F.12

IT-Sicherheit

Einheit: Sicherheitsregeln im Datenschutz von Privatpersonen und Unternehmen

Redaktion RAAbits Online Informatik RAABE Verlag

© SEAN GLADWELL/Moment

Anhand eines Informationstextes erarbeiten sich die Lernenden die grundsätzlichen Sicherheitsregeln in Bezug auf Datenschutz. Anhand von Aufgaben üben sie das neu erlernte Wissen. Eine als Übersichtsblatt oder Tafelbild einsetzbares Mindmap zu den Regeln rund um sichere Kennwörter dient der zusammenfassenden Übersicht. Eine Lernerfolgskontrolle kann zum Abschluss der Einheit oder als Hausaufgabe Einsatz finden.

KOMPETENZ

Klassenstufe: 8–10
Dauer: 2–3 Unterrichtsstunden
Lernziele: Die Lernenden 1. geben die Kriterien eines sicheren Kennwortes an, 2. nennen Regeln im sicheren Umgang mit Kennwörtern, 3. nennen die Gefahren von Piraten-Software, 4. beschreiben, wer physischen Zugang zu Geräten haben sollte, 5. erklären, warum und wann Administratorrechte sinnvoll sein können.
Thematische Bereiche: Sicherheit im Internet, Datenschutz, sicheres Kennwort, Piraten-Software, Administratorrechte
Kompetenzen: Analysieren und Reflektieren

Wie ist diese Unterrichtseinheit aufgebaut?

In dieser Unterrichtseinheit erarbeiten sich Ihre Schülerinnen und Schüler zunächst anhand eines Informationstextes mithilfe von Texterschließungsmethoden die grundsätzlichen Sicherheitsregeln in Bezug auf Datenschutz. Diese üben sie an Aufgaben ein. Eine als Übersichtsblatt oder Tafelbild dienende Mindmap gibt einen Überblick über Kriterien sicherer Kennwörter. Die Einheit kann mit einer Lernerfolgskontrolle abgeschlossen werden.

Durch die Bereitstellung der Materialien auf zwei Niveaustufen ist die Lerneinheit auch für heterogene Lerngruppen geeignet.

Wie kann die Erarbeitung des Themas im Unterricht erfolgen?

Vorbereitung

- ☐ Stellen Sie ausreichend Tablets/Laptops/PCs, idealerweise ein Gerät pro Schüler/in mindestens aber ein Gerät pro Schülerpaar, zur Verfügung.
- ☐ Stellen Sie Internetzugang sicher.

Einstieg

Werfen Sie in der **ersten Doppelstunde** den Stillen Impuls **M 1** in den Raum und sammeln Sie Schülermeldungen dazu, ob es sich hierbei jeweils um sichere Kennwörter handelt. Vielleicht werden schon einige wichtige Regeln in der Herstellung von Kennwörtern genannt, sodass hiermit der Kenntnisstand der Lerngruppe oder einzelner Schülerinnen und Schüler erfragt werden kann. Leiten Sie dann zum Informationstext **M 2** zu Sicherheitsregeln im Datenschutz über.

Erarbeitung und Sicherung

Zur Erarbeitung der grundsätzlichen Sicherheitsregeln in Bezug auf Datenschutz teilen Sie den Informationstext **M 2** aus. Lassen sie die Lernenden diesen in Einzelarbeit bearbeiten. Eine Texterschließungsmethode (z. B. markieren wichtiger Begriffe, finden von Überschriften zu Teilabschnitten o. ä., sollte Anwendung finden.

Hinweis zur Binnendifferenzierung von M 2: Je nach Leistungsstand der einzelnen Schülerinnen und Schüler gibt der Informationstext auf zwei verschiedenen Niveaustufen (**M 2a** und **M 2b**) zur Verfügung. Lassen sie die Lernenden Ihre Niveaustufe entweder selbst auswählen oder teilen Sie diese direkt entsprechend aus.

Die Schülerinnen und Schüler bearbeiten anschließend die Aufgaben auf dem Arbeitsblatt **M 3**. **M 4** stellt eine als Tafelanschrieb oder zusammenfassendes Übersichtsblatt nutzbare Mindmap der Kriterien für ein sicheres Kennwort dar.

Lernzielkontrolle

M 5 dient als abschließende Lernzielkontrolle zur gesamten Einheit und kann im Unterricht oder als Hausaufgabe bearbeitet werden.

Auf einen Blick

Einstieg

Thema: Sicherheitsregeln beim Datenschutz im Internet am Beispiel des Kennwortes

M 1 **Ist das ein sicheres Kennwort?**

Erarbeitung und Ergebnissicherung

Thema: Grundsätzliche Sicherheitsregeln zum Datenschutz

M 2a **Informationstext: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz / M-Niveau**

M 2b **Informationstext: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz / G-Niveau**

M 3 **Aufgaben: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz**

M 4 **Tafelbild: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz**

Lernzielkontrolle

M 5 **Lernzielkontrolle: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz**

Erklärung zu den Symbolen

Dieses Symbol markiert differenziertes Material. Wenn nicht anders ausgewiesen, befinden sich die Materialien auf mittlerem Niveau.			
leichtes Niveau	mittleres Niveau	schwieriges Niveau	
Zusatzaufgaben	Alternative		

M 2a

Informationstext: Grundsätzliche Sicherheitsregeln in Bezug auf Datenschutz

© pixabay/CC0

Sicherheitsregeln in Bezug auf Datenschutz werden in Unternehmen in der Regel in sogenannten Sicherheitsrichtlinien festgelegt. Alle Mitarbeitenden sind verpflichtet, sich an diese Regeln zu halten, um das Unternehmen zu schützen. Die Einhaltung dieser Regeln sollte regelmäßig überprüft werden. In Unternehmen gibt es auch Software, die die Einhaltung dieser Regeln erzwingt und überwacht. Die Regeln variieren in verschiedenen Unternehmen je nach Art der zu schützenden D[illegible] der Netzwerkinfrastruktur usw. Die Sicherheitsrichtlinien müssen daher immer auf [illegible] konkrete Si[illegible]on zugeschnitten werden. Zu den Sicherheitsrichtlinien eines Unternehmens gehört zum Beispiel au[illegible]er Zugang zum Serverraum hat, ob man für den Zutritt in bestimmte Bereiche d[illegible]engebäudes eine Chip-Karte oder Security-ID benötigt u. Ä.
Einige Regeln sind jedoch allgemeingü[illegible]und auch privat tut ma[illegible]gut daran, sich an diese Regeln zu halten. Wir beschränken uns im Folgende[illegible]uf diese allg[illegible]nen Regeln.

1. Regeln für die Sicherheit von [illegible]nwor[illegible]
Hier stellt sich die Frage: Wann ist ein [illegible]ennwort sicher? Nicht sicher sind in jedem Fall Kennwörter,

- die die gesamte Abteilung/Familie ke[illegible]weil jeder mal kurz Zugriff auf die Daten des anderen braucht,
- die mit einem Post-[illegible]Zette[illegible]Monitor oder unter der Tastatur befestigt sind (sehr beliebte Aufbewahrungsplätze, oder sich in d[illegible]ersten Schreibtischschublade befinden,
- die zum Andenken an die [illegible]e Liebe nach Freund oder Freundin, nach dem geliebten Haustier oder Ähn[illegible]m benannt si[illegible]
- die e[illegible]rach lee[illegible]elassen werd[illegible]
- di[illegible]n Liebling[illegible]star oder andere leicht zu erratende Wörter beinhalten.

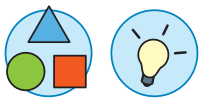
Moderne [illegible]mputer können [illegible]olche Kennwörter mit Programmen in sehr kurzer Zeit knacken, indem einfach ei[illegible]Wortliste durchprobiert wird. Das nennt man Wörterbuch-Angriff. In vielen Fällen, [illegible]im Namen [illegible]Freundin braucht man aber nicht einmal ein Programm. Da kommt man selbst m[illegible]enhändi[illegible]em Raten vermutlich in kurzer Zeit zum Ziel.

Selbst wenn e[illegible]Kennwort aus beliebigen Zeichen besteht, aber ziemlich kurz ist (z. B. 5 Zeichen), [illegible]det ein Co[illegible]puter mit einfachem Testen aller möglichen Kombinationen schnell den Zugang. Dies[illegible]s Brute-Force-Angriff bezeichnet.

Ein sicheres Kennwort sollte daher:

- mindestens 8 Zeichen lang sein (heute besser schon 16 oder noch länger – generell gilt: je länger je besser),
- aus zufälligen Buchstaben in Groß- und Kleinschreibung, Ziffern und Sonderzeichen bestehen,
- dennoch so leicht zu merken sein, dass es nicht (!) aufgeschrieben oder gar auf dem Computer gespeichert wird.

M 3 Aufgaben: Grundsätzliche Sicherheitsregeln



Aufgabe 1

Denke dir einen Kennwort-Satz aus und bilde ein sicheres Kennwort. Schütze deinen Rech[illegible]r damit. (Natürlich so, dass es dein Sitznachbar bzw. deine Sitznachbarin nicht mitbekommt[illegible]

Aufgabe 2

© Pixabay/CC0

Mache eine Liste aller Dienste im Internet, bei denen du Benutzerkonten hast, zum Beispiel Web-Mail-Anbieter, Social-Media-Plattformen, Verkaufsportale, Banken etc. Verwendest du auf jedem dieser Dienste ein einmaliges Kennwort? Gibt es Dienste, auf denen du dasselbe Kennwort verwendest? Sind die verwendeten Kennwörter sicher? Wenn du feststellst, dass deine Kennwörter unsicher sind, ändere sie möglichst bald. Installiere einen Kennwort-Manager[1], wenn du Schwierigkeiten hast, den Überblick zu behalten.

Aufgabe 3

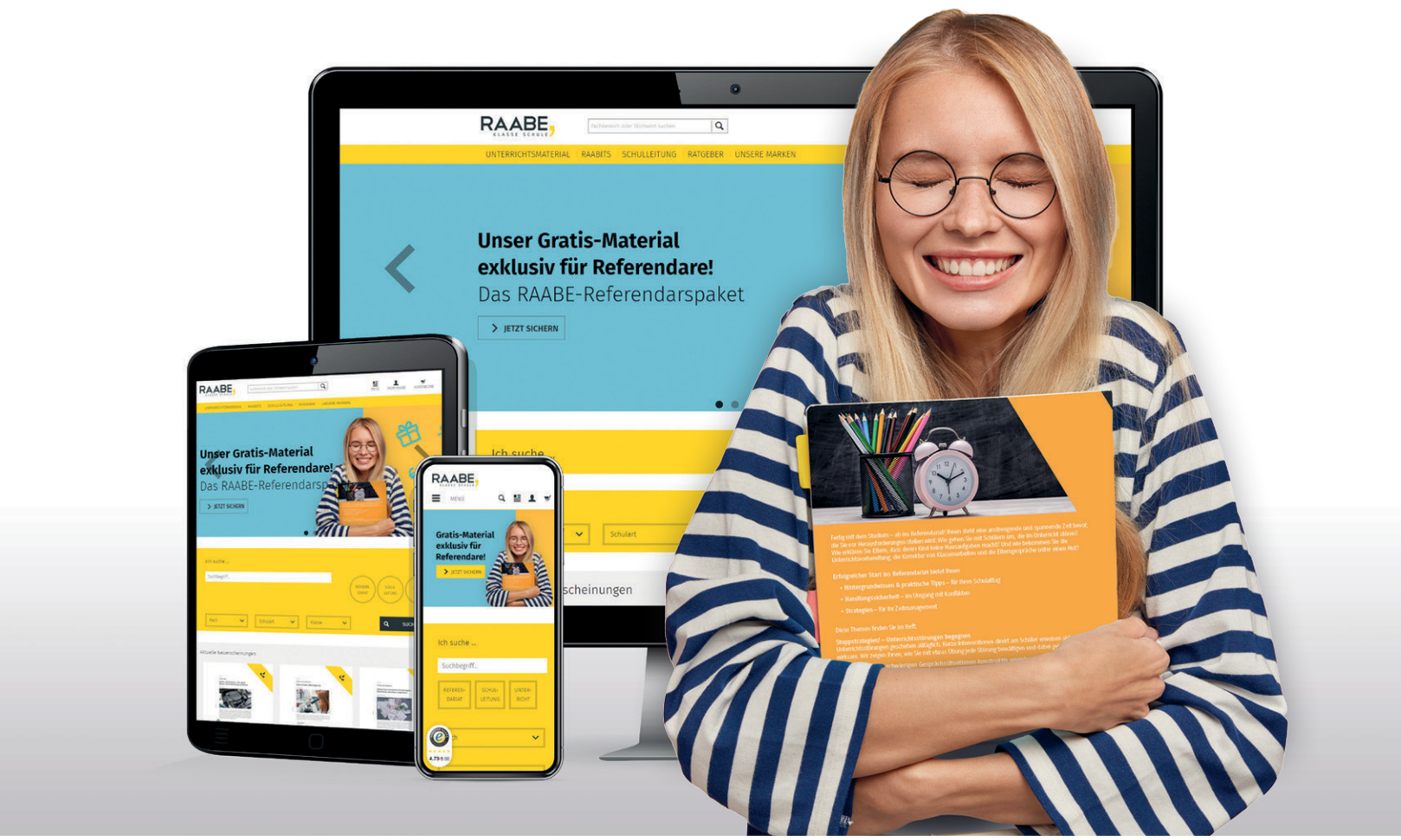
Öffne die Seite „Have i been pwned?“:https://[illegible]veibeenpw[illegible]om/ (13.04.2022). Diese Seite sammelt Daten aus bekannten Datenlecks, bei denen in der Vergangenheit E-Mail-Adressen von verschiedenen Diensten (bei dene[illegible]t) gestohlen und im Internet zugänglich gemacht wurden. Wenn du deine E-[illegible]il-Adresse eingibst, siehst du im besten Fall einen grünen Hinweis: „Good news — no pwnage found“. Das bedeutet, deine Mail-Adresse wurde noch nie (zumindest nicht in den b[illegible]ntesten Lecks) komp[illegible]ttiert. Wenn du die folgende Anzeige siehst, bedeutet das, dass deine E-Mail-[illegible] kompromittiert wurde (und möglicherweise andere Daten).

[1] Beispiele: KeePass:https://keepass.info/ oder LastPass: https://www.lastpass.com/de/pricing (13.04.2022)

RAABE
KLASSE SCHULE

Sie wollen mehr für Ihr Fach?

Bekommen Sie: Ganz einfach zum Download
im RAABE Webshop.



- **Über 5.000 Unterrichtseinheiten**
  sofort zum Download verfügbar
- **Webinare und Videos**
  für Ihre fachliche und
  persönliche Weiterbildung
- **Attraktive Vergünstigungen** für Referendar:innen
  mit bis zu 15% Rabatt
- **Käuferschutz**
  mit Trusted Shops

TRUSTED SHOPS GUARANTEE

Jetzt entdecken:

www.raabe.de