

Mens verspreek je niet!

Tijdens deze les gaan de leerlingen ervaren waar je rekening mee moet houden op social media: hoe gebruik je social media veilig en bewust? Ook leren ze wat de risico's zijn en hoe ze die kunnen vermijden. Totale duur: 1 lesuur

LESOPBOUW

- Introductie: Inventariseren: wat doen de leerlingen op social media? (5 min)
- Verdieping: Wat zijn risico's en hoe ga je daarmee om? (15 min)
- Doen: Een boardgame ontwerpen om anderen bewust te maken van de risico's (30 min)
- Afronding: Leerlingen presenteren hun boardgame

VOORBEREIDING & BENODIGDHEDEN

Van te voren kun je een aantal dingen doen:

- Lees de handleiding en lesbrief
- Digi-bord met internetverbinding: klik door de slides voor op het digibord
- Print de lesbrief voor iedere leerling
- Verzamel gekleurd papier, scharen, stiften
- Zorg voor witte A3 vellen (liefst stevig papier)

DIFFERENTIATIE

Wanneer je meer tijd hebt voor deze les kun je de leerlingen ook creatief meer uitdagen bij het ontwerpen van een spel. Laat ze bijvoorbeeld iconen ontwerpen en toepassen die ze vinden passen bij de verschillende aandachtspunten van het spel. Ook kunnen de leerlingen verschillende routes in het spel ontwerpen: voor elke veelgebruikte social media app een eigen route. Ze kunnen ook een spel ontwerpen waarbij de 'goeden' tegen de 'slechten' spelen: bijvoorbeeld de stalker, cyberpester of hacker tegen de goed voorgelichte puber.

VERBINDING MET BEROEPEN & ARBEIDSMARKT

Zo zetten ontwerpers van apps, social media platforms en andere online toepassingen de skills uit deze les ook in om risico's voor de gebruikers te beperken. Facebook probeert met name jonge gebruikers voor te lichten over cybersecurity, en heeft bijvoorbeeld een platform voor cyberpesten en werkt samen met allerlei organisaties om gebruikers van het netwerk zo goed mogelijk voor te lichten over de risico's.

DOEL VAN DE LES

Domein curriculum 2021	Leerdoelen digitale vaardigheden	Kerdoelen techniek/bevo	21st century skills
1 Veiligheid en privacy in de digitale wereld DG2.1 Veiligheid in de digitale wereld	1 Mediawijsheid De leerlingen kunnen de gangbare verborgen mechanismen om persoonsgegevens te achterhalen en/of te misbruiken benoemen en herkennen.	De leerling kan de relatie tussen accounts, privacy en persoonlijke informatie aangeven. (curriculum.nu, 2019)	1 Communiceren
2 Digitale communicatie en samenwerking DG4.2 Digitale communicatie	2 Mediawijsheid De leerling kan bewust een eigen digitale identiteit vormgeven.	De leerling kan bewust vuistregels voor (digitale) veiligheid voor zichzelf en anderen bepalen (Curriculum.nu, 2019)	2 Kritisch denken

INTRODUCTIE

Openingsslide

Mens, verspreek je niet!



Slide 2, Klassikaal

Je telefoon. Waarschijnlijk besteed je er meer tijd op dan je zelf in de gaten hebt. Je regelt er alles mee: je agenda, Magister, huiswerk, muziek en ook verschillende social media. Superhandig om contact te houden met al je vrienden, foto's te laten zien van alle leuke dingen die je doet en als je wenkies on fleek zijn! Ga in gesprek met de leerlingen over de volgende vragen:

- Welke social media gebruik je?
Check met je leerlingen wie deze social media actief gebruikt: Facebook, Instagram, Snapchat, Whatsapp, Tiktok, YouTube en eventueel andere: Twitter, Skype of Pinterest.
- Welke social media gebruiken de leerlingen het meeste? En waarom?
- Wat is het leukste aan social media?



VERDIEPING

Slide 2, Klassikaal

Veel leerlingen weten best dat er risico's verbonden zijn aan het gebruik van social media, maar vergeten ook vaak om daar tijdens het gebruik rekening mee te houden.

Stel de volgende vragen en ga hierover kort in gesprek met de klas:

- Wie weet wat Cybersecurity is? Wie kan hier voorbeelden van noemen?

Antwoord: cybersecurity is het veilig maken van de online omgeving door middel van software/online tools/versleuteling van gegevens. Hierdoor kunnen gebruikers veilig gegevens achterlaten in een digitale omgeving. Bijvoorbeeld versleutelde berichten in Whatsapp, versleutelde websites en apps van banken waardoor je veilig kan inloggen: websites waar een hangslotje zichtbaar is in de balk.

Laat je leerlingen online informatie opzoeken over cybersecurity en social media: wat voor toepassingen worden er gebruikt? Laat ze hier in groepjes een woordspin over maken

- Wie kunnen jou volgen of met jou praten? **Bijvoorbeeld:** iedereen, alleen mensen die ik persoonlijk ken, ook vrienden van vrienden
Heb je een slotje op je account? Of kan iedereen meekijken?
Je weet natuurlijk dat je geen vreemden moet toevoegen. Maar hoe zit het met vrienden van vrienden, bijvoorbeeld? Voeg je die toe, ook als je ze niet kent?
Wie heeft een 2.O account? (een account dat goed op slot zit en waar je alleen met je beste vrienden dingen deelt, waardoor je meer persoonlijke dingen kan delen)
Wat zijn de voordelen en nadelen daarvan? **Voorbeeldantwoord:** als je bijvoorbeeld ruzie krijgt weet diegene heel persoonlijke dingen van je. Ben je wel eens bang dat iemand dit tegen je gebruikt?
Zijn er cybersecurity-mogelijkheden om te zorgen dat ook hier jouw persoonlijke gegevens veilig zijn? Voorbeeldantwoorden kunnen zijn: foto's waar je geen screenshot van kan maken, of berichten die na een aantal uur verdwijnen



- Wat voor berichten post jij? Welke informatie deel je? Vertel je algemene of persoonlijke dingen? Bijvoorbeeld: leeftijd, adres, school, exacte locatie (kaart op snapchat of letterlijk locatie vermelden in bericht) en of je alleen thuis bent
Natuurlijk denk je goed na bij elk bericht dat je post. Maak in groepjes een korte checklist die goed is om in je achterhoofd te hebben voordat je een bericht post
Voorbeeld van vragen voor een checklist: Wie lezen dit allemaal? Komt het misschien anders over dan ik het bedoel? Geef ik misschien informatie die je liever niet met veel mensen wil delen? Is het respectvol naar anderen toe?
- Wat voor foto's deel je? Bijvoorbeeld: selfies, locatie, foto's van anderen
Maak in groepjes een korte checklist: waar moet je eigenlijk even over nadenken voordat je een foto post?
Voorbeeld van vragen voor een checklist: wie krijgen de foto te zien? Is het een foto waar je mee gepest kan worden? Of iemand anders die erop staat? Wil je liever niet dat mensen die je niet goed kent deze foto zien? Heb je toestemming gevraagd aan anderen op de foto?
- Heb je wel eens iets vervelends meegemaakt online? **Bijvoorbeeld:** pesten, stalken, nepprofielen ongewenst contact met vreemden of ongewenst delen van je informatie
Wat doe je als iemand op social media op een vervelende manier met jou of iemand die je kent omgaat?
Antwoorden kunnen zijn: iemand waarschuwen als ik vervelende berichten over hem/haar voorbij zie komen, mensen aanspreken op vervelend gedrag online, melden aan een volwassene die kan helpen.

BEROEPENSLIDE/ARBEIDSMARKT

Slide 3, Handig om te leren om...

Vertel: Je weet nu al best veel over hoe jij je zo veilig mogelijk kan gedragen op internet. Gelukkig zetten veel ontwikkelaars van social media platforms zich ook in om te zorgen dat jij internet zo veilig mogelijk kan gebruiken. Grote bedrijven zoals YouTube en Facebook werken met cybersecurity-experts om te zorgen dat niet alleen hun eigen informatie, maar ook die van jou, niet in de verkeerde handen terecht komt. Een cybersecurity-expert zorgt bijvoorbeeld dat een website niet gehackt kan worden (zo komt niemand jouw wachtwoord te weten en kan niemand jouw privé berichten ooit lezen). Maar er zijn nog veel meer manieren waarop cybersecurity-experts zorgen voor een veilige internet-omgeving.

Laat het videofragment zien. Let op: het fragment is in het Engels. Als je leerlingen dit lastig vinden kun je het geluid zacht zetten en het zelf vertalen.



DOEN

Slide 4, Groepswerk

Zoals we hebben gezien is niet alleen de hacker die bedrijven helpt belangrijk in het voorkomen van nare problemen op internet. Het is ook heel belangrijk om anderen voor te lichten: uit te leggen wat je beter wel en niet kunt doen op internet. Dat gaan jullie nu zelf doen. Als iemand voor de klas staat te vertellen wat je wel en niet moet doen gaan, heb je misschien niet altijd zin om te luisteren of denk je “dat weet ik toch allang!”. Daarom gaan jullie een game ontwerpen. Als iemand de hele game goed uitspeelt kan hij of zij veilig gebruikmaken van social media, en snapt de speler ook hoe en wanneer cybersecurity wordt ingezet om hem of haar te beschermen. Je spel mag lijken op een bordspel als ganzenbord, mens-erger-je-niet of een ander spel, maar er moeten een paar belangrijke onderdelen in zitten. Die lees je terug in de lesbrief. Daar vind je ook wat voorbeelden van hoe spellen eruit zien... Voor het geval het al vreselijk lang geleden is dat je offline een spel deed!

Verdeel de klas in groepjes en laat elke groep een game ontwerpen. Deel naast de lesbrieven en A3-vellen ook stiften, scharen en gekleurd papier uit.



AFRONDING

Slide 5, Klassikaal / Groepswerk

Dus, we hebben besproken hoe we social media gebruiken en wat de valkuilen zijn. De meeste bedrijven doen hun best om te zorgen dat je zo veilig mogelijk gebruik kan maken van hun social media platforms. Daarvoor gebruiken ze cybersecurity-experts. We hebben ook geleerd dat dat niet alleen maar hackers zijn! Zelf hebben jullie games ontworpen die voor anderen nuttig zijn om te leren hoe ze veilig gebruik kunnen maken van social media.

Vraag elk groepje om in een paar minuten hun game te demonstreren en toe te lichten hoe de game de speler bewust maakt en voorlicht, en hoe cybersecurity kan worden ingezet om te zorgen dat je gegevens veilig kan delen online.

