



Online fraude

Denk niet te snel:
“Mij overkomt het niet!”

- tips en advies
- hoe voorkomen?



ZIJ SLIMMER? WIJ SLIMMER!



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

De tijd van de kromme zinnen en taalfouten is voorbij. Bovendien veranderen de criminelen heel snel van werkwijze als een vorige niet meer genoeg 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 drie T's voorkom je al heel wat onheil: let op als iets Te mooi is, een gezonde portie Twijfel is van belang en Train je goed gewoontes als je online aanwezig bent.

Voor uitgebreide en actuele info en tips:



Safeonweb.be
Digitale Gezondheidsindex



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 meestal 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](http://safeonweb.be) of de politie). Informeer je, neem je tijd en zorg voor de juiste beveiliging.

TO DO: DE VIERDE T!

Kreeg je toch met online fraude te maken?

Geen geld kwijt?

- Aangifte bij de politie is niet nodig.
- Meld het valse bericht aan verdacht@safeonweb.be. Daar worden ze centraal verzameld en onderzocht. En zo kunnen ze dergelijke websites trachten te blokkeren.



Toch geld kwijt?

- Heb je betalingsgegevens doorgegeven, verwittig dan onmiddellijk Cardstop op 078 170 170.
- Contacteer je bank zodat de laatste betaling of frauduleuze rekening eventueel geblokkeerd kan worden. Doe dit snel, binnen de 24 uur!
- Doe aangifte bij de politie. Breng alle nuttige bewijzen mee: zoekertjes, berichten, mails, screenshots, toestel, ...

“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, chatbox, datingapplicatie, ...

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).
- Fraude met cryptomunten.
- Beleggingsfraude.

TE MOOI

Heel goedkoop, een niet te missen buitenkans, 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

Begin te twijfelen als de werkwijze vreemd aanvoelt (bv. regeling buiten de zoekertjessite om). Ook als je gesprekspartner een andere taal spreekt of een buitenlands rekeningnummer doorgeeft, is dit verdacht.

TRAINING

- Zorg ervoor dat je zicht hebt op de identiteit van je gesprekspartner: naam, gsm, mailadres, rekeningnummer, ...
- Verzamel nuttige documentatie: zoekertje, berichten, mailverkeer, screenshots, ...

“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?

Weblinks, mail (phishing), sms (smishing), whatsapp, sociale media, ...

Wat?

Via valse weblinks of profielen ontfoetselen fraudeurs informatie om zo 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 weggeef-acties 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 dit ontving.

“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, chatbox, datingapplicatie, ...

Wat?

Oplichters proberen je vertrouwen te winnen door gewiekst in te spelen op je emoties. Ze vragen om 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 (risico op identiteitsfraude).
- Betaal nooit! Ook al gaan er emoties mee gepaard of word je onder druk gezet.

“Ik kreeg een telefoontje van een helpdesk omdat er een probleem met mijn pc zou zijn. Ik volgde hun instructies en moest bepaalde software installeren. Ineens werkte er niets meer. Ik moest €835 betalen om weer toegang te krijgen tot mijn bestanden”. ____ Lukas



4

ONLINE SABOTAGE

Hoe?

Hacking, gijzelvirus, helpdeskfraude, ...

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 in handen.

TE MOOI

Microsoft, Apple of andere computer-bedrijven zullen je niet ongevraagd contacteren om een probleem te melden.

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.

TRAINING

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

Klacht of aangifte?

Maak een afspraak



www.politie.sint-niklaas.be



of bel:

03 760 65 00

de Sint-Niklase
Blauwe Lijn

Meer info?

www.safeonweb.be

Voor alle actuele nieuwigheden en uitgebreidere info is dit dé referentie. Je kan er ook terecht voor praktische tips en tests waarmee je je online fraudekennis kan meten.



Safeonweb.be

Digitale Gezondheidsindex



Politie

Politiehuis
Dalstraat 26
9100 Sint-Niklaas
www.politiesint-niklaas.be

Voor alle niet-dringende vragen:

03 760 65 00

de Sint-Niklase
Blauwe Lijn

