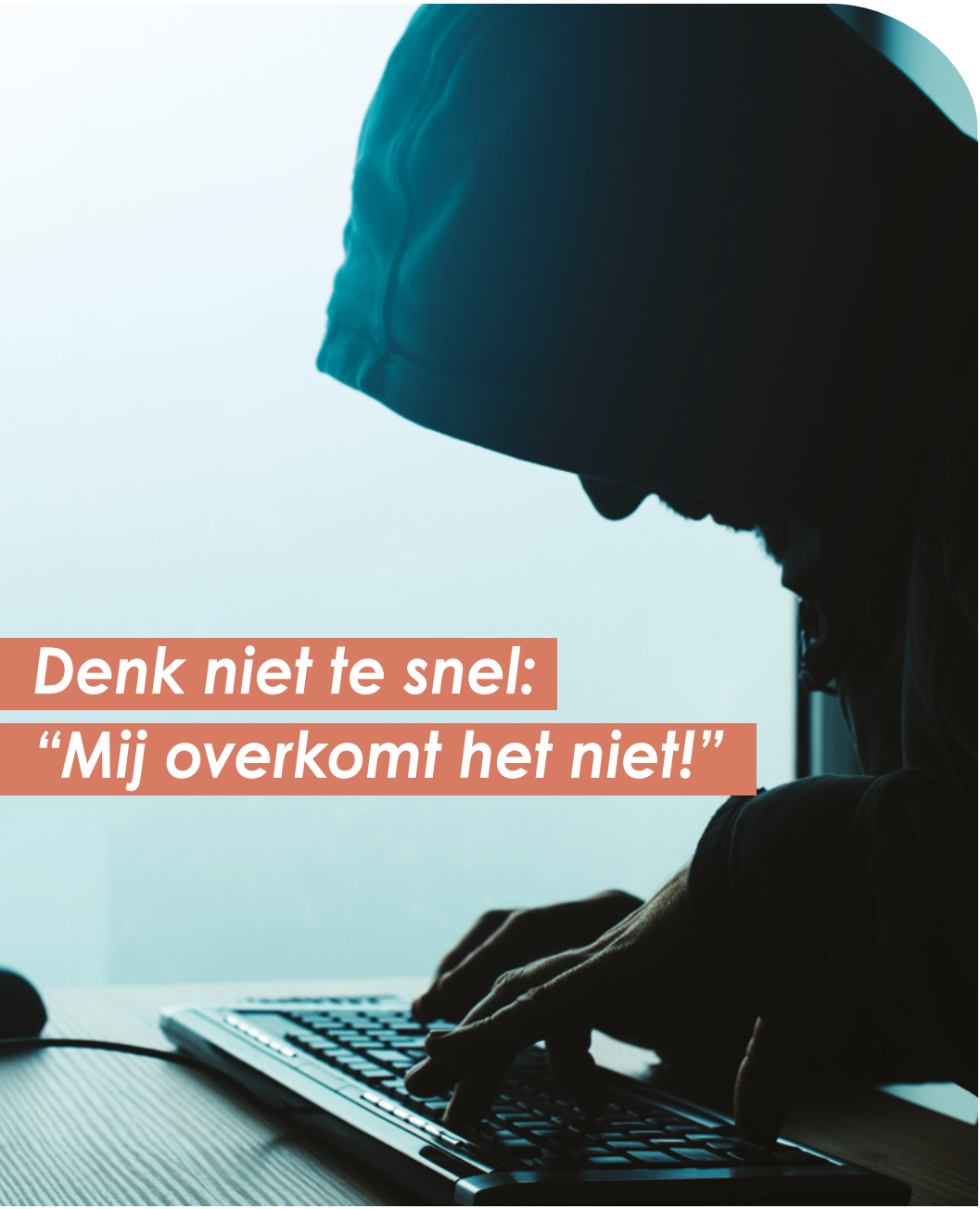
Politie
Gent

tips & tricks tegen online fraude



Denk niet te snel:
"Mij overkomt het niet!"

ZIJ SLIMMER?
WIJ SLIMMER!

Criminelen verleggen hun werkterrein steeds meer van andere misdrijven, zoals bv. inbraken, naar internetcriminaliteit. Minder risico en meer opbrengst maken online fraude aantrekkelijker.

De tijd van de kromme zinnen en vele taalfouten is voorbij. Bovendien veranderen ze heel snel van tactiek als een bepaalde werkwijze niet meer voldoende opbrengt.

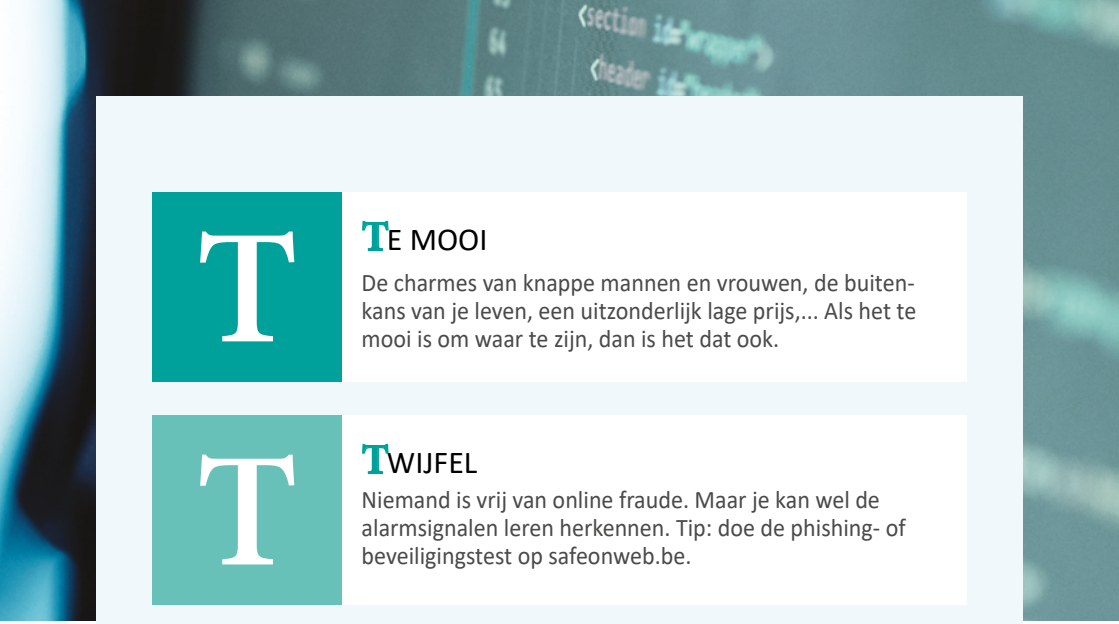
De oplichters worden slimmer en dus moeten wij dat ook zijn. Door de alarmsignalen te herkennen, op de hoogte te blijven en (tijd) te investeren in je online beveiliging.

Door de vele en snel veranderende vormen van online fraude is het onmogelijk om alles in deze folder op te sommen én altijd up-to-date te blijven.

Maar met deze 3 T's voorkom je al heel wat onheil: let op als iets Te mooi is, een gezonde portie Twijfel is van belang en Train goede gewoontes als je online aanwezig bent.

SAFEONWEB.BE

Voor alle nieuwigheden en uitgebreidere info is dit dé referentie. Safeonweb heeft ook een app die je waarschuwt voor nieuwe vormen van cyberdreigingen en online oplichting.



TE MOOI

De charmes van knappe mannen en vrouwen, de buitenkans van je leven, een uitzonderlijk lage prijs,... Als het te mooi is om waar te zijn, dan is het dat ook.

TWIJFEL

Niemand is vrij van online fraude. Maar je kan wel de alarmsignalen leren herkennen. Tip: doe de phishing- of beveiligingstest op safeonweb.be.

TRAINING

Leer jezelf goede gewoontes aan. Blijf op de hoogte van de laatste fraudetrucs (bv. via safeonweb of de politie). Informeer je, neem je tijd en zorg voor de juiste beveiliging.

TO DO: DE 4DE T!

KREEG JE TOCH MET ONLINE FRAUDE TE MAKEN?

Als je geen geld kwijt bent, is aangifte bij de politie niet nodig. Meld het wel via **verdacht@safeonweb.be**. Daar worden pogingen verzameld en onderzocht. Zo kunnen ze dergelijke websites trachten te blokkeren.

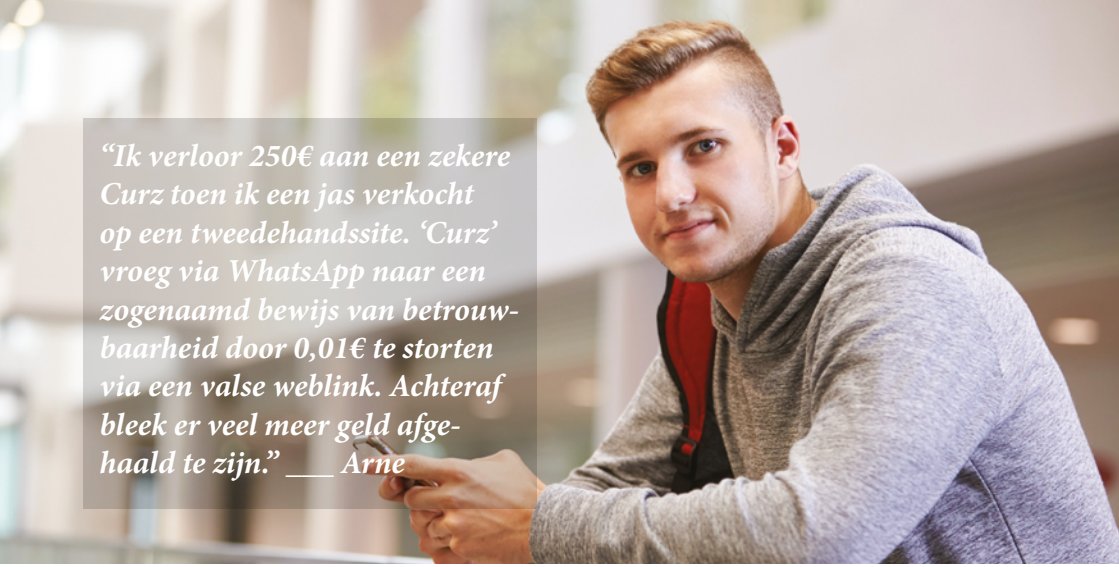
Vermoeden van oplichting of misbruik van je bankapplicatie?

De meeste banken zijn 24/7 bereikbaar via speciale fraudenummers.

Raadpleeg de website van je bank.

Geld kwijt? Reageer snel!

* Bel naar **Cardstop op 078 170 170 én je bank** om de toegang tot je rekeningen te blokkeren. Hoe sneller je dit doet, hoe groter de kans dat je geld kan recupereren.
* Doe aangifte bij de **politie**. Breng alle nuttige bewijzen mee: bankgegevens, berichten, e-mails,...



"Ik verloor 250€ aan een zekere Curz toen ik een jas verkocht op een tweedehandssite. 'Curz' vroeg via WhatsApp naar een zogenaamd bewijs van betrouwbaarheid door 0,01€ te storten via een valse weblink. Achteraf bleek er veel meer geld afgehaald te zijn." ___ Arne

1 AANKOOP FRAUDE

Hoe?

Zoekertjessites, sociale media, e-mail, chatapps (bv. WhatsApp, Messenger), datingapps,...

Wat?

* Je betaalt, maar ontvangt niets.
* Je verkoopt, maar wordt niet vergoed.
* De betaling loopt via een transportbedrijf.
* Er wordt gevraagd naar een voorschot (bv. via Western Union).

TE MOOI

Wees op je hoede voor snelle reacties en aanbiedingen die hoger zijn dan je vraagprijs.

Pas ook op als er gevraagd wordt naar een voorschot om de verkoop te bevestigen.

TWIJFEL

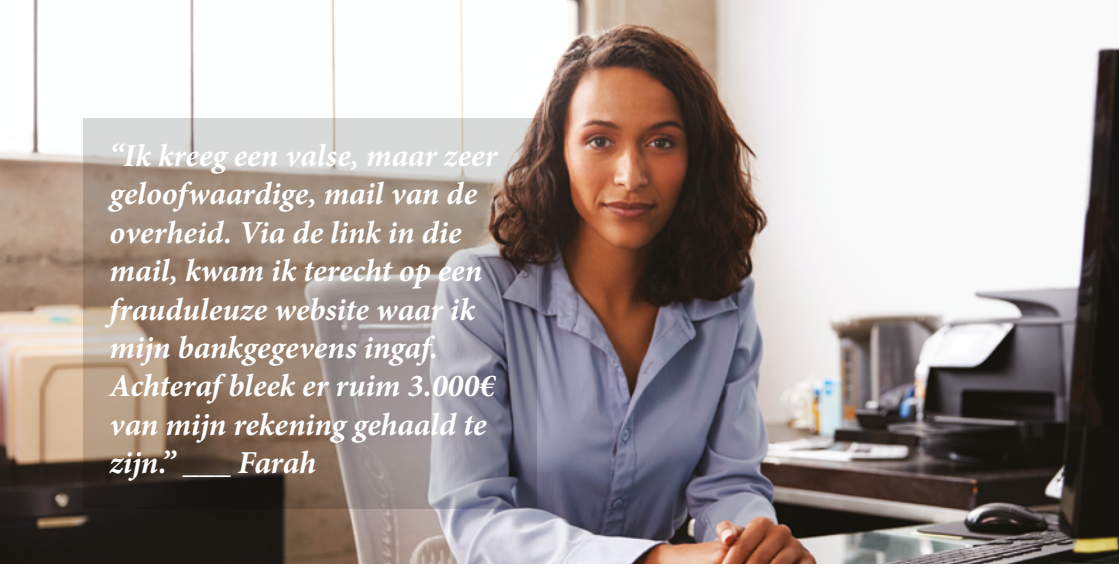
Voer je gesprek met de (ver)koper altijd op de verkoopssite en niet via bv. sms of WhatsApp.

Wees waakzaam als er gevraagd wordt om te betalen via een pakjes- of transportbedrijf.

TRAINING

* Vraag het rekeningnummer van de verkoper en betaal cash of via je eigen bank.
* Betaal nooit via een link die een (ver)koper je doorstuurt. Die links brengen je naar een valse website waar oplichters je bankgegevens ophalen.

MEER INFO OP **WWW.SAFEONWEB.BE**



"Ik kreeg een valse, maar zeer geloofwaardige, mail van de overheid. Via de link in die mail, kwam ik terecht op een frauduleuze website waar ik mijn bankgegevens ingaf. Achteraf bleek er ruim 3.000€ van mijn rekening gehaald te zijn." ___ Farah

2 LINKE LINKEN

Hoe?

E-mail, sms, chatapps (bv. WhatsApp, Messenger), sociale media,...

Wat?

Via valse weblinks of profielen ontfutselen fraudeurs informatie om geld af te troggelen, je account over te nemen of een virus te installeren (persoonlijke gegevens, logins en wachtwoorden, bankgegevens en codes,...). Vaak trachten ze je in naam van betrouwbare instanties - zoals overheid, bank, post, politie,... - in de val te lokken.

TE MOOI

Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen naar persoonlijke gegevens.

Fraudeurs sturen ook phishingberichten naar mogelijke slachtoffers die ze selecteren via valse win- of weggeefacties op sociale media.

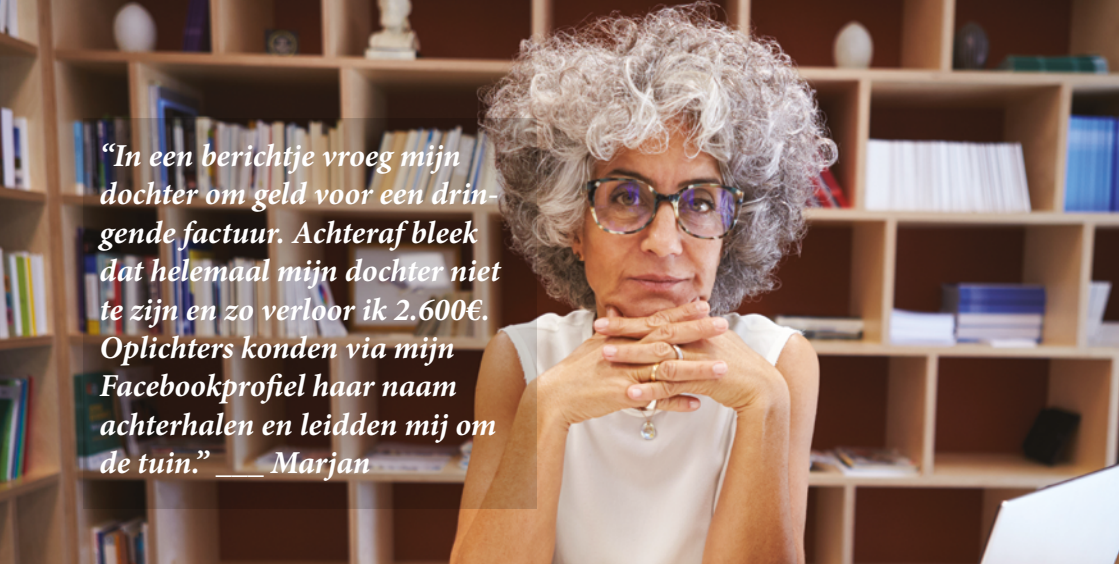
TWIJFEL

Taalfouten, een vreemd web- of mailadres, ze zetten je onder druk ("Doe het snel of..."),... allemaal signalen die alarmbelletjes zouden moeten doen afgaan.

TRAINING

* Wees zuinig met je mailadres.
* Volg geen link, maar tik zelf de website in van de bank of instelling.
* Check bij de instantie of het bericht klopt.
* Google een stukje tekst uit het bericht. Je bent zelden de enige die deze ontving.

DOE DE PHISHINGTEST OP **WWW.SAFEONWEB.BE**



"In een berichtje vroeg mijn dochter om geld voor een dringende factuur. Achteraf bleek dat helemaal mijn dochter niet te zijn en zo verloor ik 2.600€. Oplichters konden via mijn Facebookprofiel haar naam achterhalen en leidden mij om de tuin." ___ Marjan

3 EMO FRAUDE

Hoe?

Zoekertjessites, sociale media, e-mail, chatapps (bv. WhatsApp, Messenger), datingapps,...

Wat?

Oplichters proberen je vertrouwen te winnen door gewiekst in te spelen op je emoties. Ze vragen geld om naar België te kunnen reizen, je te ontmoeten, voor de achterblijvende familie te zorgen, ziekenhuiskosten van het dochtertje te betalen, een erfenis vrij te krijgen, schoolgeld te betalen,...

TE MOOI

Zoon- of dochterlief heeft dringend geld nodig? Een onverwachte erfenis die je kan verzilveren? Een knappe dame of heer die je vanuit het niets avances maakt?

Als het te mooi is om waar te zijn, dan is het dat ook.

TWIJFEL

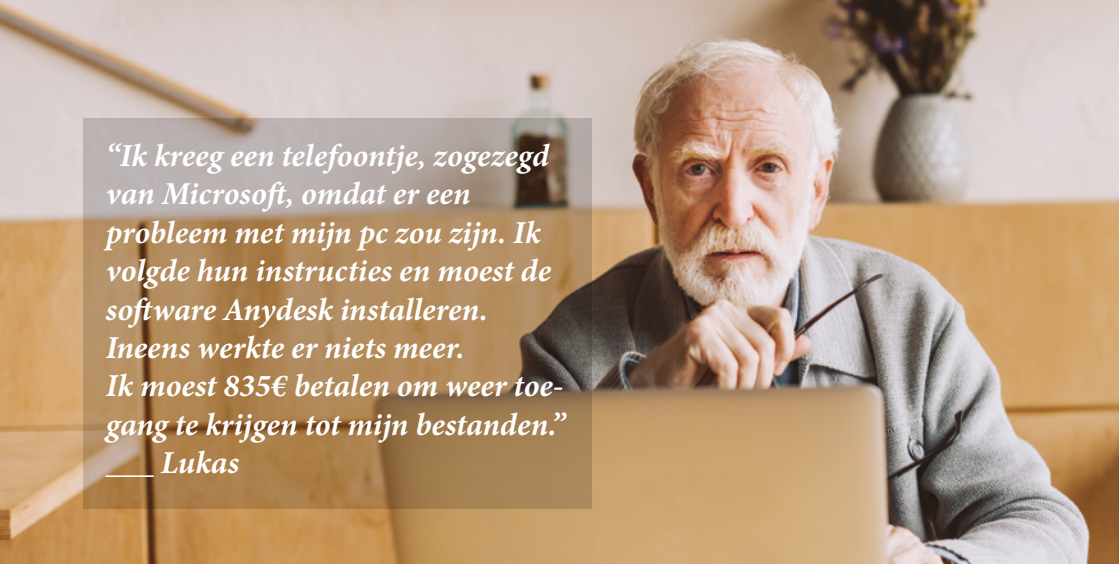
Is de dierbare aan de andere kant wel degene die je denkt?

Wees op je hoede als een onbekende je online benadert, zeker met 'zielige' verhalen.

TRAINING

* Ga de echtheid van het profiel altijd na.
* Scherm je persoonlijke gegevens zoveel mogelijk af.
* Betaal nooit! Ook al gaan er emoties mee gepaard of word je onder druk gezet.

MEER INFO OP **WWW.SAFEONWEB.BE**



"Ik kreeg een telefoontje, zogezegd van Microsoft, omdat er een probleem met mijn pc zou zijn. Ik volgde hun instructies en moest de software Anydesk installeren. Ineens werkte er niets meer. Ik moest 835€ betalen om weer toegang te krijgen tot mijn bestanden."
___ Lukas

4 TECH SCAM

Hoe?

Telefoon, gijzelvirus, hacking,...

Wat?

Met gegevens die ze online vinden, trachten oplichters in te breken in je computer. Ze installeren een virus, vergrendelen je bestanden of hacken je account.
Of je wordt opgebeld door een zogezegde medewerker van de helpdesk van een computerfirma die je laat geloven dat je een veiligheidsprobleem hebt en toegang vraagt tot je computer. Pas als je betaalt, krijg je zelf weer de controle over je toestel.

TE MOOI

Microsoft, Apple of andere computerbedrijven zullen je niet ongevraagd contacteren om je te helpen met een probleem.

Wees voorzichtig met 'interessante' maar valse e-mails die vissen naar je gegevens.

TWIJFEL

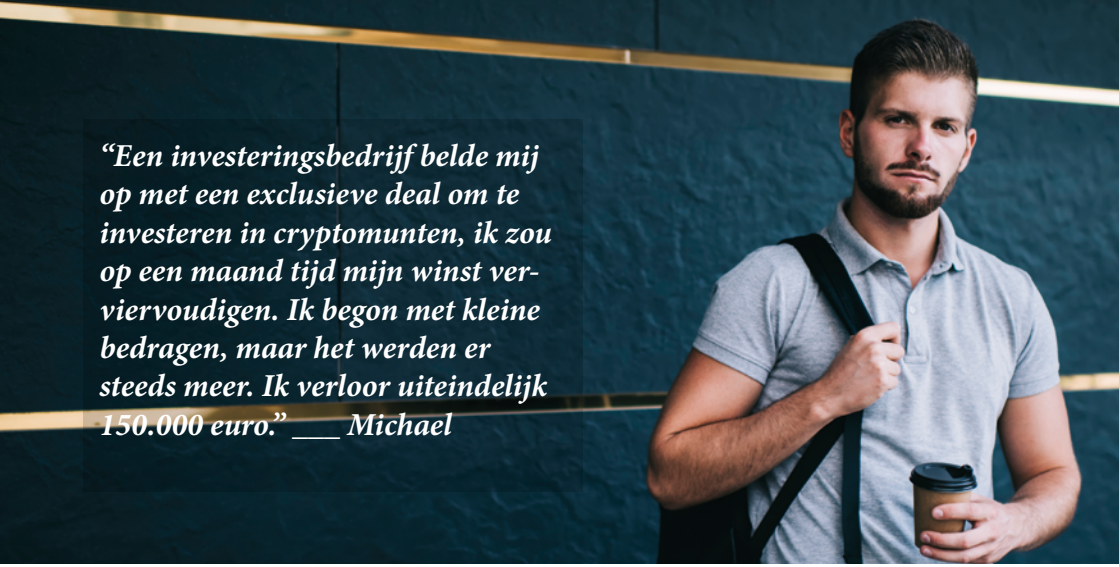
Wantrouw altijd telefoons van bedrijven die je vragen om een aantal acties uit te voeren op je computer.

Soms vragen ze om software te installeren, zoals bv. Anydesk. Hiermee kunnen ze je pc vanop afstand overnemen.

TRAINING

* Installeer een goede virusscanner.
* Gebruik sterke wachtwoorden.
* Gebruik verificatie in 2 stappen (2FA).
* Doe regelmatig updates.
* Back-up je bestanden regelmatig.

DOE DE WACHTWOORDTEST OP **WWW.SAFEONWEB.BE**



"Een investeringsbedrijf belde mij op met een exclusieve deal om te investeren in cryptomunten, ik zou op een maand tijd mijn winst verviervoudigen. Ik begon met kleine bedragen, maar het werden er steeds meer. Ik verloor uiteindelijk 150.000 euro." ___ Michael

5 BELEGGINGS FRAUDE

Hoe?

Sociale media, valse advertenties, e-mail, chatapps (bv. WhatsApp, Messenger), sms, telefoon,...

Wat?

Beleggingsfraude is een vorm van oplichting waarbij criminelen je proberen te overtuigen om geld te investeren in onbestaande of valse financiële producten (crypto, forex,...). Ze beloven vaak hoge rendementen met weinig risico, maar in werkelijkheid is het een valstrik om je geld te stelen.

TE MOOI

Er worden hoge winsten beloofd, zogezegd zonder risico.

Je wordt onder druk gezet om snel te beslissen (Een eenmalig aanbod! Een exclusieve deal!).

Soms prijzen beroemdheden nepadvertenties aan.

TWIJFEL

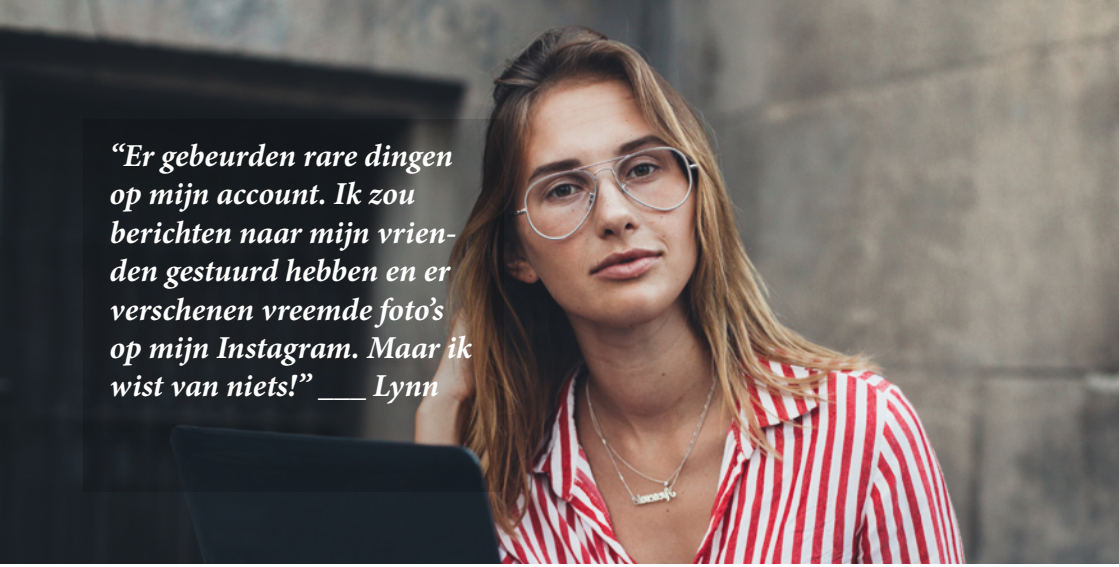
Begin te twijfelen als je ongevraagd benaderd wordt met een voorstel.

Ook als er vreemde betalingsverzoeken volgen, zoals geld overmaken naar een buitenlandse rekening of ongebruikelijke betaalmethoden.

TRAINING

* Controleer de aanbieder. Hoe? Surf naar safeonweb.be.
* Beleg niet in een financieel product als je niet begrijpt wat het precies inhoudt.
* Neem tijd om het aanbod te onderzoeken, laat je niet onder druk zetten.

DOE DE FRAUDETEST OP **WWW.SAFEONWEB.BE**



"Er gebeurden rare dingen op mijn account. Ik zou berichten naar mijn vrienden gestuurd hebben en er verschenen vreemde foto's op mijn Instagram. Maar ik wist van niets!" ___ Lynn

6 IDENTITEITS DIEFSTAL

Hoe?

E-mail, valse websites, sociale media, hacking,...

Wat?

Oplichters maken een nepaccount aan op sociale media of via e-mail. Ze gebruiken daarvoor soms de identiteit van anderen om vrienden of volgers te misleiden, aankopen te doen op het internet, valse advertenties te plaatsen, bankrekeningen te openen of kredietkaarten aan te vragen,...

TE MOOI

Verwacht je een mail of bericht en past de inhoud bij hoe je vriend normaal schrijft? Zit er een vreemde bijlage of een link bij waar je niet om vroeg?

Of een nog grotere waarschuwingsvlag: vraagt de 'vriend' om geld, codes of wachtwoorden?

TWIJFEL

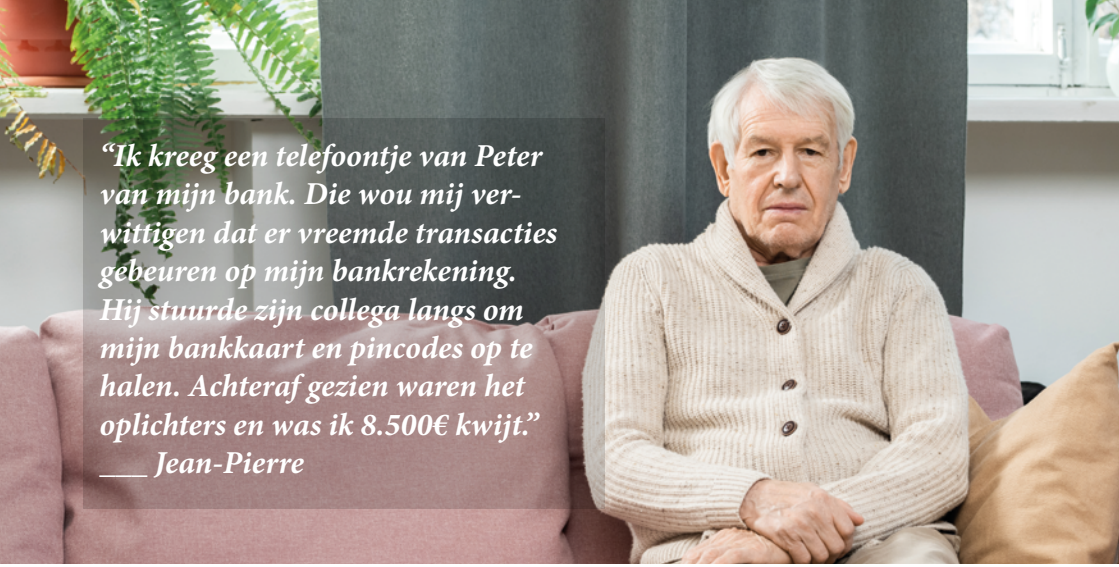
Twijfel als je je vriend niet herkent in het bericht of een bijlage.

Het nepaccount op bv. Facebook heeft weinig of geen gepubliceerde inhoud, gebruikt generieke of gekopieerde foto's, of stuurt ongebruikelijke verzoeken (bv. geld).

TRAINING

* Niet klikken, niet downloaden, niet antwoorden.
* Contacteer je vriend via een betrouwbaar kanaal.
* Verander je wachtwoorden als je per ongeluk toch op een link klikte en inloggegevens invoerde.

DOE DE WACHTWOORDTEST OP **WWW.SAFEONWEB.BE**



"Ik kreeg een telefoontje van Peter van mijn bank. Die wou mij verwittigen dat er vreemde transacties gebeuren op mijn bankrekening. Hij stuurde zijn collega langs om mijn bankkaart en pincodes op te halen. Achteraf gezien waren het oplichters en was ik 8.500€ kwijt."
___ Jean-Pierre

7

BANKKAART VISSEN

Hoe?

Meestal via de telefoon. Uitzonderlijk komen ze bij je thuis langs om je te 'helpen' om de problemen te stoppen.

Wat?

Oplichters doen zich voor als medewerkers van je bank of officiële instanties, zoals Card Stop of een ziekenfonds. Ze bellen om te waarschuwen dat er een probleem zou zijn met je bankrekening of bankkaart. Ze vissen naar je pincode, vragen om in te loggen of geld over te schrijven naar een zogezegde veilige rekening.

TE MOOI

De oplichters winnen je vertrouwen door jouw persoonlijke info te gebruiken die ze bv. verkregen via een datalek.

Ze dringen er vaak op aan om snel te handelen, om je geld veilig te stellen, zodat je geen tijd krijgt om te twijfelen.

TWIJFEL

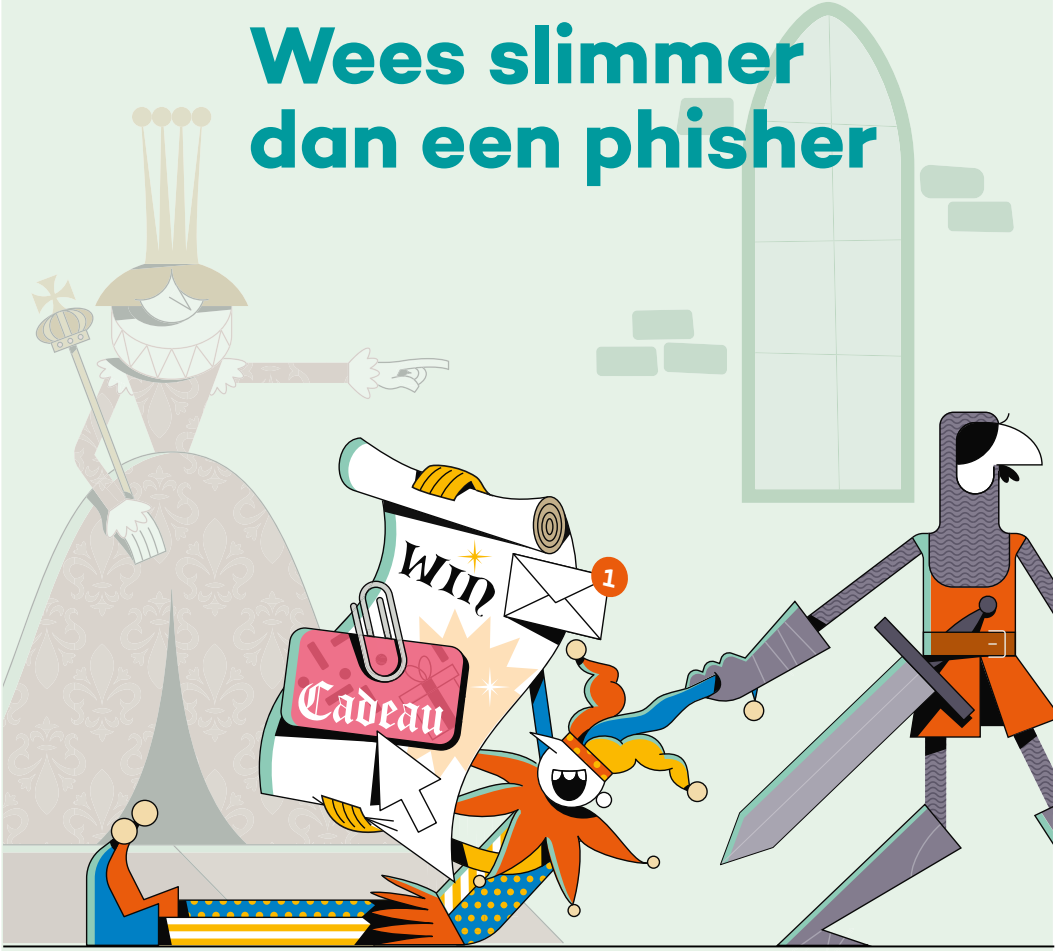
Ze proberen je urenlang aan de telefoon te houden, zodat je de kans niet krijgt om stil te staan bij wat er gebeurt.

Soms vragen ze om software te installeren, zoals Anydesk. Hiermee kunnen ze je pc vanop afstand overnemen.

TRAINING

* Geef nooit persoonlijke codes of gegevens aan vreemden. Haak in bij dergelijke telefoontjes.
* Laat geen vreemden binnen om bepaalde betaalproblemen op te lossen of je bankgegevens op te halen.

Wees slimmer dan een phisher



Altijd actuele info op zak: download de Safeonweb app

Download in de App Store

Google Play

DEEL NOOIT JE PERSOONLIJKE GEGEVENS OF CODES.
STUUR VERDACHTE BERICHTEN DOOR NAAR
VERDACHT@SAFEONWEB.BE

MEER INFO OP WWW.SAFEONWEB.BE

CENTRE FOR CYBER SECURITY BELGIUM

febelfin

CYBER SECURITY COALITION

Safeonweb.be

.be

KLACHT OF AANGIFTE?

Dringend? BEL 101

MAAK EEN

AFSPRAAK

www.politiegent.be

of bel 09 266 61 11

VU: PZ Gent, Antonius Triestlaan 12, 9000 Gent - © PZ Gent - 2025

POLITIEZONE GENT
www.politiegent.be

Politie
Gent