Webshop-fraude

Webshopfraude is wanneer je opgelicht wordt als je een online aankoop doet. Criminelen maken valse webshops om geld of persoonlijke gegevens in handen te krijgen. De producten of diensten in de webshop worden bijvoorbeeld niet geleverd of lijken helemaal niet op de aanbieding.

- Bekijk of de webshop realistisch is. Let op bij extreem lage prijzen of tijdelijke acties die te mooi lijken om waar te zijn. Vergelijk ook met andere webshops.
- Check de betrouwbaarheid van webwinkels door reviews, bijvoorbeeld Trustpilot of ScamCheck.
- Bij online winkels is het verstandig om te betalen met creditcard, want dan ben je vaak verzekerd.
- Als je kiest om te betalen met Mollie, Paypal, Buckaroo, Klarna, Riverty en Adyen, kan je contact opnemen met de klantenservice van het bedrijf. Zij kunnen je helpen.

Ben je slachtoffer geworden?

Ben je slachtoffer geworden van online fraude of oplichting? Je kan de volgende dingen doen:

- Verzamel bewijs, maak schermafbeeldingen of foto's.
- Verander je wachtwoorden als iemand je heeft gehackt of geprobeerd te hacken.
- Doe aangifte bij de politie. Dit kan via www.politie.nl of bel 0900-8844.
- Maak een melding bij de Fraudehelpdesk. Ga naar www.fraudehelpdesk.nl of bel 088-7867372.
- Heb je hulp nodig? Neem contact op met Slachtofferhulp via www.slachtofferhulp.nl of bel 0900 – 0101 of 088-7460000.

Meer tips over online veiligheid vind je op veiliginternetten.nl.

veiliginternetten.nl

veiliginternetten.nl

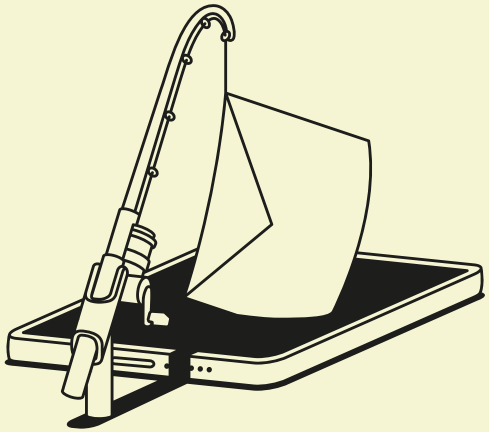
Eerste Hulp bij Online Criminaliteit

Het internet is niet weg te denken uit het dagelijks leven. Alles kan of moet online, van boodschappen tot bankzaken en zelfs een doktersafspraak. Internetcriminelen bedenken steeds nieuwe technieken om mensen online op te lichten. In deze flyer vind je informatie over het herkennen van verschillende vormen van online fraude en tips wat je kunt doen als je slachtoffer bent geworden. Heel belangrijk om je te realiseren; Het kan iedereen overkomen.

Phishing

Criminelen doen zich voor als een bank of andere organisatie via de mail, sms, of Whatsapp. Ze vragen je om op een linkje te klikken of om ergens je persoonlijke gegevens in te vullen.

- Check het e-mailadres van de afzender.
  - Twijfel je of het bericht echt is? Bel de organisatie of het bedrijf op een bekend nummer om het te checken.
- Controleer altijd een link voordat je erop klikt. Criminelen kunnen namelijk een link vervalsen en het echt doen lijken.
  - Check de URL van een link door er met je muis op te gaan staan (niet klikken natuurlijk!).
  - Let op vreemde spelling of tekens in de URL.
- Per ongeluk geklikt? Volg deze stappen:
  - Verander je wachtwoorden. Doe dit via een ander apparaat.
  - Doe een virusscan, en verwijder eventueel zelf het virus.



Hulpvraag-fraude

Criminelen doen zich vaak voor als een vriend, familielid of een andere bekende. Ze vertellen je dat ze een dringend probleem hebben en vragen vervolgens om geld. De criminelen proberen je onder druk te zetten, en vragen je op een link te klikken.

Stuurt iemand je een bericht of word je opgebeld en vertrouw je het niet?

> Hoi Pap!
>
> Mijn telefoon is kapot, dit is mijn nieuwe nummer. Zou je wat geld over kunnen maken?

- Bedenk of het bericht lijkt op hoe de afzender normaal ook communiceert.
- Bel de bekende of stuur ze een bericht op het nummer dat jij zelf hebt opgeslagen in je contacten. Dus niet het nieuwe, onbekende nummer.
- Check of diegene jou om geld gevraagd heeft voor een probleem.
- Was diegene het niet? Bel je bank en leg de situatie uit.

Helpdesk-fraude

Criminelen doen alsof ze helpdeskmedewerkers zijn van grote, bekende bedrijven of organisaties, zoals een verzekeringsmaatschappij of een bank. Ze bellen of mailen en vragen je om je persoonlijke gegevens te controleren of in te vullen via een link of app. Ze kunnen je gegevens gebruiken om in te loggen op je accounts of om geld te stelen. In andere gevallen vragen ze je om geld over te maken, bijvoorbeeld naar een 'veilige' rekening. Dit vraagt een bank nooit aan je.

- Als je twijfelt over een telefoontje, hang dan op. Negeer mails die je niet vertrouwt. Organisaties vragen nooit zomaar om je persoonlijke informatie of bankgegevens.
- Bel de organisatie via het bekende nummer als je twijfelt over een telefoontje of mail. Check of het klopt. Zo niet, blokkeer de afzender.

> We bellen u omdat we vreemde activiteiten op uw rekening zien.
>
> We willen uw geld overmaken naar een veilige kluisrekening.

Doe aangifte bij de politie en maak een melding bij de Fraudehelpdesk.