Digitale Gesellschaft e.V. | Groninger Straße 7 | 13347 Berlin
digitalegesellschaft.de | info@digitalegesellschaft.de @digiges | 030 450 840 18

DIGITALE GESELLSCHAFT

Workshop 5: Basispaket Sicherheit

Zielgruppe: 5./6. Klasse, Grundschule im Quartiersmanagement Gebiet Pankstraße (Berlin-Wedding)

Dauer: 80 Minuten (2x40 Min + 10 Min Pause)

Lernziele:

- Gefahren im Netz kennenlernen und Möglichkeiten, sich davor zu schützen, bewerten lernen
- verstehen, wie ein Smartphone vor unberechtigten Zugriffen geschützt werden kann
- erkennen, welche Bedeutung sichere Passwörter haben und wie unsichere Passwörter geknackt werden können
- eine Ahnung davon bekommen, welche Passwörter/PINs sicherer als andere sind
- den Messenger-Dienst Signal kennen lernen, der eine Datenschutz-freundliche Alternative zu WhatsApp darstellt

Material:

- Arbeitsblatt: gute PINs schlechte PINs (siehe pdf-Anlage)

Thematischer Einstieg:

Nachdem die Lernenden in den vorherigen Workshops einige Probleme des Internets kennengelernt haben, ist es nun an der Zeit, den Schülern und Schülerinnen Methoden an die Hand zu geben, sich vor den Gefahren zu schützen. Im Rahmen einer Doppelstunde können selbstverständlich nur wenige Aspekte aufgegriffen werden.

Zentral für die Sicherheit im Internet und am Smartphone sind gute Passwörter und PINs, die nicht einfach „erraten" werden können. Deshalb wird den Teilnehmenden zunächst einmal vermittelt, welche persönlichen Daten oder auch Onlinekonten durch Passwörter und PINs geschützt werden. Dann werden erste Einblicke gegeben, welche Methoden Angreifer benutzen, wenn sie versuchen, sich in fremde Accounts einzuloggen. Dabei

werden Brute-Force- und Wörterbuch-Attacken thematisiert. Mit diesem Wissen lassen sich sichere Passwörter und PINs generieren.

Dass das Geschäftsmodell von WhatsApp das Sammeln von persönlichen Daten ist, haben wir bereits in vorherigen Workshops besprochen und die Teilnehmenden für die Problematik sensibilisiert. Als Alternative probieren wir Signal als Messenger-App auf dem Smartphone aus. Viele Menschen würden gerne von WhatsApp zu einer besseren Alternative wechseln, jedoch ist das Problem dabei, dass alle ihre Kontakte WhatsApp verwenden und man auf der alternativen Plattform ohne Kontakte dasteht. Durch die Installation der App auf den Geräten der ganzen Klasse, lässt sich dieses Problem zunächst vielleicht umgehen.

Weitere Hintergrundinformationen zum Thema

- Klicksafe: App-Berechtigungen / Apps und Datenschutz: https://www.klicksafe.de/themen/kommunizieren/apps/apps-datenschutz/ und Privatsphäre-Einstellungen: https://www.klicksafe.de/themen/kommunizieren/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/
- Wie funktioniert ein Computer? aus der Sendung mit der Maus: https://www.youtube.com/watch?v=5PJZz04JGjs
- Was steckt in einem Smartphone? https://blog.deinhandy.de/ratgeber/26012017/was-steckt-in-einem-smartphone
- Beispiel: Taschenlampe sammelt Daten - https://www.teltarif.de/taschenlampe-android-app-nutzerdaten-ausspioniert/news/53617.html
- Spiegel Online: App-Berechtigungen, was erlauben und was nicht? http://www.spiegel.de/netzwelt/web/app-berechtigungen-was-erlauben-was-nicht-a-1172615.html
- Berechtigungen: Was wissen Apps über mich? https://www.handysektor.de/artikel/berechtigungen-was-wissen-meine-apps-ueber-mich/
- Cryptoparty: https://www.cryptoparty.in/
- Die häufigsten Passwörter und PINs: https://www.netzpiloten.de/die-25-haufigsten-passworter-und-pins/
- EFF (Electronic Frontier Foundation): Secure Messaging? More Like A Secure Mess: https://www.eff.org/de/deeplinks/2018/03/secure-messaging-more-secure-mess

Ablauf Workshop:

I. Erste Stunde: Messenger-Dienst Signal

1. Einstieg: Geschäftsmodell Daten

Zum Einstieg wird auf die letzte Stunde zurückgeblickt, wie das Geschäftsmodell mit persönlichen Daten im Netz funktioniert. Das Gespräch wird auf WhatsApp und die datenschutzfreundliche Alternative Signal gelenkt.

2. Praxisteil: Signal (20 Min)

Die Lernenden sollen Signal ausprobieren. Dafür steht ihnen ein Internetzugang zur Verfügung. Bevor es losgeht, werden Regeln definiert, wie die Schüler und Schülerinnen ihr Smartphone in der Unterrichtsstunde einsetzen dürfen.

Folgende Aufgaben erhalten die Teilnehmenden:

1. Verbinde dein Smartphone mit dem WLAN
2. Suche die App SIGNAL im App Store auf deinem Smartphone und installiere sie
3. Beginne einen Dialog mit deinem Nachbarn / deiner Nachbarin
4. Eröffne eine Gruppe, der du alle deine Freunde aus der Klasse hinzufügst, falls du noch zu keiner Gruppe eingeladen wurdest. Schreibe eine Nachricht in die Gruppe.
5. Versende ein Foto
6. Versende eine Sprachnachricht

3. Reflexion

Die Teilnehmenden bewerten, das gerade Erlebte:

- Wo liegen die Unterschiede zwischen WhatsApp und Signal?
- Welches sind die Vor- und Nachteile?
- Können Sie sich vorstellen, weiter Signal zu nutzen?

Es wird erklärt, dass es zu vielen populären Diensten im Internet datenschutz-freundlichere Alternativen gibt.

II. Zweite Stunde: Handy-Sperrmethoden

1. Einstieg ins Thema

Diskussion: Wer von euch, würde mir sein Smartphone über die Pause überlassen?

- Wenn nein, warum nicht?
- Erarbeiten, was man darauf alles gespeichert hat.

Welche Möglichkeiten gibt es, das eigene Smartphone zu schützen?

- Pin-Codes, Gesichts/Iris-Scan, Muster
- Wie sicher ist was?
- PIN-Codes relativ sicher, solange niemand anderes zusieht

Was ist ein sicherer PIN-Code und was ist ein unsicherer?

(Wie würden wir vorgehen, wenn wir einen Code knacken wollen?)

Ansehen der am auf häufigsten verwendeten PINs und Diskussion, warum diese nicht gut sind (siehe Glossar als pdf-Anlage).

2. Regeln für gute Pins

Die Schüler und Schülerinnen notieren die Regeln für gute PINs aus dem Glossar (siehe pdf-Anlage).

3. Arbeitsblatt (10 Min):

Die Teilnehmenden bearbeiten das Übungsblatt „gute PIN? Schlechte PIN?“ (siehe pdf-Anlage)

4. Wie merkt man sich eine komplizierte PIN?

Die Lernenden diskutieren „Eselsbrücken“ zum Merken komplizierter PINs.

Zum Beispiel:

- „Ich bin 09 geboren, meine Mutter 1975 und meine Großmutter 1958“ - das ergibt das Passwort: 097558

- „Montags habe ich 6 Stunden Schule, Dienstag 8, Mittwoch 7, Donnerstag 9 und Freitag 5. Samstag habe ich frei (0)“ - das ergibt das Passwort: 687950
- Samstags habe ich 2019 immer frei – das ergibt das Passwort: Shi2019if

5. Erstellen eigener PINs samt Merkhilfe

Die Lernenden erhalten, z.B. in zweier Gruppen, die Aufgabe, sich eine PIN auszudenken und dazu eine Möglichkeit, wie sie sich diese merken können – beispielsweise über einen Satz. Am Ende werden diese vorgestellt und diskutiert.

Weiterführende didaktische Ideen

- Verschlüsselung thematisieren, indem man die Lernenden eigene Nachrichten nach einem vorgegebenen, einfachen Verfahren verschlüsseln und von anderen Lernenden wieder entschlüsseln lässt.
- https-Verschlüsselung nutzen
- Sicherheit von biometrischen Systemen thematisieren und ausprobieren (Gesichtsscanner durch Fotos überlisten, Fingerabdruckscanner durch Fingerabdruckkopie etc.)
- Selbst erstellte Passwörter können auf Webseiten wie https://checkdeinpasswort.de überprüft werden (Dabei sind die angegebenen Zeiträume, die zur Entschlüsselung notwendig wären, im Zeitalter von Cloud-Computung nicht mehr zeitgemäß.)

Anhang

- PIN Sicherheit
- Glossar Basispaket Sicherheit