DigiVeiliger

Veilig en beschermd online

Inhoudsopgave

Introductie 03

Online oplichting 04

ABCD'tje 04

Denk goed na voordat je iets deelt 04

Voorbeelden van online oplichting 05

VeiligWijzer + stap voor stap 07

Handige websites 13

Opgelicht? 13

Hulp nodig? 14

Meer leren? 14

Met vertrouwen online 14

Introductie: Veilig en beschermd online

Steeds meer dingen gaan tegenwoordig via internet. Denk aan internetbankieren, e-mails lezen, foto's bekijken en verhalen lezen van familieleden die op reis zijn of informatie opzoeken. Daarvoor gebruiken we apparaten zoals een computer, tablet of smartphone. Dat is vaak handig en snel. Maar het is ook belangrijk om te weten hoe je dit veilig doet.
Helaas zijn criminelen ook in de online wereld te vinden. Ze proberen in te breken op je apparaten of accounts, of willen persoonlijke gegevens van je hebben. Ook wordt er vaak ongemerkt informatie over jou verzameld. Daarom is het goed om te weten hoe je jezelf kunt beschermen.

Dit boekje geeft meer informatie over:

- hoe je je accounts kunt beveiligen;
- hoe je je apparaten kunt beveiligen;
- hoe je veilig kunt internetten;
- wat je kunt doen om je privacy te beschermen;
- handige websites;
- wat je moet doen als je toch bent opgelicht.

Blader door dit boekje en leer hoe je met een paar stappen je apparaten, accounts en gegevens veilig houdt. Zo kun je veiliger gebruikmaken van internet.

Informatie over veilig en beschermd online

Online oplichters kunnen op verschillende manieren contact met je zoeken: via de mail, sms, WhatsApp of door te bellen. Ze doen zich voor als een bekende organisatie (je bank), de overheid of zelfs als een familielid. Ze proberen je te laten klikken op een link, persoonlijke informatie te delen of een betaling te doen. Gelukkig kun je jezelf goed beschermen: gebruik sterke wachtwoorden, voer updates uit en controleer links voordat je erop klikt.

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.

Voorbeelden van online oplichting

Krijg je een bericht? Bijvoorbeeld een e-mail of een sms, denk dan aan het ABCD'tje. Controleer altijd of het bericht betrouwbaar is.

Digimail

Vattenfall - Betalingsherinnering

Vattenfall
info@vattenfalll.nl

Geachte heer/mevrouw,

Op **7 mei** hebben wij geprobeerd € 250,42 van uw rekening af te schrijven. Dit is helaas niet gelukt. Wij verzoeken u het openstaande bedrag **voor 30 juni** te betalen om afsluiting of extra kosten te voorkomen.

Betaal direct via iDEAL

Notanummer: 373019608
Bedrag: € 250,42

Met vriendelijke groet,
Vattenfall

Uitleg voorbeeld

De afzender lijkt betrouwbaar, maar de naam Vattenfall is fout gespeld (met 3 keer de letter 'l'). Controleer het e-mailadres op de officiële website van het bedrijf en kijk naar eerdere mails die je hebt gekregen.

- In de mail staat een emotionele truc. Ze willen dat je je schuldig voelt omdat de betaling niet is gelukt. En ze zetten je onder druk om snel te betalen, om afsluiting of extra kosten te voorkomen.
- Er is een standaard aanhef. In **echte** e-mails van bedrijven staat vaak een persoonlijke aanhef, zoals je achternaam.
- Bedrijven verwijzen je vaak door naar je persoonlijke account voor meer informatie. Nu staat er direct een betaallink.

Uitleg voorbeeld

De afzender is onbekend. Vaak staat bij een sms van de organisatie welk bedrijf het is in plaats van het nummer. **Let op!** Oplichters kunnen ook een betrouwbaar nummer overnemen.

- Er wordt ingespeeld op emotie: Je moet snel je gegevens bijwerken om nog van diensten gebruik te kunnen maken.
- De link gegeven kan onbetrouwbaar zijn.
- Ga altijd zelf naar de website om in te loggen in je persoonlijke omgeving in plaats van door op de link te klikken.

Uitleg voorbeeld

De afzender is onbekend. Bovendien sturen bedrijven of organisaties vaak geen bericht via WhatsApp.

- Er wordt ingespeeld op emotie: Je moet zo spoedig mogelijk contact opnemen.
- Het telefoonnummer dat erbij staat kan onbetrouwbaar zijn.
- Controleer altijd op de website van de bank zelf welk telefoonnummer je moet bellen.

VEILIGWIJZER

Veilig en beschermd online

1. Gebruik sterke wachtwoorden

2. Log in met 2 stappen

3. Gebruik een virusscanner

4. Voer updates uit

5. Wees voorzichtig met openbare wifi

6. Controleer websitelinks

7. Gebruik toestel-beveiliging

8. Maak back-ups

9. Accepteer niet zomaar cookies

Accounts beveiligen

Criminelen proberen in te breken op je account of op je computer. Dit doen ze bijvoorbeeld door je wachtwoord te raden of te stelen, ze sturen een nepmail waarin ze vragen om je inloggegevens of ze zetten een virus op je apparaat.

Je kunt zelf een aantal dingen doen om je accounts te beveiligen:
- Gebruik sterke wachtwoorden
- Log in met 2 stappen
- Gebruik een virusscanner
- Voer updates uit
- Let op met het gebruik van openbare wifi

Scan de QR-codes op de volgende pagina's om de tips te bekijken.

1. Sterke wachtwoorden

Gebruik voor ieder account een ander wachtwoord. Zo hebben oplichters niet direct toegang tot al je accounts.

Hoe maak je sterke wachtwoorden?
- Maak het oplichters niet te makkelijk. Gebruik geen standaard wachtwoord (1234, Welkom123) of een wachtwoord met persoonlijke gegevens (naam/geboortedatum).
- Zorg ervoor dat het wachtwoord bestaat uit kleine letters, hoofdletters, cijfers, speciale tekens en minimaal 12 tekens.
- Gebruik een wachtwoordzin.

Bewaar je wachtwoorden in een wachtwoordmanager (een app op je telefoon) of schrijf ze op in een boekje. Voeg dan wel een extraatje toe aan het wachtwoord, maar schrijf dit niet op: bijvoorbeeld achter elk wachtwoord een extra teken of getal.

2. Inloggen in met 2 stappen

Heeft een crimineel je wachtwoord, maar gebruik jij inloggen in 2 stappen? Dan kan de crimineel nog steeds niet inloggen.

Als je het inloggen in 2 stappen hebt ingeschakeld, moet je inloggen met meer dan alleen je wachtwoord. Je krijgt bijvoorbeeld een code via een sms of een e-mail. De crimineel moet dan ook kunnen inloggen in je mail of jouw telefoon in handen hebben om te kunnen inloggen.

3. Virusscanner

Criminelen kunnen een virus op je apparaat zetten. Bijvoorbeeld als je op een onveilige link klikt of een onveilige bijlage in een e-mail opent. Zo kunnen ze je gegevens of wachtwoorden stelen. Installeer daarom een virusscanner. Dit programma waarschuwt je bij een virus of als je op een gevaarlijke website zit.

4. Updates uitvoeren

Voer updates uit op al je apparaten. Zo blijft je apparaat beter beveiligd en maken criminelen minder kans om in te breken.

5. Openbare wifi

Openbare wifi is internet dat voor iedereen beschikbaar is. Je hebt geen wachtwoord nodig of je kunt inloggen met een algemeen wachtwoord dat iedereen krijgt. Je vindt het vaak in hotels, cafés, stations en campings.

Openbare wifi is vaak niet goed beveiligd. Zo kunnen criminelen meekijken wat je aan het doen bent. Gebruik het dus niet voor gevoelige zaken, zoals bij internetbankieren.

Veilig internetten

Het internet is heel handig, maar je moet wel goed opletten op welke website je terechtkomt.

Tips om veilig te internetten:

- Download niet zomaar iets van het internet
- Controleer een link
- Controleer of er een slotje (of ander icoon) in de adresbalk staat
- Controleer of er https staat (met een s)
- Twijfel je? Controleer de link dan op checkjelinkje.nl

6. Websitelinks controleren

- Kijk naar het deel tussen https:// en de eerste /

- Kijk naar het deel tussen de laatste twee punten

- Https://www.belastingdienst.nl.test.nl/betaling/inloggen.html

- Let ook op spelfouten: https://www.rab0bank.nl

7. Toestel beveiliging

Toegangscode (Android-toestel)

Gebruik een toegangscode, zoals een pincode, je vingerafdruk of gezichtsherkenning. Zo voorkom je dat anderen je telefoon of computer kunnen gebruiken.

Toegangscode (Apple-toestel)

Gebruik een toegangscode, zoals een pincode, je vingerafdruk of gezichtsherkenning. Zo voorkom je dat anderen je telefoon of computer kunnen gebruiken.

8. Back-ups

Een back-up is een kopie van je bestanden, zoals foto's en documenten. Gaat je telefoon stuk of raak je hem kwijt? Dan heb je nog een kopie van belangrijke bestanden.

9. Cookies

Cookies zijn kleine bestanden die websites opslaan om informatie te onthouden. Websites gebruiken cookies voor persoonlijke reclame. Accepteer niet zomaar alle cookies. Klik op 'weigeren' of op 'alleen functionele cookies'. Verwijder af en toe cookies.

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

Online privacy

Het is belangrijk om zelf te bepalen welke informatie je over jezelf deelt met anderen. Als er veel informatie over je te vinden is op het internet, dan kunnen oplichters hier misbruik van maken. Ongemerkt verzamelen apps en websites ook allerlei informatie over je.

Instellingen telefoon (Android-toestel)
Controleer welke apps op je telefoon toegang hebben tot sommige functies. Niet alle apps hebben toegang nodig tot bijvoorbeeld je camera, microfoon of locatie.

Instellingen telefoon (Apple-toestel)
Controleer welke apps op je telefoon toegang hebben tot sommige functies. Niet alle apps hebben toegang nodig tot bijvoorbeeld je camera, microfoon of locatie.

Kopie-ID app
Criminelen kunnen zich voordoen als jou. Ze maken misbruik van je gegevens. Voorkom identiteitsfraude door niet te veel informatie te delen en de Kopie ID app te gebruiken.

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

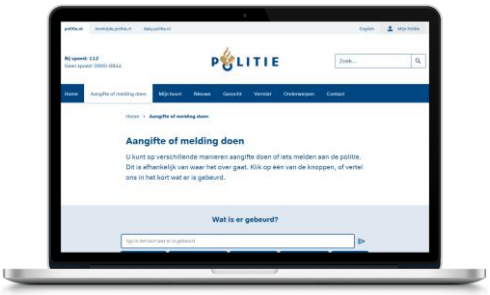
Handige websites

fraudehelpdesk.nl
veiliginternetten.nl
politie.nl
checkjelinkje.nl
https://www.politie.nl/informatie/checkjehack.html
https://veiliginternetten.nl/wachtwoordkraaktest/
hetccv.nl/tool-cyberweerbaarheid
https://hetccv.nl/hulp-bij-online-criminaliteit/
opgelicht.nl
seniorweb.nl
slachtofferhulp.nl

Opgelicht?

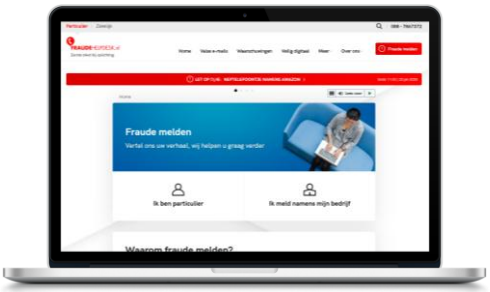
Doe dan aangifte bij de politie.

- 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 de 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 communiceren 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: **A**lert – **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 met de VeiligWijzer. Je kunt altijd bellen of mailen naar het bedrijf waar je een bericht van krijgt om te controleren of het echt is.

Notities

DigiVeiliger

Veilig en beschermd online

Veilig en beschermd online

Dit boekje is een samenvatting van de les ‘Veilig en beschermd online’. Het bevat de belangrijkste tips en aandachtspunten om je accounts te beveiligen, je apparaten te beveiligen en je online privacy te beschermen. Dit is handig om nog eens rustig door te lezen.

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

zeker online

© Stichting Digisterker