INFORMATIEBLAD

OMGAAN MET DE RISICO'S VAN INTERNET

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG IN DE ZORG

INFORMATIEBLAD OMGAAN MET DE RISICO'S VAN INTERNET

Deze lesmodule bestaat uit een Informatieblad, Opdrachtblad en Antwoordblad. Lees eerst dit Informatieblad en maak daarna de opdrachten van het Opdrachtblad. De juiste antwoorden vind je ten slotte in het Antwoordblad.

Digitale communicatie

Sinds de komst van internet en sociale media is onze manier van communiceren en nieuws vergaren drastisch veranderd. Er ligt een digitale wereld aan onze voeten die veel kansen biedt maar ook risico's met zich meebrengt. In deze lesmodule krijg je handvatten aangereikt om bewuster om te leren gaan met digitale communicatie.

Digitale communicatie en betrouwbaarheid

Op internet vind je veel informatie. Denk bijvoorbeeld aan het nieuws op de website van de NOS. Maar ook via sociale media zoals Facebook wordt informatie verspreid. Kun je die informatie eigenlijk wel vertrouwen? Moet je alles wat je ziet of leest op internet voor waar aannemen?

Het internet is van ons allemaal. Iedereen kan dus ook informatie op het internet zetten. Daarom moet je extra kritisch kijken naar digitale informatie. Soms wordt de waarheid van informatie per ongeluk verdraaid. Soms wordt de waarheid ook bewust verdraaid. Nieuwsberichten waarin de waarheid verdraaid is, noemen we nepnieuws.

Nepnieuws

Nepnieuws is nieuws dat niet waar is. De maker stuurt het de wereld in, in de hoop dat mensen het geloven en dat ze het snel zullen verspreiden. Waarom eigenlijk?

- De maker verdient er geld aan. Hoe meer mensen op een artikel klikken, hoe meer geld de maker verdient via getoonde advertenties.

- De maker probeert de mening van zoveel mogelijk mensen te beïnvloeden. Bijvoorbeeld in de aanloop naar verkiezingen, zodat meer mensen op een bepaalde partij zullen stemmen.

Hoe herken je nepnieuws? Lees de volgende acht tips:

1. Check de *bron*. Wie is de afzender van het bericht? Is deze betrouwbaar? Controleer bij websites bijvoorbeeld de disclaimer of de kop 'Over ons'.
2. Check de *link*. Makers van nepnieuws proberen een link vaak op een betrouwbare link te laten lijken. Soms is het verschil met een betrouwbare link maar heel klein. Een handige website hiervoor is www.checkjelinkje.nl
3. Check de *datum*. Nieuws hoeft niet altijd nep te zijn, maar kan ook oud of achterhaald zijn. Oud nieuws is niet altijd meer waar.
4. Check het *doel*. Probeert het bericht je over te halen om iets te kopen? Dan is het reclame en geen nieuws.
5. Check de *titel* en de *tekst*. Een titel met veel uitroeptekens of hoofdletters is doorgaans minder betrouwbaar. Ook spelfouten kunnen daarop wijzen.
6. Check *waar* het staat. Alleen op sociale media, of ook op bekendere en meer betrouwbare nieuwssites?
7. Check wie hun *mening* geven. Als twee mensen iets vinden, betekent dit niet dat heel Nederland dat vindt.
8. Check de *foto's*. Wanneer en waar zijn ze eerder gebruikt? Dit kun je zien via images.google.com.

Tip: Kom je nepnieuws tegen? Of twijfel je aan de betrouwbaarheid van een bericht? Deel het dan niet!

WEETJE?! Vooral 65-plussers herkennen nepnieuws niet. Zij delen het maar liefst zeven keer zo vaak als dertigers, en ruim twee keer zo vaak als veertigers en vijftigers.

Deepfake

Misschien heb je wel eens een video gezien waarin een bekend persoon iets heel raars zijn. Dat kan bijna niet waar zijn! En soms is het dan ook niet waar. *Deepfake* is de verzamelnaam voor software waarmee je nepvideo's kan maken die bijna niet van echt te onderscheiden zijn. Door middel van *machine learning* of *kunstmatige intelligentie* leert de software van bestaande afbeeldingen en video's en maakt daarvan weer nieuwe, nepvideo's.

Het wordt steeds moeilijker om deepfake video's van echt te onderscheiden. Het netwerk Mediawijsheid geeft de volgende tips:

1. Let op *visuele aanwijzingen*: als de mond onnatuurlijke bewegingen maakt of de persoon in de video geen één keer met de ogen knippert, is de kans groot dat de video nep is. Dit is ook het geval als je vervaagde pixels ziet of als de mond niet in lijn met de rest van de gezichtsuitdrukking beweegt.
2. Let op de *bron* van de video: komt de video van een onbekende afzender? Dan kan dat ook een aanwijzing zijn dat de video onbetrouwbaar is.

3. Ga na op welk *platform* video nog meer te vinden is: als er een nieuwswaardig onderwerp in de video centraal staat (bijvoorbeeld een pikante uitspraak van een politicus), dan zullen andere media dit nieuws ook brengen. Probeer het onderwerp van de video te bevestigen via meerdere bronnen.

Zoekmachines

Om betrouwbare informatie op het internet op te zoeken, zoals nieuws of vakliteratuur, kun je gebruik maken van online zoekmachines. *Google* is het meest bekend. *Bing* is de zoekmachine van Microsoft en ook *Yahoo!* wordt nog veel gebruikt.

Met één klik op de knop worden je duizenden zoekresultaten gepresenteerd. En hoe weet je welke informatie je moet aanklikken? Het is goed om je bewust te zijn van het feit dat zoekmachines werken met *algoritmes*. Op basis van jouw surfgedrag op het internet worden zoekresultaten gepresenteerd waarvan het algoritme heeft bepaald dat jij de informatie relevant of interessant vind.

Daarnaast worden op de eerste pagina van jouw zoekresultaten vaak reclames geplaatst. Bedrijven kunnen geld betalen om als eerste door jou gezien te worden. Dat betekent niet dat het altijd de relevantste of betrouwbaarste informatie is.

Spammails

Alle ongewenste emails worden *spammails* genoemd. Sommige mails zijn ongewenste reclame of nieuwsbrieven waar je niet op zit te wachten. Vaak kunnen deze mails niks kwaad en vind je helemaal onderaan de mail een link waarmee je je kunt afmelden voor volgende mails. Soms ontvang je misleidende informatie in je mailbox. Dan spreken we over nepmails of *phishingmails*. Phishing is het 'vissen' door criminelen naar inloggegevens en persoonsgegevens van gebruikers. Wat willen ze bereiken met het sturen van nepmails?

- Je geld of persoonsgegevens krijgen.
  Ze doen zich dan bijvoorbeeld voor als je bank, een overheidsinstelling of bedrijf.

- Computervirussen verspreiden.
  Je computergegevens worden daardoor versleuteld en daarmee kunnen ze je afpersen.

Spammails zijn

Hoe herken je nepmails? Lees de volgende zes tips:

1. Check de *afzender*. Het kan lijken of je de afzender kent. Maar kijk goed naar het e-mailadres. Klopt het? Of is het vaag, erg lang of net iets anders dan het emailadres dat je gewend bent? Zo ja, dan is het waarschijnlijk een nepmail.
2. Check de *aanhef*. Bedrijven waar je klant bent, weten of je een man of een vrouw bent. Of ze weten je voor- of achternaam. Bij een algemene aanhef, zoals 'Beste meneer/mevrouw' moet je uitkijken!

3. Vragen ze om *persoonsgegevens*? Uitkijken! Banken of overheidsinstanties vragen nooit via e-mail om dit soort gegevens.
4. Wees alert op *links*. Klik nooit zomaar op een meegestuurde link in een e-mail. Het kan een computervirus bevatten.
5. Let op *taalgebruik en vormgeving*. Is dit anders dan andere e-mails van dezelfde instantie? Zie je spelfouten? Dan is het waarschijnlijk een nepmail.
6. Wees alert op *bijlagen*. Is het een zip-bestand? Dit is altijd verdacht. Facturen en aanmaningen worden nooit op deze manier verstuurd.

Tip: Twijfel je nog of een e-mail echt of nep is? Bel dan de geclaimde instantie om te checken of ze de mail wel hebben verstuurd!

Cookies

Als je surft op internet, laat je cookies achter. Cookies zijn kleine tekstbestanden die na het bezoeken van een website opgeslagen worden op je computer. Soms zijn cookies nodig, deze heten *functionele cookies*. Cookies zorgen er namelijk voor dat een website goed werkt. Ook onthouden ze jouw voorkeursinstellingen. Bijvoorbeeld als je een wachtwoord hebt ingevoerd. Die hoef je een volgende keer dan niet meer in te vullen. Wees hier wel voorzichtig mee. Het onthouden van wachtwoorden gebeurt niet altijd op een veilige manier.
In de lesmodule Veiligheid lees je hier meer over!

Soms zijn cookies niet zo nodig, deze heten *niet-functionele cookies*. Dan onthouden cookies je surfgedrag. Ze onthouden waar jij allemaal op klikt. Zo kunnen organisaties zien wat jouw interesse heeft. Je kent het vast wel: je hebt via een zoekmachine naar een vakantie gezocht. Als je later weer op internet zit, zie je steeds een reclame van die heerlijke zonvakantie voorbijkomen. Dit is mogelijk door de niet-functionele cookies.

WEETJE?! Je kunt zelf kiezen of en welke cookies je verwijdert. Als je bijvoorbeeld functionele cookies verwijdert, worden ook je opgeslagen wachtwoorden verwijderd. Als je niet-functionele cookies verwijdert, wordt je surfgedrag verwijderd! Weten hoe het werkt? Klik op https://veiliginternetten.nl/themes/situatie/instructiefilmpjes-cookies-beheren/.

Digitale communicatie en jouw voetafdruk

Je weet nu wat je kan doen om bewust om te gaan digitale informatie die jij *ontvangt*. Maar ga je ook bewust om met digitale informatie die jijzelf of iemand anders over jou *verspreidt*?

Digitale voetafdruk

Alles wat jij op internet achterlaat, bewust of onbewust, bepaalt jouw *digitale voetafdruk*. Dat kunnen foto's, filmpjes of berichten zijn die jij bewust op het internet zet. Maar ook informatie die anderen over jou plaatsen. Of websites of sociale media die jouw online gedrag volgen. Google maar eens je naam. Vind je veel of weinig informatie over jezelf, met of zonder foto's?

Is dit informatie die je zelf op internet hebt geplaatst? Of informatie die anderen over jou op internet hebben gezet? De informatie die je vindt, wordt jouw digitale voetafdruk genoemd.

De hele wereld kan online zien wat jij achterlaat. Ook je collega's en je huidige werkgever. Ook een potentiële nieuwe werkgever. Of cliënten en patiënten waarmee je werkt. Jouw digitale voetafdruk kan beïnvloeden hoe mensen tegen je aankijken. In zowel positieve als negatieve zin. Denk daarom goed na over wat je op internet zet. Als iets er eenmaal op staat, krijg je het niet zomaar meer van af.

Een bericht over vrijwilligerswerk dat je doet zal positief overkomen. Maar niet alles wat je op internet plaatst is even geschikt om aan de hele wereld te laten zien. Sommige informatie kan nadelig uitpakken. Denk aan je vakantieplannen die inbrekers op ideeën brengen. Klachten over je baas die niet gewaardeerd zullen worden. Of intieme informatie over je (klein)kinderen, vrienden of jezelf die hen of jou in diskrediet kunnen brengen.

Tip: op internet gelden dezelfde regels als in de echte wereld. Iets wat je niet hardop in de trein durft te zeggen, plaats je beter ook niet op internet!

WEETJE?! Via de privacyinstellingen van sociale media bepaal jijzelf met wie jij welke persoonlijke informatie deelt. Privacyinstellingen zitten vaak goed verstopt boven- of onderin de startpagina. Het loont de moeite ze goed te lezen en in te stellen zoals jij dat wenst!

Gedrags- en mediacode

Veel organisaties vinden het belangrijk duidelijke afspraken met hun medewerkers te maken over welk gedrag wel en niet gewenst is op de werkvloer. Hoe je omgaat met collega's, cliënten en eigendommen van de organisatie leggen ze dan vast in een *gedragscode*. Hierin worden ook vaak regels omtrent het digitaal gedrag van medewerkers omschreven. Soms zijn deze apart opgenomen in bijvoorbeeld een *mediacode*. Hoe dit is vastgelegd verschilt per organisatie. Zoek daarom eens uit *of* en *hoe* jouw organisatie de regels omtrent digitale normen en waarden heeft vastgelegd en *welke* regels daarin precies worden vermeld.

Je weet nu hoe je bewuster om kunt gaan met de risico's die digitale communicatie met zich mee brengen. Je bent klaar om het Opdrachtblad te maken van de lesmodule Digitale Communicatie.

Bronnen:

- www.mediawijsheid.nl/nepnieuws
- www.mediawijsheid.nl/deepfake/
- H. Spiering, *Vooral ouderen verspreiden nepnieuws via Facebook*, 9 januari 2019, www.nrc.nl
- www.veiliginternetten.nl

Deze module is gemaakt door De Nova Learning in opdracht van ’s Heeren Loo en bewerkt door Jongleert in opdracht van Utrechtzorg.

Heb je opmerkingen of vragen over deze module? Mail dan naar info@digivaardigindezorg.nl