



Safeonweb^{.be}

ONLINE OPLICHTING:
HOE HERKENNEN,
VOORKOMEN EN REAGEREN



Voor meer info en andere vormen
van oplichting bezoek safeonweb.be



CENTRE FOR
CYBERSECURITY
BELGIUM

.be

Phishing



Phishing is een vorm van online oplichting waarbij gebruik wordt gemaakt van valse e-mails, websites, sms-berichten, QR-codes etc. met als doel je persoonlijke gegevens te verzamelen.

- Denk na vooraleer je klikt. Aanbiedingen kunnen misleidend zijn.
- Geef nooit wachtwoorden, bankkaartcodes of responscodes van een digipass via e-mail, telefoon, sms of sociale media.
- Controleer het adres van de afzender en de URL van de links die je ontvangt.
- Leer hoe je verdachte berichten kunt herkennen op surfenzonderzorgen. safeonweb.be.



Beleggingsfraude

Je wordt per telefoon of e-mail (of via het gehackte account van een vriend) gecontacteerd door een zogenaamd investeringsbedrijf dat voorstelt om aandelen of andere financiële producten te kopen. Het kan ook een nepadvertentie zijn waarin een beroemdheid deze investeringen aanprijst.

- Wees op je hoede voor ongevroegde financiële voorstellen en sta hier kritisch tegenover.
- Controleer de identiteit van de dienstverlener : naam, hoofdzetel, contactgegevens.



PC-probleem (Tech Scam)

- Pas op voor telefoontjes van bedrijven die je vragen om een aantal acties uit te voeren op je computer.
- Als er een pop-up verschijnt die aangeeft dat je computer geblokkeerd is, neem dan geen contact op met het getoonde nummer. Voer een antivirusscan uit.
- Installeer nooit applicaties of software die worden aangeboden door een zogezegde helpdesk want die kan de controle over je apparaat overnemen.

Ik ben Marc van de Microsoft-helpdesk. Je computer heeft een beveiligingsprobleem. Ik ga de controle over je computer overnemen om je te helpen.

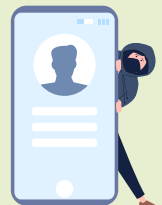


Identiteitsdiefstal/gehackt account

«Er gebeuren vreemde dingen op mijn account: ik zou berichten naar mijn vrienden hebben gestuurd zonder dat ik het wist, er verschijnen berichten en foto's op mijn pagina ook al heb ik niets gepubliceerd.»

Je account is waarschijnlijk het doelwit van een hacker die zich toegang kon verschaffen.

- Heb je nog toegang tot je account? Wijzig dan onmiddellijk het wachtwoord van dit account en al je andere accounts en stel je contactpersonen op de hoogte.
- Heb je geen toegang meer tot je account? Gebruik de herstelopties ("wachtwoord vergeten") om weer toegang te krijgen en verander vervolgens al je wachtwoorden.
- Schakel tweestapsverificatie in. Als eerste stap log je in op je account met je wachtwoord. Als tweede stap stuurt je account een code naar je mobiele telefoon, die je invoert om toegang te krijgen tot je account.
- Gebruik voor elk account een ander (sterk) wachtwoord en sla je wachtwoorden op in een wachtwoordkluis. Dit is een online kluis waar je je wachtwoorden per account kan opslaan. De kluis is zelf ook met een wachtwoord beveiligd.



Oplichting via verkoopsites



Oplichting van kopers of verkopers op verkoopsites. Dit kunnen nepverkopers, -kopers of -websites zijn.



- Pas op voor te snelle reacties en aanbiedingen die hoger zijn dan de vraagprijs. Controleer het profiel van de koper/verkoper.
- Voer je gesprekken met kopers/verkopers altijd op de verkoopsite en niet via sms of WhatsApp bijvoorbeeld.
- Betaal nooit via een link die je is toegestuurd door een koper of verkoper. Deze links brengen je naar een valse website waar oplichters om je bankgegevens vragen.
- Voer nooit je persoonlijke gegevens in op de site van een transportbedrijf via een link van de koper/verkoper.

Hallo, is dit item nog beschikbaar? Ik bied €500 voor je tafel. Ik kan ze niet komen ophalen, dus een DPD-chauffeur komt ze ophalen. Ik betaal je via overschrijving.

Bericht dat zogezegd van de politie afkomstig is



Oplichting via e-mail gebaseerd op de urgentie en ernst van de vermeende overtredingen.

- Reageer nooit op dit soort berichten en ga niet in op verzoeken om geld.
- Blokkeer de afzender.
- Neem contact op met de afzender via contactgegevens die je zelf hebt opgezocht.

Mijn checklist voor onlineveiligheid

- ✓ Ik geef nooit **wachtwoorden**, **bankkaartcodes** of **antwoordcodes** via e-mail, telefoon, sms of sociale media.
- ✓ Ik bescherm mijn mailbox en socialmedia-accounts met een **tweestapsverificatie**.
- ✓ Ik installeer **updates** zodra ze beschikbaar zijn.
- ✓ Ik installeer een **antivirus** op mijn computer, als ik er nog geen heb.
- ✓ Ik maak een **back-up** van mijn bestanden in de cloud of op een externe harde schijf.

Te laat, je bent slachtoffer geworden. Wat kan je doen?

Heb je je bankgegevens doorgegeven, frauduleuze geldopnames van je rekening opgemerkt of geld overgemaakt naar een oplichter?

- **Neem contact op met Card Stop** op 078 170 170 om de toegang tot je rekeningen te blokkeren.
- **Neem contact op met je bank.** Hoe sneller je je bank op de hoogte stelt, hoe groter de kans dat je het geld terugkrijgt.
- **Dien een klacht** in bij de lokale politie. Zorg dat je zoveel mogelijk informatie hebt: rekeningafschriften, screenshots van het frauduleuze bericht of de frauduleuze website, het profiel van de verdachte en de gesprekken ermee, de geïnstalleerde applicatie etc.

TOOLS OM JEZELF TE BESCHERMEN

HEB JE EEN VERDACHTE E-MAIL OF EEN VERDACHT BERICHT ONTVANGEN?

Stuur het naar verdacht@safeonweb.be en verwijder het vervolgens. Verdachte bijlagen en links worden automatisch geanalyseerd. Als een minder oplettende internetgebruiker op deze link klikt, krijgt hij een duidelijke waarschuwing om deze pagina niet te bezoeken.

INSTALLEER DE SAFEONWEB BROWSER EXTENSIE

De Safeonweb browser extensie waarschuwt je wanneer je een onbeveiligde website bezoekt en meldt dat het gevaarlijk is om je gegevens in te voeren. Een kleurcode (zichtbaar in de werkbalk) vertelt je of de website betrouwbaar is of niet. Lees op safeonweb.be hoe je deze extensie installeert.

BEKIJK ONZE E-LEARNINGREEKS “SURFEN ZONDER ZORGEN”

Leer hoe je oplichting en verdachte berichten kan herkennen via onze e-learningreeks op surfenzonderzorgen.safeonweb.be.

DOWNLOAD DE SAFEONWEB APP

De Safeonweb app informeert je over de bedreigingen waar het land momenteel mee te maken heeft en geeft advies over hoe je je online veiligheid kunt verbeteren.

De app is gratis verkrijgbaar voor iOS in de [App Store](https://www.apple.com/nl/app-store/) en voor Android in de [Google Play Store](https://play.google.com/store/apps/details?id=com.safeonweb).

MEER INFO?

- safeonweb.be/nl
- surfenzonderzorgen.safeonweb.be/nl/modules

Volg Safeonweb op

