



DigiVeiliger

Kennismaking met online veiligheid



Introductie	03
Informatie over veilig online zijn	04
De voordelen van het internet	04
Informatie over veilig online zijn	05
ABCD'tje	05
Denk goed na voordat je iets deelt	05
Hoe kunnen oplichters je benaderen?	05
Oplichtingstrucs + toelichting	06
Voorbeelden van online oplichting.....	08
Tips over online veiligheid en bescherming	10
Handige websites	11
Opgelicht?	11
Hulp nodig?	12
Met vertrouwen online	12
Tips	13

Introductie: Kennismaking met online veiligheid

In onze digitale samenleving kunnen we niet meer zonder internet. We bankieren online, houden contact met familie en vrienden, doen aankopen met een paar klikken en regelen steeds meer zaken via onze telefoon of computer. Het internet biedt enorme voordelen: gemak, snelheid, toegang tot informatie en contact met anderen. Maar naast al die mogelijkheden zijn er ook risico's. Criminelen maken slim gebruik van het internet om mensen te misleiden om zo toegang te krijgen tot geld of persoonlijke gegevens. Daarom is het belangrijk om een goede basis te hebben in online veiligheid.

Dit boekje geeft meer informatie over:

- de voordelen en mogelijkheden van het internet;
- veelgebruikte trucs van oplichters;
- voorbeelden van oplichtingsmails en sms'jes;
- tips over online oplichting en veiligheid;
- handige websites;
- wat je moet doen als je toch bent opgelicht.

Blader door dit boekje en ontdek hoe je veilig en bewust online kunt zijn. Het vormt een stevige basis om met vertrouwen te internetten.

De voordelen van het internet

De online wereld biedt veel mogelijkheden en gemak.

- Altijd toegang tot informatie: Je kunt snel nieuws lezen, iets opzoeken of leren over een onderwerp dat je interesseert.
- Gemakkelijk contact houden: Via e-mail, berichtenapps en sociale media kun je eenvoudig communiceren met familie, vrienden en kennissen.
- Online diensten regelen: Steeds meer zaken kun je digitaal regelen, zoals bankzaken, afspraken maken of formulieren invullen.
- Online winkelen: Je kunt producten vergelijken, beoordelingen lezen en aankopen doen zonder de deur uit te gaan.
- Leren en ontwikkelen: Er zijn talloze online cursussen, instructievideo's en leerplatforms beschikbaar om nieuwe vaardigheden te ontwikkelen.

Informatie over veilig online zijn

Bij online veiligheid gaat het om veilig en bewust gebruikmaken van het internet. Of je nu bankiert, berichten verstuurt, online winkelt of informatie opzoekt: je doet dit vaak via je computer, tablet of telefoon. Online veiligheid betekent dat je je persoonlijke gegevens beschermt en weet hoe je risico's kunt herkennen en voorkomen.

Online veiligheid heeft verschillende voordelen:

- Je verkleint de kans dat anderen misbruik maken van jouw gegevens of geld.
- Je herkent sneller verdachte berichten, telefoontjes of websites.
- Je kunt met meer vertrouwen en rust gebruikmaken van internet.
- Je weet wat je moet doen als er toch iets misgaat.

ABCD'tje

Onthoud het ABCD'tje om zo veilig mogelijk online te zijn.



Alert

Wees alert dat er oplichters zijn die je op verschillende manieren kunnen benaderen en blijf op de hoogte van oplichtingstrucs



Bescherm

Bescherm je apparaten. Zorg ervoor dat ze goed beveiligd zijn, up-to-date zijn en dat je sterke wachtwoorden gebruikt



Controleer

Controleer altijd de afzender, de inhoud, de links en voer niet zomaar een actie uit



Deel

Deel verdachte berichten of links met de organisatie en praat hierover met bekenden. Twijfel je of het betrouwbaar is? Neem dan contact op met de organisatie

Denk goed na voordat je iets deelt!

Vraag jezelf altijd: *Zou ik deze informatie ook in het echte leven delen?* Zou je zomaar je pincode of adres aan een vreemde geven? Doe dat online ook niet. Gebruik je gezond verstand en wees kritisch op wat je online tegenkomt.

Hoe kunnen oplichters je benaderen?

Oplichters gebruiken verschillende manieren om contact met je op te nemen. Ze kunnen je bijvoorbeeld benaderen via: e-mail, sms, WhatsApp of ze bellen je. Vaak doen ze alsof ze van een bekende organisatie zijn, zoals een bank, een webwinkel of een overheidsinstantie. Ze willen je persoonlijke gegevens of geld krijgen. Ze proberen je vaak bang te maken, zodat je snel iets doet. Blijf daarom rustig en neem de tijd.

Oplichtingstrucs



1. Inspelen op emoties



2. Te mooi om waar te zijn



6. Voordoen als bekende (instantie)



3. Onverwachts



5. Verdachte links, e-mails, nummers



4. Persoonlijke gegevens of geld

Oplichtingstrucs: toelichting

1. Inspelen op emoties

Oplichters proberen je bang of ongerust te maken of ze zetten je onder tijdsdruk. Ze zeggen bijvoorbeeld dat er iets mis is met je bankrekening of dat je snel iets moet regelen. Zo hopen ze dat je sneller reageert zonder goed na te denken.

2. Te mooi om waar te zijn

Je krijgt een aanbod dat heel aantrekkelijk lijkt. Bijvoorbeeld een dure telefoon voor bijna niets of een grote geldprijs. Vaak klopt het niet. Als iets te mooi klinkt om waar te zijn, is dat meestal ook zo.

3. Onverwachts

Je krijgt ineens een bericht over een pakket, betaling of probleem waar je niets van weet. Dat is een waarschuwingssignaal. Wees extra voorzichtig bij berichten die je niet verwacht.

4. Vragen om persoonlijke gegevens of geld

Een echte bank of organisatie vraagt nooit zomaar om je pincode, wachtwoord of andere persoonlijke gegevens. Ook vragen ze niet om snel geld over te maken.

5. Verdachte links, e-mails, nummers

Soms lijkt een e-mail of sms echt, maar klopt het e-mailadres of telefoonnummer niet. Of de link ziet er vreemd uit. Klik niet zomaar op een link en bel bij twijfel zelf het officiële nummer van de organisatie.

6. Voordoen als bekende (instantie)

Oplichters doen soms alsof ze van een bank of de overheid zijn of een bekende, zoals een familielid. Controleer altijd of het bericht echt is. Neem bij twijfel zelf contact op via de officiële website of het bekende telefoonnummer.

Digimail

Openstaande vordering - Infomedics



Infomedics

rekening@mijninfomedics.nl



Dossiernummer: 35624310

Betaaltermijn: uiterlijk binnen 7 werkdagen na ontvangst van dit bericht

Bedrag: 155,54

Geachte heer/mevrouw,

Volgens onze gegevens is de betaling voor **Dossier: 35624310** nog niet ontvangen. Wij verzoeken u het openstaande bedrag binnen deze termijn te voldoen via iDEAL/Wero. Hiermee voorkomt u dat aanvullende kosten in rekening worden gebracht.

[Ga naar Mijn Infomedics om te betalen .](#)

Met vriendelijke groet,
Infomedics - Debiteurenadministratie

Uitleg voorbeeld

Infomedics stuurt rekeningen alleen van het adres: rekening@infomedics.nl, niet rekening@mijninfomedics.nl. Ook al lijkt de afzender betrouwbaar, controleer altijd de rest van de mail!

- In de mail staat een emotionele truc om binnen 7 werkdagen het bedrag te betalen. Anders komen er aanvullende kosten.
- Er is een standaard aanhef. In **echte** e-mails van Infomedics word je vaak aangesproken met meneer/mevrouw + je achternaam.
- De opmaak lijkt op een e-mail van Infomedics: het logo klopt en de kleuren zijn juist. Maar oplichters kunnen mails namaken.
- Je kunt altijd het betaalkenmerk controleren op de website: infomedics.nl/zorgconsument/rekeningchecker

Voorbeelden van online oplichting

Uitleg voorbeeld

De afzender is een onbekend nummer. Vaak staat bij een sms van een pakketdienst de naam, zoals PostNL of DHL. **Let op!** Oplichters kunnen een nummer overnemen. Controleer daarom de rest van de sms.

- Er wordt ingespeeld op emotie: Je moet snel betalen.
- Het bedrag is klein. Daarmee hopen ze dat je het wel wilt betalen.
- Een betaalverzoek vis sms bevat geen link bij PostNL. De sms bevat alleen de barcode van de zending en het verzoek om zelf naar de PostNL-website te gaan.



Uitleg voorbeeld

De afzender is een onbekend nummer. Daarnaast stuurt de Belastingdienst geen sms om iets te betalen, maar ook niet als je iets ontvangt. Berichten van de Belastingdienst ontvang je via MijnOverheid.

- De link wijkt af van de officiële website. De Belastingdienst vraagt nooit om op een link te klikken. Je moet altijd zelf inloggen op belastingdienst.nl
- Ze spelen in op je gevoel: Je kunt het bedrag direct aanvragen. En geld ontvangen is natuurlijk fijn. Maar daarom moet je goed opletten.



Tips over online veiligheid en bescherming



Werk apparaten bij

Zorg ervoor dat je telefoon, computer en alle apps up-to-date zijn. Je hebt dan de nieuwste en meest veilige versie.

Gebruik sterke wachtwoorden

Een sterk wachtwoord bestaat uit hoofdletters, kleine letters, cijfers, symbolen en minstens 12 tekens. Gebruik voor elk account een ander wachtwoord.



Wachtwoordmanager

Een wachtwoordmanager is een app op je telefoon en/of computer waarin je wachtwoorden veilig worden opgeslagen. Je hoeft alleen het hoofdwachtwoord te onthouden.

Tweestapsverificatie

Zet tweestapsverificatie aan. Dit biedt extra beveiliging. Met dit extra slot moet iemand je wachtwoord weten en je telefoon in handen hebben om in te loggen.



Openbare Wi-Fi

Vermijd het gebruiken van gevoelige informatie, zoals bankieren, op openbare Wi-Fi.

Antivirusprogramma

Bescherm je computer tegen virussen.



Back-up

Maak regelmatig een kopie van belangrijke bestanden.

Scan de QR-codes om de webpagina met tips te bekijken.

Handige websites

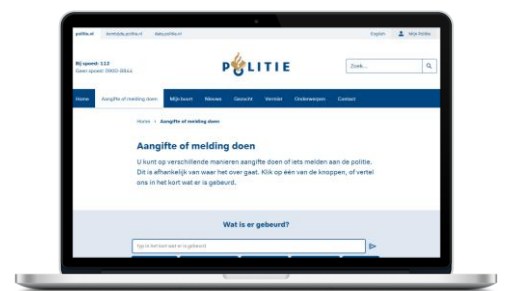
fraudehelpdesk.nl
veiliginternetten.nl
politie.nl
checkjelinkje.nl
veiligbankieren.nl
seniorweb.nl

hetccv.nl/tool-cyberweerbaarheid
opgelicht.nl
slachtofferhulp.nl
haveibeenpwned.com
wieheeftgebeld.nl/

Opgelicht?

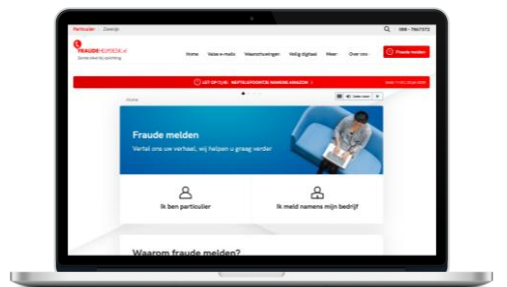
Doe dan aangifte bij de politie.

- Bel 0900-8844
- Ga naar het politiebureau
- Doe online aangifte via:
politie.nl/aangifte-of-melding-doen



Meld het bij de Fraudehelpdesk.

- Bel 088-786 73 72
- Ga naar fraudehelpdesk.nl
- Zij geven ook tips wat je moet doen, zoals:
 - bankrekening blokkeren
 - computer controleren op virussen
 - wachtwoord wijzigen



Neem contact op met de organisatie waar je bent opgelicht (bijvoorbeeld bij je bank of Marktplaats).

Door deze stappen te volgen help je anderen ook veilig online te blijven.

Hulp nodig?

Heb je hulp nodig, bijvoorbeeld bij een wachtwoordmanager of tweestapsverificatie? Daarvoor kun je terecht bij de bibliotheek. Bezoek een spreekuur waar anderen je helpen met digitale vragen.

Je kunt ook contact opnemen met de DigiHulplijn:

- Bel 0800-1508
- Mail naar vragen@digihulp.nl
- Stel je vraag via WhatsApp (scan de QR-code)



Meer leren?

Ga naar digiveiliger.nl voor meer oefeningen en tips. Of bezoek de lokale bibliotheek voor hulp en workshops over online bankieren of online veiligheid.



Met vertrouwen online

Je weet nu beter waar je allemaal op moet letten om zo veilig mogelijk online te zijn. Krijg je een bericht? Denk dan aan het ABCD'tje:

Alert – **B**escherm – **C**ontroleer – **D**eel

Vertrouw op je gezond verstand. Twijfel je over een bericht? Neem dan rustig de tijd om het te controleren. Zie je één of meerdere oplichtingstrucs terugkomen? Let dan goed op. Je kunt altijd bellen of mailen naar het bedrijf waar je een bericht van krijgt om te controleren of het echt is.

Belangrijke telefoonnummers

Zet belangrijke telefoonnummers in je contactenlijst, zoals het officiële nummer van je bank. Word je gebeld door iemand die zegt dat hij van de bank is en vertrouw je het niet? Hang dan op en bel zelf het nummer dat je al hebt opgeslagen. Zo weet je zeker dat je de echte organisatie belt.

Schrijf belangrijke telefoonnummers ook op in een schriftje. Als je telefoon gestolen wordt, weet je in ieder geval snel welk nummer je moet bellen om je bankpas te blokkeren.

Pasjes en telefoon

In sommige telefoonhoesjes kun je je pasjes bewaren. Dat is handig, maar ook riskant. Als je je telefoon verliest of als deze wordt gestolen, ben je meteen ook je bankpas en identiteitskaart kwijt. Bewaar belangrijke pasjes daarom liever apart. Zo verklein je de kans dat iemand tegelijk toegang krijgt tot je telefoon én je pasjes.

Onbekende telefoonnummers controleren

Word je gebeld door een onbekend nummer? Neem niet op en controleer het nummer op de website: wieheeftgebeld.nl. Op deze website kun je een telefoonnummer invullen. Je ziet dan of andere mensen ervaringen hebben gedeeld met dit nummer. Soms blijkt het te gaan om opdringerige verkopers of telefonische oplichting. Let op: bel een onbekend nummer niet zomaar terug, vooral niet als het een buitenlands nummer is.

DigiVeiliger

Kennismaking met online veiligheid



Dit boekje is een samenvatting van de les 'Kennismaking met online veiligheid'. Het bevat de belangrijkste tips en aandachtspunten om veilig te online te zijn. Handig om nog eens rustig door te lezen.

Gebruik dit boekje als geheugensteuntje:
bij twijfel, altijd eerst even checken!

Zeker online