DIGITAL CHECK NRW

Digital weiterwissen.

Cybersicherheit

sicher digital unterwegs

Dieses Material wurde im Rahmen des **#DigitalCheckNRW** entwickelt und soll dazu dienen Medienkompetenz zu fördern. Es gibt Anregungen zu verschiedenen Methoden. Diese können je nach Bedarf angepasst und verändert werden.

Legende für die Methodensammlung

- Ziel
- Methode
- Fragen
- Einstieg
- Link
- Hinweis
- Ablauf
- Vertiefung

Cybersicherheit: sicher digital unterwegs

Noch schnell den Staubsauger-Roboter anschalten, die Familie per Video anrufen, die letzte Fahrradstrecke per App nachverfolgen oder den Timer der Kaffeemaschine neu programmieren – der technische Fortschritt bietet eine ganze Reihe von Möglichkeiten. Die Steuerung der Geräte, Bankgeschäfte, die Kommunikation mit Freund*innen, das Lesen der aktuellen Nachrichten und wichtige Einkäufe – alles erfolgt häufig über Apps, die auf das Smartphone oder Tablet heruntergeladen und installiert werden. Welche Daten man dabei genau preisgibt und welche Einstellungsmöglichkeiten für die private Sicherheit getätigt werden können, ist dem / der Nutzer*in oft gar nicht richtig bewusst.

Ziele:

- Sichere Passwörter erstellen können
- Apps richtig installieren
- Nutzungsbedingungen von Apps kennenlernen
- Sichere Einstellungen bei Apps kennenlernen und vornehmen können
- Fakeshops erkennen

Einstieg

Zu Beginn bietet es sich an, mit den Teilnehmenden zum Thema „Smart Home“ ins Gespräch zu kommen. Nutzen Sie hierfür die untenstehenden Fragen und finden Sie heraus, welche digitalen Geräte die Teilnehmenden besitzen und nutzen. Die Auflistung der Endgeräte dient als Orientierung, da vielen Menschen gar nicht bewusst ist, wie viele digitale Geräte sie im Alltag nutzen.

Fragen zur Anregung:

Die Auflistung gilt als Orientierung für die / den Kursleiter*in:

Licht	Heizung / Thermostat
TV	Waschmaschine / Trockner
Spülmaschine	Kaffeemaschine
Wasserkocher	Jalousien
Saugroboter	Mähroboter
Garagentor	Türschloss
Kamera / Alarmanlage	E-Bike/ E-Auto

Nach dem Einstieg bietet es sich an, gemeinsam die ersten Schritte für die Nutzung eines neuen Endgeräts durchzugehen. Nehmen wir den Saugroboter als Beispiel. Nachdem alles ausgepackt und aufgebaut wurde, muss die passende App installiert werden. Einer der ersten Schritte bei der Installation wird die Auswahl eines Passwortes sein. Greifen Sie das Thema auf und sprechen sie gemeinsam über „Sichere Passwörter".

Dazu kann die Website **checkdeinpasswort.de** genutzt werden, aber dabei beachten: Niemals wirklich genutzte Passwörter eingeben! Die Website gibt eine Orientierung darüber, welche Kriterien ein Passwort (un)sicherer machen.

Auf der Website **haveibeenpwned.com** kann zusätzlich nachgeschaut werden, ob die eigene E-Mailadresse in bereits bekannten, öffentlichen Datenbanken auftaucht („Have I been pwnd?" bedeutet umgangssprachlich so viel wie „Wurde ich besiegt?"). Falls ja, sollte das Passwort schnell geändert werden.

Kriterien für ein sicheres Passwort:

- Ein Passwort sollte nicht für mehrere Zugänge (Apps, E-Mails, Onlineshops) genutzt werden.
- Ein Passwort sollte mindestens acht Zeichen lang sein, je länger desto bsser.
- Es sollte aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen, die bunt durchmischt sind.
- Manche Dienste bieten eine Zwei-Faktor-Authentifizierung an, also einen zusätzlichen Schutz neben dem Passwort. Diese sollte eingerichtet werden.

Bei der Installation der neuen App gibt es verschiedene Einstellungsmöglichkeiten, die berücksichtigt werden sollten. Um eine Idee davon zu erhalten, welche Daten eine App speichert und welche Berechtigungen sie benötigt, können folgende Fragen exemplarisch für die App eines Staubsauger-Roboters gestellt werden:

Die Bedeutungen einzelner App-Berechtigungen können hier nachgelesen werden:

https://appcheck.mobilsicher.de/berechtigungen

Es ist in der Regel sinnvoll, auf Erfahrungsberichte zurückzugreifen. In Bezug darauf, welche Daten Apps von den Nutzer*innen speichern, gibt es auch leicht verständliche technische Analysen, die weitreichende Einblicke gewähren:

Apps analysieren mit Exodus Privacy (für Android):
reports.exodus-privacy.eu.org/de/
Welche Tracker bindet meine Lieblings-App ein und welche Zugriffsberechtigungen für das System und meine Daten möchte sie?

Apps analysieren mit TrackerControl (für iOS):
ios.trackercontrol.org
Welche Tracker und Drittanbieter in meinen Apps „schnüffeln" in meinem Smartphone oder in meinen Daten? Hier werden immer wieder neue Berichte zu iOS-Apps hochgeladen.

Fakeshops:

Fakeshops stellen ein hohes Risiko für persönliche Daten dar. Im Internet stößt man schnell auf verlockende Angebote, doch es ist nicht immer leicht herauszufinden, ob der Shop wirklich echt ist.

Einstieg:

Nutzen Sie die Fragen und gehen Sie mit den Teilnehmenden ins Gespräch.

- Was sind Fakeshops?
- Worauf achtest du bei unbekannten/neuen Shops?
- Wie kannst du überprüfen, ob es sich um einen seriösen Onlineshop handelt?
- Bist du schon einmal auf einen Fakeshop hereingefallen?
- Wie bist du damit umgegangen?

Auf der Seite **https://www.watchlist-internet.at/liste-betruegerischer-shops/** lassen sich Shops finden, die unter Beobachtung stehen. Suchen Sie vor Beginn der Unterrichtseinheit einen Shop heraus, den Sie gemeinsam mit den Teilnehmenden unter die Lupe nehmen wollen.

- Was für Auffälligkeiten gibt es?
- Was kommt den Teilnehmenden seltsam vor?
- Gibt es Kriterien, die einen Fakeshop entlarven? Wie könnten diese aussehen?

Kommt Ihnen ein Shop seltsam vor, können Sie auf der Seite der Verbraucherzentrale prüfen, ob es sich Fakeshop handelt:

https://www.verbraucherzentrale.de/fakeshopfinder-71560

FAKESHOPS?
SO ERKENNST DU SIE

DIGITAL CHECK NRW

Es gibt einige Merkmale, die darauf hinweisen können, dass ein Onlineshop ein Fakeshop sein könnte.

1

Zu gute Preise

Wenn die Angebote viel günstiger sind als anderswo, solltest du misstrauisch sein.

2

Merkwürdige Domainnamen

Stimmt die Domain (der namensgebende Teil der Internetadresse) mit dem Namen des Shops überein? Werden ungewöhnliche Endungen wie „.de.com“ verwendet, die auf eine deutsche Seite hindeuten, aber dann doch eine internationale Endung nutzen?

3

Kein Impressum

Seriöse Shops haben immer ein Impressum mit Kontaktinformationen der Verantwortlichen und ihrer Handelsregisternummer, denn diese Angaben sind für Anbieter verpflichtend.

4

Seltsame Bezahlmethoden

Wenn am Ende des Bestellprozesses nur unsichere Bezahlmethoden wie z. B. Überweisung per Vorkasse angeboten werden oder andere als vorher angegeben, ist Vorsicht geboten.

5

Kein HTTPS

Achte darauf, dass die Adresse des Shops mit "https://" beginnt. Das „s“ steht für „secure“ (sicher) und zeigt, dass die Verbindung verschlüsselt ist, was zumindest für erhöhte Sicherheit und Seriosität spricht.

MEHR INFORMATIONEN:
WWW.DIGITALCHECK.NRW