DEEL 3 Wat te doen bij ...?

Weet jij hoe je zorgt voor cyberveiligheid?

ACHTERGRONDINFO

De opkomst van het **internet** heeft onze samenleving grondig veranderd. Een leven zonder internet is nog nauwelijks in te beelden. Een groot deel van de bevolking is altijd en overal online: thuis, op school, op het werk. We zijn actief op sociale media, regelen onze bankzaken online en benutten het internet om bij te leren of om ons te amuseren. Internet en e-mail hebben veel voordelen, maar kennen ook een keerzijde: cybercriminaliteit, zoals phishing, malware, hacking, DDosaanvallen en bankkaartfraude. Iedereen kan worden geconfronteerd met oplichting via het internet.
Het is belangrijk dat mensen zich vooraf wapenen tegen die vorm van **criminaliteit** en voorzichtig zijn wanneer ze online gaan. Daarom vind je in de informatiebrochure de belangrijkste tips voor de ouders. Je kunt de tips ook met de kinderen in de klas bespreken. Meer informatie over cyberveiligheid vind je op safeonweb.be.

In deze les beperken we ons tot cyberveiligheid, nl. het beschermen van je online gegevens en van je toestellen. Wil je meer informatie over veilig internetten, sociale media en online pesten, dan kun je terecht op de website van Childfocus.

LESDOELEN

- De leerlingen weten dat ze voorzichtig moeten zijn als ze online gaan.
- De leerlingen houden gevoelige informatie en wachtwoorden privé.
- De leerlingen kunnen enkele voorbeelden geven van gevaren op het internet.
- De leerlingen weten hoe ze met die gevaren moeten omgaan.
- De leerlingen durven te praten over problemen op het internet.

MATERIAAL

Bijlage 1

- checklist (bijlage 1)
- internet
- papier

LESVERLOOP

1) Instap

Als je een wachtwoord gebruikt voor bijvoorbeeld je schoolcomputer of om op het internet te gaan, dan kun je het startscherm op het digibord laten zien. Nodig enkele leerlingen uit om te proberen het wachtwoord te kraken. Vraag of de leerlingen het slim vinden dat je een wachtwoord hebt, of ze zelf wachtwoorden gebruiken en waarvoor (game-accounts, sociale media, toegang laptop, computer, gsm, bankrekening). *Heeft iemand zijn wachtwoord al eens met iemand anders gedeeld? Met wie dan? Was dat verstandig?* Laat ze aangeven waarom wachtwoorden belangrijk zijn.

2) Kern

Maak vijf groepjes en laat elk groepje informatie opzoeken over een deelonderwerp. Laat een digitale presentatie (PowerPoint) maken die ze aan de klas tonen. Geef aan dat ze moeten uitleggen wat het onderwerp is, hoe je vooraf extra veilig kunt werken en wat je moet doen als het toch misgaat.
De deelonderwerpen zijn:

- back-ups maken
- computervirussen en virusscanners
- phishing en spam
- wachtwoorden
- hacken en updaten

Nu de leerlingen weten wat phishing is, wat goede en slechte wachtwoorden zijn en welke informatie ze beter wel of niet delen, kunnen ze ook het level 'Surf jij veilig?' van de online game BE-Ready spelen.

3) Verwerking

Elke leerling maakt individueel een checklist van wat je voor, tijdens en na internetcriminaliteit kunt doen. Bespreek eventueel eerst hoe een checklist eruitziet. Bespreek de checklists klassikaal of kijk ze als huiswerk na. Eventueel kun je op basis van de checklists van de kinderen één definitieve checklist (laten) maken en die meegeven naar huis. In de bijlage vind je een voorbeeld van een checklist (bijlage 1).

Bijlage 1

Naam: .....

IK BEN CYBERVEILIG!

Overloop deze checklist en ontdek wat je kunt doen om jezelf online te beschermen.

VOOR

- ◯ Ik deel nooit mijn **wachtwoorden** met anderen en verander ze vaak. Je wachtwoord is zoals je tandenborstel: die geef je ook niet aan anderen en je vervangt hem regelmatig! Zorg ook voor een sterk wachtwoord.
- ◯ Ik maak regelmatig een **back-up** en doe regelmatig **updates**, samen met mijn ouders.
- ◯ Ik weet dat niet alle berichten op het internet echt zijn. Ik kan een **vals bericht** herkennen. Ik antwoord nooit op een vals bericht en verwijder het meteen.
- ◯ Ik ben **voorzichtig** met wat ik **deel**. Je weet niet wie kan meelezen!
- ◯ Ik **bedek** mijn **camera**, gebruik een sticker of webcamcover. Je doet je gordijnen toch ook dicht als je niet wilt dat mensen kunnen binnenkijken?

TIJDENS

Bij een computervirus:

- ◯ Ik vraag mijn ouders om de **virusscanner** te **activeren**. Als er een virus aanwezig is, helpt de virusscanner me om het virus te verwijderen.
- ◯ Als ik nog geen virusscanner geïnstalleerd heb, **kies** ik samen met mijn ouders een betrouwbare scanner (safeonweb.be/nl/heb-je-een-virus) en laat die zijn werk doen.

Wanneer mijn account gehackt is:

- ◯ Ik **scan** mijn computer op virussen met mijn **virusscanner**. Ik **vervang** onmiddellijk al mijn **wachtwoorden**. Ik doe dat vanop een veilig toestel, dus niet het toestel waarop mijn gegevens werden gestolen.

Bij een ander computerprobleem:

- ◯ Ik vraag **raad** aan een volwassene, bijvoorbeeld aan mijn ouders of een leerkracht. Hoe sneller je een computerprobleem meldt, hoe beter je geholpen kunt worden.

NA

Als ik het slachtoffer ben van cybercriminelen:

- ◯ Ik **verwittig** mijn ouders en ga met hen naar de politie.