auf so viel Bereitschaft zur Mitwirkung zu treffen.

04 Field Research

Zusammenfassung

Zur Validierung unserer Erkenntnisse aus dem Desk Research und zur Vertiefung unseres Verständnisses der Zielgruppe führten wir qualitative Interviews und Tests mit sechs Personen durch. Im Fokus standen drei zentrale Themen: die Einschätzung des eigenen Cyberverhaltens, die emotionale Wahrnehmung von Phishing sowie die gewünschte Form der Wissensvermittlung (siehe Abbildung 4).

Im Hinblick auf das Cyberverhalten unserer Zielgruppe kombinierten wir Likert-Skalen mit einem Paper-Test. Die Ergebnisse zeigen, dass mehrere Personen ihr eigenes Risiko und ihre Fähigkeiten zur Phishing-Erkennung überschätzen. Die Korrelation zwischen subjektiver Risikoeinschätzung und tatsächlicher Erkennungsfähigkeit fällt mit –0.6 moderat negativ aus (siehe Tabelle 4). Dies lässt auf eine gewisse Selbstüberschätzung schliessen, insbesondere bei drei der sechs Personen. Einzelne Testpersonen zeigten durch absolvierte Schulungen eine realistischere Selbsteinschätzung, während andere konkrete Vorgehensweisen nannten, jedoch eine geringe Awareness erkennen liessen. Die Daten liefern Hinweise auf kognitive Verzerrungen wie den Dunning-Kruger-Effekt.

Bezogen auf die emotionale Wahrnehmung des Themas Phishing zeigt sich ein klar negativ geprägtes Bild. Mithilfe von Adjektivkarten (siehe Tabelle 5) wurden sowohl persönliche Gefühle als auch die Einschätzung des sozialen Umfelds erhoben. Häufig genannte Begriffe wie verwirrt, überfordert und ängstlich unterstreichen eine hohe emotionale Belastung. Vier von sechs Personen wählten überwiegend oder ausschliesslich negativ konnotierte Adjektive. Besonders auffällig war die Verschiebung von ursprünglich neutralen hin zu klar negativen Einstellungen bei einzelnen Interviewten (siehe Tabelle 8). Gleichzeitig zeigen zwei andere Personen eine Entwicklung hin zu einem positiveren Umgang mit dem Thema, insbesondere in Bezug auf ihr soziales Umfeld. Die Wahrnehmung der eigenen Kompetenz bleibt jedoch oft hinter dem Vertrauen in das Umfeld zurück, was auf ein fehlendes Sicherheitsgefühl und punktuell auftretende Hilflosigkeit hindeuten kann.

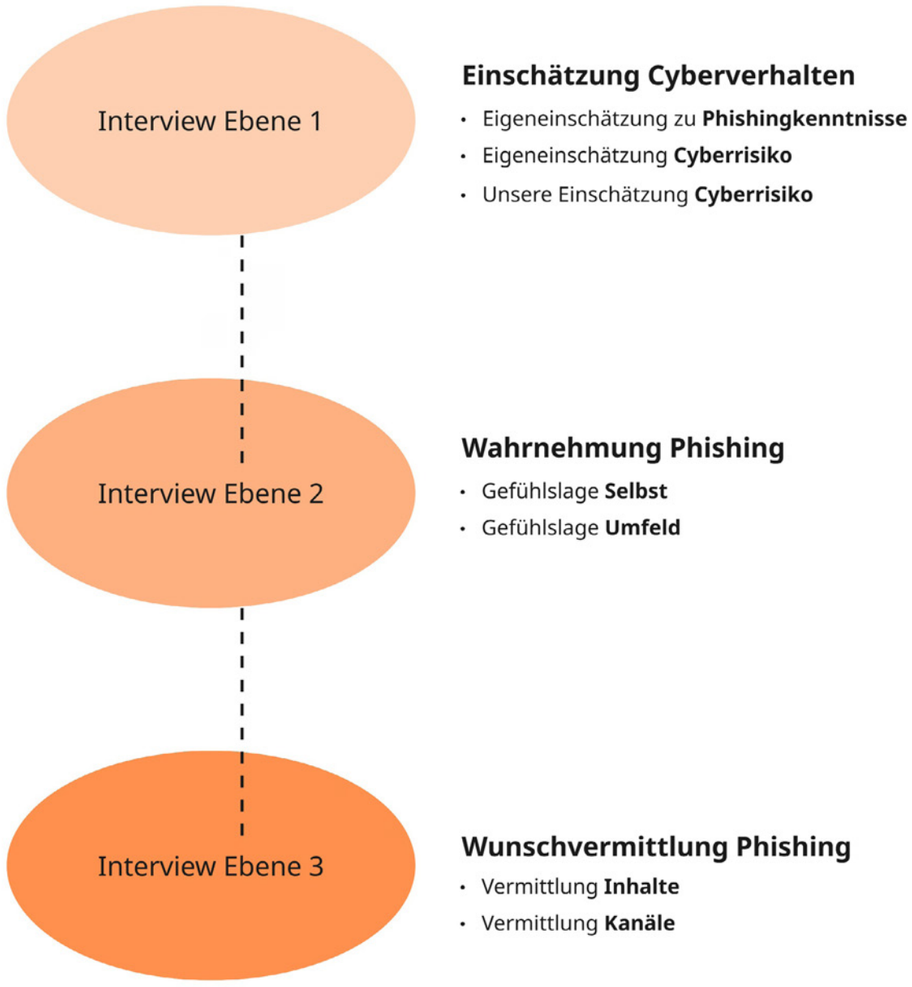
In Bezug auf die gewünschte Vermittlung von Phishing-Inhalten gaben die Interviewten klare Präferenzen für bestimmte Inhalte und Kanäle an (siehe Abbildung 7 – 11). Besonders geschätzt wurden Informationen zu aktuellen Vorfällen, psychologischen Angriffsmustern und Erfahrungsberichte anderer Betroffener. Diese Inhalte wurden als spannend und hilfreich eingestuft. Definitionen hingegen wurden als unwichtig und langweilig bewertet. Bei den bevorzugten Vermittlungskanälen (siehe Abbildung 10 – 11) dominieren Kurzvideos, die von allen sechs Personen ausgewählt und am höchsten gewichtet wurden. Interaktive Installationen und Webseiten folgten in der Präferenz. Die gewählten Formate deuten auf ein hohes Interesse an anschaulichen, zugänglichen und zeiteffizienten Informationsformen hin.

Im Field Research führten wir semi-strukturierte Interviews und Tests mit sechs Personen aus unserer Zielgruppe durch. Unser Ziel war es, weiterführende Erkenntnisse über die Zielgruppe zu erlangen und unser Desk Research zu validieren.

Dabei fokussierten wir uns auf folgende Forschungsfragen:

- Schätzen die Interviewpersonen ihr eigenes Cyberrisiko realistisch ein?
- Wie wird das Thema Phishing von den Interviewpersonen wahrgenommen?
- Wie soll das Thema Phishing für die Interviewpersonen vermittelt werden?

Abbildung 4: Interview Ebenen des Field Research



04.1 Einschätzung Cyberverhalten

Um die Einschätzung des Cyberrisikos und der Fähigkeiten zur Phishingerkennung der Interviewpersonen zu erfassen, wurden zwei Likert-Skalen verwendet und ein Paper-Test durchgeführt. Wobei die jeweiligen Aussagen in der Analyse kombiniert wurden, um das Cyberverhalten der Interviewten einzuschätzen.

04.1.1 Eigeneinschätzung Phishingkenntnisse & Cyberrisiko

Die erste Likert-Skala dient dazu, die eigene Einschätzung zur Phishing-Erkennung zu ermitteln. Die zweite Skala erfasst die Einschätzung des individuellen Cyberrisikos. Anhand des Paper-Tests wurde ermittelt, inwiefern Salienz, Verhaltensabsicht und Intention bei den Interviewpersonen vorhanden sind. Dazu wurde das konkrete Vorgehen bei der Validierung eines Phishing-E-Mails abgefragt.

04.1.2 Unsere Einschätzung Cyberrisiko

Im Paper-Test wurde den Testpersonen folgendes Szenario vorgelegt:
Du arbeitest in der Einkaufsabteilung der grössten schweizer Importwarenfirma, in der du für die Einkäufe zuständig bist. In deiner Arbeit kommunizierst du vorwiegend über E-Mails. Wie gehst du vor, um diese E-Mail auf Echtheit zu prüfen?
Der Paper-Test umfasste zudem eine gedruckte Ansicht eines von uns für diesen Test erstellten Phishing-E-Mails.

04.1.3 Auswertung Cyberverhalten

Zur Analyse des Cyberrisikos der Interviewpersonen haben wir die drei Teile des Interviews ausgewertet und miteinander verglichen. Zur Auswertung der Likert-Skala wurden die Antworten der Testpersonen wie folgt quantifiziert:

Tabelle 4: Korrelation zwischen Phishingerkennung und Cyberriskio anhand von Likert-Skala (N = 6)

Person	Phishing Erkennung	Cyberrisiko
1	3	4
2	3	4
3	3	3,5
4	4	4
5	4	3
6	4	3
Korrelation	-0,5570860145	

Die Skala reicht von 1 «Tief» bis 5 «Hoch». Die zugrunde liegende Theorie besagt, dass das Cyberrisiko negativ mit der Phishing-Erkennung korreliert. Die Berechnungen ergaben mit -0.6 nur eine mittlere negative Korrelation zwischen Phishing-Erkennung und Cyberrisiko. Da es sich hierbei um Selbsteinschätzungen handelt, zeigen die Werte eine moderate Selbstüberschätzung bei drei der Testpersonen. Dies könnte ein Hinweis darauf sein, dass Personen aus dieser Zielgruppe sich tendenziell überschätzen.

Vergleicht man die vorliegenden Daten mit den Ergebnissen der Paper-Tests, in denen die konkrete Vorgehensweise zur Phishing-Erkennung getestet wurde, so zeigt sich, dass die Testpersonen ohne negative Korrelation die gleichen konkreten Vorgehensweisen wie die anderen Testpersonen anwenden. Es besteht jedoch die Möglichkeit, dass sie ein höheres Vertrauen in ihre Technik haben und mehr Erfahrung in der Phishing-Prävention besitzen.

Es besteht auch die Möglichkeit, dass es sich hierbei um den Dunning-Kruger-Effekt handelt. In diesem Zusammenhang ist es interessant zu bemerken, dass die Interviewperson (Person 4), die das umfangreichste Compliance-Training erhalten hat, sowohl bei der Phishing-Erkennung als auch beim Cyberrisiko die gleiche Einschätzung aufwies. Im Interview mit dieser Person wurde eine erhöhte Awareness festgestellt, was darauf hindeutet, dass ihre Selbsteinschätzung möglicherweise durch das Wissen beeinflusst wurde, dass Phishing generell schwer zu erkennen ist.

Bei zwei anderen Interviewpersonen (Person 5 und 6), sind zwar konkrete Vorgehensweisen bekannt, insbesondere in Bezug auf das Szenario des Tests, jedoch fehlt es ihnen an der notwendigen Awareness.

04.2 Wahrnehmung Phishing

Um herauszufinden, wie das Thema Phishing von den Interviewpersonen wahrgenommen wird, befragten wir sie mithilfe von Adjektivkarten (siehe Tab. 5). Dazu konnten die Interviewpersonen drei Adjektive aus einem Stapel von 12 positiv, 13 negativ und 9 neutral konnotierten Adjektiven auswählen, die von uns zuvor bestimmt wurden.

Tabelle 5: Adjektivliste für Interviewfragen

Positiv	Negativ	Neutral
Ermutigt	Traurig	Überrascht
Zufrieden	Enttäuscht	Neugierig
Begeistert	Frustriert	Nachdenklich
Aufgeregt	Ängstlich	Zurückhaltend
Gelassen	Verärgert	Ausgeglichen
Dankbar	Nervös	Skeptisch
Optimistisch	Einsam	Ruhig
Vertrauensvoll	Verwirrt	Befremdet
Liebevoll	Bedrückt	Unbeeinflusst
Kreativ	Überfordert	
Entschlossen	Unzufrieden	
Entspannt	Verzweifelt	
	Zerrissen	

04.2.2 Gefühlslage Selbst

Zuerst wurden die Interviewten nach ihrer eigenen Emotionalen verbindung zum Thema Phishing befragt. In dieser Erhebung dominieren eindeutig negativ konnotierte Adjektive, beispielsweise frustriert (N = 2), enttäuscht (N = 2) sowie verwirrt (N = 2). Positive oder neutrale Adjektive wie neugierig (N = 3), kreativ (N = 1) und nachdenklich (N = 2) sind ebenfalls vertreten, jedoch in der Minderheit und häufig in einem negativ gefärbten Kontext eingebettet. Drei von sechs befragten Personen (Person 4, 5 und 6) verwendeten mindestens zwei negativ konnotierte Adjektive; bei Person 4 finden sich ausschliesslich negative Zuschreibungen.

Es lassen sich drei wiederkehrende Adjektivkombinationen identifizieren, die jeweils zweimal genannt wurden: neugierig und skeptisch (beide tendenziell neutral), skeptisch und verwirrt (neutral und negativ) sowie nachdenklich und skeptisch (beide eher negativ konnotiert). Person 2 verwendete ausschliesslich neutrale Adjektive. Insgesamt wurden neutrale Adjektive einmal häufiger genannt als negativ konnotierte.

Tabelle 6: Resultate zu Adjektive in Bezug zum Thema Phishing (Eigene Wahrnehmung)

Person 1	Kreativ	Enttäuscht	Skeptisch
Person 2	Neugierig	Nachdenklich	Skeptisch
Person 3	Verwirrt	Neugierig	Skeptisch
Person 4	Frustriert	Einsam	Überfordert
Person 5	Enttäuscht	Frustriert	Neugierig
Person 6	Verwirrt	Nachdenklich	Skeptisch

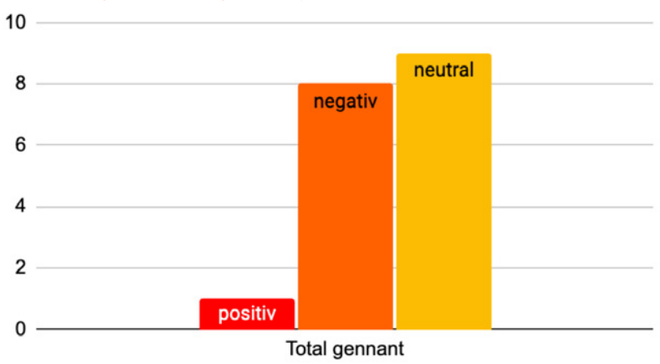
Häufige Kombinationen

- Neugierig - Skeptisch: 2×
- Skeptisch - Verwirrt: 2×
- Nachdenklich - Skeptisch: 2×

Wertung der Adjektive

- Negativ: 8×
- Neutral: 9×
- Positiv: 1×

Abbildung 5: Wertung der Adjektive



Diese Ergebnisse deuten auf eine insgesamt eher verunsicherte oder emotional belastete Wahrnehmung von Phishing hin. Keine der befragten Personen beschreibt ihre Wahrnehmung ausschliesslich positiv. Neutralere Adjektivkombinationen mit negativer Färbung treten am häufigsten auf – ein Hinweis auf die Ernsthaftigkeit oder die potenzielle Bedrohung, die Phishing aus Sicht der Befragten darstellt.

04.2.2 Gefühlslage Umfeld

Um ein umfassenderes Bild der Wahrnehmung des Themas Phishing zu erlangen, befragten wir die Interviewpersonen auch dazu, wie das Umfeld dem Thema gegenübersteht, also wie die Percieved Norm dort ist. Auch bei dieser Frage wurden die Interviewpersonen aufgefordert, drei Adjektive zu wählen.

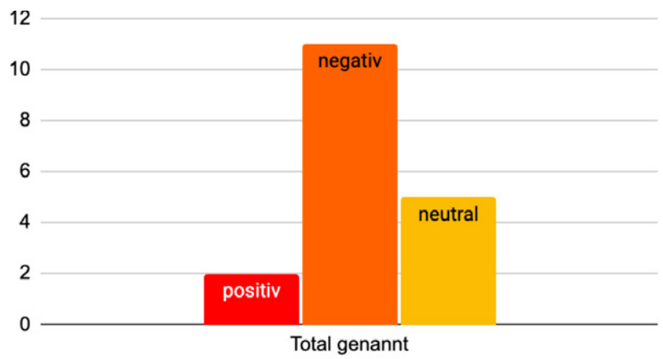
Tabelle 7: Resultate zu Adjektive in Bezug zum Thema Umfeld und Phishing (Percieved Norm)

Person 1	Ängstlich	Nachdenklich	Skeptisch
Person 2	Verärgert	Verwirrt	Überfordert
Person 3	Entspannt	Überfordert	Unbeeinflusst
Person 4	Gelassen	Überfordert	Befremdet
Person 5	Verwirrt	Verzweifelt	Unbeeinflusst
Person 6	Ängstlich	Verärgert	Verwirrt

Häufige Kombinationen

- Verärgert - Verwirrt: 2×

Abbildung 6: Wertung der Adjektive



Wertung der Adjektive

- Negativ: 11×
- Neutral: 5×
- Positiv: 2×

Hier sehen wir überwiegend negative Adjektive wie Überfordert (N = 3), Verwirrt (N = 3), Ängstlich (N = 2) und Verärgert (N = 2). Das einzige Doppelpaar ist Verwirrt und Verärgert, was jedoch beide negative Adjektive sind. Vier von sechs Personen (Person 2, 5, 6 und teilweise Person 1) haben mindestens zwei negativ konnotierte Adjektive gewählt, drei davon ausschliesslich negative.

Dies deutet auf eine insgesamt eher belastete, stressige oder konfliktreiche emotionale Grundlage in dieser Gruppe hin. Keine der Personen hat ausschliesslich positiv konnotierte Adjektive gewählt, was auf eine gewisse emotionale Belastung oder Ernsthaftigkeit hindeuten kann.

04.2.3 Kombination der Gefühlslagen

Im Zusammenhang mit Salienz, Achtsamkeit und Verhaltensabsicht bezog sich die Frage «Welche drei Adjektive verbindest du mit dem Thema Phishing?» auf die subjektive Wahrnehmung der Interviewten. Die Kategorie Perceived Norm (Umfeld) wurde hingegen mit der Frage «Wie verhält sich dein Umfeld dem Thema Phishing gegenüber?» erhoben. Dabei ging es stärker um die Fremdwahrnehmung, insbesondere in Bezug auf das soziale Umfeld.

Tabelle 8: Veränderung der Emotionslage (Links: Gefühlslage Selbst, Rechts: Gefühlslage Umfeld)

Person	+	=	-	→	+	=	-	Veränderung
1	1	1	1	→	0	2	1	Positiv verloren, Neutralität gestiegen
2	0	3	0	→	0	0	3	Von voll neutral → voll negativ
3	0	2	1	→	1	1	1	Positiv dazugewonnen
4	0	0	3	→	1	1	1	Weniger negativ, mehr Ausgeglichenheit
5	0	1	2	→	0	1	2	Unverändert
6	0	1	2	→	0	0	3	Neutralität verloren, mehr Negativität

Es ist auffällig, dass sich bei zwei Interviewten (Person 2 und Person 6) eine signifikant negativere Haltung manifestierte. Sie wandten sich von einer ursprünglich neutralen oder ausgeglichenen Position ab und äusserten ausschliesslich negative Einschätzungen. Auch eine andere interviewte Person (Person 1) verliert im Verlauf positive Assoziationen und bewegt sich in Richtung Neutralität, ohne jedoch eine Zunahme negativer Konnotationen zu zeigen. Dies könnte ein Hinweis darauf sein, dass sich mehrere Personen in Bezug auf ihr Umfeld als hilflos oder ohnmächtig erleben. Dies wird durch Aussagen wie «Meine Eltern, meine Grosseltern wissen teilweise nicht, welche Cookies sie angeklickt haben, wo sie überall ihre E-Mails geteilt haben» oder «Verwirrt, weil meine Eltern es nicht verstehen und darum sind sie verwirrt» deutlich gemacht.

Tabelle 9: Veränderung der emotionalen Haltung zwischen den Fragen

Konnotation	Aufgabe 1	Aufgabe 2	Aufgabe 3
Positiv	1	2	+1
Neutral	8	5	-3
Negativ	9	11	+2

- Negativität insgesamt gestiegen (von 9 auf 11)
- Neutralität gesunken (von 8 auf 5)
- Positives leicht gestiegen, aber auf sehr niedrigem Niveau (von 1 auf 2)

Es ist zudem bemerkenswert, dass die betreffenden Personen die Gefahren durch Phishing durchaus erkennen, da sie in ihrem Umfeld bereits mit konkreten Fällen von Phishing oder Social Engineering konfrontiert waren (wie bei Person 2). Allerdings verfügen sie nicht über klare Strategien, um sich effektiv davor zu schützen.

Bei den Personen 3 und 4 ist hingegen eine positive emotionale Entwicklung zu beobachten. Beide Parteien wiesen zu Beginn eine eher negative Einstellung auf. Im weiteren Verlauf konnten jedoch positive Konnotationen hinzugewonnen werden. Dies lässt auf eine veränderte, optimistischere Wahrnehmung im Kontext der zweiten Fragestellung schliessen, welche sich auf das soziale Umfeld fokussiert. Die Ergebnisse deuten darauf hin, dass die untersuchten Personen ihrem Umfeld tendenziell mehr Vertrauen schenken als sich selbst. Dieser Umstand könnte darauf hindeuten, dass das Umfeld bereits ein gewisses Mass an Awareness aufweist, wie es bei Person 4 der Fall ist. Alternativ könnte das Thema auch in dem sozialen Kontext kaum thematisiert werden und es existieren keine bekannten Vorfälle, wie es bei Person 3 der Fall ist.

Person 5 zeigt keine signifikanten Veränderungen, weder in positiver noch in negativer Richtung. Die Angabe, dass ein Austausch mit den Eltern stattgefunden hat, könnte darauf hinweisen, dass zwischen der Selbstwahrnehmung und der Einschätzung des Umfelds kaum Differenzen bestehen. Die individuelle Einstellung gegenüber Phishing scheint in diesem Kontext massgeblich vom unmittelbaren sozialen Umfeld beeinflusst zu sein.

04.3 Wunschvermittlung Phishing

Um die Frage «Wie soll das Thema Phishing den Interviewpersonen vermittelt werden?» zu analysieren, durchliefen die Teilnehmenden zwei aufeinanderfolgende Interview-Schritte. Im ersten Schritt vervollständigten sie ein Raster, in dem verschiedene Vermittlungsinhalte entlang zweier Dimensionen eingeordnet wurden – von langweilig bis spannend sowie von unwichtig bis hilfreich. Im zweiten Schritt erhielten sie Spielgeld, das sie in verschiedene Vermittlungskanäle investieren konnten.

04.3.1 Vermittlung Inhalte

Zur Sortierung der Vermittlungsinhalte legten wir den Interviewpersonen die folgenden Inhalte vor:

- Psychologische Aspekte
- Merkmale
- Definitionen
- Geschichten von anderen (Testimonials)
- Infos zu aktuellen Vorfällen
- Unterstützung nach einem Phishing-Angriff
- Allgemeine Informationen
- Eigener Vorschlag (für Vermittlungsinhalt)

Abbildung 7: Aufteilung der Quadranten des zwei Achsen Diagramm

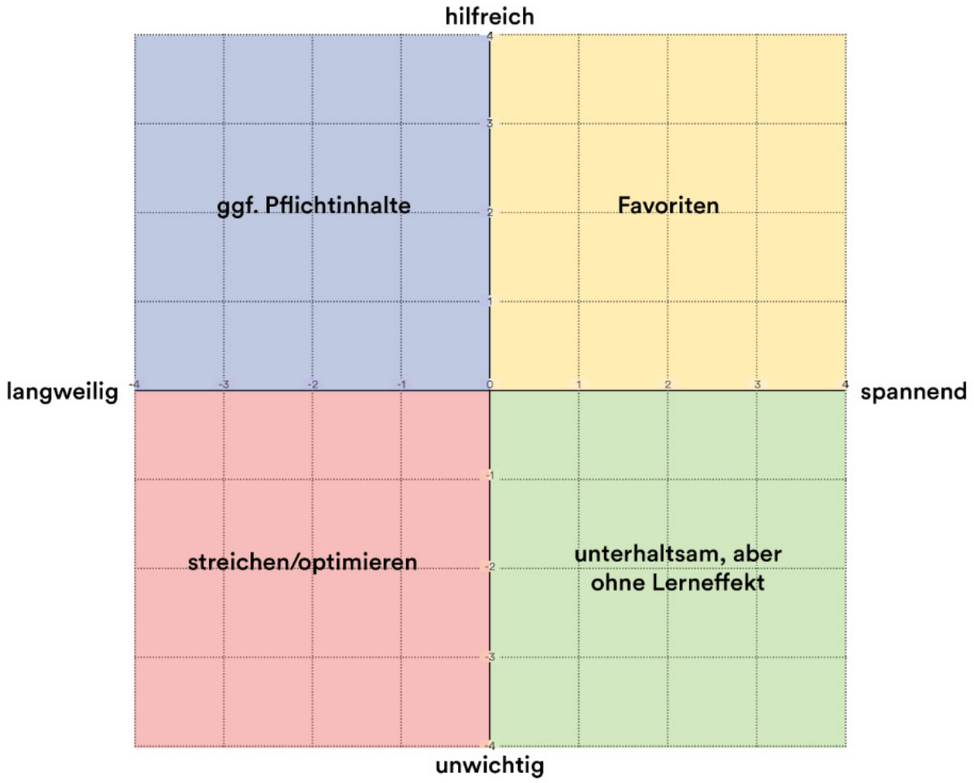


Abbildung 8: Auswertung Raster (Durchschnitt) – Inhalt des Vermittelten

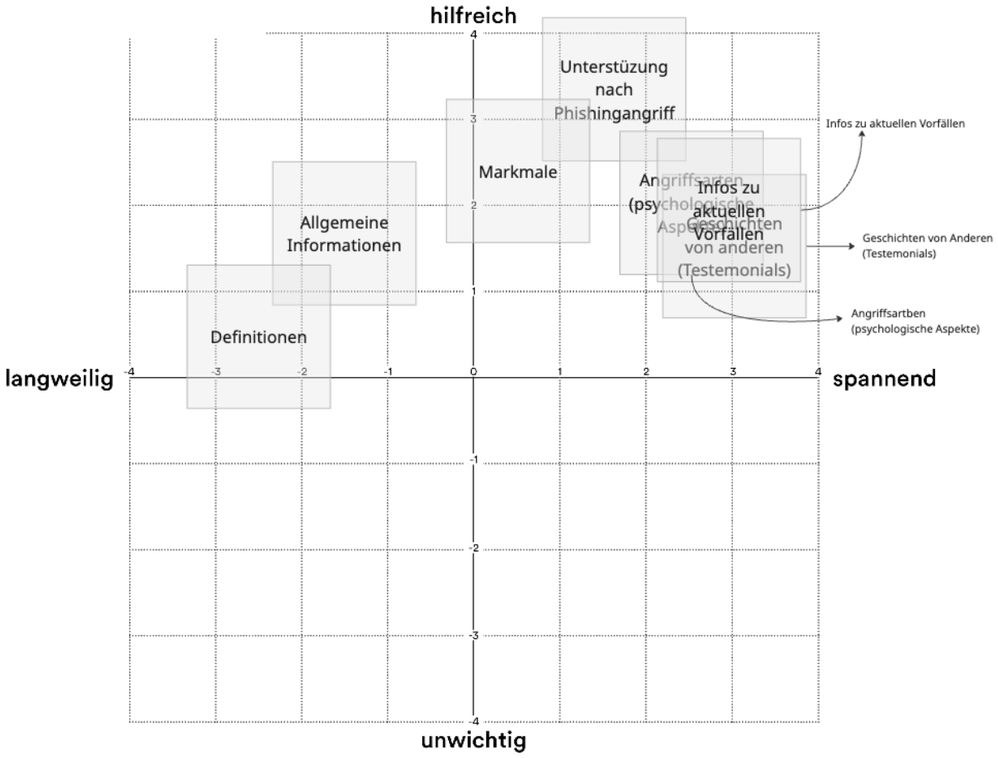
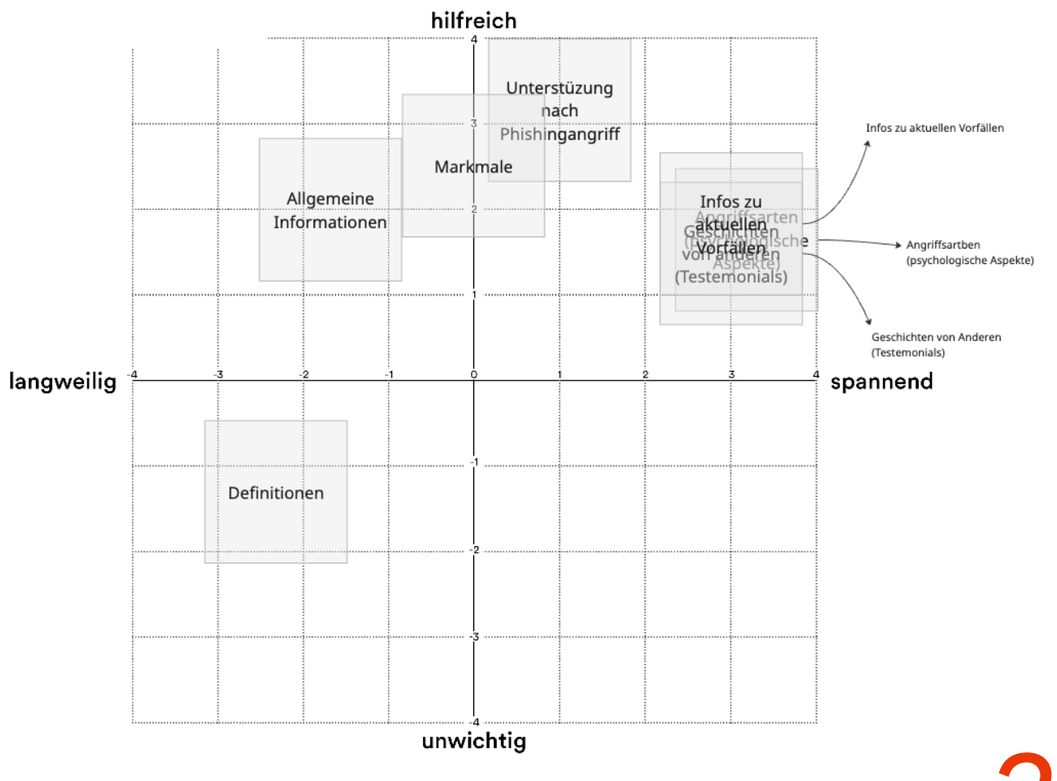


Abbildung 9: Auswertung Raster (Median) – Inhalt des Vermittelten



Bei der Analyse der Vermittlungsinhalte erweist sich der Median als die geeignetere Auswertungsmethode, da bei dieser kleinen Datenerhebung die Werte einzelner Datenpunkte signifikant voneinander abweichen. Dies könnte möglicherweise darauf zurückzuführen sein, dass den Testpersonen lediglich eine beschriftete X- und Y-Achse vorgegeben wurde, jedoch kein klar definiertes Feld mit festen Werten. Die Wahl dieses Vorgehens erfolgte mit Bedacht, um den Fokus weniger auf die konkreten Werte der einzelnen Vermittlungsinhalte zu lenken, sondern vielmehr auf die subjektiv empfundene Gewichtung zwischen den vorgeschlagenen Inhalten.

Es kann im Allgemeinen festgestellt werden, dass Informationen zu aktuellen Vorfällen, Angriffsarten mit Bezug auf psychologische Aspekte sowie Geschichten von anderen Betroffenen als am hilfreichsten und spannendsten bewertet wurden. Die betreffenden Inhalte wurden eindeutig dem Quadranten Favoriten zuzuordnen. Die Unterstützung nach einem Phishingangriff wird ebenfalls als besonders hilfreich eingeschätzt, jedoch als weniger spannend bewertet. Sie befindet sich dennoch im Favoriten-Quadranten. Die Merkmale werden als hilfreich, aber weder spannend noch langweilig empfunden. Sie befinden sich im Übergangsbereich zwischen den Quadranten Favoriten und Pflichtinhalte. Allgemeine Informationen werden hingegen als hilfreich, aber langweilig empfunden und sind damit klar im Quadranten Pflichtinhalte einzuordnen.

Die Definition wird im Median als einziger Inhalt sowohl als langweilig als auch unwichtig eingestuft. Sie befindet sich demnach im Quadranten Streichen/Optimieren. Es ist interessant zu bemerken, dass kein Inhalt im Quadrant Unterhaltsam, aber ohne Lernwert (spannend, aber unwichtig) gelandet ist. Dies könnte auf die von uns getroffene Vorauswahl der Vermittlungsinhalte zurückzuführen sein.

04.3.2 Vermittlung Kanäle

Um die Vermittlungskanäle zu definieren, legten wir den Interviewpersonen folgende möglichen Vermittlungskanäle vor:

- Newsletter
- Broschüre
- Website
- App
- Workshop
- Interaktive Installation
- Wearable
- Game
- Video (Kurzformat)
- Video (Langformat)
- Eigener Vorschlag für einen Vermittlungskanal

Die Interviewpersonen erhielten von uns fünfmal 100.- Spielgeld. Dieses konnten sie nach Belieben auf die vorgegebenen Vermittlungskanäle verteilen.

Abbildung 10: Auswertung Buy a Feature – Total investiert nach Kanal

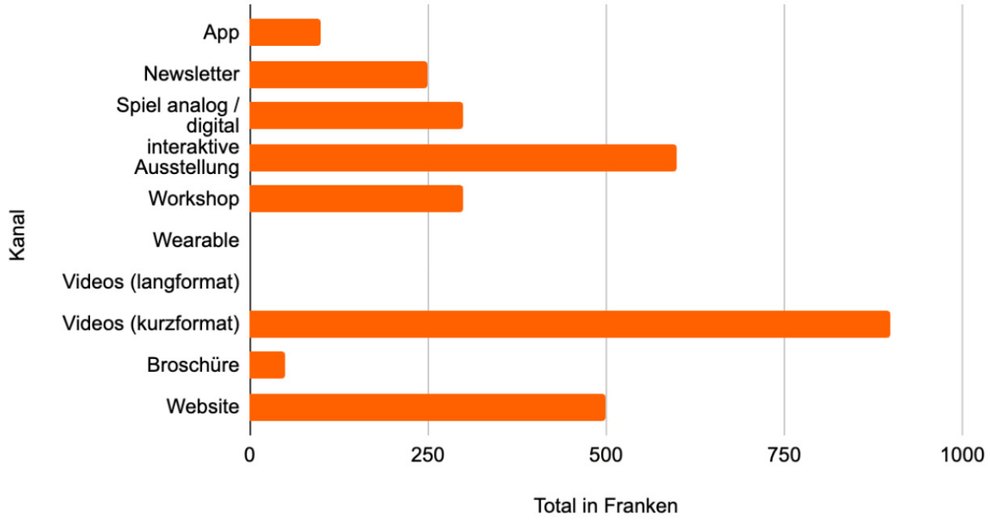
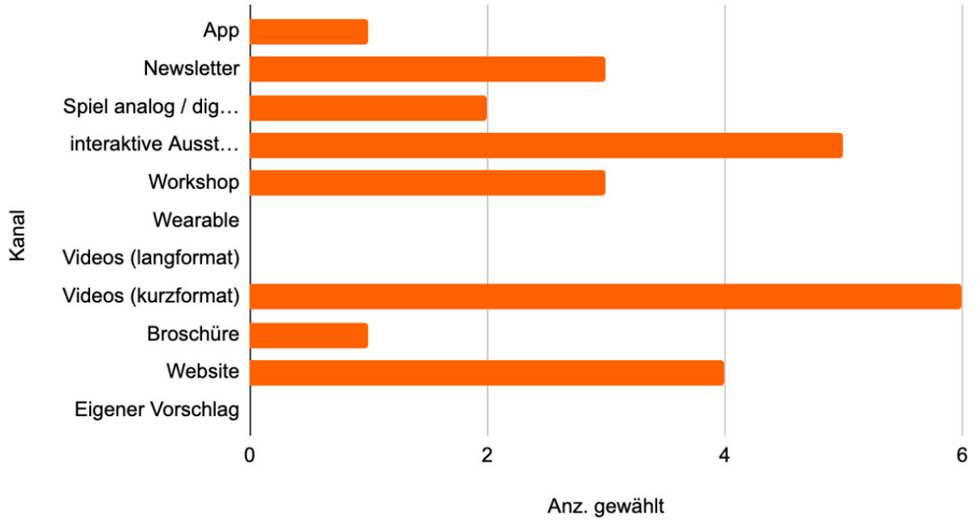


Abbildung 11: Auswertung Buy a Feature – Total wie oft der Kanal gewählt wurde



Die Auswertung der Interviews hat ergeben, dass eine klare Präferenz für Kurzvideos besteht. Diese wurden von allen sechs Personen gewählt und insgesamt am höchsten gewichtet. Die nachfolgende Kategorie ist interaktive Installation, welche von fünf Personen präferiert und als zweitwichtigstes Format evaluiert wurde. Die Webseite wurde von vier Personen an dritter Stelle gewählt und erhielt die dritthöchste Gewichtung. Die nachfolgend genannten Kanäle Newsletter und Workshop wurden mit einer identischen Gewichtung von jeweils drei Stimmen gewählt.

Es ist interessant zu beobachten, dass die Mehrheit der Personen sich vorwiegend für interaktive Formate oder solche mit geringem Zeitaufwand interessiert. Die Webseite ist von hoher Relevanz, da sie die Möglichkeit bietet, gebündelte Informationen zu vermitteln und kontinuierlich als Referenzquelle zu dienen. Es besteht die Möglichkeit, dass die Webseite aufgrund ihrer Unterstützung nach Phishing-Angriffen eine höhere Gewichtung erhielt.

04.4 Fazit

Das Interview wurde gezielt so konzipiert, um eine Vielzahl an qualitativen Daten zu generieren. Zu diesem Zweck wurden Aufgaben gewählt, die die Interviewpersonen dazu anregten, sich intensiv mit den Fragestellungen auseinanderzusetzen. Hierzu gehörten die Bereitstellung von Adjektiven zur Unterstützung bei der Beantwortung der Fragen, die Vorlage eines Rasters, in dem die Interviewpersonen ihre Einordnung erstellen konnten, sowie die Präsentation eines konkreten Szenarios, in das sie sich hineinversetzen konnten. Darüber hinaus wurden sie mit fiktivem Geld in die Rolle der Entscheidungsträger:innen gesetzt. Der Einsatz dieser Methoden führte zu guten Resultaten. Zudem wurde von den Interviewpersonen angegeben, dass sie sich durch die Methoden motiviert fühlten und ausführlichere und tiefgründigere Antworten gaben.

05 Kombination der Erkenntnissen

Zusammenfassung

Die Verbindung von Desk- und Field-Research ermöglicht eine ganzheitliche Betrachtung des Themas Phishing-Awareness. Während der Desk Research theoretische Konzepte und Best Practices liefert, spiegelt der Field Research die tatsächlichen Bedürfnisse, Wahrnehmungen und Verhaltensweisen der Zielgruppe wider. Die Auswertung beider Ansätze zeigt, dass erfolgreiche Awareness-Massnahmen mehrere Ebenen gleichzeitig berücksichtigen müssen, darunter Zielgruppenbezug, Relevanz im Alltag, emotionale Ansprache und soziale Einbettung (siehe Abbildung 12).

Die Analyse macht deutlich, dass Wissen allein nicht ausreicht, um nachhaltiges Sicherheitsverhalten zu fördern. Entscheidend sind eine aktive Auseinandersetzung mit dem Thema, konkrete Handlungsmöglichkeiten und ein niederschwelliger Zugang zu den Inhalten. Gleichzeitig zeigt sich, dass emotionale Faktoren, wie Verwirrung, Angst oder Überforderung, eine zentrale Rolle spielen. Positiv erlebte Lernelemente und sozial eingebettete Vermittlungsformen können jedoch das Sicherheitsbewusstsein stärken und zur langfristigen Verhaltensänderung beitragen.

Aus der Verbindung von Theorie und Praxis lassen sich klare Leitlinien für die Umsetzung ableiten. Awareness-Massnahmen sollten alltagsnah, visuell ansprechend und handlungsorientiert gestaltet sein. Ziel ist es, Phishing-Sensibilisierung nicht als isolierte Informationskampagne, sondern als kontinuierlichen Lernprozess zu verstehen, der nachhaltig im Alltag der Zielgruppe verankert ist.

Die Verbindung von Desk- und Field-Research erlaubt es uns, das Thema Phishing Awareness aus einer ganzheitlichen Perspektive zu betrachten. Während der Desk Research theoretische Konzepte, Best Practices und Expertenmeinungen liefert, stellt der Field Research sicher, dass diese Erkenntnisse mit den tatsächlichen Bedürfnissen, Wahrnehmungen und Verhaltensweisen unserer Zielgruppe abgeglichen werden. Die Verbindung beider Ansätze verdeutlicht, dass erfolgreiche Awareness-Massnahmen mehrere Dimensionen gleichzeitig berücksichtigen müssen. Die Aspekte Zielgruppenbezug, Relevanz im Alltag, emotionale Ansprache sowie soziale Einbettung sind von entscheidender Bedeutung.

Unsere kombinierte Auswertung haben wir in einer visuellen Übersicht zusammengefasst. Dabei haben wir zentrale Erkenntnisse in folgende Themenbereiche unterteilt: Zielgruppe einbeziehen, Awareness erzeugen, Gesprächsthema schaffen und Emotionen auslösen. Diese Kategorien überschneiden sich teilweise und verdeutlichen so die Komplexität und Verwobenheit erfolgreicher Kommunikationsstrategien.

Zielgruppe einbeziehen:

Aus dem Desk Research geht eindeutig hervor, dass Sicherheitsmassnahmen individualisierbar, kontextsensibel und niederschwellig sein müssen. Dieses Prinzip wurde im Field Research bestätigt. Die Teilnehmenden empfanden Formate wie Kurzvideos, kompakte Informationsformate und Websiten als zugänglich und hilfreich. Auch der Wunsch nach konkreten, handlungsrelevanten Inhalten statt abstrakter Theorie wurde mehrfach geäussert.

Awareness erzeugen:

Die theoretischen Grundlagen aus dem Desk Research betonen, dass Wissen allein nicht ausreicht – entscheidend sind Salienz, Gewohnheit und Verhaltensabsicht. Dies deckt sich mit den Aussagen der Interviewten, die zwar über Phishing informiert sind, ihre Fähigkeiten aber häufig überschätzen.

Gesprächsthema schaffen:

Ein zentrales Ergebnis beider Forschungsstränge ist, dass Informationssicherheit nur dann nachhaltig wirken kann, wenn sie in sozialen Kontexten verankert ist. Aus dem Desk Research wissen wir, dass Peer-Groups als Multiplikatoren wirken können. Im Field Research zeigte sich, dass das Thema Phishing im sozialen Umfeld der Befragten selten aktiv thematisiert wird, obwohl ein hohes Informationsbedürfnis vorhanden ist.

Emotionen auslösen:

Sowohl Desk als auch Field Research betonen die emotionale Dimension des Themas. Während der Desk Research zeigt, wie motivierendes Storytelling, Positivität und Selbstwirksamkeit motivierend wirken, offenbart der Field Research, dass viele Menschen Phishing mit Verwirrung, Angst oder Überforderung verbinden. Dennoch konnten wir beobachten, dass positive emotionale Entwicklungen möglich sind, insbesondere durch empathische Ansprache und greifbare Beispiele.

Ableitung für die Umsetzung:

Aus der Verbindung von Theorie und Praxis ergeben sich klare Leitlinien für die Gestaltung wirksamer Phishing-Awareness-Massnahmen. Zentrale Erfolgsfaktoren sind eine konsequente Ausrichtung an der Lebensrealität der Zielgruppe, die Einbindung emotionaler und sozialer Komponenten sowie eine didaktisch kluge Aufbereitung der Inhalte. Formate sollten niedrigschwellig, visuell ansprechend und handlungsorientiert sein. Das Ziel besteht darin, Awareness nicht als isolierte Informationskampagne, sondern als kontinuierlichen, kulturell eingebetteten Lernprozess zu gestalten. Nur so kann sich ein nachhaltiges Sicherheitsverhalten etablieren.

Abbildung 12: Erkenntniss Clustering. Desk Research: Gelb, Field Research: Orange

06 Sprint 1

Zusammenfassung

Im ersten Sprint wurden basierend auf den Erkenntnissen aus der Researchphase erste konzeptionelle Ideen entwickelt und direkt mit Nutzerfeedback validiert. Zentrale Elemente waren eine strukturierte Ideation-Phase und ein anschliessendes Hallway-Testing. Ziel war es, kreative, aber gleichzeitig fundierte Ansätze zu generieren, die sich an den realen Bedürfnissen und Erwartungen der Zielgruppe orientieren.

Für die Ideation nutzten wir eine eigens entwickelte Methode, bei der durch das zufällige Kombinieren von Research-Erkenntnissen neue Ideenimpulse geschaffen wurden. In zwei Iterationen wurden zunächst auf Basis der ursprünglichen und später einer neu strukturierten Kategorisierung (siehe Abbildung 13 und 14) zahlreiche Ideen entwickelt, geclustert und bewertet (siehe Abbildung 15). Besonders vielversprechend erschienen dabei Konzepte aus den Bereichen Interaktion, Personalisierung und Emotionalisierung. Unter anderem entstand die Idee einer interaktiven Telefonzelle sowie ein Format aus der Hacker-Perspektive.

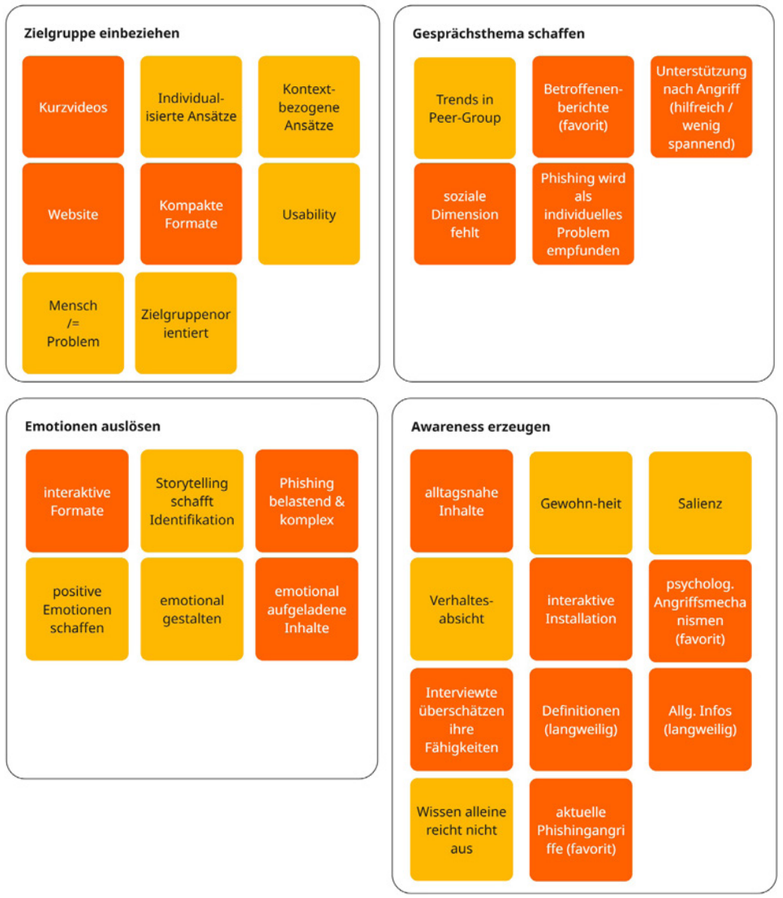
Diese beiden Konzepte wurden in Form von Storyboards (Siehe Abbildung 16 und 17) im Rahmen eines Hallway-Testings mit Studierenden unterschiedlicher Fachrichtungen getestet. Das informelle, qualitative Feedback bestätigte das Potenzial beider Ansätze, zeigte aber auch wichtige Optimierungsmöglichkeiten auf, etwa hinsichtlich Zugänglichkeit und Einstiegsbarrieren. Besonders geschätzt wurden die spielerischen und interaktiven Elemente, die als wirkungsvoll zur Steigerung von Awareness wahrgenommen wurden. Die Ergebnisse flossen direkt in die Weiterentwicklung der Konzepte ein.

Der erste Sprint schloss direkt an die Researchphase an und hatte zum Ziel, basierend auf den gewonnenen Erkenntnisse erste konzeptionelle Ansätze zu entwickeln und diese mithilfe eines schnellen Nutzerfeedbacks zu validieren. Der Sprint bestand aus einer strukturierten Ideation-Phase zur Generierung erster Ideen sowie einem anschliessenden Hallway-Testing, bei dem erste Konzeptansätze auf ihre Desirability und Verständlichkeit überprüft wurden.

06.1 Ideation 1

Für die Ideation setzten wir eine kreative Methode ein, die wir intern als Würfelmethode bezeichneten. Ziel dieser Methode war es, gezielt Erkenntnisse aus dem Research miteinander zu kombinieren, um innovative Ideen zu entwickeln. Dabei wurden die gewonnenen Erkenntnisse aus unterschiedlichen Kategorien zufällig durch einen Würfel ausgewählt und anschliessend miteinander kombiniert. Die zufällige Kombination diente dabei als Impulsgeber für ungewöhnliche, aber dennoch research-basierte Ideen.

Abbildung 13: Erkenntniss Kategorisierung 1



Die Methode wurde in zwei Iterationen durchgeführt. In der ersten Runde orientierten wir uns an den vier zentralen Kategorien, die sich aus der Synthese des Desk- und Field Research ergeben hatten:

Aus jeder dieser Kategorien wurde jeweils eine Erkenntnis gewürfelt und mit den anderen kombiniert, um daraus erste Ideenansätze abzuleiten.

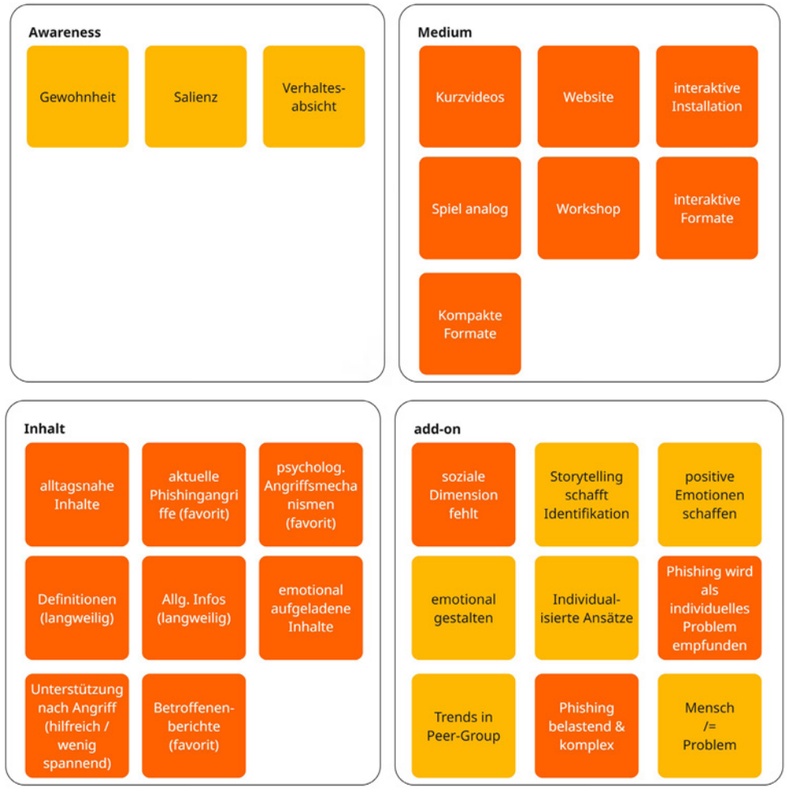
- Zielgruppe einbeziehen
- Awareness erzeugen
- Gesprächsthema schaffen
- Emotionen auslösen

Im zweiten Durchlauf entschieden wir uns für eine Neukategorisierung der Erkenntnisse, um konkretere und vielfältigere Ideen zu ermöglichen. Die neuen Kategorien lauteten:

- Awareness
- Medium
- Inhalt
- Add-ons

Abbildung 14: Erkenntniss Kategorisierung 2

Auch hier wurde pro Ideation-Runde je eine Erkenntnis aus jeder Kategorie gewürfelt und miteinander kombiniert. Diese neue Struktur ermöglichte eine gezieltere Auseinandersetzung mit potenziellen Formaten, Inhalten und Kanälen und führte zu einem breiteren Spektrum an möglichen Lösungsansätzen.



Durch die beiden Iterationen der Ideation-Phase entstand eine grosse Vielfalt an ersten Ideen, die unterschiedliche inhaltliche, mediale und emotionale Ansätze abdeckten. Um ein klareres Verständnis über wiederkehrende Muster und inhaltliche Schwerpunkte zu gewinnen, wurden die Ideen anschliessend geclustert. Dabei entstanden die Überkategorien SOS-Help, Testimonials, Personalisiert, Beispiele, Interaktion, Videos, Hacker-Perspektive sowie spielerisch & humorvoll.

Abbildung 15: Ideation Inhalte Clustering Prozess

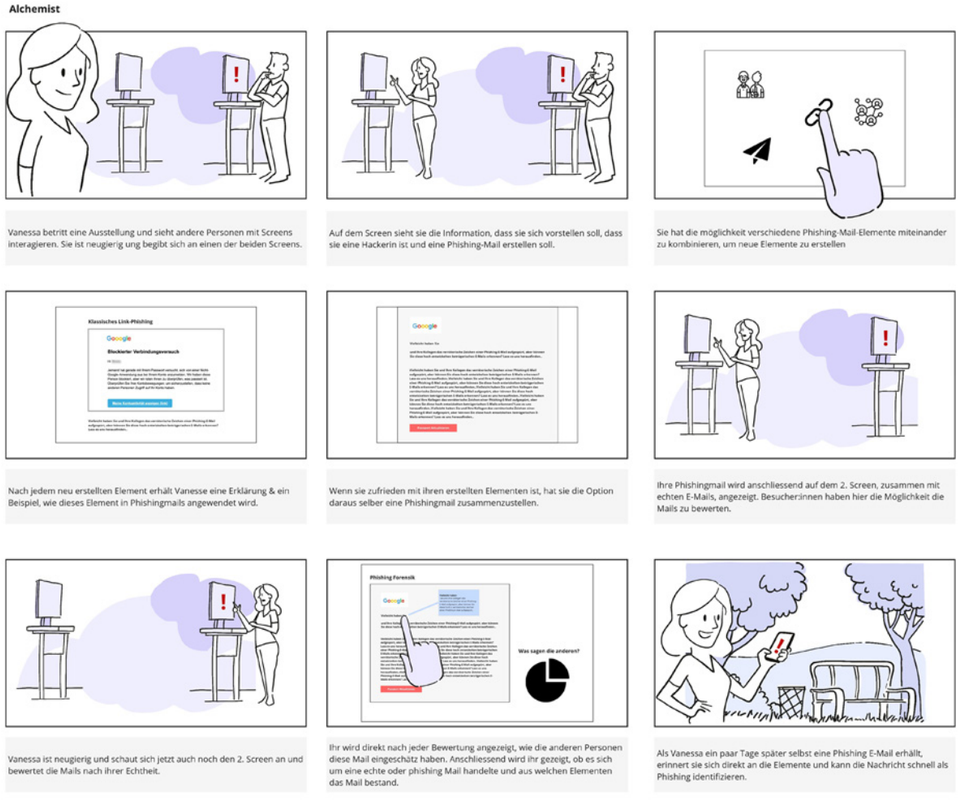
Aus diesen Clustern wählten wir vier Kategorien aus, die im Hinblick auf die Ergebnisse der Researchphase besonders anschlussfähig und vielversprechend erschienen. Auf Basis dieser Gruppen entwickelten wir jeweils eine konkretere Konzeptidee, die wir in einem ersten Schritt informell Mitstudierenden präsentierten. Das qualitative Feedback half uns dabei, die Konzepte weiter zu schärfen und eine fundierte Auswahl zu treffen.

Im Anschluss entschieden wir uns, zwei Ideen vertieft auszuarbeiten. Zum einen die interaktive Telefonzelle, die es möglich macht Geschichten zu Phishing in einem geschützen Rahmen zu hören oder davon zu sprechen, und zum anderen die Hacker-Perspektive, die durch interaktive und spielerische Weise ermöglicht die Merkmale von Phishingmails zu erkennen und selbst eine zu erstellen.

06.2 Hallway-Testing 1

Für beide Konzepte entwickelten wir je ein Storyboard, das den geplanten Ablauf und die Nutzerinteraktion veranschaulicht. Mit diesen Storyboards führten wir ein Hallway-Testing durch, bei dem wir Studierenden beide Konzepte vorlegten und sie um ihre Einschätzung baten – insbesondere in Bezug auf Interesse, Verständlichkeit und thematische Relevanz. Die Studierenden wurden direkt vorort im Hochschulgebäude angesprochen.

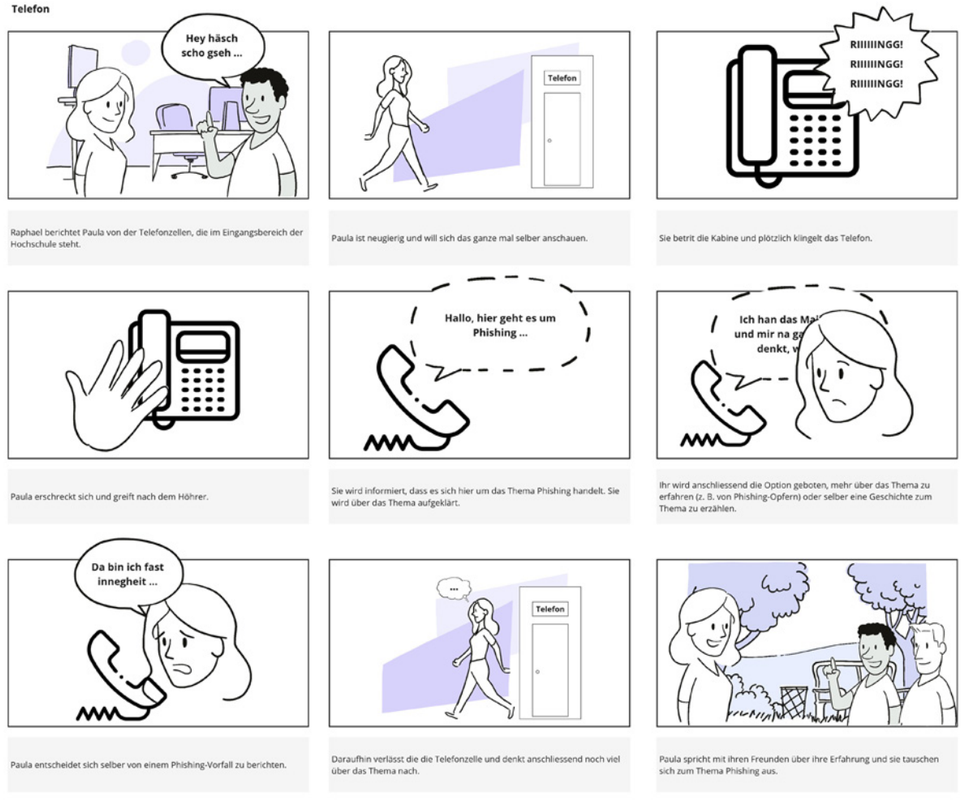
Abbildung 16: Storyboard Hacker-Perspektive



Das Testing wurde mit fünf verschiedenen Personengruppen durchgeführt, bestehend aus jeweils ein bis drei Personen. Die Teilnehmenden kamen aus unterschiedlichen Departments der Hochschule Luzern, darunter Design Film Kunst , Uni/PH sowie das Departement Wirtschaft. Um möglichst spontane und ehrliche Reaktionen zu erhalten, wurden die Studierenden direkt in den Hochschulgebäuden der jeweiligen Departments angesprochen und zur Teilnahme gebeten.

Die Auswertung des Hallway-Testings lieferte wichtige Erkenntnisse für die weitere Konzeptentwicklung. So zeigte sich, dass das Betreten einer Telefonzelle und das tatsächliche Telefonieren für einige Teilnehmende eine gewisse Hemmschwelle darstellte. Gleichzeitig wurde deutlich, dass eine niedrigschwellige, einleitende Interaktion ohne unmittelbaren Handlungsdruck als deutlich zugänglicher wahrgenommen wird. Besonders positiv bewertet wurde die Interaktivität beider Konzepte – sie wurde nicht nur als ansprechendes Element empfunden, sondern auch als wirkungsvoller Faktor zur Förderung von Awareness im Kontext von Phishing. Diese Einsichten flossen direkt in die weitere Ausarbeitung und Verfeinerung der Konzepte ein.

Abbildung 17: Storyboard Telefon



07 Sprint 2

Zusammenfassung

Im zweiten Sprint lag der Fokus auf der inhaltlichen Schärfung und der gezielten Weiterentwicklung des Konzepts. Anstatt erneut zahlreiche Ideen zu generieren, wurden die wichtigsten Erkenntnisse aus dem Hallway-Testing sowie aus einem Gespräch mit der IT-Security-Awareness-Expertin Cornelia Puhze vertieft. Besonders betont wurde dabei die Bedeutung von emotionalem Storytelling, positiven Einstiegen und der Förderung von Achtsamkeit im Umgang mit Phishing.

In der Ideation-Phase wurde bewusst freier gearbeitet. Im Zentrum stand die Frage, wie man das komplexe Thema Phishing für Studierende niederschwellig, humorvoll und wirksam erfahrbar machen kann. Ein entscheidender Impuls war die metaphorische Verbindung von Phishing mit dem klassischen Fischen – eine Analogie, die spielerisch Interesse weckt und gleichzeitig thematisch trägt.

Auf Basis dieser Leitidee wurden vier zentrale Lernziele formuliert:

1. Phishing als systemisches Problem sichtbar machen
2. Vertrauen als Einfallstor verdeutlichen
3. Dringlichkeit als Auslöser für impulsives Handeln entlarven
4. Eine positive, selbstwirksame Haltung fördern

Daraus entstanden vier interaktive Ausstellungsstationen. Darunter eine physische Abstimmung, ein sprechender Fisch, eine Angelruten-Interaktion und eine Wand mit positiven Botschaften zum Mitnehmen. Die Konzepte wurden anhand eines Storyboards (Siehe Abbildung 19) in einem zweiten Hallway-Testing mit Studierenden validiert. Besonders hervorgehoben wurde die kreative Metapher des Fischens, die das Thema greifbarer machte, sowie die spielerischen Elemente, die einen niederschwelligen Zugang ermöglichten. Das Feedback bestätigte den eingeschlagenen Weg und lieferte konkrete Anregungen zur weiteren Ausarbeitung.

«Als Teil von Switch CERT unterstützt sie die Schweizer Bildungs-, Forschungs- und Innovationsgemeinschaft, um den «Faktor Mensch» in der Informationssicherheit wirksam zu adressieren. Gerüstet mit einem MA in Political Communications, erlernte sie ihr Handwerk in Privatwirtschaft, öffentlichem Sektor und NGOs in Zürich und London.» (Quelle: https://www.switch.ch/en/cornelia-puhze)

Der zweite Sprint diente der inhaltlichen Schärfung und Weiterentwicklung unserer bisherigen Arbeit. Im Unterschied zu Sprint 1 stand nicht mehr die Generierung möglichst vieler Ideen im Vordergrund, sondern die Auswahl und Vertiefung jener inhaltlichen Elemente, die aus Nutzersicht das meiste Potenzial versprachen. Dafür wurden die im ersten Sprint entstandenen Ideenkonzepte bewusst zur Seite gelegt, um sich gezielt auf die konkreten Erkenntnisse aus dem Hallway-Testing zu konzentrieren.

Zusätzlich führten wir im Anschluss an Sprint 1 ein Gespräch mit Cornelia Puhze, IT-Security-Awareness-Spezialistin bei Switch CERT. Das Gespräch bestätigte nicht nur zentrale Erkenntnisse aus unserem Desk und Field Research, sondern ergänzte sie um wertvolle Perspektiven aus der professionellen Praxis.

Ein zentrales Thema war die Bedeutung von Storytelling. Durch das Erzählen emotional nachvollziehbarer Geschichten könne eine starke Identifikation mit dem Thema geschaffen werden – ein Ansatz, der besonders hilfreich sei, um abstrakte Sicherheitsrisiken greifbarer zu machen. Darüber hinaus betonte Puhze die Relevanz von positiven Emotionen und Neugierde als Einstiegspunkte. Nur wenn sich Menschen emotional angesprochen fühlen, seien sie auch bereit, sich intensiver mit dem Thema auseinanderzusetzen. Ein weiterer wichtiger Punkt war die Förderung von Achtsamkeit. Ziel müsse es sein, Nutzer:innen vom rein impulsiven, heuristischen Handeln in ein analytisches, bewusstes Denken zu bringen. Dies sei zentral, um nachhaltiges Bewusstsein für Sicherheitsfragen zu schaffen. Schliesslich wies sie darauf hin, dass das Thema Informationssicherheit häufig mit einem Gefühl von Hilflosigkeit verbunden sei. Es sei daher wichtig, zu vermitteln, dass es sich um ein gesamtgesellschaftliches Problem handelt und dass man nicht allein ist.

07.1 Ideation 2

Viele dieser Impulse fanden sich bereits in unseren eigenen Recherchen wieder. Insbesondere die Wichtigkeit von emotionaler Ansprache und Achtsamkeit. Um einen klaren Überblick zu schaffen, wurden alle relevanten Erkenntnisse aus dem Research in einer strukturierten Übersicht zusammengeführt und priorisiert nach ihrer Bedeutung für unsere Zielgruppe.

Abbildung 18: Erkenntniss priorisierung. Desk Research: Gelb, Field Research: Orange

Mit höchster Priorität bewerteten wir das Erzeugen positiver Emotionen durch emotional gestaltete Inhalte, die Integration einer sozialen Dimension, die Entwicklung interaktiver Formate sowie die Schaffung von Salienz – also der Fähigkeit, in einer potenziellen Risikosituation an informationssicherheitskonformes Verhalten zu denken. Als ebenfalls sehr wichtig identifizierten wir den Einsatz von Kurzvideos, Betroffenenberichten sowie narrativen Formaten, die durch Storytelling Identifikation ermöglichen.

Basierend auf dieser Priorisierung, den Erkenntnissen aus dem Gespräch mit Cornelia Puhze sowie den Rückmeldungen aus dem ersten Hallway-Testing entwickelten wir im Rahmen von Ideation 2 weitere Konzeptideen. Anders als in der ersten Ideation-Phase folgten wir dabei keinem expliziten methodischen Vorgehen. Stattdessen arbeiteten wir bewusst freier, diskutierten unterschiedliche Umsetzungsmöglichkeiten und pitchten uns gegenseitig Ideen, um spontan auf Einfälle reagieren und gemeinsam weiterdenken zu können.

Im Zentrum stand dabei die Frage, wie wir das Thema Phishing so gestalten können, dass es für unsere Zielgruppe der Studierenden niedrigschwellig, humorvoll und zugleich wirksam erfahrbar wird. Früh zeichnete sich ab, dass ein direkter Zugang zum Thema Phishing häufig mit einer gewissen inhaltlichen Abwehr oder Überforderung einhergeht. Um diese Hürde zu senken, wurde uns im Verlauf der Ideation 2 klar, dass es eine inhaltliche Brücke braucht – ein narratives oder visuelles Element, das Aufmerksamkeit erzeugt, neugierig macht und den Einstieg erleichtert.

Den entscheidenden Impuls lieferte ein informelles Gespräch mit unserem Mentor Stefan Fraefel, in dem er beiläufig eine Anekdote über das Fischen erzählte. Die sprachliche und thematische Nähe zwischen Phishing und Fischen öffnete für uns eine neue Perspektive. Die Kombination beider Themen versprach genau jene humorvolle, aber inhaltlich tragfähige Verbindung, die wir suchten. Aus dieser Erkenntnis entwickelte sich die zentrale Idee, Phishing über die visuelle und metaphorische Ebene des Fischens zu erzählen – mit einem spielerischen Ton, der sowohl Interesse weckt als auch subtil in das Thema Informationssicherheit einführt.

07.2 Konzeption der Ausstellung

Nachdem wir die zentrale Leitidee entwickelt hatten, Phishing über die visuelle und metaphorische Ebene des Fischens erfahrbar zu machen, stand für uns die inhaltliche Ausgestaltung der Ausstellung im Fokus. Dabei stellte sich zunächst die Frage, welche spezifischen Aspekte des Themas Phishing wir überhaupt vermitteln wollten. Um hier Klarheit zu schaffen, entwickelten wir vier übergeordnete Lernziele, die jeweils eine zentrale Erkenntnis aus unserer Recherche aufgriffen.

1. **Phishing ist ein systemisches Problem.**
   Viele Menschen glauben, dass nur unaufmerksame oder «technisch naive» Personen Opfer von Phishing werden. Dieses Stigma wollten wir aufbrechen, indem wir aufzeigen, dass es sich um ein weit verbreitetes und systemisch bedingtes Problem handelt.
   Methodik: Sichtbarmachen kollektiver Betroffenheit.

2. **Vertrauen ist ein zentrales Einfallstor.**
   Phishing funktioniert oft, weil es den Betrüger:innen gelingt, sich das Vertrauen der Opfer zu erschleichen – sei es über das Design, die Sprache oder die vermeintlichen Absender.
   Methodik: Metaphorische Darstellung von Täuschungsmechanismen.

3. **Dringlichkeit triggert impulsives Handeln.**
   Phishing-Nachrichten zielen häufig darauf ab, Stress oder Zeitdruck auszulösen. Dadurch handeln Menschen weniger bewusst.
   Methodik: Nutzer:innen zur Selbstreflexion und zum Innehalten animieren.

4. **Positive Einstellung fördert nachhaltige Auseinandersetzung.**
   Anstatt mit Angst zu arbeiten, wollten wir durch positive Emotionen eine zugängliche Haltung zum Thema fördern.
   Methodik: Vermittlung positiver Glaubenssätze als mentale Anker.

Im Anschluss daran sammelten wir im Team mögliche Umsetzungsideen für diese vier Lernziele. In einem kreativen Brainstorming skizzierten wir auf Post-its zahlreiche metaphorische und thematische Bezüge zwischen Phishing und dem klassischen Fischen.

Im nächsten Schritt ordneten wir alle gesammelten Ideen systematisch den vier Lernzielen zu – mit Blick auf ihre erwartete Wirksamkeit sowie ihre praktische Umsetzbarkeit. Aus dieser Sortierung kristallisierten sich schliesslich vier interaktive Stationen für die Ausstellung heraus.

1. **Systemisches Problem sichtbar machen**
   Interaktion: Besuchende können physisch abstimmen, ob sie selbst oder jemand in ihrem Umfeld bereits von Phishing betroffen war.
   → Ziel ist es, kollektive Betroffenheit sichtbar zu machen und das Gefühl von Isolation aufzulösen.

2. **Vertrauen als Einfallstor inszenieren**
   Interaktion: Ein sprechender Fisch berichtet von den Ködern, auf die er hereingefallen ist, z. B. Fake-Mails der Schweizer Post oder QR-Code-Betrug bei Parkgebühren.
   → Ziel ist es, Bewusstsein für typische Angriffsmuster zu schaffen, ohne mit dem moralischen Zeigefinger zu agieren.

3. **Dringlichkeit hinterfragen**
   Interaktion: Besuchende nehmen Platz in einem Boot und kurbeln eine Angelrute ein, woraufhin ein Video abgespielt wird. Darin erzählt ein Fischer, dass man beim Fischen vor allem eines brauche: Ruhe und Geduld.
   → Ziel ist es, zur Selbstreflexion anzuregen und impulsives Handeln zu durchbrechen.

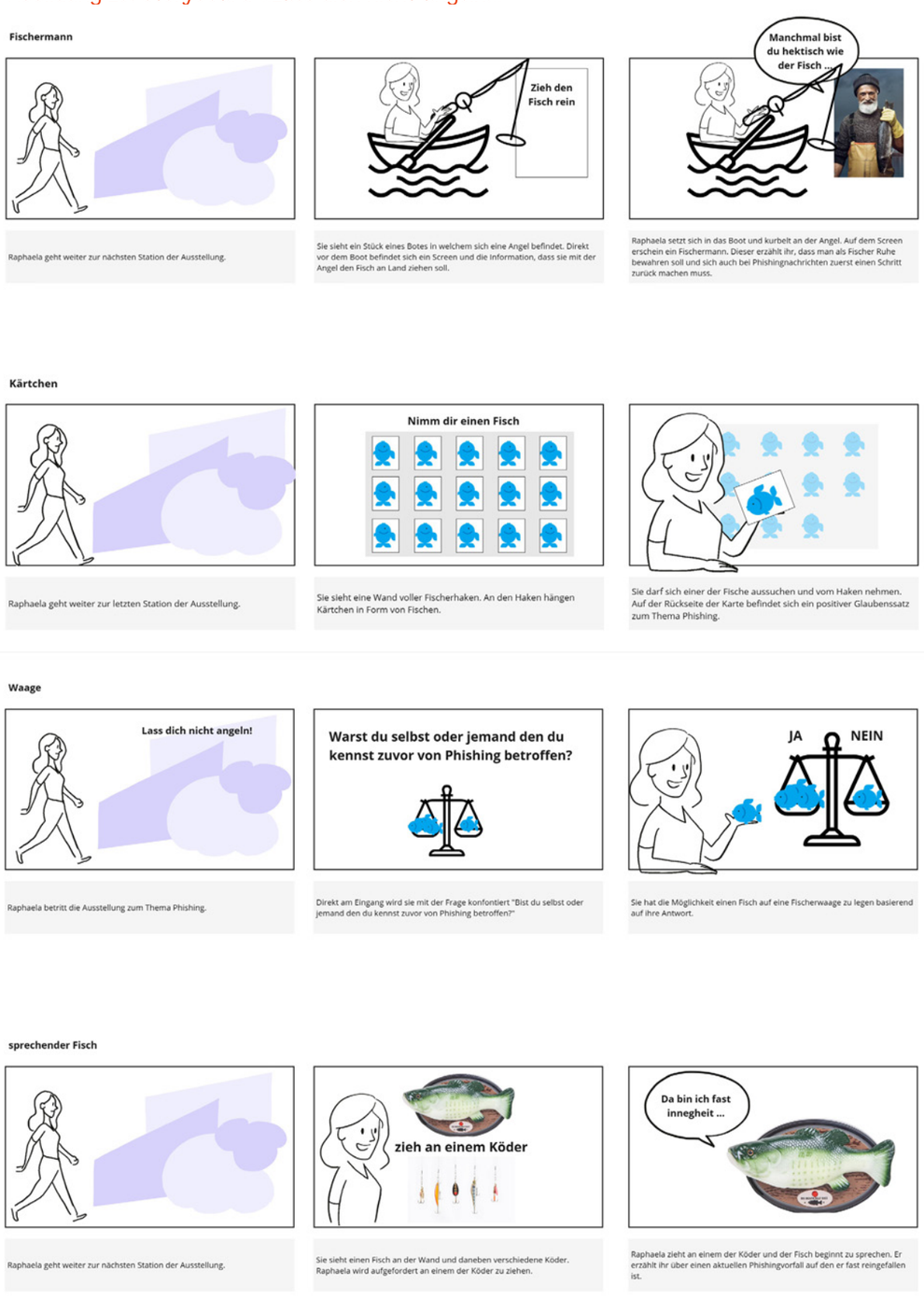
4. **Positive Einstellung fördern**
   Interaktion: Eine Wand mit vielen kleinen Angelhaken, an denen Fische aus Papier hängen. Auf der Rückseite befindet sich jeweils ein positiver Glaubenssatz.
   → Ziel ist es, mit einem kleinen physischen Erinnerungselement eine bestärkende Botschaft mitzugeben.

07.3 Hallway-Testing 2

Alle vier Stationen wurden anschliessend in einem gemeinsamen Storyboard festgehalten und visuell ausgearbeitet (siehe Abbildung 19). Um erste Rückmeldungen aus der Zielgruppe zu erhalten, führten wir daraufhin ein weiteres Hallway-Testing durch. Dafür gingen wir direkt auf Studierende im Gebäude ihres Hochschuldepartements zu und präsentierten ihnen das Storyboard in informellen Kurzinterviews. Insgesamt wurden sieben Personen in drei Kleingruppen befragt. Das Feedback fiel insgesamt sehr positiv aus. Besonders hervorgehoben wurde der sprechende Fisch, der durch seine humorvolle und gleichzeitig aufklärende Art die grösste Aufmerksamkeit auf sich zog. Die metaphorische Verbindung zwischen Phishing und Fischen wurde als verständlich, kreativ und hilfreich empfunden. Sie trug dazu bei, das komplexe Thema zugänglicher zu machen, ohne dabei dessen Ernsthaftigkeit zu untergraben. Auch die interaktiven Elemente der Ausstellung fanden grossen Anklang, da sie das Thema auf spielerische Weise

erlebbar machten. Eine Testperson äusserte darüber hinaus den Wunsch nach konkreteren Handlungsanweisungen oder anschaulichen Beispielen, wie andere mit Phishing-Situationen umgegangen sind. Insgesamt bestätigte das Testing jedoch unseren konzeptionellen Ansatz und gab uns wertvolle Hinweise für die Weiterentwicklung der Stationen.

Abbildung 19: Storyboard «Lass dich nicht angeln!»



08 Umsetzung

Zusammenfassung

Die Umsetzung der Ausstellung folgte den Prinzipien des nutzerzentrierten UX-Designs. Ziel war es, die komplexe Thematik Phishing nicht nur kognitiv zu vermitteln, sondern durch emotional ansprechende, interaktive Elemente erfahrbar zu machen. Jede Station der Ausstellung trägt dabei ein spezifisches Lernziel, ist aber zugleich Teil einer übergeordneten Erzählung, die Besucher:innen spielerisch und ohne Druck ins Thema einführt.

Station 1: Systematisches Problem sichtbar machen

Statt auf Zahlen oder Schaubilder setzte die erste Station auf eine kollektive Geste. Besucher:innen hängen Holzfische an ein echtes Fischernetz – orange, wenn sie selbst betroffen waren, blau, wenn es jemanden aus ihrem Umfeld traf. So entsteht über die Zeit ein wachsendes, physisches Abbild der Betroffenheit, das das systemische Ausmass von Phishing emotional greifbar macht. (Siehe Abbildung 22 – 24)

Infostation 1: Was ist Phishing?

Diese Infostation dient als inhaltliche Grundlage und erklärt kompakt, was Phishing ist, wie es funktioniert und warum es so weit verbreitet ist. Damit schafft sie einen niedrigschwelligen Einstieg und ermöglicht es allen Besuchenden, unabhängig vom Vorwissen, die anschliessenden Stationen besser einzuordnen. (Siehe Abbildung 25)

Station 2: Vertrauen als Einfallstor inszenieren

Im Zentrum dieser Station steht Phishilla, ein sprechender Fisch, der über verschiedene Phishing-Angriffe berichtet. Ausgelöst durch NFC-versehene Köder erzählt sie auf unterhaltsame Weise Geschichten aus ihrem Freundeskreis, die reale Angriffsformen wie E-Mail-, SMS- oder QR-Code-Phishing thematisieren. Die technische Umsetzung erfolgte durch die Modifikation eines Big Mouth Billy Bass, der nun statt Liedern personalisierte Audiospuren abspielt. Humor, Nahbarkeit und Storytelling machen diese Station besonders zugänglich trotz inhaltlicher Tiefe. (Siehe Abbildung 26 – 30)

Station 3: Dringlichkeit hinterfragen

Diese Station thematisiert das psychologische Prinzip künstlicher Dringlichkeit, das häufig in Phishing-Angriffen genutzt wird. Anstelle einer erklärenden Ansprache konfrontiert sie die Besuchenden mit einem stillen Video. Ein Hecht schwimmt zögerlich um einen Köder, begleitet von beruhigenden Audioimpulsen, die zum Innehalten anregen. Die Station vermittelt Achtsamkeit nicht nur als Konzept, sondern als direkte Erfahrung – durch Verlangsamung, Stille und subtile Spannung. (Siehe Abbildung 31 – 34)

Infostation 2: Mehr als Wissen?

Die zweite Infostation öffnet den Raum für Reflexion. Reicht Wissen allein, um sich vor Phishing zu schützen? Die Antwort bleibt bewusst offen. Statt moralischer Belehrung betont die Station die Rolle von Haltung, Selbstvertrauen und sozialem Austausch und macht deutlich, dass auch das Hereinfallen auf eine Phishing-Attacke kein persönliches Scheitern, sondern ein Lernanlass ist. (Siehe Abbildung 35)

Station 4: Positive Einstellung fördern

Zum Abschluss lädt die Ausstellung dazu ein, sich selbst bewusst «ködern» zu lassenn, allerdings mit positiver Absicht. Besucher:innen wählen aus einer Vielzahl an Köderkarten, auf deren Rückseiten ermutigende Glaubenssätze zum Thema Informationssicherheit stehen. Diese Kärtchen, im Riso-Druck gestaltet, dienen als mentale Anker für den digitalen Alltag. Die letzte Station schliesst die Ausstellung mit einer stärkenden Botschaft ab – selbstwirksam, humorvoll und nachhaltig in Erinnerung bleibend. (Siehe Abbildung 36 – 38)

Die Ausstellung wurde auf Grundlage der Erkenntnisse aus dem nutzerzentrierten UX-Prozess entwickelt. Dabei war es uns wichtig, die vielschichtigen Aspekte von Phishing nicht nur informativ, sondern auch erfahrbar zu machen. Jede Station verfolgt ein eigenes Ziel, ist aber Teil einer gemeinsamen Erzählung. Die Besuchenden sollen nicht nur Wissen aufnehmen, sondern sich emotional und spielerisch mit dem Thema auseinandersetzen, ohne Druck, aber mit Wirkung. In den folgenden Abschnitten wird beschrieben, wie die einzelnen Stationen konkret umgesetzt wurden und wie sie funktionieren.

Die Ausstellung wurde auf Grundlage der Erkenntnisse aus dem nutzerzentrierten UX-Prozess entwickelt. Dabei war es uns wichtig, die vielschichtigen Aspekte von Phishing nicht nur informativ, sondern auch erfahrbar zu machen. Jede Station verfolgt ein eigenes Ziel, ist aber Teil einer gemeinsamen Erzählung. Die Besuchenden sollen nicht nur Wissen aufnehmen, sondern sich emotional und spielerisch mit dem Thema auseinandersetzen, ohne Druck, aber mit Wirkung. In den folgenden Abschnitten wird beschrieben, wie die einzelnen Stationen konkret umgesetzt wurden und wie sie funktionieren.

Abbildung 20: Ausstellungsplan (Wand Links und Wand Mitte)

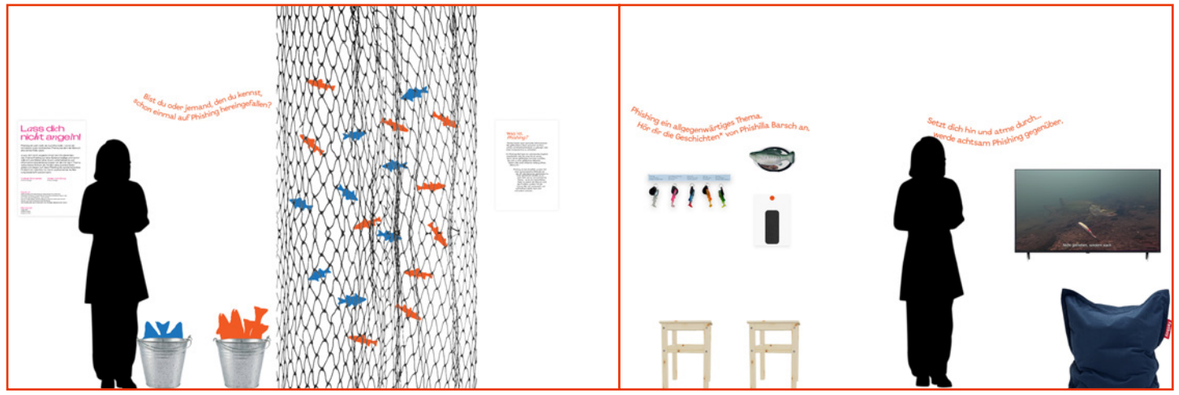
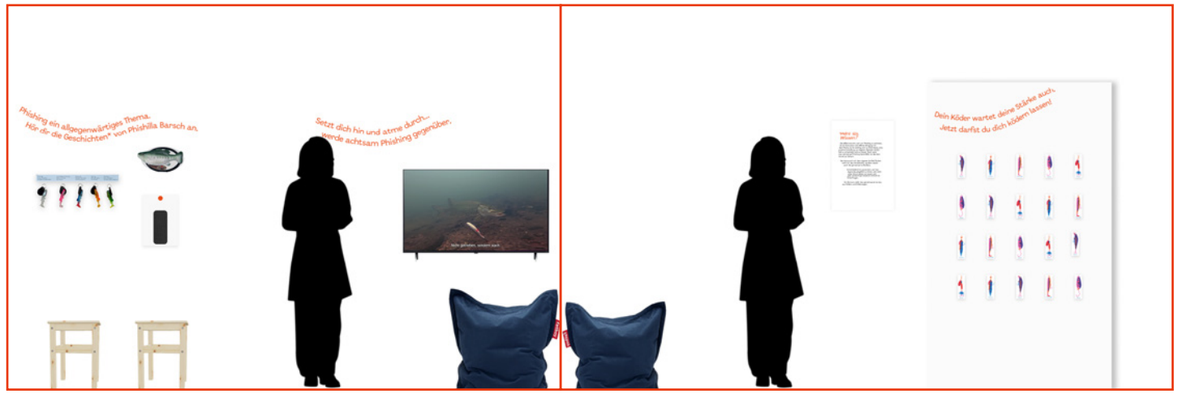


Abbildung 21: Ausstellungsplan (Wand Mitte und Wand Rechts)



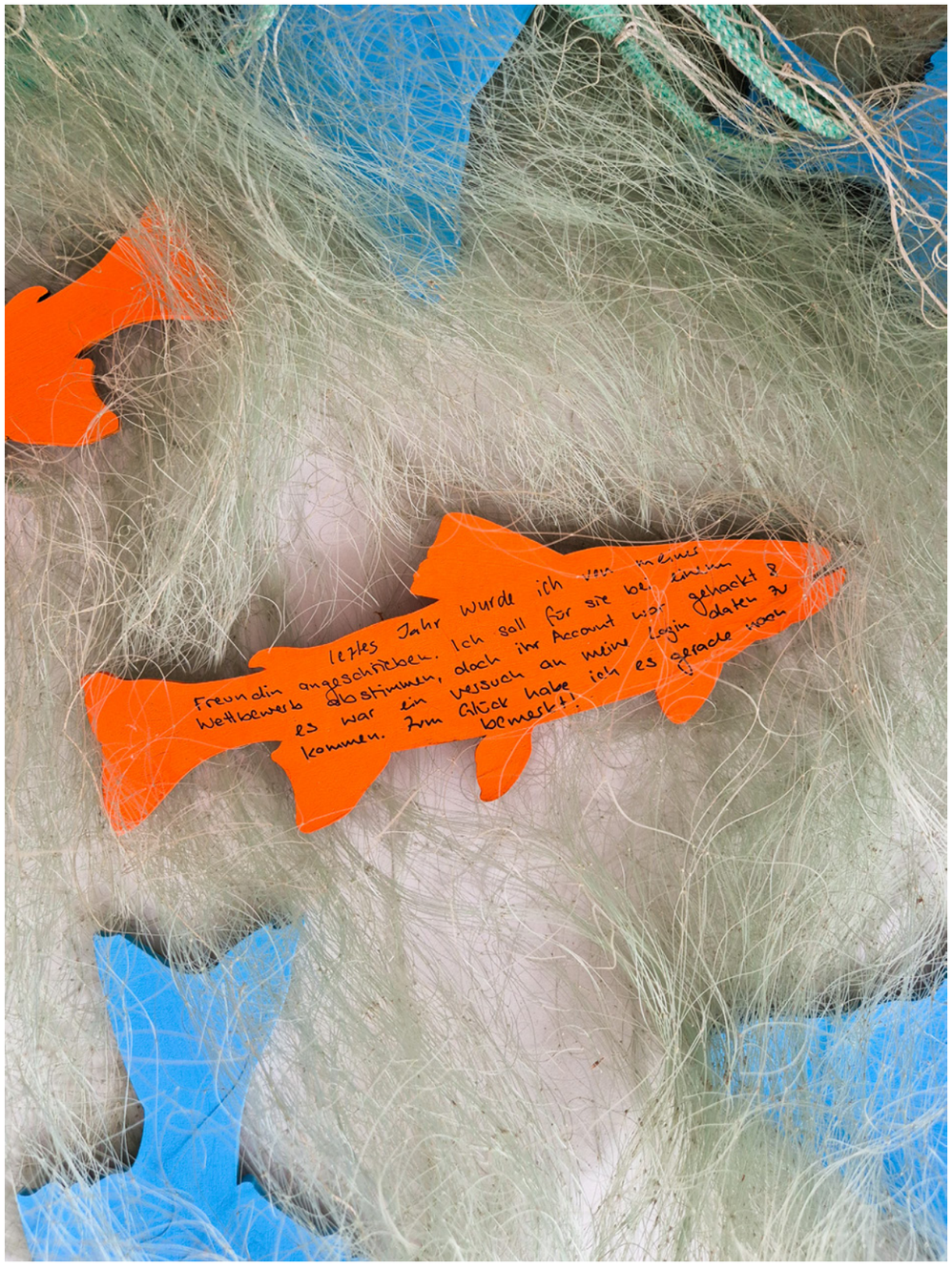
08.1 Station 1: Systemisches Problem sichtbar machen

Für die erste Station der Ausstellung entschieden wir uns, das systemische Ausmass von Phishing nicht über ein digitales oder statistisches Element, sondern durch eine kollektive, physische Geste der Besuchenden erfahrbar zu machen. Statt der zunächst angedachten Umsetzung mittels einer Waage, fiel die Wahl schliesslich auf ein grossflächiges Fischernetz als zentrales Gestaltungselement. Dieses Netz symbolisiert nicht nur das Motiv des Fangens, sondern steht auch sinnbildlich für die Vielzahl und Gleichzeitigkeit von Betroffenheiten im Kontext von Phishing.

Abbildung 22: Fische im Netz

Das Fischernetz selbst wurde uns freundlicherweise vom Berufsfischer Lui zur Verfügung gestellt, der am Eierhals Hotel und Restaurant tätig ist und mit seiner Unterstützung zur Authentizität der Installation beitrug.

Abbildung 23: Phishing-Geschichte auf Fisch



Die Besuchenden haben an dieser Station die Möglichkeit, einen kleinen Holzfisch auszuwählen und diesen ins Netz zu hängen. Dabei stehen zwei unterschiedliche Fischformen zur Verfügung, die jeweils eine bestimmte Art der Betroffenheit visualisieren. Ein orangefarbener Zander steht dafür, dass man selbst bereits Phishing erlebt hat. Ein blauer Egli hingegen symbolisiert, dass jemand aus dem eigenen Umfeld betroffen war. Beide Fischarten wurden mithilfe eines Lasercutters aus

Holz gefertigt und ermöglichen es den Teilnehmenden, direkt auf den Fisch ihr persönliches Erlebnis mit Phishing zu notieren – sei es eine kurze Anekdote, ein Stichwort oder eine Erfahrung.

Abbildung 24: Blau Egli (jemandes anderes Betroffen), Orange Zander (selbst Betroffen)

Durch das fortlaufende Anbringen weiterer Fische entsteht im Verlauf der Ausstellung ein wachsendes, visuell eindrucksvolles Gesamtbild, das die Verbreitung von Phishing greifbar macht. Die Idee hinter dieser Interaktion ist es, auf subtile, aber einprägsame Weise zu vermitteln, dass Phishing kein isoliertes Einzelphänomen ist, sondern viele Menschen betrifft – direkt oder indirekt.

08.2 Infostation 1: Was ist Phishing?

Diese erste von zwei Infostationen bildet einen wichtigen Orientierungspunkt innerhalb der Ausstellung. Sie verfolgt das Ziel, allen Besuchenden eine gemeinsame inhaltliche Grundlage zu bieten, indem sie in kompakter Form erklärt, was Phishing ist, wie es funktioniert und weshalb es so verbreitet ist. Da sich unsere Ausstellung nicht nur an Personen mit Vorwissen richtet, sondern möglichst niedrigschwellig gestaltet sein soll, war es uns wichtig, zentrale Begriffe und Mechanismen verständlich zu erläutern. Die Infostation schafft damit einen informativen Rahmen, in dem die nachfolgenden interaktiven Stationen besser eingeordnet und reflektiert werden können. Sie macht deutlich, dass Phishing kein technisches Randthema ist, sondern uns alle betrifft und gerade deshalb lohnt es sich, genauer hinzusehen.

Abbildung 25: Infotafel – Was ist Phishing?

08.3 Station 2: Vertrauen als Einfallstor inszenieren

An der zweiten Station der Ausstellung erwartet die Besuchenden ein sprechender Fisch namens Phishilla, der auf charmante und humorvolle Weise von verschiedenen Phishing-Vorfällen erzählt. Ziel dieser Station ist es, das Thema Vertrauen als zentrales Einfallstor für Angriffe zu thematisieren ohne abschreckend zu wirken oder Angst zu erzeugen. Stattdessen setzen wir auf eine humorvolle Erzählweise, die Identifikation ermöglicht und die Aufmerksamkeit der Besuchenden auf subtile Weise lenkt.

Abbildung 26: Interaktion Phishilla und Köder

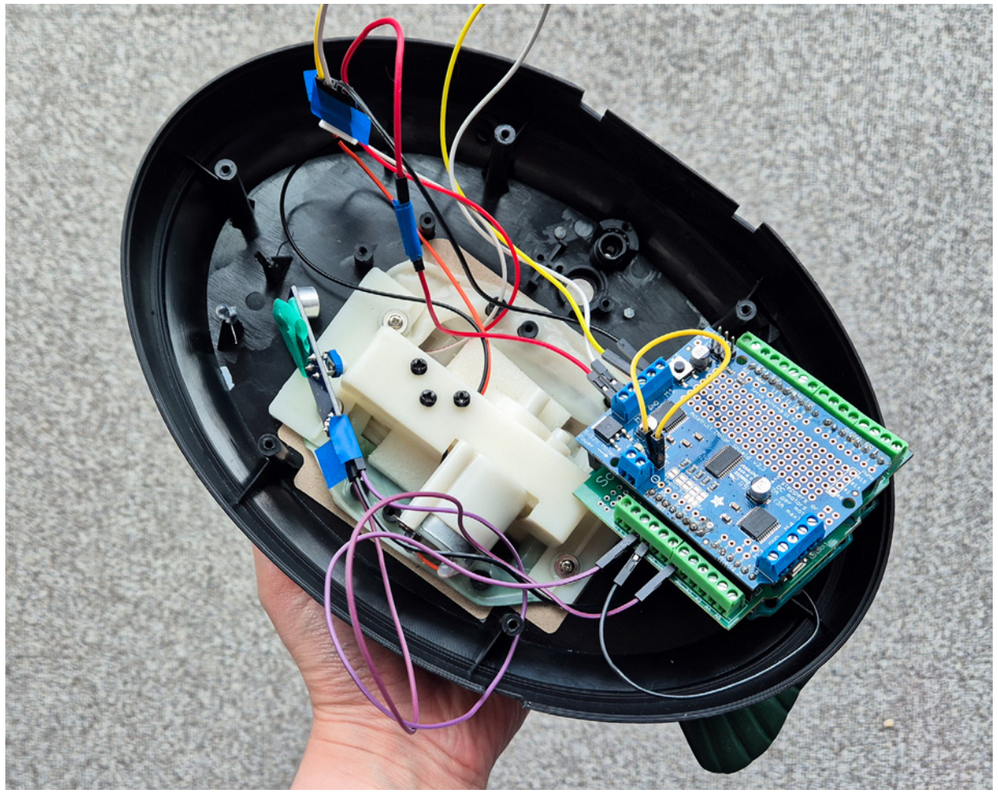
Die Interaktion funktioniert über fünf Köder, die an einer Wand befestigt sind und jeweils mit einem NFC-Tag ausgestattet wurden. Besuchende können einen Köder auswählen und an einen Sensor halten. In diesem Moment beginnt Phishilla zu sprechen und erzählt die zur Köder passende Geschichten, in der sie schildert, wie jeweils ein Freund oder eine Freundin von ihr auf einen Phishing-Angriff hereingefallen ist. Die Geschichten decken unterschiedliche Angriffsformen ab, darunter klassisches Phishing (E-Mail), Smishing (SMS), Quishing (QR-Code), Vishing (Telefonanruf) und Social Media Phishing.

Abbildung 27: Köder und Phishing-Angriffe

Abbildung 28: Köder und NFC-TAG

Abbildung 29: Big Mouth Billy Bass – Phishilla

Abbildung 30: Umbau des Big Mouth Billy Bass mittels Arduino



Die Erzählungen sind inspiriert von echten, aktuellen Vorfällen, wurden aber so überarbeitet, dass sie nahbar und verständlich bleiben. Durch die fischtypische Sprache und Erzählweise entsteht der Eindruck, als würde Phishilla tatsächlich aus eigener Erfahrung berichten, was der Station eine unterhaltsame, fast schon theatralische Qualität verleiht. Wichtig war uns dabei, dass die Inhalte trotz des spielerischen Rahmens ernst genommen werden können. Die Besuchenden sollen erkennen, wie gezielt Vertrauen missbraucht wird, ohne sich dabei belehrt oder verunsichert zu fühlen.

Technisch basiert die Installation auf einem umgebauten Big Mouth Billy Bass – einer elektronischen Wanddeko, die ursprünglich Lieder abspielte. Mithilfe eines Arduino-Boards und Sensoren haben wir Phishilla so modifiziert, dass sie statt Musik nun unsere Audiospuren abspielt, sobald ein Köder erkannt wird.

08.4 Station 3: Dringlichkeit hinterfragen

Diese Station widmet sich dem psychologischen Mechanismus der künstlich erzeugten Dringlichkeit – einer häufig eingesetzten Taktik bei Phishing-Angriffen. Ziel war es, den Besuchenden bewusst zu machen, wie stark Impulsreaktionen gesteuert werden und wie wichtig es ist, in solchen Momenten innezuhalten und vom schnellen, heuristischen Denken in ein bewusstes, analytisches Denken zu wechseln.

Abbildung 31: Still aus Video «Dringlichkeit hinterfragen»

Ursprünglich war geplant, ein Video zu zeigen, in dem ein Fischer die Besuchenden direkt anspricht und ihnen erklärt, dass man beim Fischen Ruhe bewahren muss, im Gegensatz zum hektischen Verhalten des Fisches. Im Verlauf des Gestaltungsprozesses entschieden wir uns jedoch für einen erfahrungsbasierten, subtileren Zugang. Statt einer direkten Erklärung haben wir ein atmosphärisch ruhiges Video entwickelt, das gezielt mit der inneren Unruhe der Besuchenden spielt.

Im Video ist ein Hecht zu sehen, der immer wieder um einen Köder herumschwimmt, kurz davor ist, ihn zu schnappen und sich dann doch wieder abwendet. Diese visuelle Spannung erzeugt ein Gefühl von Erwartung und Nervosität. Begleitend dazu werden in regelmässigen Abständen kurze Audiospuren eingespielt, in denen eine Stimme daran erinnert, ruhig zu bleiben, nicht sofort auf Reize zu reagieren und digitale Nachrichten ebenso mit Distanz zu betrachten. Die Botschaft ist klar: Atmen, beobachten, einen Schritt zurück machen.

Abbildung 32: Set-up der Video-Station

Abbildung 33: Still aus Video «Dringlichkeit hinterfragen»

Durch diese Inszenierung wird das zentrale Lernziel nicht nur erklärt, sondern direkt erfahrbar gemacht. Die Besuchenden müssen sich auf das ruhige Tempo des Videos einlassen und lernen dadurch intuitiv, wie sich ein Perspektivwechsel anfühlen kann. Die Station fordert damit nicht nur kognitiv, sondern auch emotional heraus. Sie veranschaulicht das Prinzip der Achtsamkeit durch das Medium selbst.

Abbildung 34: Still aus Video «Dringlichkeit hinterfragen»

08.5 Infostation 2: Mehr als Wissen?

Diese zweite Infostation ergänzt die erste grundlegende Einführung in das Thema Phishing. Während dort erklärt wird, was Phishing ist und wie es funktioniert, greift diese Station die Frage auf, ob Wissen allein ausreicht – und beantwortet sie bewusst nicht abschliessend. Der Titel «Mehr als Wissen?» ist dabei nicht nur eine thematische Fortsetzung, sondern lädt auch zur Selbstreflexion ein.

Abbildung 35: Infotafel – Mehr als Wissen?

Im Zentrum steht die Erkenntnis, dass Informationssicherheit nicht nur eine Frage von Faktenwissen ist, sondern ebenso von Haltung, Austausch und Selbstwahrnehmung. Die Inhalte dieser Station sollen Besuchende darin bestärken, dass es beim Schutz vor Phishing auch um emotionale Kompetenz, soziale Offenheit und ein gesundes Mass an Selbstvertrauen geht.

Statt mit erhobenem Zeigefinger vermittelt der Text, dass auch ein Fehlverhalten – wie das Hereinfallen auf eine Phishing-Nachricht, kein persönliches Versagen ist, sondern ein Anlass, um darüber zu sprechen und voneinander zu

lernen. Diese Haltung zieht sich als roter Faden durch die gesamte Ausstellung und findet hier einen klaren, ermutigenden Ausdruck. Die Infostation bildet damit einen ruhigen Reflexionsmoment und schliesst den Bogen vom reinen Wissen hin zu einem umfassenderen Sicherheitsverständnis.

08.6 Station 4: Positive Einstellung fördern

Am Ende der Ausstellung werden die Besuchenden noch einmal aktiv. Dieses Mal sollen sie sich ganz bewusst «ködern» lassen, allerdings im positiven Sinn. An dieser Station treffen sie auf eine Wand, an der verschiedene Kärtchen hängen, auf denen typische Fischköder abgebildet sind. Auf der Rückseite jedes Kärtchens verbirgt sich ein positiver Glaubenssatz, der sich auf den Umgang mit Phishing bezieht.

Ursprünglich war geplant, dass die Besuchenden zwischen verschiedenen Fischen wählen. Doch da sie sich durch die gesamte Ausstellung hindurch aus der Perspektive des Fisches mit dem Thema auseinandergesetzt haben, erschien es passender, am Ende nicht die Rollen zu drehen. Nun dürfen sie selbst entscheiden, welchem Köder sie sich freiwillig nähern und nehmen dabei ein symbolisches Stück Kontrolle mit nach Hause.

Abbildung 36: Köder-Karten

Jeder Glaubenssatz wurde so formuliert, dass er das Vertrauen in die eigene Handlungskompetenz stärkt und im digitalen Alltag als mentale Erinnerung an die Ausstellung dienen kann. Die Kärtchen ermutigen dazu, ruhig, aufmerksam und selbstbewusst mit digitalen Reizen umzugehen – auch in Momenten, in denen es darauf ankommt, innezuhalten und genau hinzusehen.

Abbildung 37: Köder-Karten mit jeweiligem Glaubenssatz

Die Kärtchen, die im Riso-Druckverfahren hergestellt wurden, dienen nicht nur als Erinnerungsstück, sondern sollen auch langfristig zur Salienz beitragen. Wenn man das Kärtchen aufbewahrt, ruft es im entscheidenden Moment das Thema Phishing erneut ins Bewusstsein. Auf diese Weise wird die Ausstellung mit einer positiven, stärkenden Botschaft abgeschlossen.

Abbildung 38: Köder-Karten mittels Riso-Druck

09 Schlusswort

Phishing Awareness ist ein sogenanntes «Wicked Problem». Eine komplexe Herausforderung, für die es keine eindeutige oder allgemeingültige Lösung gibt. Das Verhalten der Menschen, die ständige Weiterentwicklung von Angriffsmethoden und die emotionale Dimension des Themas machen deutlich, dass es mehr als technische Antworten braucht, um einen wirksamen Schutz zu ermöglichen.

Mit unserem nutzerzentrierten UX-Ansatz haben wir versucht, dieser Komplexität gerecht zu werden. Durch iterative Tests, echtes Nutzerfeedback und konsequent Human-Centered Design sind wir einer Lösung nähergekommen, die Menschen nicht nur informiert, sondern emotional abholt, aktiviert und stärkt. Gerade bei einem Thema wie Phishing ist es entscheidend, den Menschen nicht als Schwachstelle zu betrachten, sondern als aktiven Teil der Lösung.

Die tatsächliche Wirksamkeit unserer Ausstellung konnten wir im Rahmen dieser Arbeit nur in begrenztem Umfang untersuchen. Umso spannender wäre es, in einer weiterführenden Arbeit systematisch zu erforschen, ob und inwiefern sich das digitale Verhalten der Besuchenden nach dem Ausstellungsbesuch tatsächlich verändert und welche Faktoren dabei eine besonders grosse Rolle spielen.

10 Quellen

Anti-Phishing Working Group. (2024). Phishing Activity Trends Report, 3th Quarter 2024. https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf

Beaudet-Labrecque, O., Augsburger-Bucheli, I., & Brunoni, L. (2023). Finanzieller Missbrauch bei Personen.

BFS. (2024). Digitale Kriminalität: Modi Operandi der digitalen Kriminalität und geschädigte Personen - 2020-2023 | Tabelle. Digitale Kriminalität: Modi Operandi der digitalen Kriminalität und geschädigte Personen - 2020-2023 | Tabelle. https://www.bfs.admin.ch/asset/de/30887709

Bundesamt für Sicherheit in der Informationstechnik. (2022). Die Lage der IT-Sicherheit in Deutschland 2022.

Dörlemann, K., & Beyer, M. (2020, November 25). Warum ist das alles so kompliziert? [Audio recording]. https://open.spotify.com/episode/0EzW7vg38TxsPshHkAozHl

Dörlemann, K., Beyer, M., & Bernecker, Dr. K. (2021, Mai 26). Motivationspsychologie—Zu sicherem Verhalten motivieren [Audio recording]. https://open.spotify.com/episode/7C9q7tEHgLIXVSE6wF46fD

Dörlemann, K., Beyer, M., & Büchs, J. (2025, März 26). Tabus und Überraschungen—Storytelling mit Johannes Büchs [Audio recording]. https://open.spotify.com/episode/5GXMBDDje8L2ZqY5krehqo

Dörlemann, K., Beyer, M., & Hofmann, T. (2021, November 24). Kompliziert vs. Komplex—Human Centred Design für Security [Audio recording]. https://open.spotify.com/episode/4LIk6XHYwPw170wtUkQiT1

Dörlemann, K., Beyer, M., & Volkamer, Dr. M. (2022, Februar 23). Phishing-Training—Von Sinn und Unsinn der Tests und Simulationen [Audio recording]. https://open.spotify.com/episode/0SKx48LSeLPUPmNKAjtDsF

Ebert, Dr. N., & Zimmermann, Dr. V. (2024, November 1). Learning from Safety Science: Perspectives on Incidents and the Human Factor in Cybersecurity. Swiss Security Awareness Day 2024.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Weber, Dr. K. (2024, November 1). Give me the figures! Measuring Security Awareness. Swiss Security Awareness Day 2024.

Weber, K. (2024). Mensch und Informationssicherheit – Verhalten verstehen, Awareness fördern, Human Hacking erkennen.

Yasin, A., Fatima, R., Wen, L., JiangBin, Z., & Niazi, M. (2025). What goes wrong during phishing education? A probe into a game-based assessment with unfavorable results. Entertainment Computing, 52, 100815. https://doi.org/10.1016/j.entcom.2024.100815

Praktische Bachelorarbeit 2025
Digital Ideation Hochschule Luzern

Valérie Schneider
valerieschneider@proton.me

Vivien von Burg
vivien.vonburg@outlook.ch