Veilig online

Kinderen komen reeds van jongs af aan in contact met het internet via de tablet of smartphone. De mogelijkheden zijn onbeperkt: gamen, muziek luisteren, foto's en filmpjes delen, chatten … Ze doen het allemaal online en worden dan ook niet voor niets de digital natives genoemd. Deze themafiche gaat dieper in op hoe kinderen zich op een veilige manier kunnen begeven op het internet.

Wat je zeker moet weten over veilige wachtwoorden

1. **Een veilig wachtwoord voldoet aan een aantal voorwaarden.** Het bevat kleine letters, hoofdletters, cijfers en symbolen zoals * of #. Geef nooit je wachtwoord door. Je gebruikt ook best verschillende wachtwoorden voor verschillende accounts. Je kan ook eens een wachtzin gebruiken in plaats van een wachtwoord. Dit is een zin die je makkelijk kan onthouden, maar toch moeilijk te kraken is door hackers omdat die zo lang is. Verander je wachtwoorden regelmatig. Zo hebben hackers nog minder kans om je account te kraken.

2. **Oh nee, je bent je wachtwoord vergeten! Wat nu?** Bij de meeste websites kan je jouw wachtwoord resetten, maar bij sommige websites is dit wat moeilijker. Je kan je wachtwoorden wel opschrijven en op een veilige plaats bewaren, maar je kan ook gebruik maken van een '**wachtwoordmanager app**' zoals LastPass, 1Password … Dit zijn wachtwoordmanager apps waarop je al je verschillende wachtwoorden kan bewaren. Om deze te raadplegen heb je een 'master password' nodig, vaak in combinatie met een tweestapsverificatie.

3. **Two-factor authentication of tweestapsverificatie** is een aanmeldingsmethode waarbij je twee stappen succesvol moet doorlopen vooraleer je ergens toegang tot kan krijgen. Een eenvoudig voorbeeld daarvan is het aanmelden bij de bank met een kaartlezer. De eerste stap bestaat meestal uit het invoeren van je gebruikersnaam en wachtwoord. De tweede stap kan op verschillende manier gebeuren, namelijk een sms code of code die gegenereerd wordt in een Authenticator App. Tweestapsverificatie zorgt er zo voor dat je een extra beveiliging kan toevoegen aan je account.

Bescherm je online privacy

1. **Privacywat?** Privacy is een abstracte term en het is voor leerlingen niet altijd even duidelijk wat ermee bedoeld wordt. Privacy gaat over de vrijheid om zelf te bepalen wat je aan wie laat zien.

2. **De nieuwe privacywet of de Algemene Verordening Gegevensbescherming** (AVG), beter gekend als de GDPR, is van toepassing wanneer persoonsgegevens verwerkt worden. Iedereen die persoonsgegevens verwerkt, moet voldoen aan de nieuwe regels en voorschriften. Dankzij de GDPR kan je bij bedrijven altijd informatie opvragen over wat zij doen met jouw gegevens, namelijk verzamelen, gebruiken, delen, beveiligen en verwerken.

3. **Raadpleeg de privacyverklaring van bedrijven of organisaties** om te weten waarvoor je toestemming geeft over je persoonlijke gegevens. Deze kan je nalezen op de website van de bedrijven en organisaties. De privacyverklaring bevat informatie zoals wie je gegevens bijhoudt

en hoe je ze kan contacteren, waarvoor ze je gegevens gebruiken, of ze je gegevens delen met anderen, hoe lang je gegevens bijgehouden worden, hoe je foutieve gegevens kan verbeteren of verwijderen en hoe je een klacht kan indienen als ze je gegevens foutief gebruiken.

4. **Baas over je gegevens**. Privacy is pas een probleem wanneer anderen informatie over onszelf gebruiken waarvoor we geen toestemming hebben gegeven. Dit geeft ons een gevoel van onmacht, waarover we terug de controle willen. Het recht op privacy voorziet ons enerzijds van regels om de controle te behouden, maar voorziet anderzijds ook een stok achter de deur voor als het misloopt. Zo mag je aan de verwerker van je persoonsgegevens altijd vragen om je gegevens in te kijken, je gegevens aan te passen waar nodig, vergeten te worden, je gegevens over te brengen naar andere sites/apps en je gegevens extra te beveiligen.

5. Ook in het **kinderrechtenverdrag** staat privacy vermeldt: ieder kind heeft recht op privacy en niemand mag zich zomaar mengen met het privéleven. Zo mag je als leerkracht de schoolresultaten van kinderen niet bespreken met anderen ouders of je niet zomaar een foto van kind online posten zonder zijn of haar toestemming. Wanneer je recht op privacy geschonden wordt op de een of andere manier, kan je als kind terecht bij de privacycommissie.

6. **Het recht om vergeten te worden.** Als je jong bent, deel je soms dingen waar je achteraf spijt van kan hebben. Jonge kinderen zijn zich vaak nog niet bewust van alle risico's of vertrouwen de verkeerde mensen. Dankzij het recht om vergeten te worden kunnen ze altijd vragen om onjuiste of oude gegevens te laten wissen. Hiervoor neem je contact op met de eigenaar van de website! Ook foto's kan je laten verwijderen, maar dat is niet altijd even gemakkelijk. Want je bent nooit helemaal zeker dat de foto echt overal verwijderd is. Iemand heeft de foto misschien gedeeld of gekopieerd of het kan nog ergens op een server staan.

7. **Privacy-instellingen helpen om je informatie het delen van informatie te beperken.** Neem de tijd om rustig je privacy-instellingen door te nemen en eventueel aan te passen. Als volwassene kan je best kinderen begeleiden want de taal is vaak moeilijk. Als gebruiker van een sociale mediaplatform kan je er zelf voor kiezen om je profiel openbaar of privé te zetten.

8. **Je smartphone is een kleine spion in je zak**. Veel producten zoals apps en websites lijken gratis, maar zijn dat eigenlijk niet. De maker van de app verkoopt gegevens over jou zodat ze je zeer gerichte reclame kunnen sturen of producten voor jou ontwikkelen. Wees dus voorzichtig als je apps installeert of informatie doorgeeft.

9. **Sharenting** is een samentrekking van parents en sharing. Het verwijst naar ouders die dingen over kinderen op het internet delen. Sharents voelen zich online gesteund in het ouderschap en kunnen er terecht met al hun vragen, maar zoeken ook soms gewoon bevestiging. Het is belangrijk dat ouders zich ervan bewust zijn dat ze zelf de controle over de privacy van hun kind in handen hebben. Daarom is het beter om twee keer na te denken of je iets deelt over je kind of niet op sociale media. Je bent nooit 100% zeker of de informatie binnen een bepaalde privékring blijft.

Wat je zeker moet weten over datawijsheid

1. **Het internet is een schat aan informatie en gegevens.** We delen heel wat informatie over onszelf online: foto's, locaties, tweets, we vinden dingen leuk en niet leuk. Al deze informatie

resulteert in data over onszelf. Dit maakt het heel wat bedrijven en organisaties makkelijker om ons gedrag te voorspellen en beïnvloeden. **Data stellen we vaak voor met cijfers en tabellen.** Je kan er dan heel wat mee doen zoals bewaren, verzamelen, bewerken en uitwisselen met anderen.

2. **Online data hebben voor- en nadelen.** Zo krijg je meer informatie op maat aangeboden omdat bedrijven meer weten wat jij leuk vindt. Nadeel is dat deze data ook je privacy schaden omdat deze vaak doorverkocht worden naar andere bedrijven.

3. **De manier waarop iets voorgesteld wordt, hangt vaak samen vanuit welk standpunt een gebeurtenis weergegeven wordt.** Cijfers geven vaak de indruk dat iets correct en betrouwbaar is. Veel meer dan wanneer een journalist spreekt over veel of een aantal. Want cijfers kunnen emoties oproepen, de aandacht trekken en mensen overtuigen. Zo kunnen cijfers positief of negatief weergegeven worden afhankelijk van de boodschap men wil brengen. De aanwezigheid van cijfers is dus belangrijker dan de inhoud en de details die cijfers geven.

4. **We leven online allemaal in onze eigen filterbubbel.** Tijdens het surfen wordt er een profiel van ons gemaakt op basis van allerlei verzamelde data, namelijk zoekgeschiedenis, cookies, e-mailverkeer, koopgedrag, posts op sociale media … Wanneer er genoeg data is verzameld over jou, zullen je zoekresultaten, aanbiedingen, reclame … helemaal worden afgestemd op wat je eerder zag. Alle andere meningen of dingen waarin je niet geïnteresseerd bent zullen worden weggefilterd. Zo ontstaat een filterbubbel, je ziet enkel dingen die jij leuk vindt of jouw mening bevestigen.

5. **Heb jij al gehoord van de ‘echokamer’?** Mensen op sociale media hebben vooral contact met vrienden, groepen of media met gelijkaardige ideeën. Zo hoor en zie je vooral meningen van mensen waarmee jij akkoord gaat, waardoor je steeds meer overtuigd geraakt over jouw eigen mening.

6. **Algoritmes** zijn voorgeprogrammeerde instructies die een bepaald probleem oplossen of bepaalde taken uitvoeren. Algoritmes zouden kunnen berekenen waarin je geïnteresseerd bent op basis van je likes en zo dit op je sociale media te laten zien.

7. **Cookies zijn kleine bestandjes met informatie** over o.a. jouw zoekgedrag en interesses. Een algoritme is een reeks instructies die ervoor zorgt dat je de zoekresultaten, filmpjes … te zien krijgt die het beste bij jou(w profiel) passen. Je kan zelf kiezen om bepaalde cookies te aanvaarden. Als je sommige cookies echter niet aanvaardt, werken sommige functies niet goed. Je kan cookies ook vergelijken met de broodkruimeltjes van Hans en Grietje. Er wordt telkens een klein kruimeltje aan informatie verzameld over jezelf, wat ervoor zorgt dat je een pad aan informatie achterlaat voor sociale media en reclamemakers.

Wat je zeker moet weten over cybersecurity en -criminaliteit

1. **Nepprofielen.** Nepprofielen worden vaak gemaakt met slechte bedoelingen. Het is dan ook belangrijk dat je een nepprofiel zo snel mogelijk leert herkennen om je veiligheid niet in gevaar te brengen. Controleer de profielfoto en andere foto's, ga na wie zijn/haar vrienden zijn, scrol door de tijdslijn en kijk welke berichten er vooral gepost zijn. Zie je iets verdacht? Praat erover met anderen, ontvriend of blokkeer.

2. **Check online shops als je veilig online wil kopen**. Check eerst of de website een https-certificaat heeft (er staat dan een 's' achter http) en ga na of de betaling via normale, veilige manieren kan verlopen. Als dit oké is, is de kans heel erg groot dat het een veilige website is.

3. **Pas op voor phishing!** Bij phishing probeert een oplichter gevoelige informatie zoals een gebruikersnaam, wachtwoord, bankkaartnummer, pincode … te verkrijgen om later te misbruiken. Phishing kan op allerlei manieren gebeuren, via de telefoon, sms, e-mail, websites … Vaak wordt gevraagd om door te klikken naar een link. Let dus zeer goed op en denk na of het bericht of telefoontje wel betrouwbaar zijn.

4. **Hacking** is een vaag begrip, maar wordt algemeen beschreven als het illegaal binnendringen in een computersysteem. Om jezelf te beschermen tegen hackers, installeer je best een antivirusprogramma. Tegenwoordig bestaan er ook **ethische hackers**. Dit zijn professionele hackers die ingehuurd worden door bedrijven om na te gaan of er een fout in hun systeem zitten. Wanneer ze het bedrijf kunnen hacken, kan het bedrijf weten waar ze hun beveiliging moeten verbeteren.

5. Een **back-up** is een reservekopie van al je data en gegevens die je kan terugvinden mocht je data en gegevens beschadigd raken of verloren zijn. Een back-up kan je bijvoorbeeld maken op een externe harde schijf, maar tegenwoordig zijn er ook back-ups in de 'cloud'.

Tips voor jou als leerkracht

Veilige wachtwoorden en privacy

Leer leerlingen wat een veilig wachtwoord is. Sterke wachtwoorden zijn onmisbaar voor een goede privacybescherming. Adviseer leerlingen om verschillende wachtwoorden of wachtzinnen te gebruiken voor verschillende diensten.

Maak leerlingen bewust van hun online privacy. Bespreek samen met de leerlingen wat volgens hen privacy is én of zij dit belangrijk vinden. Organiseer af en toe een moment waarop leerlingen kunnen nakijken wat ze online over zichzelf kunnen terugvinden. Omdat kinderen zich vaak nog niet bewust zijn van de mogelijke gevolgen, leer je hen best hoe ze hun gegevens kunnen afschermen en waarom dit zo belangrijk is.

Google jezelf. Als je je eigen naam intikt in een browser dan kan je zien welke informatie anderen op het internet over jou kunnen terugvinden. Kijk welke informatie of foto's er over jou verschijnen. Heb je liever dat sommige dingen niet zichtbaar zijn voor anderen? Dan kan je beslissen dat je je persoonlijke informatie of foto's beter moet beveiligen. Sommige persoonlijke informatie of foto's kan je misschien beter helemaal verwijderen. *Doe dit echter niet klassikaal, want dat kan cyberpesten in de hand werken. Laat hen dit eerder individueel doen, waarbij je als leerkracht wel individuele feedback kan geven aan de leerlingen.*

Ga samen op zoek. Ga samen met je leerlingen op zoek naar de *gebruiksvoorwaarden en privacy verklaringen* van enkele populaire websites, zodanig dat leerlingen leren waar ze deze kunnen vinden en kunnen nagaan wat de bedrijven met hun persoonsgegevens doen. Sta stil bij hoe bedrijven met deze gegevens aan de slag kunnen.

Laat kinderen reflecteren over hun online activiteiten en online identiteit. Een aantal vragen kunnen helpen: is de informatie die ik online plaats wel voor iedereen bedoeld? Kan ik later geen spijt krijgen van wat ik online zet? Plaats ik met mijn post ook informatie over anderen online? En heeft hij of zij daar dan toestemming voor gegeven?

Laat kinderen hun zoekgeschiedenis opzoeken, wisten ze dat je zoveel terug kan vinden over wat je online opzoekt?

 # Let op bij het gebruiken van een shockelement. Ze kunnen tot op zekere hoogte doeltreffend zijn om jongeren mediawijsheid bij te brengen. Vaak houden ze in dat leraren zich bewust onethisch gedragen om jongeren een les te leren. Je moet als leerkracht telkens rekening houden met zowel ethische, pedagogische als juridische aspecten.

Datawijsheid

Laat je leerlingen hun cookiespoor visualiseren zodat ze zicht krijgen op welke data ze doorgeven aan derden. Gebruik hiervoor Firefox-add-on Lightbeam.

Laat kinderen zelf aan de slag gaan met data. Laat hen nadenken over hoe ze data kunnen voorstellen. Maak bijvoorbeeld zelf eens een infographic over een bepaald onderwerp.

Zoek iets op via Google, stel vast hoe verschillend de zoekresultaten soms kunnen zijn door de filterbubbel.

Cybersecurity- en criminaliteit

Zoek de contactgegevens van de handelaar op, lees commentaar van andere klanten met de leerlingen als je iets online koopt. Zo kan je extra achterhalen of een website wel,degelijk echt is.

Omdat iets er leuk uitziet, is het dat nog niet altijd. Voor een kind is het vaak nog moeilijk om niet-betrouwbare links te onderscheiden van betrouwbare links. Het is dan ook veiliger om kinderen aan te leren niet op links te klikken die ze niet kennen.

#Vraag je je af of je ooit al eens gehackt bent geweest? Geef je mailadres in op https://haveibeenpwned.com/ en ga na of je al eens gehackt bent.

Ga de creatieve toer op met je leerlingen en maak eens een sociale mediaprofiel op papier. Hierbij kan je de startpagina van een sociaal netwerk zoals Facebook of Instagram namaken met allerlei foto's of tekeningen van de leerlingen.

Aan de slag

Lespakket Kids in Cyberland **www.childfocus.be/sites/default/files/cf_lessenpakket_kic_nl_definitief.pdf**
Lespakket voor leraren derde graad lager onderwijs om met kinderen te werken rond veilig internetgebruik.

Lespakket Net op 't net **www.ikbeslis.be/ouders-leerkrachten/lesmateriaal**
Een kant en klaar lespakket over het online privacy.

Infofiche online reputatie **www.mediawijs.be/tools/fiches-mediawijs-online**
Een bundeling van tips en adviezen voor ouders, leerkrachten en jongerenbegeleiders.

Lesmodules De Baas op Internet **www.debaasopinternet.nl**
Lesmodules over privacy, encryptie, big data en internetstructuren.

Have I been pwned? **www.haveibeenpwned.com**
Lesmodules over privacy, encryptie, big data en internetstructuren.

GDPR, wat? **http://mediawijs.be/mediabank/lets-keep-it-private**
Een kant-en-klaar lespakket over online privacy.

DSVM Extra: Escape game datawijs
https://www.deschaalvanm.be/pagina/escape-game
DSVM EXTRA biedt korte lessen voor het 5de en 6de leerjaar over mediawijze thema's.

Educatief materiaal

Klik-en-print veilig wachtwoord
www.medianest.be/veiligwachtwoord
Klik-en-print van MediaNest over kenmerken van een veilig wachtwoord.

Affiche Stappenplan Privacy
www.mediawijs.be/tools/stappenplan-privacy
Dit stappenplan helpt je stilstaan bij welke informatie je over jezelf vrijgeeft online.

Klik-en-print niks te verbergen! Of toch wel?
https://www.medianest.be/niks-te-verbergen-toch-wel
Wat mag jij van je kind weten en wat houden ze liever voor zichzelf?

Vriendenboekje privacy
https://www.ikbeslis.be/sites/default/files/2018-09/Klasboekje.pdf
https://www.ikbeslis.be/ouders-leerkrachten/lesmateriaal
Welke informatie geef jij allemaal prijs?

Interessante websites

Safe On Web ***www.safeonweb.be***

Clicksafe ***www.clicksafe.be***

Veilig online ***www.veiligonline.be***

Ik beslis ***www.ikbeslis.be***

Ketnet en je privacy ***https://privacy.ketnet.be***

Datawijs ***www.datawijs.be***

Thema - 'Privacy' op MediaNest **www.medianest.be/thema/privacy**

Leesvoer

- **Dossier - datawijsheid** https://mediawijs.be/dossiers/dossier-datawijsheid/dossier-datawijsheid
- **Dossier - online privacy** https://mediawijs.be/dossiers/dossier-online-privacy
- **Artikel ‘Shockeren om te leren?’** https://mediawijs.be/nieuws/moeten-we-shockeren-te-leren
- **Mediawegwijzer - Het Privacy ABC** www.mediawijs.be/tools/mediawegwijzer-privacy-abc