

Cybercrime Challenge

Dit is de vierde van in totaal vijf lessen over cyber security. Tijdens deze les gaan de leerlingen gezamenlijk in gesprek over verschillende dilemma's. Er is geen goed of fout: het gaat om het gesprek met elkaar en een mening vormen vanuit een groeiend moreel kader. De leerlingen krijgen inzicht in welke soorten cybercrime er zijn, en hoe ze zich daartegen kunnen beschermen. Ook leren ze wat de gevolgen zijn van hun keuzes. Eventueel kun je de leerlingen in de virtuele wereld van HackShield de geleerde kennis laten toepassen.

De les heeft zowel doe- als praat opdrachten en is daardoor afwisselend en interactief.

Totale duur: 1 uur.

Verbinding met beroepen en de arbeidsmarkt

De politie doet haar best om mensen te beschermen tegen cybercrime. Maar ook grote bedrijven zoals Ziggo en KPN, proberen mensen te helpen om de juiste keuzes te maken om cybercrime tegen te gaan.

Ethiek en Technologie

In deze les werken we met het ethische vraagstuk: Hoe kun je jezelf beschermen tegen cybercrime en in hoeverre hebben de keuzes die je maakt hier invloed op?

- Introductie: Keuzes kunnen de kans op cybercrime vergroten [10 min]
- Doen: De leerlingen gaan in gesprek met elkaar en noteren hun keuzes [30 min]
- Verdieping: Leerlingen bespreken de invloed van hun keuzes [10 min]
- Afronding: Samenvatting van de les [5 min]

Doel van de les

Domein curriculum 2021	Leerdoelen Digitale vaardigheden	Leerdoel (kern)vak	21st Century Skills
Data & Informatie DG1.2 Digitale data	1 Mediawijsheid De leerling weet dat je op verschillende manieren kan reageren op een mediaboodschap (bijvoorbeeld je niet laten verleiden).	1 Oriëntatie op jezelf en de wereld De leerling leert zich redzaam te gedragen in sociaal opzicht, als verkeersdeelnemer en als consument.	1 Kritisch denken
Veiligheid en privacy in de digitale wereld DG2.1 Veiligheid in de digitale wereld.	2 Media wijsheid De leerling begrijpt het belang van een veilig wachtwoord.	2 Nederlands De leerling leert informatie te beoordelen in discussies en in een gesprek dat informatief of opiniërend van karakter is en leren met argumenten te reageren.	2 Samenwerken
Veiligheid en privacy in de digitale wereld DG2.2 Privacy in de digitale wereld.	3 Mediawijsheid De leerling start met het ontwikkelen van een strategie om optimaal met media om te gaan.		

Vorbereiding

Van tevoren kun je een aantal dingen doen:

- Lees de handleiding en lesbrief
- Bekijk zelf de dilemma's waar de leerlingen mee aan de slag gaan
- Bedenk van tevoren of je de leerlingen na de les de vierde episode van HackShield laat spelen: <https://www.joinhackshield.nl> Je kunt de leerlingen ook de tip geven om dit thuis te doen.
- In iedere les ontvangen jij en de leerlingen een puzzelstukje van een QR-code. De vijf puzzelstukjes vormen samen een gehele QR-code die jullie toegang geeft tot een speciaal gedeelte van het spel HackShield!

Benodigdheden

- Digibord met internetverbinding
- Lesbrief voor de leerlingen en per leerling een pen of potlood
- Eventueel een tablet/laptop per tweetal

Wat is HackShield?

HackShield is een gratis transmediale cybersecurity game voor kinderen tussen de 8 en 12 jaar. En hun (groot)ouders, vriendjes, broertjes, zusjes, juffen, meesters en andere vrienden en bekenden. Het internet kent veel gevaren, en kinderen zijn een makkelijke prooi. Ze zijn goed van vertrouwen en weten niet (altijd) hoe ze zichzelf moeten beschermen. Daarom maakt HackShield van kinderen Cyber Agents die niet alleen zichzelf, maar ook hun omgeving kunnen beschermen tegen online gevaar!

HackShield begint met een basistraining waarin de speler alles leert over online veiligheid. Als je deze hebt voltooid mag je jezelf Junior Cyber Agent noemen. Daarna speelt de speler nieuwe content vrij, zoals de Quests (opdrachten) die de Cyber Agent samen met zijn omgeving kan uitvoeren zodat ze er samen van leren. HackShield is online te spelen via www.JoinHackShield.nl en op smartphone en tablet via de app (te downloaden in de App Store en Google Play).

Introductie, Praten met de klas

Cybercrime Challenge



Slide 1: Verschillende manieren van Cybercrime



In de voorgaande lessen zijn er verschillende vormen van cybercrime voorbij gekomen. Weten jullie nog welke? In deze les gaan we aan de hand van een aantal dilemma's in gesprek met elkaar. Er is geen goed of fout. Vorm je eigen mening. Natuurlijk kun je het ook eens zijn met elkaar. Bedenk en beargumenteer waarom je iets vindt. Ik ben van mening dat.....Omdat....Het eerste dilemma doen we samen. Als het dilemma zometeen op het bord verschijnt, blijven we stil. Je bepaalt zelf wat jij van de stelling vindt en dit noteer je op je lesbrief. Daarna gaan we met elkaar in gesprek. Ready?

Slide 2: Als je slachtoffer wordt van cybercrime kun je daar helemaal niets aan doen.



Vraag de leerlingen of ze het eens of oneens zijn met deze stelling. Waarom? Als de meningen verdeeld zijn, laat de leerlingen dan kort discussiëren samen.

Slide 3: Eigen keuzes



De keuzes die je maakt, kunnen beïnvloeden of jij wel of niet slachtoffer wordt van cybercrime. Welke keuzes hebben er bijvoorbeeld invloed op of je wel/niet gehackt wordt? En of je wel of niet slachtoffer wordt van phishing?
Maak opdracht 1 op de lesbrief.

Doen

Slide 4: Wat is jouw mening?



Vertel: Op je lesbrief staan zes stellingen. Deze ga je nu eerst voor jezelf bekijken en lezen. En daarna vorm je er je eigen mening over. Dit doe je in stilte. Vervolgens ga je in gesprek met je buurman/ buurvrouw over de zes stellingen. Wie heeft wat geantwoord? Hebben jullie ook dezelfde antwoorden gegeven? En dezelfde argumenten? Zijn jullie het eens met elkaar? Waarom wel/ niet?

Verdieping

Slide 5: Het gevolg



Maak de les weer plenair wanneer dat volgens jou het moment is. De leerlingen zijn uitgesproken met elkaar. Geef een aantal leerlingen de beurt: hoe is het gegaan? Wat ontdekten jullie? Hadden jullie een verschil in mening? Wat zat dat in?

Hebben jullie ook iets geleerd van een ander? Wil iemand daar iets over zeggen?

Bespreek de verschillende keuzemogelijkheden en de gevolgen. Begrijpen de leerlingen de gevolgen van hun keuzes?

Beroepenslide/arbeidsmarkt

Slide 6: Opletten!



De politie doet haar best om mensen te beschermen tegen cybercrime. Maar ook grote bedrijven zoals Ziggo en KPN, proberen mensen te helpen om de juiste keuzes te maken om cybercrime te voorkomen. Waarom zouden bedrijven als Ziggo en KPN dit doen, denken jullie?

Hoe ver mag de politie gaan volgens jou? Mogen ze iedereen volgen op het internet omdat als je niets hebt gedaan, dat dan toch niet erg is? Wat vind jij?

Er is steeds meer vraag naar mensen die strategieën kunnen bedenken om cybercrime te voorkomen. Of degene die cybercrime pleegt op te sporen. Wie lijkt zo'n beroep wel wat? En hoe zou zo'n baan heten? Wat ben je dan?

Afronding

Slide 7



Dit was de vierde les over cybercrime. We hebben deze les geleerd dat onze keuzes de kans op cybercrime kunnen beïnvloeden. Hoe kunnen we ons het beste beschermen tegen cybercrime?

Hebben jullie ook al HackShield gespeeld? HackShield is een game die je gratis kunt spelen. Thuis of op school. Er staat op de slide weer een stukje QR-code klaar. Als we alle vijf de lessen volgen krijgen we vijf stukjes die samen 1 QR-code vormen. Daarmee krijgen we toegang tot iets speciaals in de HackShield game. Bewaar je lesbrief en stukje QR-code goed! (Of laat de leerlingen die lesbrief inleveren met hun naam erop geschreven)