Training: mediawijsheid, de basis (voor Android-telefoons)

Inhoudsopgave

Wat zijn social media?

Wat zijn social media? Dat weet toch iedereen? Maar geef er maar eens woorden aan.
Dat is nog niet zo makkelijk. Want hoort WhatsApp er nou wel of niet bij bijvoorbeeld? En is het nou social media of sociale media? Wij kiezen voor het eerste: social media. Aan het einde van deze training weet jij er ook van alles van!

De belangrijkste kenmerken van social media zijn:

- Snel en gemakkelijk contact en in gesprek met andere mensen.
- Een-op-een contact of in groepen tegelijk.
- Brengen mensen samen op bepaalde onderwerpen.
- Je kan er foto's, video's, teksten en geluid delen.
- Je kunt er live contact hebben met anderen
- Alles wat je deelt kan door anderen worden gezien/gelezen.
- Soms kun je het aantal mensen dat berichten kan zien beperken.
- Via internet, wifi of een G4 (online) verbinding te bereiken.
- Toegang via smartphones, tablets, smartwatches, laptops en pc.
- Er zitten voor- en nadelen aan, daarover later meer.

Voorbeelden van social media

Er zijn in de wereld heel veel socialmediaplatformen.
In ons land zijn er maar een paar die we veel gebruiken. Ieder jaar wordt er gekeken welke dat zijn.

Welke voorbeelden van social media ken je allemaal? Schrijf ze eens op in de onderstaande balk

Hieronder zie je de Nederlandse top-5 voor 2019.
1. WhatsApp
2. Facebook
3. YouTube
4. Instagram
5. LinkedIn

Had je ze allemaal opgeschreven? Omcirkel het juiste duimpje.

	2018	2019	+/- (#)	+/- (%)
	11,5 miljoen	11,9 miljoen	+ 380.000	+ 3%
	10,8 miljoen	10,1 miljoen	- 640.000	- 6%
	8,0 miljoen	8,7 miljoen	+ 720.000	+ 9%
	4,1 miljoen	4,9 miljoen	+ 830.000	+20%
	4,4 miljoen	4,6 miljoen	+ 250.000	+6%

Enkele andere bekende en veel gebruikte platformen zijn: Pinterest, Twitter (stond tot voor kort in de top 5), Snapchat, Tumblr, WeChat en Foursquare.

In het onderstaande schema uit 2018 zie je welke leeftijd op welk platform actief is.

Opdracht 1:

Hoe zit dat met jouw leeftijdsgroep? Op welk platform is die vooral actief? Vul de top 3 hieronder in:

1
2
3

Bron: Jaarlijks social media onderzoek door Newcom: https://www.newcom.nl/

% gebruik	15-19 jaar	20-39 jaar	40-64 jaar	65 - 79 jaar	80+
	97%	93%	86%	67%	38%
	72%	89%	77%	69%	58%
	86%	74%	54%	38%	21%
	12%	45%	36%	14%	7%
	73%	46%	22%	9%	6%
	23%	26%	21%	9%	9%
	19%	30%	21%	12%	8%
	72%	32%	7%	1%	1%

Beeld: Newcom

Waarvoor gebruik je social media?

Op ieder social mediaplatform is wat anders te doen. Mensen gebruiken elk platform weer net voor iets anders.

We nemen de top 5 kort door:

1. WhatsApp: snelle berichtjes sturen naar bekenden en collega's.
2. Facebook: de levens van bekenden volgen en ontspanning.
3. YouTube: video's kijken, muziekclips bekijken.
4. Instagram: de levens van bekenden volgen en mooie plaatjes kijken.
5. LinkedIn: je zakelijke netwerk onderhouden, contacten volgen en warm houden, kennis delen, vacatures vinden.

Opdracht 2

Welke social media gebruik jij zelf? Wat is jouw persoonlijke top-3?

1. .....

2. .....

3. .....

Waarom?

Waarom gebruik je eigenlijk social media? Doe je dat zomaar? Omdat het leuk is? Of omdat het makkelijk is? Heb jij weleens nagedacht over waarom je social media gebruikt?

Opdracht 3

Kies een dag van de week.
Zet eens op een rijtje wat op die dag met internet en social media hebt gedaan.
Geef hieronder antwoord op de volgende vragen:

- Hoe ziet jouw dag eruit van opstaan tot slapen gaan?
- Op welke momenten gebruik je internet en social media?
- Welke social media gebruik je dan?
- Wat doe je daar dan mee?
- Wat wil je ermee bereiken?
- VUL 1 DAG IN HET SCHEMA HIERONDER IN

	Tijd?	Welke social media?	Wat gedaan?	Waarom?
Na het opstaan				
Ochtend				
Tussen de middag				
Middag				
Avond				
’s Nachts				

Redenen om social media te gebruiken kunnen bijvoorbeeld zijn:

- Contact met familie, vrienden en bekenden
- Iets opzoeken
- Ontspanning
- Iets delen met anderen
- Iets vieren
- Iets bespreken, afspreken of wat regelen

Opdracht 4 - Even je kennis testen

Herken je deze socialmedialogo's? Vul in wat het volgens jou is.

Dit is:

……

Ben je aangemeld? Ja / nee

Omdat ……

……

Dit is:

……

Ben je aangemeld? Ja / nee

Omdat ……

……

Dit is:

……

Ben je aangemeld? Ja / nee

Omdat ……

……

Dit is:

……

Ben je aangemeld? Ja / nee

Omdat ……

……

Dit is:

……

Ben je aangemeld? Ja / nee

Omdat ……

……

LinkedIn / WhatsApp / Snapchat / Twitter / Instagram

Forum

Op het internet zijn ook allerlei fora (enkelvoud: forum) te vinden.
Ze worden ook wel eens ‘online community’ genoemd.
Het zijn online platformen waar je met anderen in gesprek kunt gaan, vaak over een bepaald thema.

Dit zijn dus geen social media, maar ze kunnen wel een sociale functie hebben.
En vaak zie je dat deze fora ook accounts of groepen op social media hebben.
Een veelgebruikt forum is bijvoorbeeld NUjij! Van Nu.nl. Daar kunnen lezers reageren op nieuws en ook met elkaar discussiëren. Om daaraan mee te kunnen doen, moet je wel eerst een account hebben en inloggen.

Opdracht 5:

Zoek op www.nu.nl een nieuwsbericht van vandaag op en bekijk de reacties.

Zoek daarop ook de huisregels en lees die.
Ze zijn ook op social media te gebruiken om het daar een beetje gezellig te houden.

Wat kunnen mensen van jou zien op social media?

Door middel van de instellingen op social media kan je bepalen wie welke informatie van jou te zien krijgt. Ook kun je instellen of anderen jouw berichten weer mogen delen. Je kunt zelfs instellen of mensen mogen reageren op jouw berichten. Sommige informatie wil je alleen delen met mensen die je vertrouwt. Dit regel je allemaal met de privacy-instellingen van het social mediaplatform.

Op https://veiliginternetten.nl/themes/situatie/welke-informatie-zichtbaar-op-mijn-sociale-media/ kun je van Twitter, Facebook, Instagram en LinkedIn precies zien hoe je de privacy-instellingen aanpast.

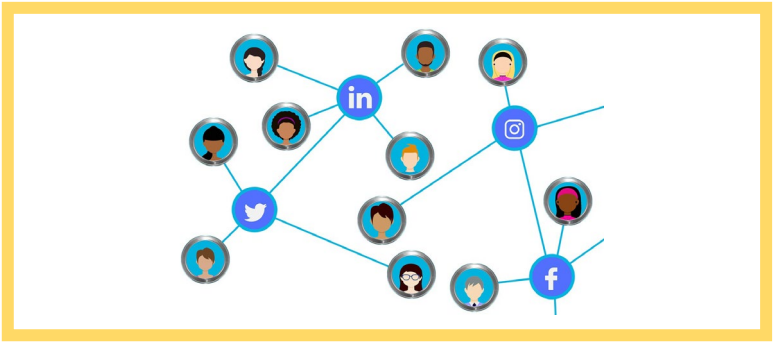
Opdracht 6:

Bekijk je privacy-instellingen op de social media waarop jij actief bent
en pas ze eventueel aan. Gebruik de website:
https://veiliginternetten.nl/themes/situatie/welke-informatie-zichtbaar-op-mijn-sociale-media/

Lees en kijk tips

Wil je een goed boek over privacy lezen dan is dit een aanrader: 'Je hebt wel iets te verbergen.' Je krijgt een kijkje achter de schermen en gaat heel anders naar je smartphone kijken. Je kan het bij Bol.com bestellen of je kunt het lezen bij de (online) bibliotheek als je daar lid van bent

Heb je een uurtje over? Dan is deze documentaire ook interessant. Hoe staat het ervoor met onze privacy? En hebben we nou echt niks te verbergen?
Klik op:
https://youtu.be/FUyB0Tsj6jE of zoek op YouTube naar 'Panopticon - Peter Vlemmix'



Zuinig zijn op je netwerk

Veilig internetten en op social media informatie delen begint natuurlijk ook bij met wie jij omgaat online. Dus wie er in jouw online netwerk zitten. Hoe je netwerk eruitziet, hangt heel erg af van wie jij toelaat.

Opdracht 7:

Beantwoord de volgende vragen voor jezelf.

1. Laat je iedereen toe? Kies A of B

A. Ik laat alleen mensen toe die ik ken
B. Ik laat ook mensen toe die ik niet persoonlijk ken

2. Ken je iedereen persoonlijk?

JA/NEE

3. Accepteer je mensen meteen die jou een verzoek sturen of verwacht je een persoonlijk bericht voor je hem of haar toelaat? Maak je keuze.

A. Ik accepteer iemand meteen zonder persoonlijk bericht
B. Ik accepteer iemand pas met een (persoonlijk) bericht erbij

4. Wie zijn de lezers van jouw social mediaplatformen? Hebben ze dezelfde interesses bijvoorbeeld? Vinden zij dezelfde dingen leuk? Omschrijf jouw volgers eens in onderstaand blok:

Opdracht 8:

Nog een laatste filmpje, om dit toch wat serieuze verhaal met een lach af te sluiten.

Wat zou jij doen wanneer iemand jouw vriend wil zijn en je gaat volgen?
Bekijk hoe mensen daarop reageren in deze video. https://youtu.be/aDycZH0CA4I
Of zoek op YouTube naar 'Can I be your friend?'

Social media en veiligheid

Social Media zijn vaak leuk en lekker makkelijk om te gebruiken. We weten ook dat er veel gevaren zijn op social media. Anderen kunnen bijvoorbeeld je foto's verkeerd gebruiken of jouw informatie stelen. Je kan zelf veel doen om te zorgen dat dit jou niet gebeurt.

We kijken daarom samen even naar de gevaren van social media. Ook online moet je goed voor jezelf en voor anderen zorgen. Het is net als in de echte wereld.

Wat zijn de gevaren?

Net als in de echte wereld, zijn er genoeg dingen waar je goed op moet letten. We gaan het hebben over de volgende 'gevaren van het internet':

- Wachtwoorden
- Je online identiteit
- Wat je kan doen als het mis gaat
- Cyberpesten
- Hacken
- Phishing
- Wat je online deelt
- Online netwerken

Natuurlijk moet je oppassen

In dit filmpje zie je hoe gewone mensen verrast worden door een ‘waarzegger’ die alles van ze schijnt te kunnen zien ….

https://youtu.be/F7pYHN9iC9I
Of zoek op YouTube naar
‘Amazing mind reader reveals his 'gift''

Opdracht 9:

Welke informatie zou deze waarzegger over jou kunnen vinden online?

Wachtwoord

Veilig online begint met jouw wachtwoorden. Met een wachtwoord bescherm je je computer, smartphone of tablet. Al je socialmedia-accounts hebben ook een wachtwoord. Zo ben jij de enige die ze kan gebruiken.

Maar hoe onthoud je nou je wachtwoorden? Want je wachtwoorden op een briefjes schrijven is niet slim. Wat als iemand anders dat briefje vindt?

Een wachtwoord onthoud je in je hoofd. Of je gebruikt een wachtwoordmanager. Dit is een app die je kunt installeren en die al jouw (nieuwe) wachtwoorden opslaat. Heel handig!

Je hebt misschien wel eens gehoord over zwakke en sterkte wachtwoorden.
Een zwak wachtwoord is bijvoorbeeld: Wachtwoord123. Dat kan iedereen bedenken!
Een sterk wachtwoord is bijvoorbeeld: HTGi786$%09OPkl#$
Om zo’n sterk wachtwoord te onthouden zijn er handige trucjes. Gelukkig maar!

Opdracht 10:

Heb jij al een wachtwoord? Schrijf het dan hier **NIET** op! Maar denk er wel even goed aan: is het een sterk of een zwak wachtwoord? Waarom?

‘Wachtwoorden? Lastig!’

Wachtwoorden moet je dus verzinnen en onthouden. En dan moeten ze ook nog ‘sterk’ zijn.
Mensen kiezen daarom vaak de naam van een huisdier, partner of kinderen en voegen er cijfers aan toe, zoals 1234, 4321 of je trouwdatum of geboortedatum.
Dat zijn zwakke wachtwoorden.
Die wachtwoorden zijn heel snel en gemakkelijk door een ander te bedenken en te kraken.

Stappenplan

Een sterk, wachtwoord is makkelijker te maken dan je denkt.
Lees dit stappenplan maar eens. Mensen die verstand hebben van online beveiliging raden deze manier aan.

Opdracht 11:

Pak pen en papier en schrijf mee met de volgende stappen. Je ziet je sterke wachtwoord dan vanzelf ontstaan. Of print de laatste pagina van deze module uit en schrijf daarop mee.

1. Verzin een wachtzin

Een hele zin dus, en niet één woord! Die zin mag niet te kort zijn. Gebruik minimaal 8 woorden. Je wachtwoord voor Facebook kan bijvoorbeeld zijn:

Dit wachtwoord heb ik op 1 september bedacht voor Facebook

2. Vervang letters door cijfers

Van de i kan je een 1 maken, van de B een 8, of de kleine letter b een 6 en van de o (letter) een 0 (cijfer).

De datum in de wachtzin kan je vervangen door het nummer van de maand te noemen.
1 september wordt dan 19
De wachtzin ziet er dan zo uit:

D1t wachtw00rd heb 1k op 19 8edacht voor Faceb00k

3. Gebruik van ieder woord de eerste letter

Je wachtzin wordt dan een wachtwoord, veel minder lang, maar toch te onthouden.
De voorbeeldzin voor Facebook wordt dan:

Dwhio19bvF

Opdracht 12:

Hier doen we even een tussen-check. Tel het aantal tekens waaruit jouw wachtwoord nu bestaat. In ons geval zijn het er 10. Sterke wachtwoorden hebben minimaal 8 tekens. Hoe meer hoe beter. Daarom moest je oorspronkelijke zin zo lang zijn!

4. Bedenk welke letter een hoofdletter moet zijn

Dat kan iedere derde letter zijn.

DwHiO19bVF

Of alleen de eerste en de laatste. Maar dat is minder sterk.

Dwhio19bvF

5. Gebruik 'speciale tekens'

Dat zijn bijvoorbeeld deze: ! @ # $ % ^ & * ( ) + = ? > < _ -

Je wachtwoord kan er dan zo uit zien:

@DwHiO19BvF-

Opdracht 13:

Check je wachtwoord

Natuurlijk wil je wel weten of je wachtwoord sterk genoeg is. Zowel je oude als je nieuwe wachtwoord kan je controleren op deze site:
https://veiliginternetten.nl/wachtwoord-check/
Hoe komt ons voorbeeld wachtwoord uit de test?

Wat doe je met je wachtwoorden?

Wachtwoorden moet je goed onthouden en goed bewaren. Je hebt ze vaak nodig. Met deze tips lukt dat zeker:

1. Geef nooit iemand je wachtwoord (net zoals je nooit je pincode af moet geven).
2. Zorg dat niemand mee kan kijken als je je wachtwoord intypt.
3. Gebruik verschillende wachtwoorden voor verschillende websites.
4. Wissel je wachtwoorden, bijvoorbeeld iedere maand een nieuwe.
5. Laat je wachtwoord niet rondslingeren in de buurt van je computer, tussen je spullen of in je agenda.
6. Sla je wachtwoorden niet in een simpel bestandje op je computer op. Gebruik een wachtwoordmanager.
7. Laat je wachtwoorden niet in de e-mail staan.
8. Geef je wachtwoord nooit aan bedrijven die erom vragen.
9. Verander je wachtwoord als je hoort dat een website is gehackt.
10. Soms vraagt je browser (de app waarmee je op internet gaat) of je het wachtwoord wilt opslaan. Dat kun je beter niet doen.

Bron: https://veiliginternetten.nl/themes/basisbeveiliging/situatie/mijn-wachtwoord-sterk-genoeg/?type=q

Opdracht 14:

Nu jij! Maak al je wachtwoorden sterk en veilig.

Hoe veilig zijn jouw wachtwoorden? Doe de check. En verzin ten minste één nieuwe.

Test het wachtwoord dat je gebruikt om in te loggen via de site
https://veiliginternetten.nl/wachtwoord-check/
Goed of niet? En het wachtwoord voor je meest gebruikte socialmedia-account?
Ga zo al je wachtwoorden langs.

Verzin als het niet sterk genoeg is volgens het stappenplan een nieuw wachtwoord.

1. Verzin een zin (minimaal 8 woorden)
……

2. Vervang letters van door cijfers
……

3. Gebruik van ieder woord alleen de eerste letter
……

Doe de tussencheck, heb je minimaal 8 tekens gebruikt?

4. Bedenk waar de hoofdletters moeten komen
……

5. Voeg speciale tekens toe
……

6. Doe de sterkte-check op: https://veiliginternetten.nl/wachtwoord-check/

Tip:

Print het blad met dit stappenplan uit. Of schrijf het over. En gebruik het voor ieder wachtwoord dat je gaat veranderen.

Social media en privacy

Er is veel te doen over social media en privacy. Dat is ook niet vreemd.
Alle socialmediaplatformen zijn erop gericht dat jij deelt wat jij op dat moment doet of denkt. En dat doen we ook allemaal.

Socialmediaplatformen maken met die informatie een profiel van je aan. En ze verkopen die informatie aan bedrijven die reclame willen maken of andere diensten aan willen bieden.

Maar het kan altijd erger. Hoever laat jij het gaan?

Opdracht 15:

Wat zou jij doen wanneer er iemand aanbelt en vraagt of hij foto's van je kinderen mag zien? Bekijk hoe mensen daarop reageren in deze video. https://youtu.be/JgScpIKj8Fg
of zoek op YouTube naar 'Mag ik foto's van uw kinderen zien?'

Je deelt meer dan je weet

Weet jij wat er allemaal over jou op internet staat? Waarschijnlijk niet. Overal op internet heb je sporen achtergelaten. Ook zonder dat je het weet.

Je smartphone deelt bijvoorbeeld veel informatie met bedrijven doordat apps toegang hebben tot je gegevens en internetgeschiedenis. Als je een website bezoekt, dan gaat er veel informatie naar andere bedrijven dan waarmee jij op dat moment contact zoekt.

Opdracht 16:

Bekijk de volgende video:

In een split-second bieden commerciële bedrijven op jouw informatie
om daarna razendsnel advertenties op je af te sturen.
In deze video zie je hoe dat gaat. https://youtu.be/38PRxR7U5bY
Of zoek op YouTube naar 'Veilig internetten campagne- Je deelt meer dan je weet'

Wat zijn cookies?

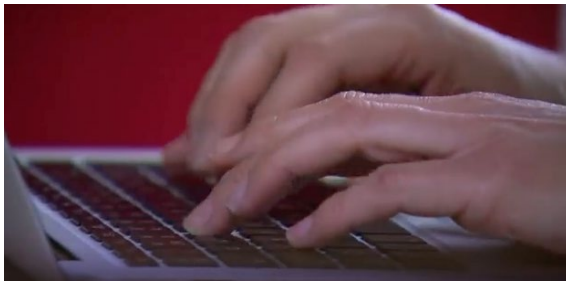
Cookies zijn kleine stukjes software die op je computer of telefoon komen te staan. Dat gebeurt als jij een website bezoekt. Je geeft er vaak zelf toestemming voor. Een bouwer van een website mag dat vragen. De kleine stukjes software op websites zijn nodig om de website goed te laten werken. Maar ze kunnen ook bijhouden wat jij doet op die site en ze onthouden dingen voor je. De bouwers van websites leren op die manier hoe mensen de website gebruiken en waar mensen naar zoeken. Dat is handig om de website beter te maken. Maar de informatie kan ook gebruikt worden om jou advertenties te laten zien die passen bij jouw interesses. Die cookie-informatie is zo belangrijk dat bedrijven daar veel geld voor willen betalen. En deze informatie delen ze met andere bedrijven. Zo kunnen zij jou ook gaan volgen.

Opdracht 17:

Het jij weleens een website bezocht waar gevraagd werd of je cookies accepteerde?
Wat heb je gedaan? Heb je op JA of op NEE geklikt? En waarom maakte jij die keuze?

Opdracht 18:

Bekijk de volgende video over cookies:



Bekijk dit filmpje over de geheimzinnige wereld achter cookies:
https://youtu.be/5ZjrM354x0g
Of zoek op YouTube naar 'Digitale gluurders | De Kennis van Nu | NTR'

Zoekmachines

Zoekmachines zijn handig voor jou om informatie te vinden. Maar ze onthouden ook informatie over jou. Daarom zijn zoekmachines voor bedrijven ook handig om mensen beter te leren kennen. Om jou beter te leren kennen. Zonder dat je ze hebt gesproken. Door jezelf te 'Googlen' kom je er voor een deel achter wat er te vinden is door anderen.

Opdracht 19: Google en ik

Tegenwoordig wordt heel veel informatie online bewaard, bijvoorbeeld op websites. Zelfs informatie die vroeger nog helemaal niet digitaal was, is nu gewoon via een simpele zoekopdracht op Google te vinden. Heb jij dat ook gemerkt in de vorige opdracht? Er was vast wel iets over je te vinden, of niet?

Google jij jezelf wel eens? Probeer het maar.
Wat kan jij over jezelf vinden?

.....

.....

En wat vind je daarvan?

.....

Er staat veel informatie op websites. Maar er blijven ook veel sporen achter aan de achterkant van een website als jij daar iets aanklikt. Informatie over jouw interesses en de manier waarop jij op een website informatie bekijkt bijvoorbeeld. Het kan zijn dat je een keer gezocht hebt naar drop op internet en dat je dan opeens allerlei reclames over drop te zien krijgt als je de volgende keer inlogt.

Met die informatie kunnen bedrijven precies inschatten welke informatie jij nodig hebt om iets te kopen of te kiezen. Soms kan dat handig zijn, omdat je een beetje gestuurd wordt en je niet meer alle mogelijke keuzes te zien krijgt. Maar het kan ook vervelend zijn.

Opdracht 20:

Probeer het maar eens! Ga op internet op zoek naar bijvoorbeeld mobiele telefoons. Bezoek een paar aanbieders van mobiele telefoons. Open daarna de website www.nu.nl. Wat valt je op?

En wat vind je daarvan?

……..

Je kunt hier eigenlijk niets aan doen. Houd het dus maar in gedachten wanneer je de volgende keer iets gaat opzoeken. Je kunt wel zorgen dat je geen advertenties meer ontvangt! Kijk maar eens op https://www.consumentenbond.nl/internet-privacy/wat-is-een-adblocker.

Je hebt net geprobeerd informatie te vinden over jezelf. Misschien voelde het een beetje raar om jezelf op te zoeken op internet. Meestal zoeken mensen geen informatie over zichzelf op, maar over een ander. Bijvoorbeeld als je bij een bedrijf solliciteert. Dat bedrijf kijkt dan op internet om een beter beeld van jou te krijgen.

In de volgende opdracht ga je proberen informatie te vinden over een ander. Maak er een spel van. Dat wordt vast leuk!

Opdracht 21: Spel!

Spel!

Pak stiften en grote vellen papier.
En tenminste twee smartphones, tablets of computers met internetverbinding.
Wanneer iemand niet zelf kan of wil schrijven, zorg je voor een maatje.
Laat iemand de tijd bij houden.
Je kan dit in tweetallen doen, of in twee grotere groepen.

Doel:
Schrijf in 5 minuten zo veel mogelijk van wat jij weet te vinden **op social media** over je tegenstander op het papier. Wie de meeste dingen heeft opgeschreven, wint.

De persoon die de tijd bijhoudt, start en stopt het spel (en ja, ook dat kan met je smartphone!).

Klaar …? Af!

Voorkom dat informatie verspreid wordt zonder jouw toestemming

Er is een aantal dingen dat je moet weten en doen om ervoor te zorgen dat jouw (privé-)informatie niet (ongewenst) via internet verspreid wordt.

Op deze site krijg je tips hoe jij zelf jouw informatie kunt beveiligen:
https://www.webwijzer.nl/beveiliging/privacy-online.html

Noem minimaal 2 soorten anti tracking software die je op deze website kunt vinden:
1.
2

Opdracht 22: Wat deel je liever niet?

Welke informatie wil jij niet delen met anderen? Schrijf de onderwerpen die je niet wilt delen met anderen in het onderstaande blok.

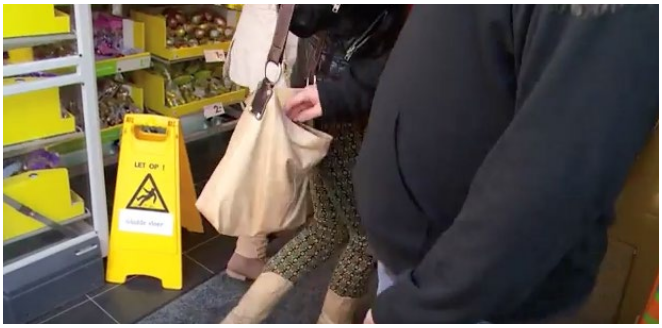
Is er iets in jouw leven dat voor jou echt privé is?
Dat schrijven we uiteraard hier ook niet op.

Identiteitsfraude, wat moet je doen?

Als iemand anders jouw naam, adres en telefoonnummer (persoonlijke gegevens) gebruikt, om bijvoorbeeld online spullen te kopen, noemen we dat identiteitsfraude. Zo iemand doet net of hij jou is en kan onder jouw naam van alles doen op internet. Bijvoorbeeld aankopen doen in webwinkels die jij dan moet betalen.

Opdracht 23:

Dat wil je natuurlijk niet.
In deze video van de Fraudehelpdesk leer je daar meer over.
https://youtu.be/ywgyDVwNhQY
of zoek op YouTube naar 'Identiteitsfraude voorlichting.'



Wie mag om jouw paspoort, rijbewijs of identiteitskaart vragen?

……

……

Welke drie dingen moet je doen voordat je een kopie van je paspoort, rijbewijs of identiteitskaart geeft?

1.
……

2.
……

3.
……

Een persoon blokkeren, verwijderen of ontvolgen

Op de sociale media kun je een persoon blokkeren. Deze persoon heeft dan geen toegang meer tot de informatie die jij op jouw social media account zet. Ook kun je mensen verwijderen uit jouw contacten- of vriendenlijst. Dan hebben jullie helemaal geen linkje meer met elkaar. Dat werkt net zo goed. En zet iemand anders dingen op social media die jij zelf liever niet meer ziet? Dan kun je in veel apps stoppen met het volgen van deze personen.

Je kunt ook mensen of informatie die anderen delen rapporteren. Dit betekent dat je aan het sociale medium (bijvoorbeeld Facebook of Instagram) laat weten dat je informatie hebt gezien waar jij niet blij mee bent. Of waarvan je vindt dat je dat niet op internet zou moeten zetten. Het sociale medium kan dan bepalen of zij die persoon blokkeren. Hieronder lees je hoe dit allemaal werkt.

Wat gebeurt er als je een persoon blokkeert?

Wanneer een persoon wordt geblokkeerd, betekent dit:

- dat die persoon geen gesprek met je kan beginnen
- dat die persoon niet meer kan zien wat je op je tijdlijn plaatst
- dat deze persoon je niet meer kan uitnodigen voor een evenement, groep, ...
- dat deze persoon je niet meer kan toevoegen als vriend

Dankzij deze optie kan je een persoon van je vriendenlijst verwijderen en dus kiezen van wie je informatie kan bekijken.
Als je zaken privé wilt houden, is het belangrijk dat je profiel is ingesteld op ‘alleen voor vrienden'. Anders kan iedereen je gedeelde inhoud bekijken. Hou er rekening mee dat zelfs als je een persoon geblokkeerd hebt, hij of zij vaak toch nog commentaar, reacties of gemeenschappelijke evenementen kan zien van jou. Dit komt doordat je dan allebei bevriend bent met dezelfde persoon.

Opdracht 24:

Open een van jouw social media-apps en bekijk jouw vrienden en volgers. Ben je het eens met alles wat zij plaatsen? Kruis Yes (ja) of No (nee) aan.

Heb jij al eens het gevoel gehad dat je iemands berichten liever niet meer zou zien?

Kun je personen blokkeren in applicaties?

Deze blokkeringsmogelijkheid bestaat ook voor bepaalde apps, zoals Facebook, die veel gebruikt worden om met elkaar te communiceren. Je kan er een persoon blokkeren, zodat deze geen berichten meer ontvangen van die persoon.

Hoe blokkeer je iemand?

Hieronder vind je voorbeelden en richtlijnen die laten zien hoe je iemand op de verschillende netwerken blokkeert.

Hoe blokkeer je iemand op Facebook?

Wanneer je iemand blokkeert, kan deze persoon jou niet meer taggen of inhoud bekijken die je op je tijdlijn plaatst.

Nieuwe versie van Facebook

- Klik rechtsboven in Facebook op .
- Selecteer Instellingen en privacy > Instellingen.
- Klik in het linker menu op Blokkeren.
- Voer in het gedeelte ‘Gebruikers blokkeren’ de naam in van de persoon die je wilt blokkeren en klik op Blokkeren.
- Selecteer de specifieke persoon die je wilt blokkeren in de lijst die wordt weergegeven en klik op Blokkeren > [naam] blokkeren.

Oudere versie van Facebook

- Klik rechtsboven in Facebook op en kies Instellingen.
- Klik in het linker menu op Blokkeren.
- Voer in het gedeelte ‘Gebruikers blokkeren’ de naam in van de persoon die je wilt blokkeren en klik op Blokkeren.
- Selecteer de specifieke persoon die je wilt blokkeren in de lijst die wordt weergegeven en klik op Blokkeren > [naam] blokkeren.

Opmerking: als je iemand zo niet kunt vinden, ga dan naar het profiel van de persoon zelf en selecteer Blokkeren in het menu ··· rechtsonder op zijn/haar omslagfoto.

Handig om te weten: personen worden niet gewaarschuwd wanneer je ze blokkeert. Je kunt dus gewoon iemand blokkeren zonder dat die persoon het weet.

Deblokkeren

Het kan natuurlijk zo zijn, dat je na een tijdje weer contact wilt hebben met iemand die je eerder geblokkeerd hebt. Dat kan. Je kunt via dezelfde weg de geblokkeerde personen weer deblokkeren. Je ben dan niet meteen weer vrienden van elkaar. Als je iemand deblokkeert en je wilt ook weer vrienden worden, dan moet je deze persoon weer opnieuw uitnodigen.

Hoe blokkeer je iemand op Instagram?

Op Instagram volg je andere mensen. Dat is iets anders dan vrienden zijn zoals op Facebook. Als je vrienden bent, heb je daar allebei toestemming voor gegeven. Op Instagram kun je iemand anders volgen. Die persoon hoeft daar meestal geen toestemming voor te geven. Ben je bijvoorbeeld fan van Rapper Boef? Grote kans dat je hem kunt volgen op Instagram.

Nu gaan we het hebben over hoe je stopt met het volgen van de ander. Dan kan bijvoorbeeld als je het niet fijn vindt wat de ander op Instagram laat zien. Zo stop je met iemand volgen:

- Ga naar het profiel van de persoon die je niet meer wilt volgen.
- Tik op Volgend en daarna op Niet meer volgen om te bevestigen.

Wanneer je bent gestopt met het volgen van een persoon, staat er Volgen in plaats van Volgend op zijn of haar profiel. Personen worden niet gewaarschuwd wanneer je stopt met volgen. Je kunt dus gewoon stoppen met iemand volgen zonder dat die persoon het weet.

Opmerking: als je account is ingesteld op privé, kun je zelf mensen verwijderen uit je lijst met volgers. Je kunt ook anderen blokkeren. Als je iemand blokkeert, kan de geblokkeerde persoon jouw foto's of video's niet meer zien en jouw Instagram-account niet meer zoeken. De geblokkeerde persoon wordt niet gewaarschuwd als hij of zij wordt geblokkeerd.

Hoe blokkeer je iemand op WhatsApp?

Je kunt mensen waar je contact mee hebt op WhatsApp blokkeren. Als je dat doet, kan die persoon je geen berichten meer sturen en niet meer bellen. Ook je statusupdate kunnen zij niet meer zien.

Een contact blokkeren

Om een persoon/contact te blokkeren op WhatsApp zijn er drie manieren:

1.
- Open WhatsApp Instellingen > Account > Privacy > Geblokkeerd > Voeg toe....
- Zoek het contact dat je wilt blokkeren en tik op het contact.

2.
- Open de chat met het contact, tik op de naam van het contact > Blokkeer contact > Blokkeer of Rapporteer contact > Rapporteer en blokkeer, waardoor het nummer gerapporteerd en geblokkeerd wordt.

3.
- Veeg naar links op de chat met de contactpersoon in je tab Chats, tik op Meer > Contactinformatie > Blokkeer contact > Blokkeer of Rapporteer contact > Rapporteer en blokkeer, waardoor het nummer gerapporteerd en geblokkeerd wordt.

Een onbekend nummer blokkeren

Bij onbekende nummers heb je geen idee van wie dat nummer is.
Je hebt een aantal manieren om een onbekend nummer te blokkeren:

- Als je voor het eerst een bericht krijgt van een onbekend nummer: open de chat en tik op Blokkeer > Blokkeer.
- Open de chat met het onbekende telefoonnummer, tik op het telefoonnummer > Blokkeer contact > Blokkeer of Rapporteer en Blokkeer, waardoor het nummer gerapporteerd en geblokkeerd wordt.

Belangrijk:

- Berichten, oproepen en statusupdates die zijn verzonden door een geblokkeerd contact zijn niet zichtbaar op je telefoon en worden nooit afgeleverd.
- Je laatst gezien, online- en statusupdate en wijzigingen aan je profielfoto zijn niet meer zichtbaar voor geblokkeerde contacten.

- Als je een contact blokkeert, wordt deze niet verwijderd uit je contactlijst en jij wordt ook niet verwijderd uit de lijst van deze contactpersoon. Om een contact te verwijderen, moet je hem of haar verwijderen uit het adresboek van je telefoon.

Opdracht 25: Woordzoeker mediawijsheid

Tussendoor een leuke puzzel met alle woorden die je in deze training leert. Vul de letters in en bekijk welke letters overblijven. Aan het einde van de training kun je het antwoord lezen.

Mediawijsheid

F	A	C	E	B	O	O	K	B	W	Y
O	G	Y	V	G	E	I	M	L	A	C
N	I	B	L	O	G	I	A	O	C	A
T	L	E	G	O	E	K	R	K	H	V
V	I	R	I	G	G	R	G	K	T	I
O	E	C	N	L	E	E	A	E	W	R
L	V	R	T	E	V	W	T	R	O	P
G	N	I	M	M	E	T	S	E	O	T
E	O	M	E	R	N	E	N	N	R	N
N	E	E	T	T	S	N	I	E	D	N
A	I	D	E	M	L	A	I	C	O	S

BLOKKEREN
CYBERCRIME
FACEBOOK
GEGEVENS
GOOGLE
INSTAGRAM
NETWERK
ONTVOLGEN
ONVEILIG
PRIVACY
SOCIALMEDIA
TOESTEMMING
WACHTWOORD

Oplossing

Informatie over de plek waar jij bent

We hebben eerder al gezien dat veel apps op je smartphone persoonlijke gegevens gebruiken en onthouden. Bijvoorbeeld je locatie, de plek waar je op dit moment bent. Als je dit niet wilt, is het belangrijk om de instellingen van je privacy na te kijken. We gaan nu kijken hoe dat werkt

De plek waar jij bent wordt op veel smartphones 'locatie' genoemd.
Binnen Android zijn er weinig mogelijkheden om dit aan te passen.
Je kunt per app bepalen of je wel of geen locatiegegevens wilt laten zien. Soms is het handig als je telefoon weet waar je bent. Bijvoorbeeld bij apps waarbij je iets in de buurt zoekt; Marktplaats of de Kringloop App. Maar bij de meeste apps is het niet nodig om je locatie aan te hebben staan.

- Open het overzicht met alle apps door te tikken op Apps of door van beneden naar boven over het scherm te vegen (Android 8.0 en hoger).
- Tik op Instellingen.
- Tik op Apps.
- Tik rechtsboven op het pictogram van de drie puntjes.
- Tik op App-machtigingen.
- Er opent een overzicht van de onderdelen waarvan apps gebruikmaken.
- Tik op Locatie.
- Achter de naam van de app staat een grijze of blauwe/groene schuifbalk. Is het schuifbalkje grijs, dan heeft de app geen toegang tot de camera. Is het balkje blauw/groen, dan heeft de app wel toegang. Wil je de toegang intrekken, tik dan op het blauwe schuifbalkje.
- Tik op Toch weigeren.

Opdracht 26:

Welke apps gebruiken jouw locatie? Schrijf de apps op die nu jouw locatie gebruiken. Vind jij dat voor al deze apps oké?

Vind jij dat voor al deze apps oké? Omcirkel het juiste duimpje.

Internetten

In de internetapp Google Chrome kan je ook wat instellingen wijzigen.

- Tik op **Chrome**. Tik daarvoor eventueel eerst op de map **Google**.
- Tik rechtsboven op het pictogram met drie puntjes.
- Tik op **Instellingen**.
- Tik op **Privacy**.
- Je ziet een overzicht van de instellingen
- Wil je niet dat websites cookies opslaan om je voorkeuren te onthouden? Haal dan het vinkje weg achter *Pagina's vooraf laden voor sneller browser en zoeken*.

Apps downloaden

De apps in de Play Store worden niet altijd even goed gecontroleerd op veiligheid en privacy. Voor je een app downloadt, kan je het beste via internet opzoeken hoe de app bekend staat. Dat kan bijvoorbeeld door bij Google de naam van de app plus het woord ‘veiligheid’ of ‘ervaringen’ in te typen. Als je ziet dat mensen niet positief zijn, kan je de app beter niet downloaden.

Advertenties speciaal voor jou

Google geeft iedereen die Google gebruikt een advertentie-ID. Dat is een soort hulpmiddel om te kunnen volgen wat jij precies doet op internet.
In de advertentie-ID wordt precies opgeslagen wat jij doet, bijvoorbeeld welke websites jij bezoekt.

Opdracht 27:

Loop de volgende stappen door als je niet wilt dat Google jou op internet in de gaten houdt om jou advertenties te kunnen sturen:

- Open het overzicht met alle apps door te tikken op Apps of door van beneden naar boven over het scherm te vegen (Android 8.0 en hoger).
- Tik op Instellingen
- Tik op Google.
- Tik op Advertenties.
- Schuif het schuifje achter 'Afmelden voor personalisatie van advertenties' naar rechts.
- Tik op OK ter bevestiging.

Cybercrime

Heb jij weleens een verhaal gehoord of gelezen over wat er mis kan gaan op social media? Misschien heb je zelf weleens iets vervelends meegemaakt. Maar weet je ook wat die gevaren precies zijn? En wat jij er zelf aan kan doen? We kijken samen naar de volgende gevaren van internet en social media:

- Phishing
- Hacken
- Ddos aanvallen
- Openbare wifi
- Fake news

Opdracht 28:

Heb jij al weleens iets gezien op social media wat niet oké was? Wat was dat en wat heb je toen gedaan?

De onderwerpen hierboven komen het meest voor, maar er zijn er meer.
Hieronder vind je links naar een aantal websites die meer uitleg geven over sommige gevaren.
Ga daar maar eens kijken. Zoals op de volgende site:

Meldknop.nl

Kijk op
https://www.meldknop.nl
Op deze site gaat het om de thema's die hier genoemd zijn, als onderdeel van pesten, seks, oplichting en lastigvallen.
Je vindt er een heleboel informatie over wat online echt niet kan en mag en wat je eraan kan doen.

Zo is er bijvoorbeeld echt een ‘meldknop’ die je kan installeren op je computer. Dan kan je het meteen laten weten als je dit gedrag online tegenkomt.

Opdracht 29:

Zou jij zelf een ‘meldknop’ installeren op jouw computer? Waarom wel of waarom niet?

Phishing

Phishing is een Engels woord. Het betekent letterlijk: ‘vissen’. Het wordt gebruikt als criminelen proberen jouw gegevens te krijgen. Dit doen ze vaak via mailtjes of via Whatsapp. Als criminelen die gegevens hebben kunnen ze die misbruiken. Bijvoorbeeld om spullen te kopen of geld van je rekening te halen.
Heel vervelend en lastig. Zorg dus dat je phishingberichtjes herkent!

Opdracht 30:

Bekijk deze video om te leren wat phishing is. En wat je moet doen om het te voorkomen: https://youtu.be/kYoHGqhALJg. Of zoek op YouTube naar ‘Phishing: wat is het en wat doe je eraan?’

Phishingmail

Phishingmails zijn heel vervelend en kunnen ook heel gevaarlijk zijn. Criminelen hengelen (vissen) naar jouw inlog-, bank- of persoonlijke gegevens. Om jouw geld afhandig te maken. Zij lokken je via een link naar een valse website en verleiden je daar om gegevens in te vullen.
Vervolgens halen ze geld van je bankrekening. Klik dus bij twijfel niet op de link.

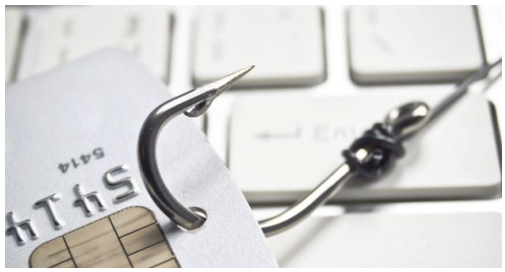
Herken jij welke van de 12 mails zijn verstuurd door oplichters om je geld of gegevens buit te maken? Typ de onderstaande link op internet en doe de phishing-quiz van de Consumentenbond.

bron: tijdgeest.eu

consumentenbond

Doe de phishing-quiz van de Consumentenbond:
https://www.consumentenbond.nl/veilig-internetten/phishing-quiz

Leer hoe je phishing nog meer kan herkennen:
https://www.mediawijsheid.nl/phishing/



Hé mam, dit is mijn nieuwe nummer…

Helaas wordt phishing steeds persoonlijker. Dan wordt het dus lastig om te weten of iets klopt of niet.

Op WhatsApp bijvoorbeeld sturen criminelen berichtjes met de melding dat iemand een nieuw telefoonnummer heeft. Jij herkent dat nummer niet, maar ja, dat klopt toch? Het is nieuw!

Toch kunnen criminelen op deze manier bij gegevens komen waar jij ze niet wilt hebben. Of ze kunnen van afstand in jouw telefoon meekijken. Denk dus altijd goed na voor je een berichtje opent of beantwoord of voor je iemand belt.

Hieronder zie je een voorbeeld:

Opdracht 31:

Wat zou je kunnen doen als je een berichtje krijgt van iemand die zegt dat hij of zij een nieuw nummer heeft. Hoe kom je erachter of dat klopt, zonder dat je dat nummer gebruikt?

Praat eens met andere mensen over deze vraag. Hoe gaan zij daarmee om?

Quiz tussendoor: test je kennis!

Je hebt nu best veel informatie gelezen en opdrachten gemaakt veilig internetten. Een korte quiz met 6 vragen.
Veel spelplezier.
Open de onderstaande link om de quiz te maken
https://veiliginternetten.nl/quiztool/gegevens-beschermen/

Had je alle 6 de vragen goed?

Superknap gedaan.

Sommige vragen zijn misschien nog lastig? Geen probleem in deze training krijg je nog meer informatie en opdrachten over veilig internetten.

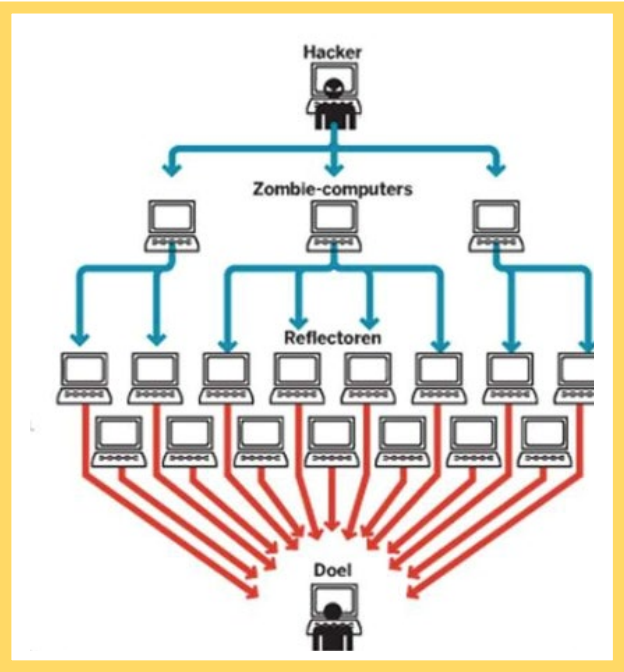
Hacken

Hacken is het inbreken van criminelen in je computer om je gegevens en/of je bestanden te stelen of te gijzelen. Gijzelen betekent dat je zelf niet meer bij jouw gegevens kan, totdat je losgeld (vaak in bitcoins) betaalt.

Hacken heeft alles te maken met onze privacy.
Een ander heeft niets met jouw informatie te maken.
Wanneer je voorzichtig bent met jouw privacy, jouw instellingen zo veilig mogelijk maakt, is het voor criminelen (hackers) niet zo gemakkelijk meer.

Jij kunt het voorkomen!

Hacken komt niet alleen voor bij grote bedrijven. De meeste hacks gebeuren doordat mensen op links in e-mails klikken. Daarmee installeer je, zonder dat je het merkt, software op je computer.
Jij ziet dat niet, maar de hacker wel. De hacker kan met die software in je bestanden kijken en ermee doen wat hij wil.



Ddos aanval

Komt die hacker dan speciaal voor jou? Vaak niet. Als de hacker zijn software op heel veel computers kan zetten, kan hij die computers allemaal tegelijk gebruiken.

Samen met heel veel andere computers laat de hacker jouw computer meedoen in een aanval op een bedrijf. Door jouw computer en heel veel andere computers te hacken, kan de hacker ervoor zorgen dat bedrijven door duizenden computers tegelijk worden aangevallen.

Als al die computers zich tegelijk op de website van een bedrijf melden, dan werkt die website niet meer. Zie het als een file: als er te veel auto's rijden, dan loopt het verkeer vast en staat alles stil.

Bedrijven vinden het niet fijn als alles stil staat. Een bedrijf dat stil staat lijdt verlies. Tijd is geld. En dat is nu precies wat de hacker leuk vindt. Misschien willen bedrijven wel veel betalen? Dan zorgt de hacker wel dat de aanval weer stopt.

Openbare wifi

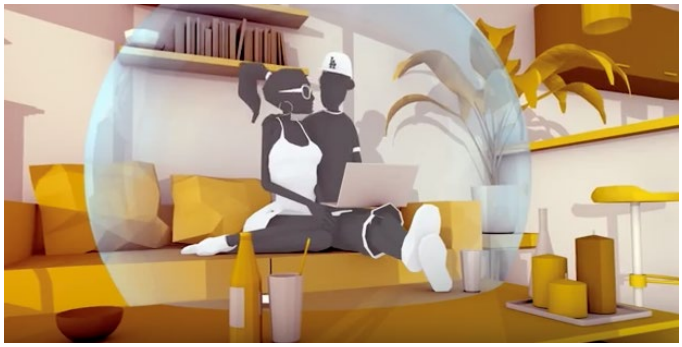
Op veel plaatsen is gratis wifi beschikbaar. Bijvoorbeeld in bus, de trein of in het café. Dat lijkt heel fijn. Je hoeft je databundel niet te gebruiken en kan toch aan de slag op internet. Anders moet je alles met 4G doen en dat kan duur zijn.

Toch is dat wel een stuk veiliger. Want … weet jij of er verderop iemand zit mee te kijken met wat jij online doet? Soms is dat natuurlijk niet zo erg. Maar een openbaar netwerk is niet beveiligd. Jij kan er ook zo op, zonder een wachtwoord in te vullen. Dat kunnen anderen dus ook. Ook mensen die gegevens van anderen willen stelen. Zij weten slimme manieren om via een openbaar wifinetwerk in jouw telefoon mee te kijken.

Denk er daarom aan om echt vertrouwelijke informatie (zoals bankzaken en persoonlijke informatie) alleen te delen via een beveiligde wifiverbinding of via 4G.

Opdracht 32:

Kijk eens naar deze filmpjes:



Wees altijd voorzichtig met openbare wifi. Ook die op je werk.
Waarom? Dat zie je in deze video:
https://www.youtube.com/watch?v=pznkwYQZLKQ
Of zoek op YouTube naar
'Alert Online- Wees voorzichtig met openbare WIFI NL.'

In deze video leer je van een hacker waarom VPN belangrijk
is bij openbare wifinetwerken: https://youtu.be/jTdftBOq640
Of zoek op YouTube naar
'Isabel Provoost zoekt uit: zijn openbare wifinetwerken veilig?'

Welke apps en informatie gebruik jij vanaf nu nog in openbare wifinetwerken? En welke niet?

Opdracht 33: Nepnieuws

Hoe weet je met al die social media nu of dat wat erop staat ook echt klopt? Hoe weet je of het waar is? Kijk eens naar de volgende zinnen. Kloppen deze volgens jou? Ja of nee?

1. Je ziet het altijd meteen, wanneer een bericht op social media nep is.
2. Je gedrag op internet bepaalt welke berichten jij op social media te zien krijgt.

De antwoorden staan hieronder.

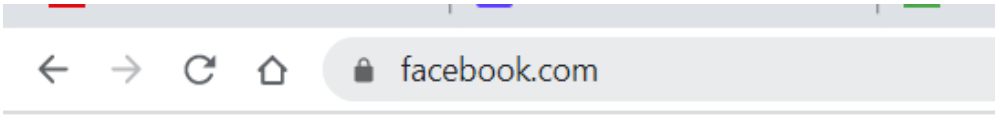
1. Nee, je hebt geen idee of de afzender of het bericht echt zijn.
2. Ja, het algoritme (een rekenmethode op basis van je gegevens en je online gedrag, ingewikkelde materie) bepaalt welke soort berichten jij wel of niet te zien krijgt.

Herken een veilige website

Internetbankieren, e-mailen, Facebooken… overal waar je inlogt wil je dat jouw persoonlijke gegevens veilig zijn. Je wilt niet dat een ander erbij kan. Op internet zijn er veilige en onveilige websites. Als je ergens inlogt, let er dan op dat je dat doet op een website met een veilige verbinding.

Tegenwoordig zijn bijna alle websites beveiligd. Deze sites kunt je als volgt herkennen:

- De URL (het adres van de website) begint met 'https://'. De s staat voor 'secure', het Engelse woord voor veilig.
- In de adresbalk staat een slotje.



Opdracht 34:

Open de volgende websites en kleur het rondje in bij de websites die volgens jou beveiligd zijn:

- ☐ www.linkedin.com
- ☐ www.ing.nl
- ☐ www.klm.nl
- ☐ www.amsterdam.nl

We zijn bijna aan het einde van de training Mediawijsheid de basis. Hopelijk ben je heel wat wijzer geworden en weet je voldoende over veilig internetten. Het antwoord van de woordzoeker is **veilig internetten.**

Media Quiz kaartje - in gesprek

Wil je digitaal pesten bespreken? Ben je nieuwsgierig naar ervaringen van anderen op het gebied van cyberpesten? Dit spel maakt vervelende situaties op internet bespreekbaar. Op de volgende bijlagen zie je kaartjes met verschillende onderwerpen. Print deze pagina's uit en maak van de onderwerpen verschillende kaartjes om te bespreken.

Instructies voor het spel:
Verdeel de kaartjes onder de aanwezigen; iedereen krijgt dus meerdere kaartjes.
Vraag per persoon welke van situaties op het kaartje het ergst en welke minder erg zijn.
Wissel de uitkomsten met elkaar uit en deel del ervaringen.

Vragen die je aan elkaar kan stellen:
Wat kan er voor vervelends gebeuren op internet?
Wat is jou weleens overkomen en wat niet?
Waar vind je erger?
Wat is snel opgelost?

Bron:mediawijsheid.n

Iemand buitensluiten bij het chatten	Roddels verspreiden via sociale media
Vervelende berichten sturen	Schelden of bedreigen bij een game
Een account hacken	Een nepprofiel maken op een datingsite plaatsen
Een bewerkte foto versturen	Een e-mailbom of Twitterbom versturen
Een wachtwoord stelen	Een uitnodiging versturen voor een nep-feest

Iemand in elkaar slaan en filmen	Ongewenste e-cards verzenden
Bedreigende mails versturen	Persoonlijke gegevens op internet zetten zonder toestemming
Vervelende berichten op een profielsite plaatsen	Een persoon te koop aanbieden op een verkoopsite
Een haatprofiel aanmaken	Een virus versturen
Filmpjes ongevraagd op internet zetten	Credits (gewonnen punten of geld) stelen bij games
Blote foto's van een ander openbaar maken	Je voordoen als iemand anders op internet