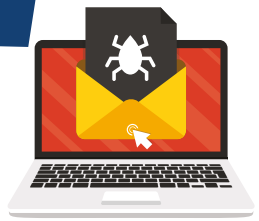
TEIL 3 Was ist zu tun bei...?



Weißt du, wie Cyber-sicherheit gewährleistet werden kann?

HINTERGRUNDINFORMATIONEN

Der Aufstieg des **Internets** hat unsere Gesellschaft grundlegend verändert. Ein Leben ohne Internet kann man sich kaum noch vorstellen. Ein Großteil der Bevölkerung ist immer und überall online: zu Hause, in der Schule, am Arbeitsplatz. Wir sind auf sozialen Medien aktiv, regeln unsere Banksachen online und benutzen das Internet, um Sachen zu lernen oder einfach Spaß zu haben. Internet und E-Mail haben viele Vorteile, aber sie haben auch eine Schattenseite: Cyberkriminalität, wie Phishing, Malware, Hacking, DDoS-Angriffe und Bankkartenbetrug. Alle können mit Betrug über das Internet konfrontiert werden.

Es ist wichtig, dass Menschen sich vorher gegen diese Form der Kriminalität wappnen und vorsichtig sind, wenn sie online sind. Deswegen werden in der Informationsbroschüre die wichtigsten Hinweise für Eltern aufgelistet. Sie können die Hinweise auch mit den Kindern in der Klasse besprechen. Weitere Informationen über Cybersicherheit finden Sie unter safeonweb.be/de.

In dieser Lektion beschränken wir uns auf Cybersicherheit, nämlich den Schutz Ihrer Online-Daten und Ihrer Geräte. Möchten Sie weitere Informationen über sichere Internetbenutzung, soziale Medien und Cybermobbing erhalten, besuchen Sie bitte die Website von Child Focus (FR) oder klicksafe.de.

ZIELE DER LEKTION

- Die Schüler/innen wissen, dass sie vorsichtig sein müssen, wenn sie online sind.
- Die Schüler/innen gewährleisten, dass vertrauliche Informationen und Passwörter privat bleiben.
- Die Schüler/innen können einige Beispiele von Gefahren im Internet geben.
- Die Schüler/innen wissen, wie sie mit diesen Gefahren umgehen müssen.
- Die Schüler/innen sprechen über Probleme im Internet.

MATERIAL

Anhang 1

- Checkliste (Anhang 1)
- Internet
- Papier

VERLAUF DES UNTERRICHTS

1) Anfang

Wenn Sie z.B. ein Passwort verwenden, um sich auf dem Schulcomputer anzumelden oder im Internet zu surfen, können Sie den Startbildschirm an dem interaktiven Whiteboard zeigen. Laden Sie einige Schüler/innen dazu ein, zu versuchen, das Passwort zu knacken. Fragen Sie, ob die Schüler/innen es eine gute Idee finden, dass Sie ein Passwort haben, ob sie selbst Passwörter verwenden und wofür (Spielkonten, soziale Medien, Zugriff auf Laptop, Computer, Handy, Bankkonto). *Hat jemand schon mal sein Passwort mit einer anderen Person geteilt? Mit wem? War das vernünftig?* Lassen Sie die Schüler/innen erklären, warum Passwörter wichtig sind.

2) Kern

Teilen Sie die Klasse in fünf Gruppen auf und lassen Sie jede Gruppe Informationen über ein Teilthema suchen. Lassen Sie sie eine digitale Präsentation (PowerPoint) machen, die sie der Klasse zeigen. Erklären Sie, dass sie erläutern müssen, was das Thema ist, wie man im Voraus sehr sicher arbeiten kann und was man machen soll, wenn es trotzdem schief läuft. Die Teilthemen sind:
- Sicherungskopien machen
- Computerviren und Virenscanner
- Phishing und Spam
- Passwörter
- Hacking und Updates

Jetzt, wo die Schüler/innen wissen, was Phishing ist, was gute und schlechte Passwörter sind und welche Informationen sie besser (nicht) teilen, können sie auch den Level „Surfst du sicher?" des Online-Spiels BE-Ready spielen.

3) Verarbeitung

Jede/r Schüler/in erstellt individuell eine Checkliste mit den Sachen, die man vor, während und nach Internetkriminalität machen kann. Besprechen Sie ggf. zuerst, wie eine Checkliste aussieht. Besprechen Sie die Checkliste in der Klasse oder korrigieren Sie sie wie eine Hausaufgabe. Sie können auf der Grundlage der Checklisten der Kinder ggf. eine einzige endgültige Checkliste machen (lassen) und diese nach Hause mitgeben. Im Anhang finden Sie ein Beispiel einer Checkliste (Anhang 1).

Name: .....

ICH BIN CYBERSICHER!

Lese diese Checkliste und entdecke, was du machen kannst, um dich online zu schützen.

VORHER

- ◯ Ich teile meine **Passwörter** nie mit anderen und ändere sie oft. Ein Passwort ist wie eine Zahnbürste: Es wird niemandem weitergegeben und wird regelmäßig ersetzt! Wähle auch ein starkes Passwort.
- ◯ Ich mache regelmäßig eine **Sicherungskopie** und führe zusammen mit meinen Eltern regelmäßig **Updates** aus.
- ◯ Ich weiß, dass nicht alle Nachrichten im Internet richtig sind. Ich kann eine **falsche Nachricht** erkennen. Ich antworte nie auf eine falsche Nachricht und lösche sie sofort.
- ◯ Ich bin **vorsichtig**, wenn ich etwas **teile**. Ich weiß ja nicht, wer mitliest!
- ◯ Ich **decke** meine **Kamera** ab, verwende einen Aufkleber oder Webcam-Cover. Man schließt die Vorhänge ja auch, wenn man nicht möchte, dass Leute reinblicken?

WÄHREND

Im Falle eines Computervirus:

- ◯ Ich bitte meine Eltern, den **Virenscanner** zu **aktivieren**. Wenn ein Virus anwesend ist, hilft der Virenscanner, das Virus zu entfernen.
- ◯ Wenn ich noch keinen Virenscanner installiert habe, **wähle** ich zusammen mit meinen Eltern einen zuverlässigen Scanner (safeonweb.be/de/hilfe-ich-habe-einen-virus) und lasse diesen seine Arbeit machen.

Wenn mein Konto gehackt wurde:

- ◯ Ich **scanne** mein Computer mit meinem **Virenscanner**.
- ◯ Ich ändere sofort alle Passwörter. Ich mache das mit einem **sicheren Gerät**, also nicht dem Gerät, von dem meine Daten gestohlen wurden.

Bei einem anderen Computerproblem:

- ◯ Ich bitte einen Erwachsenen um **Hilfe**, z.B. meine Eltern oder einen Lehrer bzw. eine Lehrerin. Je schneller du ein Computerproblem meldest, desto besser kannst du geholfen werden.

NACHHER

Wenn ich ein Opfer von Cyberkriminalität bin:

- ◯ Ich **benachrichtige** meine Eltern und gehe mit ihnen zur Polizei.