FACTSHEET: DIGITALE INFORMATIE & COMMUNICATIE

In deze factsheet van de training ‘Digitale informatie & communicatie’, vind je alle relevante informatie over het omgaan met digitale informatie en communicatie.

Het vertrouwen van informatie

Op het internet kom je veel informatie en nieuws tegen. Denk aan de site van NOS. Maar ook bijvoorbeeld op Facebook. Maar is alle informatie op internet wel te vertrouwen? Soms kan informatie worden verdraaid of wordt verkeerde informatie gebruikt.

Als nieuws niet helemaal waar is, spreek je over nepnieuws. Ook krijg je soms verkeerde informatie in je mailbox. Dan spreek je over nepmails of *phishing.*

Nepnieuws

Nepnieuws is nieuws dat niet waar is. Dit wordt de wereld ingestuurd met de hoop dat mensen het geloven. Hiervoor zijn twee redenen:

1. Hier wordt geld aan verdiend. Bijvoorbeeld doordat mensen, door zulke berichten, iets gaan kopen.
2. Het beïnvloeden van een mening kan gunstig uitpakken. Denk aan de verkiezingstijd. Als veel mensen geloven dat een bepaalde partij goede activiteiten onderneemt, stemmen ze er sneller op. Door nepnieuws kan deze mening beïnvloed worden.

Iedereen kan informatie op het internet zetten. Daarom moet je extra kritisch kijken naar informatie van internet. Is het echt en te vertrouwen? Waar moet je op letten als je dat doet? Hieronder staan de belangrijkste tips op een rij.

- Controleer de *bron*. Wie schrijft het? Bestaat de nieuwssite echt? Zoek desnoods op internet de naam van de auteur. Is hij/zij betrouwbaar?
- Controleer de *link*. Als er bijvoorbeeld .co aan het eind staat, in plaats van .com, is het nep.
- Toets de *datum.* Nieuws verandert elke dag. Er gebeuren veel nieuwe dingen. Oud nieuws is niet altijd meer waar.
- Onderzoek *het doel* van het bericht. Probeert het bericht je over te halen om iets te kopen? Dan is het reclame en geen nieuws.

- Let op *de titel* en *de tekst*. Een titel met veel uitroeptekens of hoofdletters, is doorgaans minder betrouwbaar. Ook spellingsfouten in de tekst wijzen op een mindere betrouwbaarheid.
- Kijk *waar* het wordt geplaatst. Alleen op sociale media, of ook op bekendere en meer betrouwbare nieuwssites?
- Controleer wie hun *mening* geven. Als twee mensen iets vinden, betekent dit niet dat heel Nederland dat vindt.
- Controleer of *gebruikte foto's* al eerder zijn gebruikt. Dit kun je doen via images.google.com.

Belangrijk: Deel het nepnieuws niet!

Voorbeelden van websites met nepnieuws
Er zijn ook websites die expres nepnieuws plaatsen. www.speld.nl is hier een voorbeeld van. Zij plaatsen satirische nieuwsberichten. Kijk eens naar de berichten die zij plaatsen.

Nepmails

Nieuws kan dus nep zijn. Ook e-mails die je krijgt zijn soms nep. Hiermee proberen cybercriminelen geld of gegevens van je te krijgen. Ook wordt dit gebruikt om virussen te verspreiden. Dit wordt *phishing* genoemd.

Soms is het makkelijk te zien of het om een nepmail gaat. Soms niet. Blijf altijd kritisch! Om een nepmail te herkennen kun je letten op de volgende punten:

- Controleer *de afzender*. Het kan lijken of je de afzender kent. Maar kijk eens naar het e-mailadres dat is gebruikt. Is dat het juiste e-mailadres? Of is het een variant hierop? Het officiële mailadres van de Rabobank nieuwsbrieven is bijvoorbeeld klantinfo@mail.rabobank.nl. Een nepmailadres kan bijvoorbeeld zijn klantinformatie@1mail.rabobank.com. Controleer dit goed.
- Controleer *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!
- Wordt er gevraagd om *persoonsgegevens*? Uitkijken! Banken of verzekeringsmaatschappijen vragen nooit via e-mail om dit soort gegevens. Moet je op een link klikken om de gegevens te geven? Doe dit nooit zomaar. Bel liever de instantie om te checken of ze deze gegevens echt willen hebben.
- Let op het *taalgebruik en de vormgeving*. Is dit anders dan andere e-mails van dezelfde instantie?

- Controleer de *hyperlinks*. Klik nooit zomaar op links in een e-mail. Je kunt de link controleren door je muis boven de link te houden. Zo zie je naar welke site je wordt doorverwezen. Voorkom dat je klikt op een nephyperlink.
- Wees alert op *bijlagen*. Is het een zip-bestand? Dit is altijd verdacht, omdat facturen en aanmaningen nooit op deze manier worden verstuurd. Bij twijfel kun je ook altijd de instantie bellen om te controleren of het echt van hen komt.

Het achterlaten van eigen informatie

Soms heb je dus te maken met onbetrouwbare informatie. Dit wordt naar je toegestuurd. Maar jij verspreidt ook informatie over jezelf. Dit gebeurt soms onbewust en soms bewust. Denk maar eens aan de foto's of berichten die jij op het internet zet.

Onbewuste informatieverspreiding

Wanneer je surft op internet, laat je cookies achter. Cookies zijn kleine tekstbestanden die na het bezoeken van een website opgeslagen worden op de computer. Soms zijn cookies nodig, dit worden *functionele cookies* genoemd.
Cookies zorgen er namelijk voor dat een website goed werkt. Ook onthouden ze voorkeursinstellingen.
Als je bijvoorbeeld een wachtwoord hebt ingevoerd, wordt dit onthouden. Zo hoef je je wachtwoord de volgende keer niet meer in te vullen. Wees hier wel voorzichtig mee.
Het onthouden van wachtwoorden gebeurt niet altijd op een veilige manier.
In de training Veiligheid kun je hier meer over lezen!

Soms zijn cookies niet zo nodig, dit worden *niet-functionele cookies* genoemd. Dan onthouden cookies je surfgedrag. Dit betekent dat er wordt onthouden waar jij op klikt. Zo kunnen organisaties zien wat jouw interesse heeft. Je kent het vast wel: je hebt op een reisaanbieder naar een vakantie gezocht. Als je later weer op internet zit, zie je telkens een reclame van die heerlijke zonvakantie voorbijkomen. Dit is mogelijk door de niet-functionele cookies.

Cookies kun je altijd verwijderen.
Je kunt kiezen welke cookies je wil verwijderen. Als je bijvoorbeeld de functionele cookies verwijdert, worden ook je opgeslagen wachtwoorden verwijderd. Maar als je de niet-functionele cookies verwijdert, wordt je surfgedrag verwijderd.

Hoe verwijder je cookies?
Zoek op www.veiliginternetten.nl naar 'Instructiefilmpjes: Cookies beheren' of klik op https://veiliginternetten.nl/themes/situatie/instructiefilmpjes-cookies-beheren/.
Hier vind je voor elke browser een instructiefilmpje. Dus kijk of je bijvoorbeeld Chrome, Internet Explorer, of Safari gebruikt en bekijk het juiste filmpje.

Bewuste informatieverspreiding

Je laat zelf ook informatie achter op internet. 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 gezet? Of informatie die anderen over jou op internet hebben gezet? De informatie die je vindt, wordt jouw *digitale voetafdruk* genoemd.

Kijk daarom dus altijd uit met wat je plaatst op internet. Sommige informatie kan nadelig uitpakken. Denk bijvoorbeeld aan sollicitaties. Iemand is in het verleden in aanraking geweest met diefstal, fraude of agressie. Hierover kun je dingen vinden op internet. Het is voor deze persoon lastig om een nieuwe baan te vinden, terwijl hij dit gedrag uit het verleden ver achter zich heeft gelaten.

Een digitale voetafdruk kan dus beïnvloeden hoe je tegen mensen aankijkt. Ook in positieve zin. Bijvoorbeeld als je ziet dat een collega of leidinggevende in zijn vrije tijd zich actief inzet in de medezeggenschapsraad op de school van zijn/haar kind. Je krijgt meer respect voor deze collega of leidinggevende.

Als je een foto op internet zet, kijk dan naar de privacy-instellingen. Is het zichtbaar voor iedereen? Of alleen voor een klein groepje mensen? Alles wat eenmaal op internet staat, krijg je er niet zomaar meer vanaf. Wees je hier dus bewust van!

Het omgaan met digitale informatie

Digitale informatie en communicatie is enorm toegenomen. Bijna iedereen heeft wel een mobiele telefoon, meerdere e-mailaccounts of een account op één van de sociale media zoals Facebook, Instagram, Twitter of LinkedIn. Het is ook belangrijk om te weten welke risico's het met zich meebrengt. Zo ben je je meer bewust van je eigen internetgedrag en alert op nepnieuws. En kan je hier op de juiste manier mee omgaan. Zo breng je geen schade aan jezelf en aan een ander!

De drie risico's die in deze training belangrijk zijn, zijn de volgende:

1. *Informatie kan niet zomaar verwijderd worden.*
   Wanneer iets op het internet staat, komt het er (bijna) niet meer vanaf. Als je bijvoorbeeld een foto op internet plaatst, kan iemand deze opslaan. Ook kan deze foto gedeeld worden.
2. *Niet alle digitale informatie is betrouwbaar.*
   Het is belangrijk je hier bewust van te zijn. Geloof nooit zomaar wat. Door wie is het bericht geplaatst? Wat is het belang van die persoon of dat bedrijf? Is het bericht geplaats uit commercieel belang?
   Kijk ook extra uit bij e-mails die je niet helemaal vertrouwt. Zie de punten bovenaan om te kijken waar je op moet letten.
3. *Informatie kan misleidend zijn.*
   Een website, programma of app kan gratis aangeboden worden. Maar niets is gratis! Bedenk wat hierachter zit. Op wat voor manier wordt er toch geld verdiend? Welke gegevens worden er bij het gebruik van het programma van jou gevraagd en gedeeld? Probeer erachter te komen waarom iets gratis lijkt.

Bronnen:

- www.mediawijsheid.nl/nepnieuws
- www.speld.nl
- www.veiliginternetten.nl