InforMiert: Informationssicherheit von Arbeitnehmer*innen mit Migrationsgeschichte stärken

InforMiert

Workshopmaterialien - Deutsch

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

ORIENTEXPRESS

GEFÖRDERT DURCH
Digifonds
AK WIEN

Einleitung

Liebe Leser:innen,

die folgenden Workshopunterlagen sind im Rahmen des Projekts *InforMiert: Informationssicherheit von Arbeitnehmer*innen mit Migrationsgeschichte stärken* entstanden. *InforMiert* wurde von März 2023 bis Februar 2025 von den beiden Projektpartnern Orient Express - Beratungs- Bildungs- und Kulturinitiative für Frauen und der OCG (Österreichische Computer Gesellschaft) durchgeführt und durch den Digifonds der Arbeiterkammer Wien gefördert.

Das Projekt entwickelt niederschwellige Angebote rund um das Thema Informationssicherheit (Cybersecurity) für Frauen mit Migrations- oder Fluchtgeschichte. Eine wesentliche Zielsetzung besteht darin, ein Grundverständnis für digitale Prozesse – und nicht nur einzelne Anwendungen – zu fördern und somit eine Grundlage für digitale Resilienz und Souveränität zu schaffen.

Zum Auftakt der Projekttätigkeit wurde ein fachlicher Austausch zwischen den beiden Kooperationspartnern Orient Express und der Österreichischen Computer Gesellschaft (OCG) vorbereitet und durchgeführt. Im Rahmen dieses inhaltlichen Kick-Off-Workshops ging es darum, grundlegende und zielgruppengerechte Vermittlungsaspekte rund um das Bewusstsein für Informationssicherheit/Cybersecurity und digitale Resilienz zu thematisieren. Während der Projektkoordinator Orient Express Erfahrung in der Bildungs- und Beratungsarbeit einbrachte, ergänzte die OCG die Ergebnisse mit ihrer umfangreichen digitalen Fachexpertise.

Dieser Wissenstransfer fand darauffolgend in intensivierter Form, nämlich einer mehrtägigen fundierten Train-the-Trainer-Schulung statt, in deren Rahmen Projektmitarbeiter:innen, Kursleitende und Berater:innen ihr Wissen zu den Schwerpunktthemen des Projekts ausbauen konnten. Die Teilnehmenden erhielten eine Ausbildung inklusive der Möglichkeit einer Zertifizierung für den Bereich Cybersecurity. Dadurch wurden die Teilnehmenden befähigt, im Zuge von Coaching-, Bildungs- und Mentoringprozessen das Thema Cybersecurity zielgruppengerecht vermitteln zu können.

Zum einen sollte durch die Train-the-Trainer Schulung ein Überblick und ein Bewusstsein für alle Aspekte von Cybersecurity aus der Sicht der Endbenutzer:innen im persönlichen, beruflichen und gesellschaftlichen Kontext vermittelt werden. Zum anderen wurde im Zuge der Schulung aber auch bereits mit den Teilnehmenden und den

Expert:innen der OCG gemeinsam an Konzepten zur Vermittlung der Inhalte an die primäre Zielgruppe (bildungsbenachteiligte Frauen mit Migrationsgeschichte) gearbeitet.

Eine weitere Projektaktivität war die Abhaltung von zwei Fokusgruppen mit Frauen mit Migrations- oder Fluchtgeschichte, die entsprechend dem Bedarf auf Arabisch und Türkisch stattfanden. Hierbei wurden Themen herausgearbeitet, die für die Teilnehmenden besonders relevant sind. Die Ergebnisse aus diesen Fokusgruppen wurden übersetzt und für die weitere Bearbeitung protokolliert und dokumentiert.

In einem nächsten Schritt wurden, aufbauend auf den Fokusgruppenergebnissen und der Train-the-Trainer-Schulung, die Inhalte der Workshops zielgruppengerecht vorbereitet und vermittelt.

Die vorliegenden Workshop-Materialien sind somit das Ergebnis eines intensiven und partizipativen Entwicklungsprozesses, bei dem versucht wurde, die Bedürfnisse der Zielgruppe zu berücksichtigen. Ein Hauptaugenmerk der Materialien liegt auf der einfachen und niederschwelligen Vermittlung der Inhalte und dem Herunterbrechen komplexer Sachverhalte aus der Welt der digitalen Sicherheit.

Auf den folgenden Seiten finden Sie Materialien, die Sie etwa für den modularen Einsatz in Basisbildungskursen oder in anderen Formaten der Erwachsenenbildung, die sich an Menschen mit nicht-deutscher Erstsprache richten, nutzen können. Bei der Verwendung der Workshop-Materialien können einzelne Aspekte herausgegriffen werden, die nicht der Reihenfolge in diesem Dokument entsprechen. Dementsprechend müssen die Workshop-Materialien nicht als Gesamtpaket eingesetzt werden. Der modulare Einsatz der Materialien ermöglicht eine Flexibilität, die für die Arbeit mit der Zielgruppe notwendig und sinnvoll ist.

Wir wünschen viel Erfolg beim Einsatz der Workshop-Materialien!

Ablaufplan Workshop

Kurzbezeichnung	Thema	Sozialform	Material	Zeit (in Min.)
1. Einstieg (Seite 1)	1.1 Begrüßung und Vorstellungsrunde 1.2 Einstieg 1.3 Vorerfahrungen, Assoziationen zu dem Schlagwort „Cyber-Sicherheit“	Plenum	1.4 Flipchart (für Mindmap)	10 bis 15
2. Haus-Metapher (Seiten 2-4)	2.1 Wie schützen wir unsere Wertgegenstände? (z.B. Haus, Handtasche) 2.2 Daten & Zugänge sind wie Wertsachen 2.3 Plenum: Parallele: Cyber-Sicherheit	2.1 Kleingruppen & Plenum 2.2. + 2.3 Plenum	2.1 Bilder, kleine Zettel 2.2 Wort-Streifen 2.3 Beamer, PPT	10 10 10 bis 15 = 30 bis 35
PAUSE nach ca. 50 Minuten				15
3. Fakten rund um Sicherheit (Inhaltlicher Input) (Seiten 5-11)	3.1 Passwörter 3.2 Social Media & Apps 3.3 Einstellungen, Software, Netzwerk 3.4 Online Shopping, online Banking 3.5 Konkrete Angriffe	Präsentation im Plenum	Beamer, PPT	30
Bei Bedarf weitere kurze Pause				5
4. Quiz (Seite 12)	Praxisnahe Quizfragen	Einzelarbeit	Alle brauchen ihr Handy	20
5. Abschluss (Seite 12)	Reflexion, Factsheet, Feedback	Plenum	Handout (gedruckt & ausgeschnitten)	10 bis 15

1 Einstieg

1.1 Begrüßung und Vorstellungsrunde

Falls Sie diesen Workshop mit einer unbekannten Gruppe durchführen, stellen Sie sich zunächst selbst kurz vor und bitten Sie die Teilnehmenden sich ihre Namen und ihre Lieblings-App oder Lieblings-Internetseite zu nennen.

1.2 Einstieg

Stellen Sie kurz und knapp den Ablauf des Workshops und den zeitlichen Rahmen des Workshops (und wann Pausen geplant sind) vor.

Erklären Sie, dass es darum geht, gemeinsam Informationen zu sammeln, wie man das Internet möglichst sicher nutzen kann.

1.3 Assoziationen

Fragen Sie: „Welche Wörter, Erlebnisse, Gefühle fallen Ihnen zu „Cyber-Sicherheit“ ein?“ Notieren Sie auf einem Flipchart oder der Tafel mit.

2 Hausmetapher

2.1 Wie schützen wir unsere Wertgegenstände?

1. Lassen Sie die Teilnehmenden in Kleingruppen (2-3 Personen) folgende Frage besprechen: ***„Wie schützen wir unsere Wertgegenstände? bzw. Wo haben wir sie?“*** Workshopleitung verteilt kleine Zettel: ***„Bitte schreiben Sie einen Begriff/eine Idee pro Zettel auf.“***

2. Teilnehmende sammeln Begriffe

3. Im Plenum stellen die Teilnehmenden ihre Begriffe vor

4. Breiten Sie nun eine Reihe von Abbildungen auf einem Tisch auf (siehe Anhang 6.1). Die Bilder mit der gleichen Nummer sollten nebeneinander liegen:
   „Schauen Sie sich bitte die Bilder an, und überlegen Sie, wofür die Bilder im Zusammenhang mit der vorherigen Frage stehen könnten. Wählen Sie ein Bild und erklären Sie, was es bedeuten könnte.“
   Sollte einer der zuvor gesammelten Begriffe dazu passen, wird der Zettel (mit dem Begriff) dazu gelegt.

5. Die übrigen Bilder (die nicht gewählt/beschrieben wurden) werden am Ende durch unsere Erklärungen ergänzt (z.B. Türe abschließen; Fenster schließen; Schlüssel an einem sicheren Ort; Entscheiden, wen ich reinlasse; Wertgegenstände innerhalb des Hauses aufbewahren (bzw. nur Dinge mit geringem Wert draußen lassen); innerhalb des Hauses sichere Orte suchen (Safe, Versteck → Sich diese Orte merken)).

2.2 Daten & Zugänge sind wie Wertsachen

1. Wir müssen auch im digitalen Raum auf unsere „Wertsachen“ aufpassen. Frage die Teilnehmenden: ***„Was sind solche ‚Wertgegenstände‘ im digitalen Raum?“*** (Mögliche Antworten: z.B. Daten (Fotos, Namen, Adressen). Die Gefahr besteht in verletzter Privatsphäre, Identitätsklau, finanziellem Schaden (beispielsweise bei geklauten Zugangsdaten für Bankkonten)).

2. Legen Sie nun Papierstreifen mit verschiedenen Begriffen aus (siehe Anhang 6.2) und bitten Sie die Teilnehmenden: ***„Wählen Sie einen Begriff aus, den Sie kennen. Überlegen Sie bitte, zu welchem Bild der Begriff passt.“***

→ **Die technische Welt entwickelt sich immer weiter; jeder Fortschritt, jede neue Entwicklung hat Sicherheitslücken. Angreifer:innen versuchen, schnell die Lücke auszunutzen. Cyber-Security-Expert:innen versuchen, die Lücke wieder zu schließen.**

2.3 Parallele: Cyber-Sicherheit (Plenum)

Um die Überlegungen und Reflexionen der Teilnehmenden rund um Datensicherheit zusammenzufassen, können Sie nun eine Power-Point-Präsentation teilen, die Analogien zwischen analogem und digitalem Raum visualisiert. **„Wir sehen wir uns jetzt in einer kurzen Präsentation an, worüber wir gerade gesprochen haben. Dabei geht es um den Vergleich von Sicherheit im digitalen Raum und Sicherheit im analogen Raum".**
(Die folgende Tabelle hier ist nur eine Übersicht für die Workshopleitung und zeigt, was in der Präsentation vorkommt)

Digitaler Raum	*Analoger Raum (Haus, Straße...)*	*Digitaler Raum*	*Analoger Raum (Haus, Straße...)*
Sicheres Passwort	*Türschloss & Schlüssel*	*Firewall*	*Zaun*
Passwort auf Post-It	*Schlüssel unter Fußabstreifer (Türmatte), Schlüssel steckt außen im Schloss*	*Öffentliches WLAN, öffentliche Ladestationen*	*Haustür/Fenster steht offen*
Fotos und Gedanken auf Social Media teilen	*öffentliche Familienalben, Tagebücher (Wie geht es mir mit Einträgen, die ich vor Jahren gemacht habe – sie sind noch online verfügbar?)*	*Spam-Nachrichten (z.B. SMS: Handy weg, bitte Geld, Vertreter (Werbung im Internet), Falschmeldung: Bestellung ist angekommen: klicke auf diesen Link*	*Menschen, die bei dir klingeln (Trickbetrüger (z.B. jmd. sagt er ist von der Polizei oder ein Enkelkind))*
Allen Apps erlauben, auf den Standort zuzugreifen	*Komplize informiert, dass eine Person einkaufen/im Urlaub ist und das Haus somit leer steht*	*Online-Banking in einer Menschenmenge*	*Haus, bei dem die Wände aus Glas sind oder ein privates Gespräch, das für alle hörbar ist.*
Antivirus-Software	*Alarmanlage/Bewegungsmelder*	*Datendiebstahl, Identitätsdiebstahl (Standort, Social Media, online-Einkaufen)*	*Einbruch*

„Was fehlt noch? Was fällt Ihnen noch ein, wie wir uns im digitalen Raum schützen können."

3 Fakten rund um Sicherheit (Inhaltlicher Input)

Kapitel 3 bietet Informationen und Fakten rund um das Thema Sicherheit im digitalen Raum. Wir empfehlen, die **InforMiert- Power-Point-Präsentation** mit Schlagwörtern zu teilen und sich bei Ihrem Input an den folgenden Informationen zu orientieren.

3.1 Passwort

*** Welche Passwort-Typen gibt es? Was sind die Vor- und Nachteile?**

- Wisch-Muster: Die Spur kann auf dem Handy-Bildschirm gesehen werden (Fingerabdrücke)
- Passwort, PIN-Code: Wenn ein Passwort aus nur 4 Stellen besteht und rein numerisch ist, ist es zu einfach → zu sicheren Passwörtern siehe weiter unten
- Finger-Abdruck, Gesichtserkennung:
  - Vorteil: Ich muss mir nichts merken & es ist sehr fälschungssicher,
  - Nachteil bei Finger-2Abdruck: bei kleinen Verletzungen am Finger oder mit Brille, Kopftuch, Schal erkennt das Handy die Person manchmal nicht, außerdem hat das Handy dann Ihren Fingerabdruck gespeichert.

*** Sicherer Umgang mit Passwörtern:**

- Passwörter sollen im Browser nie gespeichert werden
- Es ist wichtig, sich immer abzumelden/auszuloggen
- Passwörter sollen nicht für andere zugänglich sein (z.B. an Laptop angeklebte Notizzettel)
- Passwörter sollen nicht weitergegeben werden (auch nicht an Kinder, Partner:innen)
- Passwörter soll man sich gut merken (evtl. Passwortmanager[1] verwenden), evtl. an einem versteckten Ort notieren
- Unterschiedliche Passwörter für unterschiedliche Accounts verwenden (v.a. bei besonders schützenswerten Daten wie z.B. Banking)

*** Wie kommen Personen an mein Passwort?**

- Mit Hilfe von Algorithmen, durch Recherche auf Social-Media-Accounts (Geburtstag, Name des Haustiers…), durch einen Zettel am Bildschirm oder weil das Passwort anderen bekannt war (z.B. Kindern, Partner:innen)

[1] Ein Passwortmanager ist eine Software, die es Computerbenutzer:innen ermöglicht, Zugangsdaten und Passwörter verschlüsselt zu speichern, zu verwalten und zu benutzen.

*** Was ist ein sicheres Passwort?**

- Ein sicheres Passwort ist z.B. ein Satz mit Zahl und Sonderzeichen (Beispiel für Sonderzeichen geben: !”§$%&/=?)
- Man soll nicht die klassischen Passwörter nehmen, wie z.B. 1234, „Passwort”, Namen von Kindern, Partner:innen, Haustieren, Geburtsdaten
- Ein sicheres Passwort ist lang (ab 12 Zeichen), komplex und hat keinen Bezug auf die Person.
- Eine Passphrase ist eine Möglichkeit sich ein langes, sicheres Passwort bestehend aus mehreren Wörtern zu merken. So machst du eine gute Passphrase:
  - Wähle 4-5 zufällige Wörter.
  - Verbinde sie zu einem Satz.
  - Füge Zahlen und Sonderzeichen hinzu.
  - Beispiel: "BlaueBaereTanzenGerne42!"
- *Tabelle erklären (wie schnell kann ein Algorithmus dein Passwort herausfinden?)*

3.2 Social Media & Apps

*** Was sind Beispiele für Social Media?**

- WhatsApp, Signal, Telegram, Instagram, TikTok, Facebook…

*** Was poste ich auf Social Media?**

- Es ist wichtig vorsichtig zu sein, was man über sich und über andere Menschen postet.

*** Was sind die Gefahren von Social Media?**

- Was einmal online ist, kann nicht mehr kontrolliert/entfernt werden (Es wurde vielleicht schon gespeichert, heruntergeladen, oder es wurde ein Screenshot gemacht bzw. geteilt), das Unternehmen hat die Daten auch nach dem Löschen
- Es könnten personalisierte Phishing-Nachrichten erstellt werden (z.B. kann man auf Social Media sehen, welchen Spitznamen eine Freundin verwendet und dann diesen Spitznamen in einem E-Mail verwenden, sodass kein Verdacht aufkommt)
- Daten von Eltern/Haustieren etc. sind häufig Passwörter und können so auf Social Media (z.B. Instagram, Facebook) abgelesen werden
- Aufenthaltsort könnte preisgegeben werden (Gefahr von Stalking)
- Urlaubsfotos weisen darauf hin, dass man nicht zu Hause ist
- Schmuckfotos weisen darauf hin, dass man wertvolle Gegenstände besitzt

- Identitätsdiebstahl (z.B. eine andere Person erstellt einen Fake-Account über mich)
- Cybermobbing (Über mich werden Fake-Informationen gepostet, in Gruppen geschrieben)
- Fake-News (z.B. falsche Nachrichten über Politiker:innen)
- Bösartige Links (beim Anklicken, lädt sich ein Virus auf das Gerät)
- Grooming (z.B. eine ältere Person gibt sich als gleichaltrig aus und versucht so das Vertrauen zu gewinnen und will z.B. ein Treffen oder Nacktbilder)
- Es entsteht womöglich ein schlechter Eindruck für Bewerbungen, Kreditanträge, Mietverträge (vor allem wenn ich meinen richtigen Namen verwende)
- Dritte können die Infos nutzen, um personalisierte Werbung zu schicken

*** Wie kann ich Social Media sicherer machen?**

- Privatsphäre-Einstellungen: Begrenzen, wer die Beiträge sieht: z.B. Freund:innen, Freund:innen von Freund:innen (jedenfalls nicht alle)
- Telegram ist z.B. nicht verschlüsselt (im Gegensatz zu WhatsApp & Signal)
- Bewusster Konsum: Wie viel schaue ich von was an? Was (re-)poste ich? Wem folge ich? Wessen Nachrichten lese ich? Auf die psychische Gesundheit achten. → Ich weiß, dass es einen Algorithmus gibt, der mir immer mehr vom Gleichen zeigt.
- Bewusstes Posten (welche Fotos lade ich hoch, was schreibe ich), Hinterfragen der geposteten Daten von anderen (vor allem bevor ich sie teile/weiterleite). Ich denke daran, dass es Fake-News gibt und überprüfe die Informationen mit Hilfe von seriösen Quellen.
- Unangemessene, verdächtige, kriminelle Inhalte auf der Plattform melden
- die Identität von anderen überprüfen (vielleicht ist das nicht die Person, die sie vorgibt zu sein)
- Menschen/Accounts blockieren
- Vor dem Download von (unbekannten) Apps kann man z.B. darauf achten, wie oft diese schon heruntergeladen wurde (wenn ich z.B. irgendeine App suche, um meine Jogging-Zeiten zu tracken)

3.3 Einstellungen, Software, Netzwerk

* Öffentliches WLAN, öffentliche Ladebuchsen

- nicht verwenden, ist unsicher, weil es leicht durch Dritte manipuliert werden kann

* Firewall, Antivirus-Software, Ad-Blocker

- Eine Firewall ist wie ein Zaun. Sie schützt das Gerät davor, dass gefährliche Inhalte heruntergeladen werden. Vor allem für Computer sind Firewalls sinnvoll. Am Handy sind viele Funktionen, die Firewalls erfüllen, schon im Betriebssystem enthalten.
- Antiviren-Software, was ist das? Eine Antivirus-Software ist ein Programm, das das Gerät auf gefährliche Dateien untersucht. Vor allem für Computer ist eine Antivirus-Software wichtig. Neuere Computer (ab Windows 10) haben so eine Software bereits installiert.
- Bei Handys ist es wichtig, Apps nur aus den vorgesehenen App-Stores herunterzuladen und regelmäßig Updates zu machen. Wenn man das beachtet, genügt in der Regel die standardmäßige Software!
- Ein Ad-Blocker ist eine Software, die Werbung reduziert bzw. nicht anzeigt. Auf Apple-Handys können Ad-Blocker installiert werden. Für Android-Handys ist es nicht so einfach, aber auch möglich. Für einen Computer sind Ad-Blocker auch empfehlenswert, allerdings kann es sein, dass manche Dienste/Websites nicht funktionieren, wenn ein Adblocker aktiv ist. Dann kann man den Adblocker für diese Seite auch deaktivieren *(Kostenlose Beispiele: uBlock Origin, Adguard)*.

* Cookies

- Cookies sind kleine Dateien im Handy und Computer, die sich Informationen merken, die schon einmal eingegeben wurden. Zum Beispiel schlägt dir eine Internetseite dank aktivierter Cookies deine Emailadresse beim Login vor, sodass du sie nicht jedes Mal wieder eingeben musst. Ein anderes Beispiel ist, dass der Warenkorb noch befüllt ist, wenn du später nochmal auf die Seite gehst.
  Cookies sind also praktisch, aber sie enthalten auch Sicherheitsrisiken: z.B., wenn mehrere Menschen ein Gerät verwenden oder wenn es Sicherheitslücken auf Homepages gibt, die Angreifer:innen ausnutzen. Es empfiehlt sich regelmäßig Cookies zu löschen. Bei der Verwendung des „Inkognito Modus" oder „privaten Modus" werden keine Cookies gespeichert.

* Internet of Things

- So werden alle „smarten“ Geräte bezeichnet. Sie haben Zugang zum Internet, sodass zwischen den Objekten Daten ausgetauscht werden können. Z.B. Smartphones, ein smarter Kühlschrank, Smartwatches, Fitness-Tracker, smarte Alarmanlagen, virtuelle Assistenten (Alexa), etc.

* Empfehlungen

- Internet-of-Things-Geräte sind unsicher, weil einige dauerhaft das Mikro & teilweise sogar die Kamera aktiviert haben. Es empfiehlt sich, sie nicht ans WLAN anzuschließen und integrierte Kameras zuzukleben.
- Allgemein empfiehlt es sich, Kameras an allen Geräten mit einem Zettel zuzukleben, auch am Handy.
  Es gibt dafür auch kleine Plastikteile. Mit einem Schieber, den man kaufen kann, kann die Kameralinse abgedeckt werden, wenn sie nicht benötigt wird.

- Es ist wichtig, voreingestellte Standard-Passwörter (z.B. von Router) zu ändern.

3.4 Online Einkaufen, Online Banking

* Gefahren

- Trickbetrug:
  - ➢ Betrüger:innen bitten womöglich um Passwörter („Guten Tag, hier ist Ihr Bankberater, es gab eine verdächtige Aktivität, wir müssen Ihr Konto kontrollieren, bitte schicken Sie uns Ihre Daten")
  - ➢ fordern auf, auf einen Link zu klicken (z.B. Ihre Sendung von „Post", DHL ist da → Bestellnummer, Auftragsnummern kontrollieren)
  - ➢ fordern auf, Geld zu schicken (z.B. Ihr Paket muss noch bezahlt werden)
  - ➢ erstellen Fake-Homepages, die so ähnlich aussehen wie jene von Amazon, Bankinstituten oder willhaben.at
  - ➢ Weitere Beispiele können hier abgerufen werden: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing_node.html

* Empfehlungen

- starkes Passwort, 2-Faktor-Authentifizierung (Bsp. Online Banking & digitales Amt)
- Es ist nicht ratsam, im öffentlichen Raum sensible Daten einzugeben (es kann jemand in der U-Bahn hinter dir stehen/sitzen)
- bei online-shopping: Kreditkarteninformation nicht speichern
- Auf Seriosität von Homepages achten (wenn es z.B. kleine Unterschiede in der Web-Adresse oder im Design gibt, lieber nochmal googlen. Z.B. ob sie vielleicht ihr Design verändert haben)
- Bei verdächtigen Anrufen/Nachrichten: Kenne ich Absender:in? Spam/unerwünschte Anrufer:innen melden/blockieren! Kriminelles Verhalten melden.
- Nur erste Seite Google-Treffer verwenden (Qualität der Seite kann Hinweise auf Sicherheit der Seite geben. Z.B. Grammatik, Rechtschreibung, Shopping-Websites: Qualitative Fotos, Preisgestaltung sinnvoll, klare Angaben zum Rücksenden, Versandinformationen & Datenschutzrichtlinien, auch fragwürdigere Werbung kann ein Indiz sein. Gibt es ein Impressum, eine Info-Seite, eine Kontakt-Seite?)

- Auf eine sichere Verbindung achten. Diese erkennt man am https und an einem kleinen Schloss in der Adress-Zeile. Man kann auf das kleine Schloss klicken: „Verbindung ist sicher“

- Lesezeichen setzen (von z.B. Bank-Seiten)

3.5 Und wenn ich angegriffen werde?

* Links & Anhänge

- nicht auf Links klicken & keine Anhänge öffnen/herunterladen (am Computer kann man mit der Maus drüberfahren und sieht den wahren Absender/Link)

* Der Mensch als Gefahrenquelle

- Trickbetrug mit verschiedenen Methoden:
  - ➢ z.B. ich bin dein Chef, IT-Spezialist, Bankberater, Kind, Verwandte*r
  - ➢ oft Forderungen, Tippfehler, unpassende Anrede (Hallo, Name von Emailadresse, „Mama“, „Mitarbeiterin“), emotionale Inhalte: „Ich hatte einen Unfall…”
  - ➢ oft machen sie Zeitdruck oder geben vor eine Autoritätsperson zu sein (z.B. von einer Behörde)

* Empfehlungen

- Was kann ich tun, wenn meine E-Mail-Adresse gehackt wurde? Passwort ändern, wenn es nicht mehr geht: Provider[2] informieren
- Woran kann ich erkennen, dass mein Handy gehackt wurde? Handy: langsame Bandbreite, schneller Akku-Verbrauch
- Spam-Nachrichten erkennen:
  - ➢ Kenne ich Absender:in?
  - ➢ Gibt es dubiose Anhänge?
  - ➢ Ist ein Link enthalten? (Mit der Maus darüberfahren, dann sehe ich wo der Link hinführt, ohne ihn anzuklicken), ein Button ist auch ein Link
  - ➢ Wird betont, dass es dringend ist?

[2] Ein E-Mail Provider ist das Unternehmen, dass die E-Mail-Dienstleistung zur Verfügung stellt (z.B. Gmail, GMX, Yahoo Mail, Outlook, etc.)

- ➢ Wird ein Geschenk, eine Spende in Aussicht gestellt?
- ➢ Sind Rechtschreibung oder Grammatik fehlerhaft?
- ➢ Enthält die Nachricht eine Aufforderung, personenbezogene Informationen offenzulegen?
- ➢ Gibt es eine unpassende Anrede?

- Umgang mit Spam-Nachrichten:
  - ➢ Als Spam markieren, nicht auf Links klicken, keine Anhänge öffnen,
  - ➢ Vermeintliche Absender informieren (z.B. IT-Admins, Bank, Kind…)
  - ➢ NICHT ANTWORTEN
  - ➢ als Spam markieren oder löschen

4 Quiz

Zur Wiederholung des Inputs aus Kapitel 3 haben wir mehrere kurze Quizze erstellt:

Quiz 1	Mein sicheres Passwort	
Quiz 2	Sicher im Internet	
Quiz 3	Betrügerische Nachrichten	

5 Abschluss

5.1 Reflexion & Feedback

Bitten Sie die Gruppe im Plenum zu teilen, welche Informationen Sie sich zu den verschiedenen Themen mitnehmen und welche Schritte sie als Nächstes setzen werden. Hier ein Überblick der behandelten Themen:

- Passwörter
- Social Media & Apps
- Einstellungen, Software, Netzwerk
- Online-Shopping, Online-Banking
- Konkrete Angriffe

5.2 Fact-Sheet:

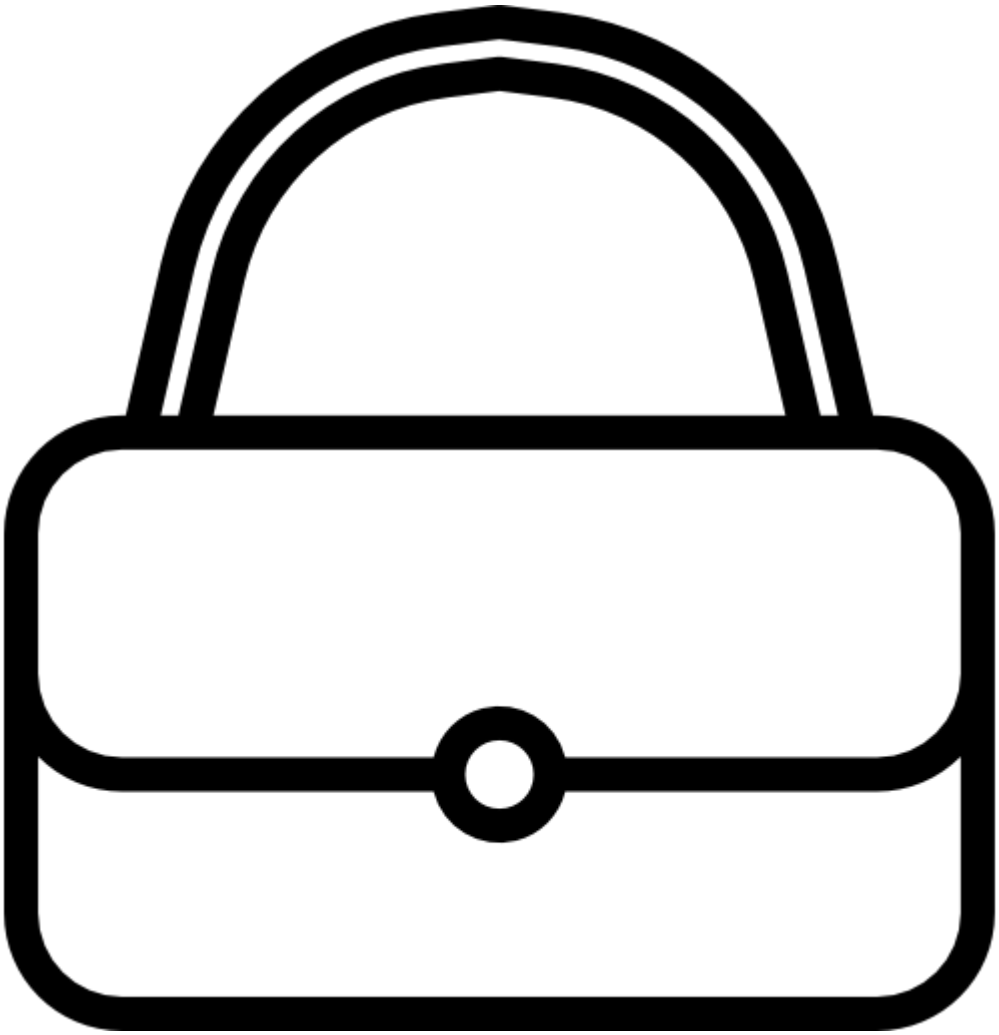
Teilen Sie abschließend das Handout aus (siehe Anhang 6.3), um allen Teilnehmenden die wichtigsten Informationen im Pocket-Format mitzugeben.

6 Anhang

6.1 Bilder

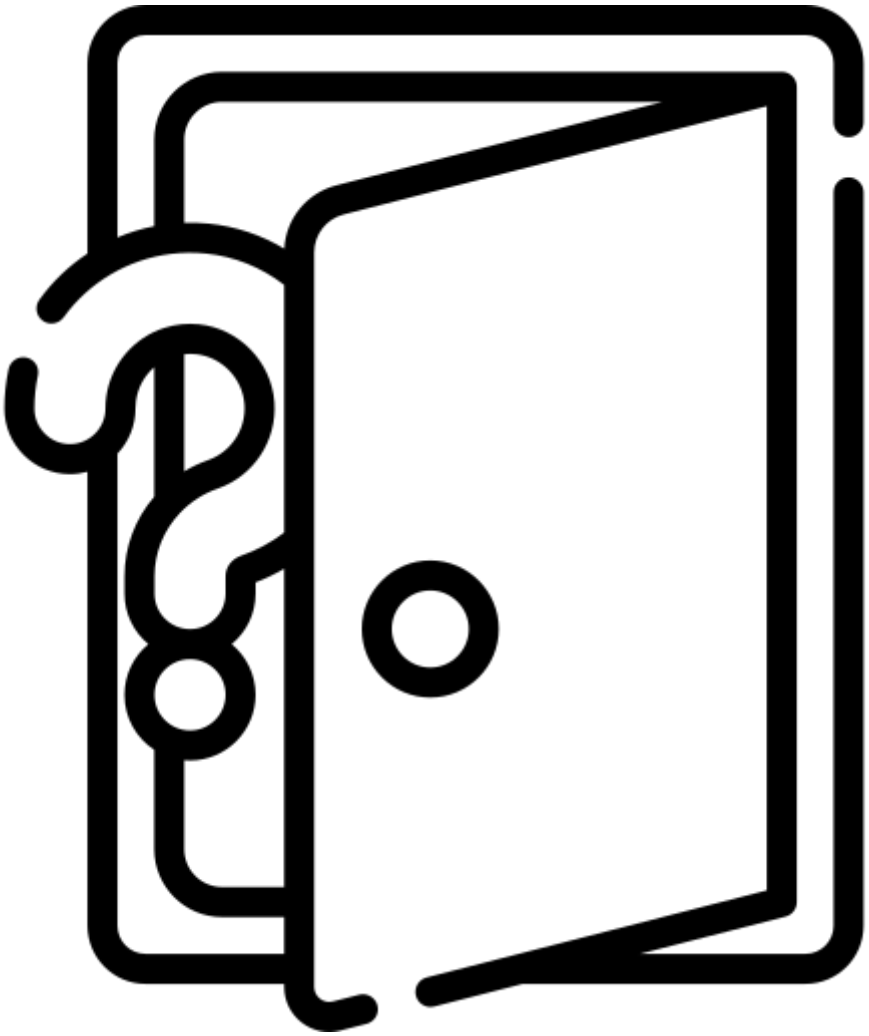
[3]

[3] Quelle: https://www.freepik.com/icon/house_3661264#fromView=search&term=haus&page=1&position=20&track=ais

 [4]

2

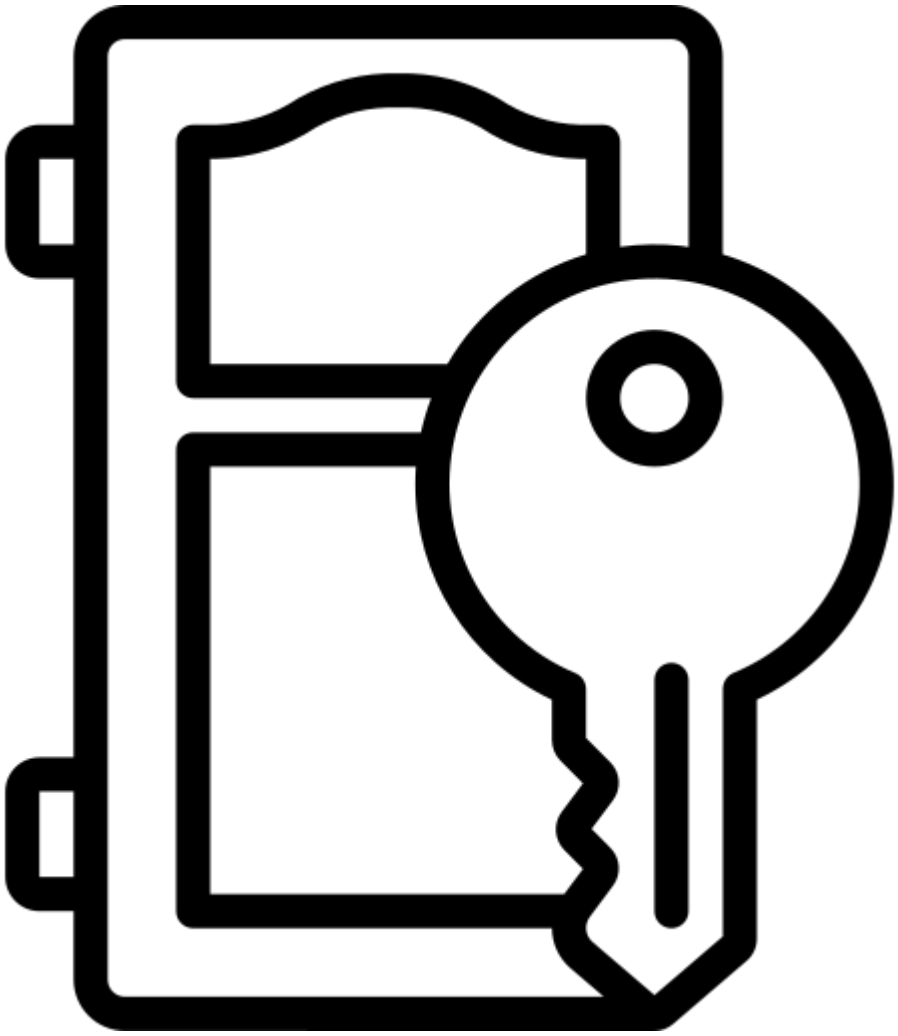
[4]Quelle:
https://www.freepik.com/icon/hand-bag_1115877#fromView=search&term=handtasche&page=1&position=0&track=ais



[5]

8

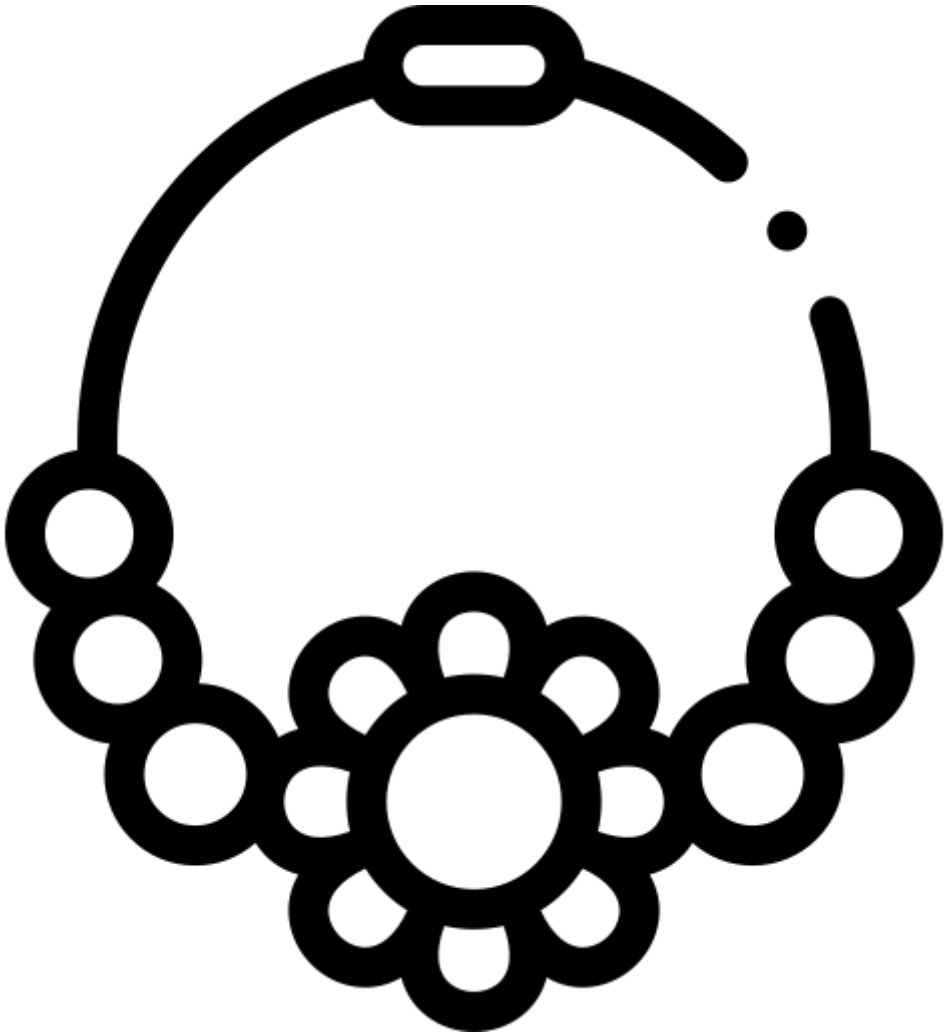
[5] Quelle: https://www.freepik.com/icon/unknown_6750369#fromView=resource_detail&position=8



[6]

2

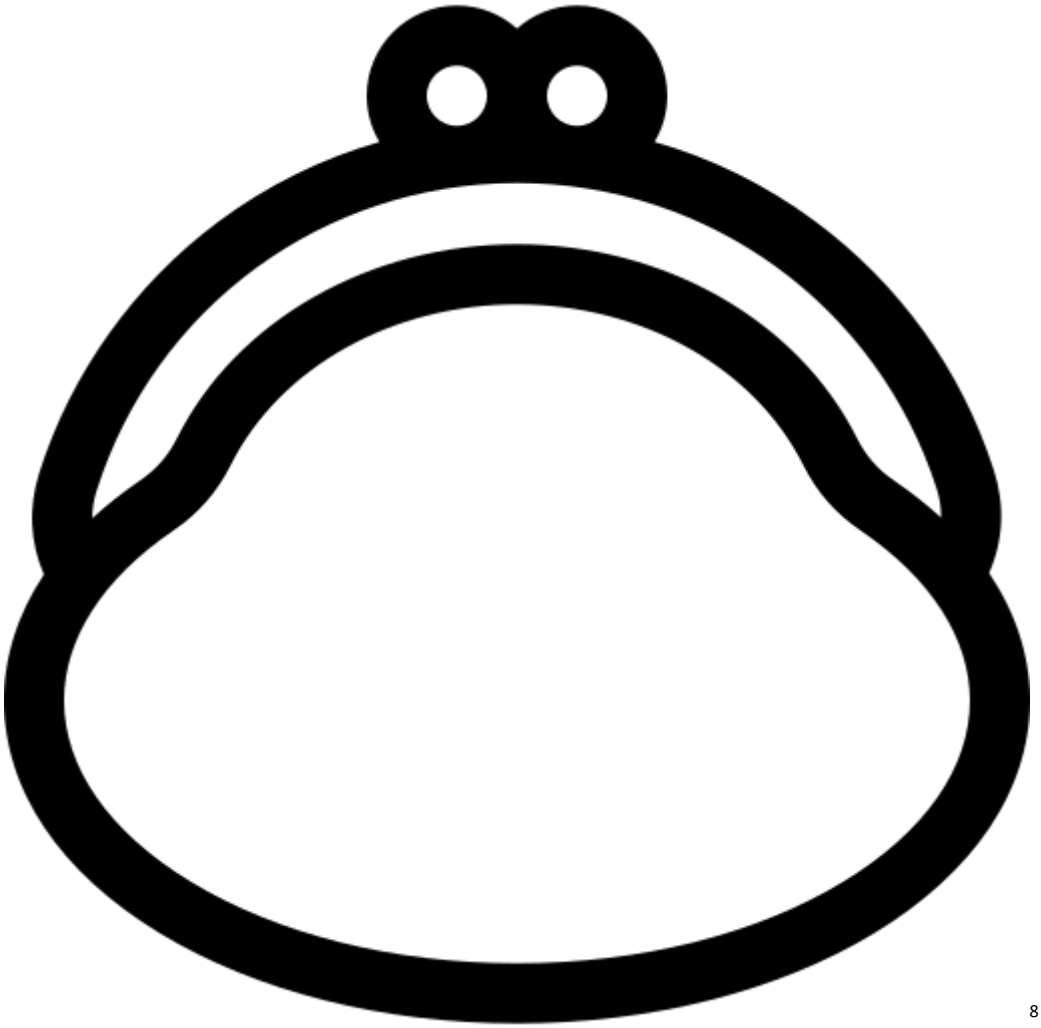
[6]Quelle: https://www.freepik.com/icon/door_4428869#fromView=search&term=t%C3%BCr+mit+schl%C3%BCssel&page=1&position=45&track=ais&uuid=9b188067-b4c9-4ea4-9d60-ea0de4ffd57c



[7]

2

[7]Quelle: Icon by Freepik
https://www.freepik.com/icon/necklace_2439418#fromView=search&term=perlenkette&page=1&position=3&track=ais



[8]

2

[8]Quelle: Icon by Freepik
https://www.freepik.com/icon/coin-purse_3609254#fromView=search&term=portemonaie&page=1&position=20&track=ais

[9]

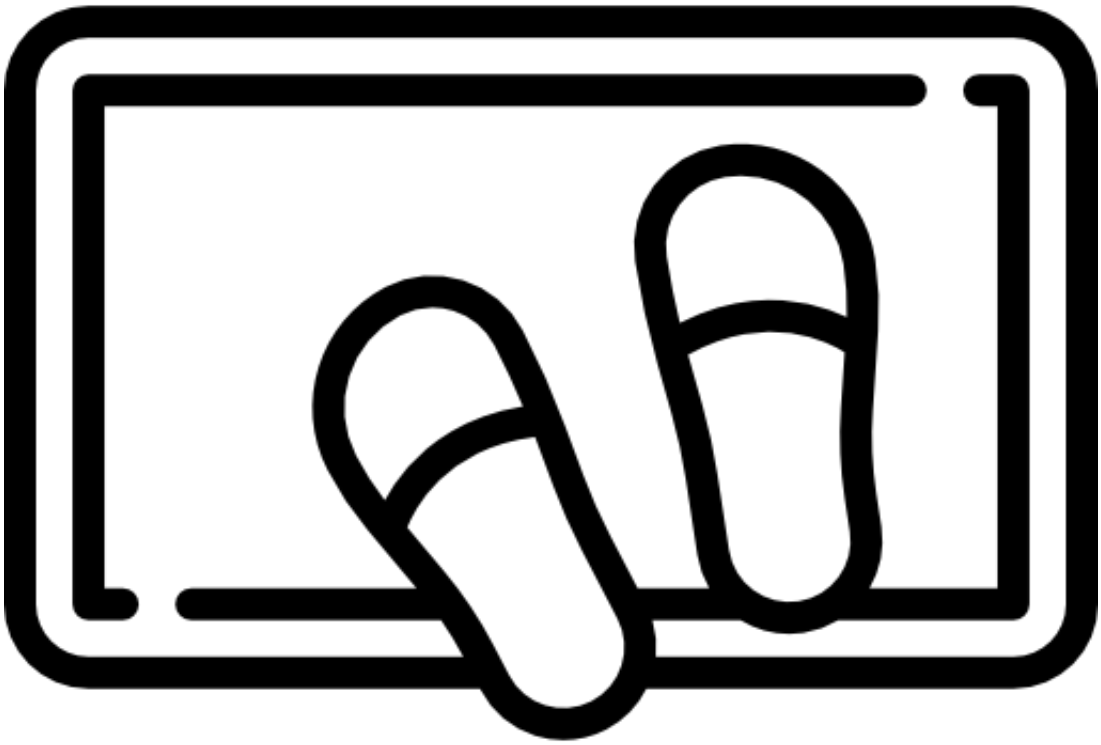
4

[9]Quelle: Icon by IconMarketPK
https://www.freepik.com/icon/photoalbum_8890925#fromView=search&term=Fotoalbum&page=1&position=7&track=ais

[10]

2

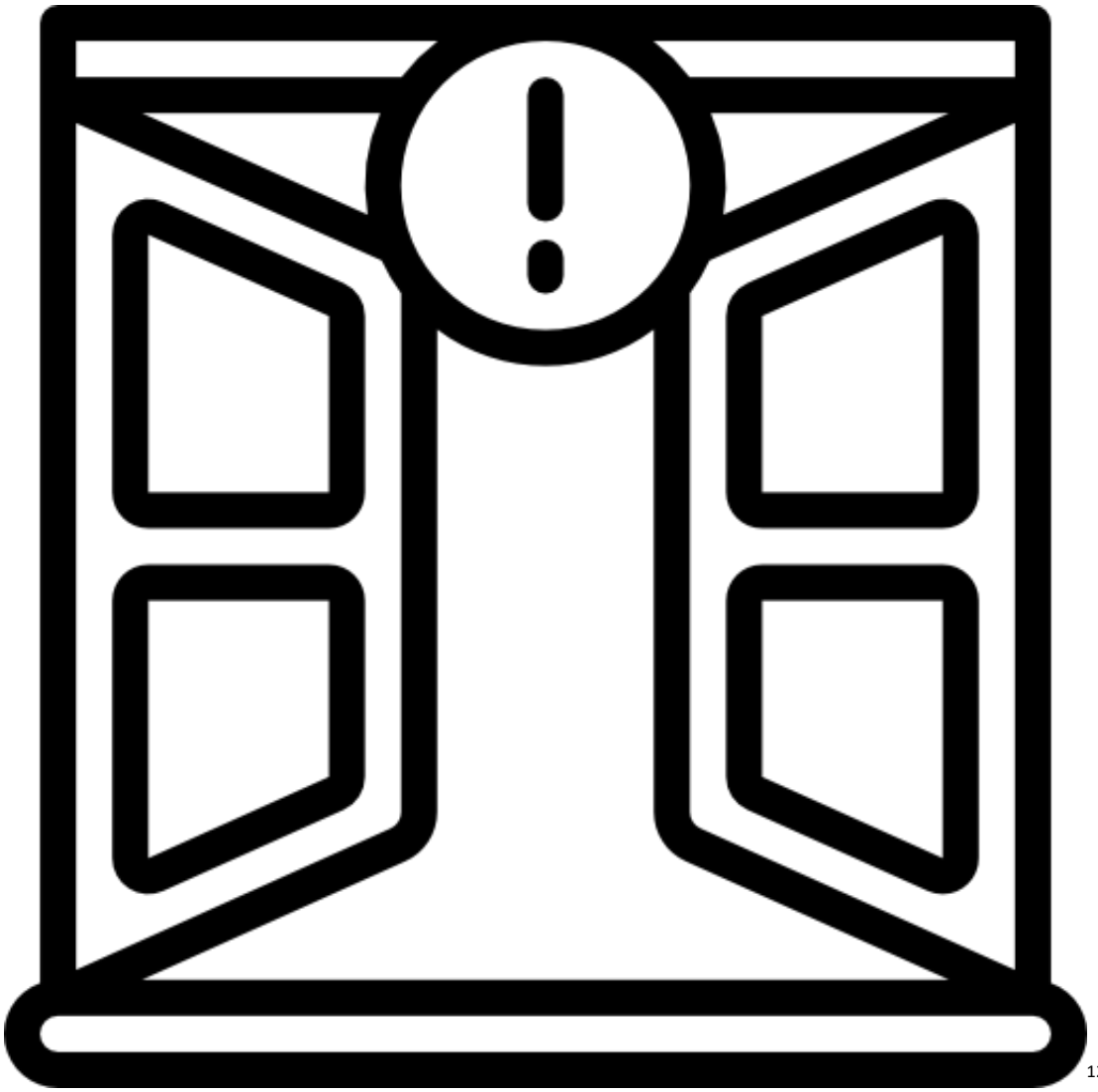
[10] Quelle: Icon by Muhammad Atif
https://www.freepik.com/icon/padlock_9731518#fromView=search&term=Vorh%C3%A4ngeschloss&page=1&position=26&track=ais



[11]

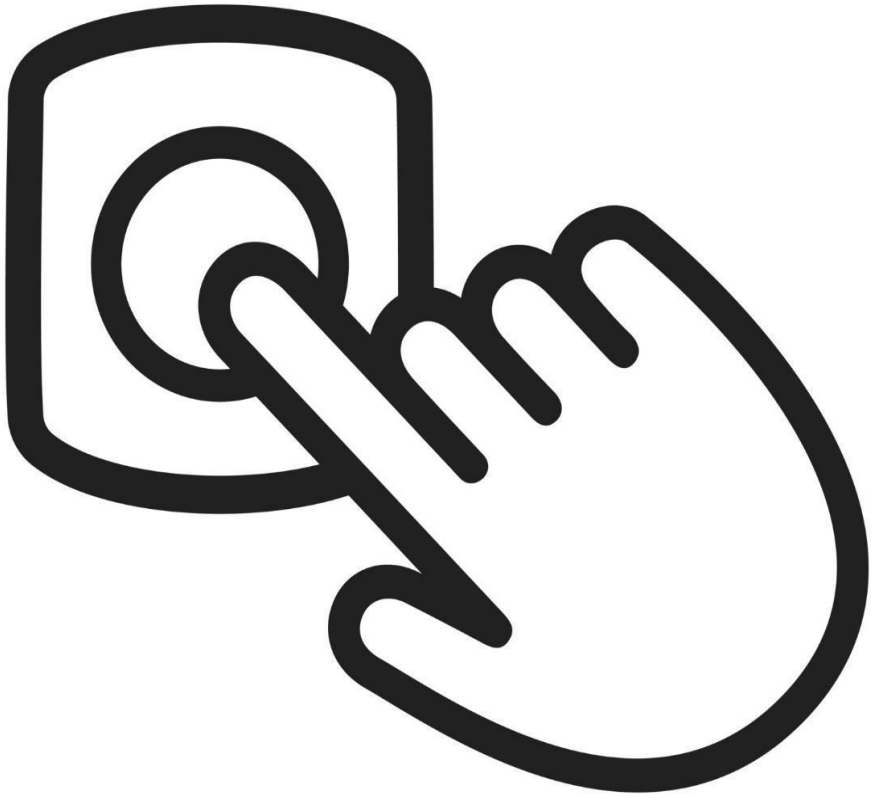
3

[11] Quelle: Icon by Freepik
https://www.freepik.com/icon/slippers_1047125#fromView=search&term=Fu%C3%9Fmatte&page=1&position=0&track=ais

 [12]

8

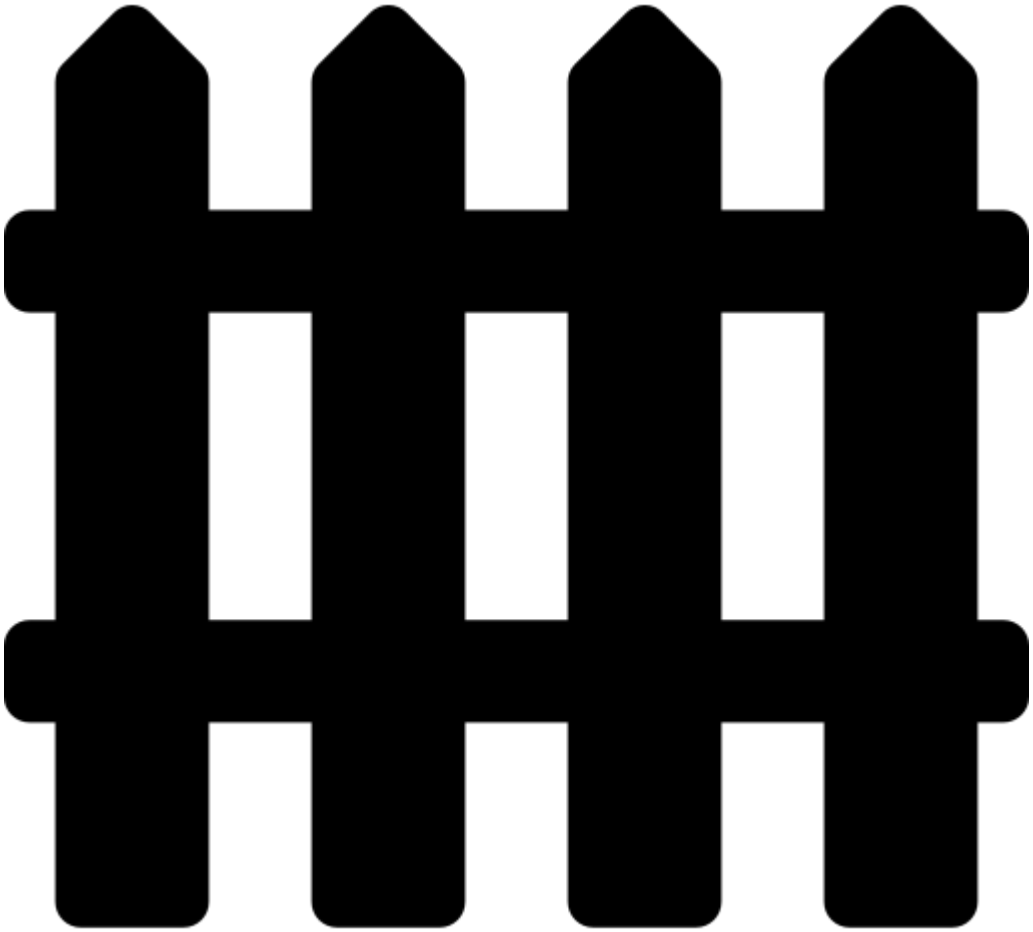
[12] Quelle: https://www.freepik.com/icon/window_1035855



[13]

9

[13] Quelle: https://de.vecteezy.com/vektorkunst/6081752-turklingel-symbol-flat-style-design-umriss-zeichen-vektor-illustration-isoliert-auf-weissem-hintergrund



[14]

7

[14] Quelle: https://www.freepik.com/icon/fence_1723484#fromView=search&term=fence&page=1&position=32&track=ais?log-in=google

[15]

10

[15] Quelle: Dieses Bild wurde mit KI generiert

 [16]

6

[16] Quelle: Dieses Bild wurde mit KI generiert

17

?

[17] Quelle:
https://www.freepik.com/free-photo/high-angle-modern-laptop-office_5904591.htm#query=Passwort%20auf%20Postit%20am%20Computer%20free&position=17&from_view=search&track=ais&uuid=8a61e46e-7e54-4bbc-aec6-dd633967c451

[18]

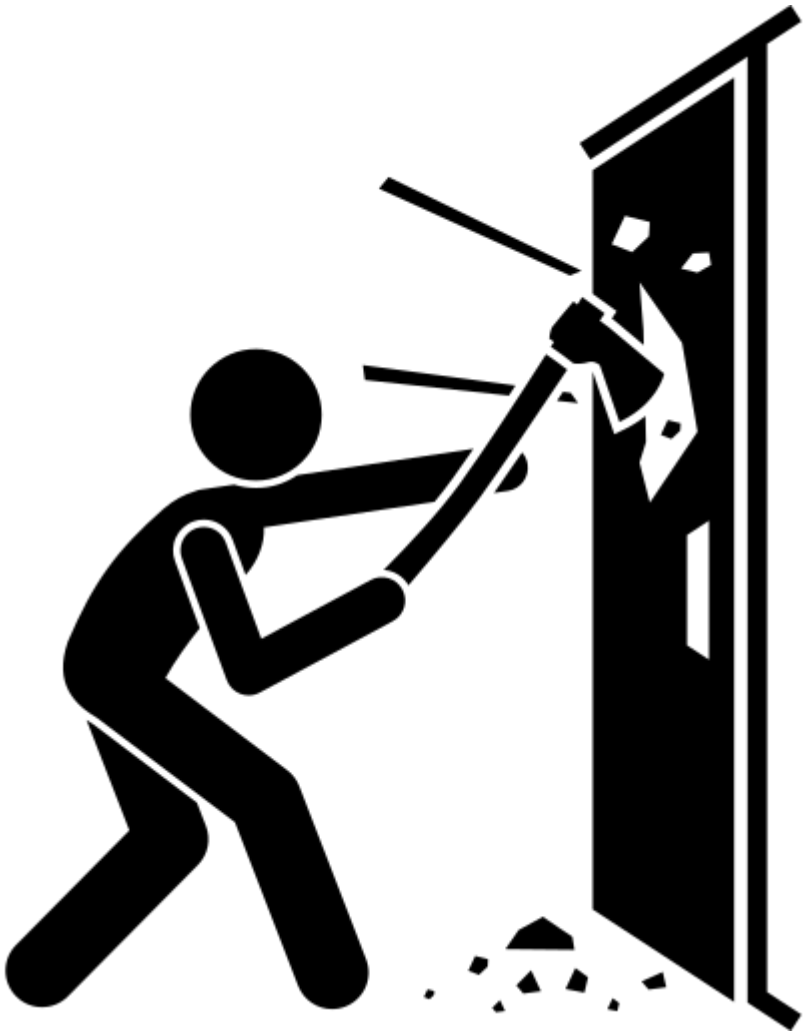
9

[18]Quelle: https://www.freepik.com/icon/people_9936484#fromView=search&term=menschen+vor+haust%C3%BCr+&page=1&position=26&track=ais&uuid=deb63186-ae8b-478d-b072-6a6f1eccc607

[19]

9

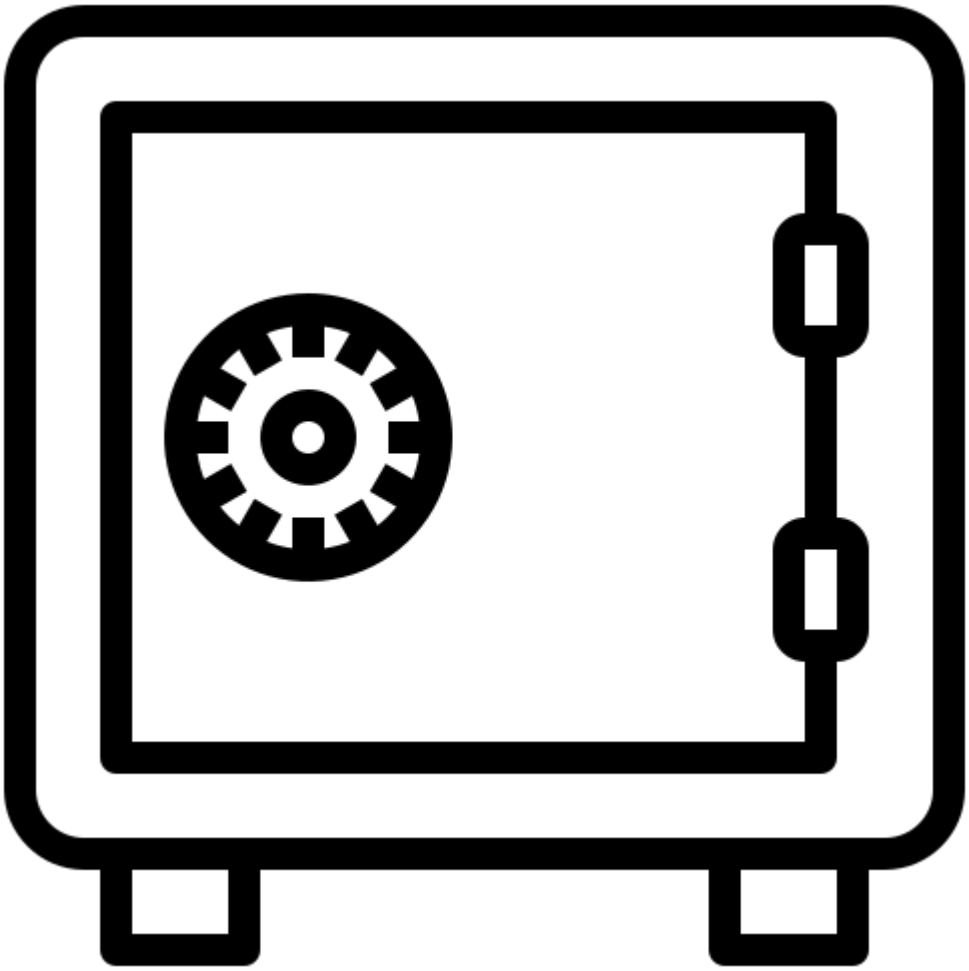
[19] Quelle: https://www.freepik.com/icon/knocking-door-office-worker_62295#fromView=search&term=vertreter+t%C3%BCr&page=1&position=29&track=ais&uuid=de6a43b3-0d7e-473d-ab17-27a605149fdd



[20]

11

[20] Quelle: https://www.freepik.com/icon/person_9925148#fromView=search&term=burglar&page=1&position=15&track=ais



[21]

2

[21] Quelle: https://www.freepik.com/icon/safe-box_2091874#fromView=search&term=safe&page=1&position=71&track=ais

[22]

6

[22] Quelle: eigenes Bild

6.2 Wortstreifen

Passwort
Pincode
öffentliches WLAN
öffentliche Ladebuchsen
Firewall
Social Media
Anti-Virus
Wo schaue ich auf mein Handy?
Online-Banking

Online-Einkauf
Persönliche Daten
Standort
Hacking
Identitätsdiebstahl
Fake-News
Betrügerische Nachrichten
Spam Nachrichten
Werbung

6.3 Digitale Sicherheit im Überblick