Project: Weet wat je deelt

Verantwoording voor de leraar

Veiligheid en Privacy, het zijn woorden die de laatste jaren veel aandacht krijgen. We zijn steeds meer online bezig en worden van alle kanten in de gaten gehouden, benaderd en verleid. Dit gaat zoals in het echte leven vaak op een slinkse manier. We zijn ergens ingetrapt voor dat we het in de gaten hebben.

Met kennis van zaken creëren en vergroten de leerlingen de eigen digitale veiligheid en denken ze na over de kansen en risico's. Leerlingen leren omgaan met hun online identiteit en zijn zich ervan bewust dat zij gegevens gebruiken en sporen achterlaten bij het toepassen van digitale technologie. Ook leren zij hoe zij veiligheidsmaatregelen kunnen treffen om te voorkomen dat anderen ongewild gebruik maken van hun gegevens en van hun digitale apparaten.
Leerlingen leren bewust omgaan met persoonlijke gegevens in verschillende vormen (tekst, beeld, geluid) en na te denken over de privacy risico's van hun aanwezigheid in de digitale wereld en in media. Zij leren nadenken over hun online identiteit. Ze kiezen bewust welke gegevens ze met anderen delen en op welke wijze zij die gegevens delen.

Leerdoelen
Kennis en vaardigheden waar in deze opdracht aan wordt gewerkt:

Bovenbouw PO

- Leerlingen leren hoe ze de veiligheid van hun digitale leefomgeving kunnen beschermen.
- Leerlingen leren hoe accounts beveiligd kunnen zijn en hoe hun gegevens hiermee beschermd kunnen worden.
- Leerlingen leren hoe ze kunnen handelen bij een (mogelijk) veiligheidsprobleem.
- Leerlingen leren dat ze sporen achterlaten bij hun online gebruik en hoe dat gaat.
- Leerlingen leren dat zij het moeten aangeven als er online problemen zijn.
- Leerlingen leren dat persoonsgegevens waarde hebben voor anderen.
- Leerlingen leren actief om te gaan met het eigenaarschap van hun gegevens.
- Leerlingen leren na te denken over de gevolgen van het plaatsen van media-uitingen. Leerlingen leren zorgvuldig te zijn met andermans gegevens en de gevolgen als dat niet.

Onderbouw VO

- Leerlingen kunnen herkennen of hun online omgeving veilig is (denk aan toegangsrechten van applicaties, beveiligde verbindingen en gecertificeerde websites) en hoe ze die veiligheid zelf kunnen versterken d.m.v. tools als virusscanners, spamfilters en adblockers.
- Leerlingen weten welke technieken er bestaan om persoonlijke gegevens te beveiligen, zoals beveiligingsmethodes als biometrische technieken, encryptie en tweetraps verificatie.
- Leerlingen leren een bewuste en kritische houding aan te nemen, om zich te beschermen tegen huidige en toekomstige bedreigingen (bijvoorbeeld phishing en ransomware) en kennis hebben van technieken als botnets en DDOS-aanvallen.
- Leerlingen leren dat hun persoonlijke gegevens nooit volledig beveiligd zijn, denk bijvoorbeeld aan hacking en datalekken.
- Leerlingen leren een persoonlijk kader te ontwikkelen ten aanzien van onlinegedrag, waarbij een respectvolle houding ten opzichte van de persoonlijke integriteit de boventoon voert. Hierbij leren ze reflecteren op onveilig eigen gedrag (denk aan cyberpesten en sexting).
- Leerlingen leren de werking van technologie begrijpen, die het mogelijk maakt om hun digitale sporen in de digitale wereld te volgen en te analyseren en leren hoe verschillende partijen daarvan gebruik maken. dg1.1
- Leerlingen leren op basis van begrip van digitale technologie invloed uit te oefenen op de digitale sporen die zij achterlaten. Daarbij is zowel het eigen gedrag als het benutten van technische mogelijkheden (bijvoorbeeld ad-blockers, incognito-tabbladen, encryptie en specifieke apps) van belang.
- Leerlingen leren de inhoud van wetgeving rondom privacy-aspecten te begrijpen en hiernaar te handelen; denk hierbij aan de Algemene Verordening Gegevensbescherming (AVG).
- Leerlingen leren vanuit persoonlijk en maatschappelijk perspectief reflecteren op maatregelen die genomen kunnen worden om privacy in de digitale wereld te beschermen.
- Leerlingen besteden aandacht aan de manieren waarop digitale (persoons-)gegevens verzameld en gebruikt kunnen worden.

Lessenplan

<table>
<tr><th>Lesuur</th><th>Activiteit</th><th>Tijd</th></tr>
<tr><td>1</td><td>Introductie op het project.</td><td></td></tr>
<tr><td></td><td>De eerste opdracht is bedoeld om inzicht te krijgen in het internetgedrag van de leerlingen.
- Bekijk en bespreek het filmpje:
https://www.youtube.com/watch?time_continue=1&v=AnSSjajzYiI

- Wat vinden ze ervan (opvallend, apart, raar).
- Welk digitaal voetspoor laten zij achter. Denk aan apparaten, apps, websites, sociale media e.d.
  </td><td>15 min</td></tr>
<tr><td></td><td>Opdracht 1: wat is jouw digitaal voetspoor?
De leerlingen laten ook een digitaal voetspoor achter.
Laat de leerlingen daarvoor een Mindmap of Timeline maken
- Maak een mindmap met:
de door jouw gebruikte apparaten: pc, smartphone, tablet enz.
- Je handelingen: zoeken, gamen, streamen, online kopen enz.
- Maak een timeline van je internetgedrag over een paar dagen/week/weekend.</td><td>45 min</td></tr>
<tr><td>2</td><td>Laat de leerlingen verder werken.</td><td>30 min</td></tr>
<tr><td></td><td>Bespreek en bekijk de resultaten.
Let daarbij op:
- Of en welke persoonsgegevens ingevuld moeten worden tijdens het internet gebruik.
- Wat zijn ‘Persoonsgegevens’:
alle mogelijke soorten informatie die iets over jou als persoon onthullen zoals:
<table><tr><th colspan="3">Voorbeelden van persoonsgegevens</th></tr><tr><td>• Naam
• Telefoonnummer
• E-mailadres
• Huisadres
• Woonplaats
• Geboortedatum
• (Pas)foto's
• Vingerafdruk</td><td>• Ip-adres.
• Surfgeschiedenis
• Contacten/vrienden
• Je online winkelkarretje
• Sociale media profielen.
• Wat je ‘liked’ en shared
• Hobbies</td><td>• Gegevens die een waardering over een persoon geven, zoals bijv. een IQ
• Gevoelige gegevens zoals ras, godsdienst of gezondheid. De AVG noemt dit ‘bijzondere persoonsgegevens’ en beschermt ze extra goed.</td></tr></table>
- Vinden ze dat een bezwaar, kunnen ze die gegevens weer verwijderen en wat vinden ze daar later van.
- Kennen ze ook nog andere manieren waarop persoonlijke informatie op internet komt, zonder iets in te vullen?
Andere Onlineprivégegevens zijn: IP-adres, locatie (GPS).</td><td>30 min</td></tr>
</table>

3	**Loopt jouw veiligheid door dit internetgebruik in gevaar en hoe gaat dat?** **Laat de filmpjes zien of laat de lln dit zelf doen.** **Gebruik hierbij het invulblad.** **Cookies:** **https://www.youtube.com/watch?v=tYIsuErizt0** **Phishing**: Wat is het en zo herken je het! https://youtu.be/Wj7P4wan0UU hoe je een phishingmail herkent. **Hacken is:** https://www.youtube.com/watch?v=KFQGr5HguQU **https://www.youtube.com/watch?v=UBrH5-Kdkd8** Bespreek de filmpjes en de resultaten op het invulblad. Welke conclusies kun je trekken m.b.t de veiligheid en privacy.	30 min 30 min
4	**Slotopdracht 3.** **Maak zoveel groepen zodat elke opdracht minstens één/of twee keer gemaakt wordt** **Een poster maken (over privacy)** **Een folder/flyer maken. (Gevaren op het internet).** **Reclamefilmpje maken (Sire)** **Doel is te komen tot:** • Eén poster voor thuis/school met tips om veilig te internetten. De boodschap moet duidelijk zijn: • Welke privacy rechten heb je? • Wat kun je zelf doen ter bescherming van je privacy? - zet de locatiegegevens uit - zet je instellingen op privé – gebruik niet altijd je eigen naam - kies een sterk wachtwoord	60 min
5	Laat de opdracht afmaken. Groepen bereiden een presentatie voor van hun gemaakte product.	60 min
6	Groepen presenteren hun product: Maak verslag en probeer tot een gezamenlijk internetprotocol te komen, dat in de groep/thuis gebruikt kan worden. Laat een aantal “vrijwilligers” dit op een klasse poster verwerken.	60 min

Achtergrondinformatie

We maken veel gebruik van het internet en laten daar vele sporen achter.

Een digitaal voetspoor. Veel van onze persoonsgegevens blijven hangen. Denk aan:

Voorbeelden van persoonsgegevens		
• Naam • Telefoonnummer • E-mailadres • Huisadres • Woonplaats • Geboortedatum • (Pas)foto's • Vingerafdruk	• Ip-adres. • Surfgeschiedenis • Contacten/vrienden • Je online winkelkarretje • Sociale media profielen. • Wat je 'liked' en shared • Hobbies	• Gegevens die een waardering over een persoon geven, zoals bijv. een IQ • Gevoelige gegevens zoals ras, godsdienst of gezondheid. De AVG noemt dit 'bijzondere persoonsgegevens' en beschermt ze extra goed.

Andere gegevens zijn: IP-adres, gebruikersnaam, wachtwoord, locatie (GPS).
Deze informatie deel je vaak ongemerkt op internet. Als je iets opzoekt op internet, dan geef je al informatie weg. Je zoekt bijvoorbeeld naar voetbalschoenen. Dan 'weet' google dat jij geïnteresseerd bent in voetbal. Dat is interessante informatie voor sportzaken en schoenenzaken. Google kan jouw informatie dus verkopen aan bedrijven die sportartikelen verkopen. Door jouw gedrag op internet laat je dus een **digitaal voetspoor** achter. Dit doe je door de zoekopdrachten die je geeft, de websites die je bezoekt, de apps die je download enz. Door alles wat je deelt, bekijkt en volgt op internet wordt een beeld gemaakt van jou: wie ben jij als persoon en wat zouden je interesses nog meer kunnen zijn? Al deze gegevens worden gekoppeld tot een persoonlijk profiel. Ben je op internet, dan krijg je ook advertenties te zien, die met jouw interesses te maken hebben.
Aan de hand van jouw digitale voetspoor bepaalt de zoekmachine dus welke zoekresultaten voor jou interessant zijn. Je krijgt niet alle informatie te zien die er te vinden is over een onderwerp, maar een selectie daarvan. Dit gebeurt met cookies. Dit zijn kleine bestanden die worden opgeslagen op je computer of telefoon, waardoor bedrijven en andere organisaties kunnen volgen wat jij online doet

Privacy is:

Het recht om informatie over wie je bent, de plaats waar je je bevindt, wat je doet, met wie je contact hebt, voor je zelf te houden en te beschermen. Een recht om de persoonlijke levenssfeer te beschermen.
Dit recht wordt op het internet nogal eens bedreigd. O.a. door:
- Pop-Ups - Cookies - Phishing - Hacking

Wat zijn pop-ups?
Een venster dat verschijnt op een bepaalde pagina. Vaak is een pop-up een kleiner venster dan de oorspronkelijke pagina en wordt geladen na een bepaalde tijdsperiode of na een klik. Je kent het vast wel: je bent aan het surfen op het internet en bezoeken een website. Nadat de pagina is geladen verschijnt er een klein, nieuw venster, waarop een advertentie (of een andere kreet) te zien is. Dat is een pop-up. Pop-ups zijn vaak bedoeld als reclame en hebben de opzet om bezoekers op de pop-up te laten klikken, zodat ze naar de website van de adverteerder gaan.

Waarom worden pop-ups gebruikt?
Een pop-up vraagt aan de website bezoeker extra aandacht. Denk aan bijvoorbeeld:

- Een cookie-waarschuwing (daar heeft niemand problemen mee)
- Een advertentie voor een (gratis) product of dienst;
- Het verzoek om in te schrijven voor je nieuwsbrief;
- Het verzoek om contact op te nemen enz…..

Wat zijn cookies?

Een **cookie** is een klein tekstbestandje dat een website op de harde schijf van je computer zet als je die site bezoekt. C**ookies** kunnen gebruikers op de website uit elkaar houden en kunnen naar jou toe leiden.
Waarom is dat nodig?

- Een cookie onthoudt dat je bent ingelogd op een site, hoelang, waar je op hebt geklikt.
- Welke producten je in een winkelmandje op een webshop hebt gestopt.
- Onthoudt voorkeursinstellingen, zoals lettergrootte of taal, wat je hebt geliked en hebt ingevuld.
- https://www.youtube.com/watch?v=tYIsuErizt0

Websites moeten het je laten weten als er **cookies** worden geplaatst die je volgen (tracking cookies). Als je niet gevolgd wilt worden klik je dus op ‘niet akkoord’ als je de vraag krijgt. Dat betekent wel dat de website soms minder goed of helemaal niet werkt. Denk dus altijd goed na of je wel gevolgd wilt worden door een bepaalde site.

Wat is phishing?

Een vorm van internetfraude. Gebruikers worden naar een website gelokt. Deze website is een kopie van de echte site. Daar wordt gevraagd om een inlognaam en wachtwoord. Zo komen criminelen achter je privégegevens en hebben ze toegang tot je bankrekening.

Phishing? Wat is het en zo herken je het! https://youtu.be/Wj7P4wan0UU

Op veiliginternetten.nl staat uitgelegd hoe je een phishingmail herkent.

Phishing vindt plaats via e-mail en/of telefoon, bijvoorbeeld:

- We zijn bezig met een veiligheidsupdate, controleer uw gegevens
- Ik werk bij uw bank, mag ik uw gegevens controleren?
- U heeft een prijs gewonnen

Als je een link in een phishingmail aanklikt, word je vaak naar een nagemaakte website geleid waarbij de oplichters hopen dat je gevoelige informatie invoert, zoals je bankgegevens. Ook wanneer je een bestand opent dat meegezonden is met een phishingmail, kan je ongemerkt malware en spyware op je computer installeren. Door deze malware en spyware kunnen bijvoorbeeld belangrijke gegevens (zoals betalingsverkeer) onderschept worden.

Wat is hacken?

Hacken is het illegaal inbreken in computers of computernetwerken door het omzeilen van beveiligingsmaatregelen. Bestanden worden door hackers vaak vernietigd, beschadigd of gestolen.

https://www.youtube.com/watch?v=KFQGr5HguQU

https://www.youtube.com/watch?v=UBrH5-Kdkd8

https://www.hoezomediawijs.nl/wachtwoorden/

Enkele andere "gevaren" op het internet.

Bot: ook wel 'chatbot' of 'virtuele assistent' genoemd. Dit is software die online werkt of via een netwerk en automatisch vragen beantwoordt, commando's opvolgt (zoals een routebeschrijving naar het huis van je nieuwe vriend), of eenvoudige taken uitvoert (zoals een liedje afspelen).
Spearphishing: bij spearphishing is de aanval meer op jou persoonlijk gericht, doordat oplichters jouw persoonlijke informatie gebruiken.
Scam: een oneerlijke poging om geld te verdienen of iets waardevols te verkrijgen door mensen te misleiden.
Catfishing: een valse identiteit of account maken op een social media platform om mensen te misleiden om hun persoonlijke informatie te delen of te laten geloven dat ze met een echte persoon praten die schuilgaat achter een legitiem account, profiel of dito pagina.

Clickbait: manipulatieve online-inhoud, berichten of advertenties die zijn ontworpen om de aandacht van mensen vast te houden en ervoor te zorgen dat ze klikken op een link of webpagina, vaak om views of websiteverkeer te doen stijgen, om zo geld te verdienen.

Welke internetregels zijn belangrijk om te weten:

- Geen persoonlijke gegevens online te zetten, zoals een foto, telefoonnummer, e-mailadres, de naam van je school of je adres.
- Nooit op een link in een e-mail, op een pop-up of banner klikken.
- Niet zomaar iets downloaden, omdat het gratis is.
- Niet ingaan op contactverzoeken van onbekenden.
- Zorg voor een goede virusscanner op je computer en die regelmatig te updaten.
- Zorg dat belangrijke berichten een encryptie (versleuteling) hebben.
- Bij twijfel niets toestaan en/of overleg met ouders of leerkracht.
- Gebruik niet te makkelijke en steeds dezelfde wachtwoorden.
  Je kunt de sterkte van de wachtwoorden controleren op:
  https://veiliginternetten.nl/wachtwoordkraak-test/ .

Dit is een idee om een extra veilig paswoord te creëren:

- Minimaal 8 tekens. Langer is beter.
- Gebruik niet bij alles hetzelfde wachtwoord.
- Verander regelmatig (elk half jaar) van wachtwoord.
- Denk aan een leuke zin die je kan onthouden. Het kan je favoriete songtekst zijn, de titel van een boek, een quote uit een film, enz.
- Kies de eerste letters of de eerste twee letters van elk woord in de zin. Verander enkele letters in symbolen of cijfers.
- Kies enkele letters in hoofdletters en enkele in kleine letters.
- Overweeg een paswoordbeheerder, bijvoorbeeld een die ingebouwd is in je browser, om je paswoorden te onthouden. Zo kun je een uniek paswoord gebruiken voor elk van je accounts en hoef je ze niet allemaal te onthouden.

Wat moet je niet doen.

- Gebruik geen persoonlijke informatie (naam, adres, e-mail, telefoonnummer, de meisjesnaam van je moeder, geboortedata, enz.), of gewone woorden in je paswoord.
- Gebruik geen paswoord dat makkelijk te raden is, zoals je bijnaam, enkel de naam van je school, je favoriete voetbalteam, een cijferreeks (zoals 123456), enz. en gebruik zeker het woord “paswoord” niet!
- Deel je paswoord niet met iemand anders dan je ouders.
- Schrijf paswoorden nooit ergens op waar iemand ze kan vinden.

Welke rechten heb je als gebruiker?

Recht van inzage
Indien je wilt weten welke persoonsgegevens een organisatie over je heeft en bijhoudt, kan je dit gewoon vragen. Het bedrijf of de organisatie is verplicht om hierop te antwoorden.
Recht op correctie
Verzamelt er iemand foutieve informatie over jou? Je kan vragen om die gegevens te verbeteren. Je kan dit doen via brief, telefoon, mail of chat.
Recht om vergeten te worden
Iedereen kan vragen om onjuiste of oude gegevens te laten wissen, om welke reden dan ook. Hiervoor neem je best contact op met de eigenaar van de website of het platform in kwestie.
Recht op overdracht van gegevens
Veranderen van applicatie, staat niet langer gelijk aan het verliezen van al je content (foto's, video's, berichten, ...). De nieuwe Privacywet maakt het mogelijk om die content over te zetten naar een nieuwe applicatie. Dit principe geldt voor apps, sociale media, leveranciers, streaming diensten, enzovoort.

Beveiliging van de gegevens
Wie persoonsgegevens verzamelt is ook verplicht om deze streng te beveiligen.