Hackers de Baas

Lessenserie

Inhoud

Les 1 – Kwartet (nep of echt)

Deze activiteit is erop gericht om leerlingen op een offline manier een aantal begrippen over de online wereld te leren. De leerlingen gaan in groepjes van 4-5 leerlingen het kwartetspel één of twee keer spelen. Daarna vindt het nagesprek plaats waarin je in drie verschillende stappen vragen stelt aan de leerlingen.
*In deze les ligt het accent op de **groene kaarten** (echt of nep).*

Les 2 – Mini-presentaties (hacken)

In deze les krijgen de groepjes één van de paarse kwartetkaarten. De leerlingen gaan opzoek wat dat die begrippen betekenen. De groepjes gaan met deze informatie een mini-presentatie (maximaal 3 minuten) geven, zodat de hele klas ook weet wat deze begrippen betekenen. Er is hiervoor een werkblad gemaakt wat ingevuld kan worden.
*In deze les ligt het accent op de **paarse kaarten** (hacken).*

Les 3 – Dilemma's (baas over je gegevens)

Tijdens deze activiteit leren leerlingen een aantal begrippen rondom het feit dat je eigenaar (baas) bent over je eigen gegevens. Je bespreekt samen met de leerlingen een aantal dilemma's rondom dit onderwerp. De dilemma's worden voorgelezen en eventueel getoond op een digibord. Op een interactieve manier kunnen de leerlingen hun mening geven over deze dilemma's.
*In deze les ligt het accent op de **oranje kaarten** (baas over je gegevens).*

Les 1 – Speel het kwartet (nep of echt)

Lesduur
+/- 60 minuten

Doelgroep
Groep 7 & 8
Geschikt voor leerlingen tussen de 10 t/m 12 jaar.

Leerdoelen
De leerlingen leren...
- hoe de naam van een website is opgebouwd;
- wat sterke en zwakke wachtwoorden zijn;
- wat een verdachte website kan zijn;
- hoe iemand een computer kan binnenkomen.

De leerdoelen sluiten aan bij de overkoepelende leerdoelen van digitale geletterdheid, (kern)vak, 21st century skills en domein curriculum 2021, te vinden in bijlage 1.

Benodigdheden
- Per groepje van 4-5 leerlingen één kwartetspel
- Klaslokaal of ruimte met tafels waar groepjes van 4-5 leerlingen kunnen zitten.
  Ze kunnen eventueel ook in groepjes op de grond gaan zitten.

Begrippen
De begrippen die behandeld worden in deze les zijn:
- Subdomein
- Identiteitsfraude
- Hackers
- D-Dos
- Botnet
- Wachtwoorden
- Veilige wachtwoorden
- VPN
- Phishing

De betekenis van deze begrippen is te vinden in bijlage 2.

Algemeen
Deze activiteit is erop gericht om leerlingen op een offline manier een aantal begrippen over de online wereld te leren. De leerlingen gaan in groepjes van 4-5 leerlingen het kwartetspel één of twee keer spelen. Daarna vindt het nagesprek plaats waarin je in drie verschillende stappen vragen stelt aan de leerlingen.

*In deze les ligt het accent op de **groene kaarten** (echt of nep).*

Uitwerking

Introductie - 5 min

Vertel de leerlingen dat jullie vandaag iets gaan leren over online veiligheid, zoals een goed wachtwoord opstellen of een verdachte website herkennen. Hierover gaan jullie vervolgens een kwartetspel spelen.

Introductievragen

- Wat is online veiligheid?
  Mogelijk antwoord:
  Online veiligheid is dat je jezelf op het internet kunt beschermen tegen gevaren, zoals hacken en phishing.
- Wie weet er wat hacken is?
  Mogelijk antwoord:
  Het (illegaal) inbreken in een computer.
- Weet iemand hoe je je kan beschermen tegen een hacker?
  Mogelijke antwoorden:
  - *Goede wachtwoorden gebruiken*
  - *Niet zomaar op een linkje klikken*
  - *Geen openbare WIFI gebruiken*
  - *Webcam Cover*
  - *Antivirussoftware*

Kern – 30 min

Maak groepjes van 4-5 leerlingen en deel aan ieder groepje een kwartetspel uit. Leg even kort centraal uit hoe je kwartet moet spelen (in het doosje van het kwartetspel zit een speelkaart met de spelregels).

Laat de leerlingen nu éénmaal het kwartetspel spelen.
Groepjes die snel klaar zijn, kunnen het kwartetspel nog een keer spelen.

Afsluiting - 25 min

Start een nagesprek met de klas. Leg daarbij vooral het accent op de **groene kaarten** (nep of echt). Je kunt bij dit nagesprek gebruik maken van de 3 stappen van vragen stellen. Deze stappen zijn te vinden in bijlage 3.

Stel daarnaast de volgende afsluitende vragen:

- Wat heb je van deze activiteit geleerd?
- Weet je wat [begrip] betekent?
- Welk onderdeel van deze activiteit was moeilijk?
- Welk onderdeel was makkelijk?
- Zou je de informatie uit dit spel kunnen gebruiken in het echte leven?

Tijd over?
Je kunt eventueel nog nieuwe begrippen langs laten komen uit de begrippenlijst in bijlage 2.

Les 2 - Mini-presentaties (hacken)

Lesduur
+/- 60 minuten

Doelgroep
Groep 7 & 8
Geschikt voor leerlingen tussen de 10 t/m 12 jaar.

Leerdoelen
De leerlingen leren...
- wat voor type hackers er zijn;
- hoe je hacking kan voorkomen;
- hoe hackers binnenkomen;
- wat voor soort aanvallen er zijn.

De leerdoelen sluiten aan bij de overkoepelende leerdoelen van digitale geletterdheid, (kern)vak, 21st century skills en domein curriculum 2021, te vinden in bijlage 1.

Benodigdheden
- Per tweetal: een computer/tablet met internet
- Per tweetal: geprint werkblad (zie bijlage 4)
- Klaslokaal of ruimte waar de de groepjes hun mini-presentaties kunnen voorbereiden

Begrippen
De begrippen die behandeld worden in deze les zijn:
- Soorten hackers
- D-Dos
- Botnet
- Cracken
- Tweestapsverificatie
- Phishing

De betekenis van deze begrippen is te vinden in bijlage 2.

Algemeen
In deze les krijgen de groepjes één van de paarse kwartetkaarten. De leerlingen gaan op zoek het hoofdbegrip op de kaart betekent. De groepjes gaan zullen met deze informatie een mini-presentatie (maximaal 3 minuten) geven, zodat de hele klas ook weet wat deze begrippen betekenen. Er is hiervoor een werkblad gemaakt wat ingevuld kan worden.

*In deze les ligt het accent op de **paarse kaarten** (hacken).*

Uitwerking

Introductie - 5 min

Vertel de leerlingen dat ze vandaag aan de slag gaan met een aantal begrippen rondom hacken. Ze maken daarbij gebruik van het kwartetspel en een speciale website waar ze meer informatie over deze begrippen kunnen vinden. Daarna maken ze hier een mini-presentatie over en presenteren ze die aan de rest van de klas.

Kern - 30 min

Verdeel de leerlingen in tweetallen en deel ieder tweetal een werkblad uit en één van de paarse kwartetkaarten. Neem met de leerlingen de stappen op werkblad door:

- Ga naar joinhackshield.com/hackersdebaas
- Scroll naar beneden op deze pagina
- Klik op de link: **mini-presentaties**
- Zoek dan de kwartetkaart die jullie hebben gekregen
- Bekijk de video onder deze kaart
- Schrijf 5 steekwoorden op over het onderwerp op de kaart

Vertel de leerlingen dat het doel van deze minipresentatie is dat de andere leerlingen weten wat het onderwerp op jullie kaartje was en de betekenis.

Mini presentaties - 15 min

Laat de leerlingen om de beurt een mini-presentatie geven over het onderwerp wat zij op hun kaartje hebben staan. Laat ze gebruik maken van de 5 steekwoorden die ze hebben opgeschreven op hun werkblad.

Afsluiting - 10 min

Start een nagesprek met de klas. Leg daarbij vooral het accent op de **paarse kaarten** (hacken). Je kunt bij dit nagesprek gebruik maken van de 3 stappen van vragen stellen. Deze stappen zijn te vinden in bijlage 3.

Stel daarnaast de volgende afsluitende vragen:

- Wat heb je van deze activiteit geleerd?
- Weet je wat [begrip] betekent?
- Welk onderdeel van deze activiteit was moeilijk?
- Welk onderdeel was makkelijk?
- Zou je de informatie uit dit spel kunnen gebruiken in het echte leven?

Tijd over?

Je kunt eventueel nog nieuwe begrippen langs laten komen uit de begrippenlijst in bijlage 2.

Les 3 - Dilemma's (baas over je gegevens)

Lesduur
+/- 60 minuten

Doelgroep
Groep 7 & 8
Geschikt voor leerlingen tussen de 10 t/m 12 jaar.

Leerdoelen
De leerlingen leren...
- wat een goed wachtwoord is;
- hoe je phishing kan herkennen;
- hoe ze incidenten kunnen melden;
- hoe je het hackers moeilijk kan maken.

De leerdoelen sluiten aan bij de overkoepelende leerdoelen van digitale geletterdheid, (kern)vak, 21st century skills en domein curriculum 2021, te vinden in bijlage 1.

Benodigdheden
- Een presentatie met dilemma's, te vinden op: joinhackshield.com/hackersdebaas
- Ruimte waar de leerlingen kunnen staan en een kant kunnen kiezen.

Begrippen
De begrippen die behandeld worden in deze les zijn:
- Wachtwoordkluis
- Wachtzin
- Versleutelde verbinding
- VPN
- Phishing

De betekenis van deze begrippen is te vinden in bijlage 2.

Algemeen
Tijdens deze activiteit leren leerlingen een aantal begrippen rondom dat je eigenaar (baas) bent over je eigen gegevens. Je bespreekt samen met de leerlingen een aantal dilemma's rondom dit onderwerp. De dilemma's worden voorgelezen en eventueel getoond op een digibord. Op een interactieve manier kunnen de leerlingen hun mening geven over deze dilemma's.

*In deze les ligt het accent op de **oranje kaarten** (baas over je gegevens).*

Uitwerking

Introductie - 5 min

Vertel de leerlingen dat jullie het vandaag gaan hebben over gegevens en en dat jij de baas bent over jouw gegevens. Dat jullie samen een aantal dilemma's gaan bespreken en dat ze daar hun mening over mogen geven.

Kern - 30 min

Open de presentatie met de dilemma's. Lees de dilemma's voor en laat ze eventueel zien op het digibord. Laat de leerlingen een keuze maken. De leerlingen kunnen op twee manieren een keuze maken:

1. Dit kan door hun hand op te steken
2. Je kunt ook het lokaal in tweeën delen en de leerlingen gaan steeds aan de kant van hun keuze staan.

Daarna kun je iedere keer één of twee leerlingen laten motiveren waarom ze deze keuze gemaakt hebben.

Afsluiting - 25 min

Start een nagesprek met de klas. Leg daarbij vooral het accent op de **oranje kaarten** (nep of echt). Je kunt bij dit nagesprek gebruik maken van de 3 stappen van vragen stellen. Deze stappen zijn te vinden in bijlage 3.

Stel daarnaast de volgende afsluitende vragen:

- Wat heb je van deze activiteit geleerd?
- Weet je wat [begrip] betekent?
- Welk onderdeel van deze activiteit was moeilijk?
- Welk onderdeel was makkelijk?
- Zou je de informatie uit dit spel kunnen gebruiken in het echte leven?

Tijd over?

Je kunt eventueel nog nieuwe begrippen langs laten komen uit de begrippenlijst in bijlage 2.

Bijlage 1 - Leerdoelen

Leerdoelen Digitale Geletterdheid:[1]

- Mediawijsheid – Medialisering - De leerling weet dat je op verschillende manieren kan reageren op een mediaboodschap (je niet laten verleiden).
- Mediawijsheid – Media, identiteit en participatie - De leerling start met het ontwikkelen van een strategie om optimaal met media om te gaan.
- ICT-basisvaardigheden – Infrastructuur technologie - De leerling leert over de financiële waarde van verschillende soorten accounts en content.
- ICT-basisvaardigheden – Veiligheid – De leerling kan een veilig wachtwoord aanmaken
- ICT-basisvaardigheden – Veiligheid – De leerling kan op basis van vuistregels eigen veiligheid rond betalingsverkeer inschatten ICT-basisvaardigheden
- Informatievaardigheden – Presenteren – De leerling kan een passende mondelinge presentatie geven op basis van informatie.

Leerdoelen (kern)vak:[2]

- Kerndoel 3 - 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.
- Kerndoel 35 - Oriëntatie op jezelf en de wereld – De leerling leert informatie zich redzaam te gedragen in sociaal opzicht, als verkeersdeelnemer en als consument.

21st Century Skills:[3]

- Kritisch denken
- Samenwerken
- ICT – basisvaardigheden
- Mediawijsheid
- Zelfregulering

Domein Curriculum 2021:[4]

- Data & Informatie – DG 1.2 Digitale Data – Leerlingen leren wat digitale data zijn, wat het belang van data is, hoe digitale technologie met data omgaat en hoe zij zelf met digitale data kunnen omgaan.
- Veiligheid en privacy in de digitale wereld – DG 2.1 Veiligheid in de digitale wereld – Leerlingen leren dat hun persoonsgegevens op allerlei plaatsen opgeslagen worden. Zij leren hoe zij ervoor kunnen zorgen dat hun gegevens veilig zijn en wat zij moeten doen als er toch iets misgaat.
- Veiligheid en privacy in de digitale wereld – DG 2.2 Privacy in de digitale wereld – Leerlingen leren dat alles wat zij online delen, online blijft staan. Zij leren welke regels er zijn over het plaatsten van en delen van media. Zij leren wat zij kunnen doen als het misgaat.
- Digitaal burgerschap – DG 5.2 Digitale identiteit – Leerlingen leren dat de manier waarop iemand zich online presenteert niet overeen hoeft te komen met de werkelijkheid en hoe zij daarmee om kunnen gaan.

---

[1] https://www.slo.nl/vakportalen/vakportaal-digitale-geletterdheid/leerlijnen-digitale-geletterdheid/
[2] https://www.slo.nl/sectoren/po/kerndoelen/
[3] https://www.kennisnet.nl/artikel/6648/alles-wat-u-moet-weten-over-21e-eeuwse-vaardigheden/
[4] https://www.curriculum.nu/

Bijlage 2 – Begrippenlijst

Biometrische beveiliging	Een beveiliging met bijvoorbeeld een oog of vingerafdruk.
Blockchain	Is een combinatie van kleine stukjes officiele gegevens bij verschillende bedrijven of de belastingdienst. Niet al je belangrijke gegevens bijéén, maar ze hebben allemaal een klein deel. Zodat jij het alleen kan combineren. Als een puzzel.
Bot	Een computerprogramma dat vanzelf ietst doet (een chat bot bijvoorbeeld).
Botnet	Verschillende bot's die met elkaar een grote hack doen.
Cracken	Iemand die computerbeveiliging wil hacken en misbruiken.
Cybersecurity	Je digitale gegevens laten beveiligen tegen virussen, phishing en bijvoorbeeld DDOS-aanvallen.
DDos	Een computerprogramma dat heel vaak inlogt op een computernetwerk. Het computernetwerk raakt daardoor overbelast en niemand kan meer werken.
Digitale ethiek	Het nadenken over: "Kan ik dit wel online wel doen? Is dit oke, maak ik niet iemand kwaad of verdrietig door deze afbeelding online te plaatsen?
Digitale etiquette	Regels die we met elkaar afspreken over hoe we online met elkaar omgaan.
Digitale identiteit	Wie ben ik online?
Encryptie	Het omzetten van een online bericht, zodat niemand het kan lezen.
Ethical hacken	Een vorm van hacken, die bedoeld is om bedrijven te helpen zodat ze niet gehackt gaan worden.
Hackers	Het (illegaal) inbreken in computers of computernetwerken.
Incognito	Op het internet surfen zonder dat anderen kunnen zien wat je hebt gedaan.
Identiteitsfraude	Je voordoen als iemand anders.
IP-adres	Het digitale adres waarmee een computer herkend kan worden.
Malware	Software bedoeld om privégegevens te krijgen (bank en inlog gegevens)
Phishing	Een oplichter probeert je naar een valse webpagina te lokken. Zodat hij je wachtwoord kan gebruiken.
Privacy	Je eigen (online) wereld, dat hoeft niemand te weten.
Ransomware	Losgeld om een computer weer te 'bevrijden' van malware, zodat je weer bij je gegevens kan komen.
Spamfilters	Software die kijkt of de e-mail die binnen komt phishing mail is.
Subdomein	Een subdomein is onderdeel van een website. De hoofdwebsite staat er altijd voor.
Tweestapsverificatie	Als je inlogt krijg je een extra beveiliging op je telefoon, of e-mail om in te loggen.
Versleuteld	Een beveiligde verbinding, bijvoorbeeld https of versleuteld op je telefoon, zodat niemand het kan ontcijferen.
Virusscanner	Software die scant of een computer virussen heeft.
VPN	Een extra beveiligde verbinding.
Wachtwoordkluis	Een veilige plek (vaak een app) waar je al je wachtwoorden kan opslaan. Deze app kan ook voor jou een sterk wachtwoord verzinnen.
Wachtzin	Een wachtwoord in de vorm van een zin.

De meeste van deze woorden komen uit de Bijlage A Digitale Geletterdheid van het voorstel van Curriculum.nu aan de Tweede Kamer.

Bijlage 3 - Drie stappen nagesprek

Stap 1: Vragen

Wie heeft het wel eens meegemaakt?
Gebruik de volgende vragen om het gesprek te starten:

- Wie heeft er wel eens een phishing e-mail gehad?
- Wie kent er iemand van wie de identiteit gestolen is?
- Wie kent er iemand van wie heel zijn computer versleuteld is door ransomware?

Stap 2: Doorvragen

- Wat is er toen gebeurd?
- Wat hebben ze toen gedaan?
- Wat was het gevolg voor die persoon (het slachtoffer)?
- Hoe kon dit gebeuren?

Stap 3: Tips

Geef tips om deze situaties te voorkomen:

- Weet met wie je praat;
  Wie is de afzender van de e-mail of het social media-account?
  Is dit het echte account, is de naam goed geschreven? Of is het misschien net een beetje anders
  Voorbeeld: Als iemand belt en zegt: 'Dit is de bank, er is een probleem met je rekening, je moet dit en dit doen'. Geloof je dat dan?
  Hoe kan je dit dan controleren? Verbreek de verbinding en bel de bank terug op een nummer dat bekend is (niet het nummer dat de persoon jou geeft).
- Weet waar je naar toe gaat;
  Als je gevraagd wordt om op een link te klikken, kijk dan eerst waar de link naar toe gaat voordat je erop klikt. Zie de kwartetkaarten van 'verdachte website' en 'Instagramsite' voor dingen waar je op moet letten. Is de URL gek, staan er veel cijfers in, schrijffouten, etc?
- Is het te mooi om waar te zijn;
  Dan is dat ook meestal zo. Je mag best op je gevoel vertrouwen. Als het niet goed voelt, controleer dan nog een keer goed 'met wie je praat' en 'waar je naar toe gaat'.
- Praat er over met je ouders, leerkracht of vrienden;
  Maak je iets geks, iets verdachts of iets dat niet pluis is mee online, praat er dan over met je ouders, leerkrachten en je vrienden. Deze mensen kunnen je helpen. Je ouders en leerkracht weten wat ze moeten doen in dit soort situaties.

WERKBLAD – LES 2

Wat moet je doen?

1. Ga naar **joinhackshield.com/hackersdebaas**
2. Scroll naar beneden op deze pagina
3. Klik op de link: 'Mini presentaties'
4. Zoek de kwartetkaart die jullie hebben gekregen
5. Bekijk de video onder deze kaart
6. Schrijf vijf steekwoorden op over het onderwerp dat op de kaart staat

Ons onderwerp is:

_____

en dit zijn onze vijf steekwoorden:

1._____

2._____

3._____

4._____

5._____

HACKSHIELD
FUTURE CYBER HEROES