T E 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.

T WIJFEL

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

T RAINING

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?

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 070 344 344.**
* 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,...

Stadionlaan 22/A, 9800 Deinze
PZ.DeinzeZulteLievegem@police.belgium.eu
www.politiedeinzezultelievegem.be
twitter.com/PolitiezoneDZL
facebook.com/PZDeinzeZulteLievegem
instagram.com/politiedeinzezultelievegem

Politie
Deinze-Zulte-Lievegem

Politie
Deinze-Zulte-Lievegem

Tips & tricks tegen internetcriminaliteit

ONLINE FRAUDE VERMIJDEN? DOE DE T-CHECK!

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

	1 AANKOOP FRAUDE	2 LINKE LINKEN	3 EMO FRAUDE	4 ONLINE SABOTAGE
HOE?	Zoekertjessites, sociale media, e-mail, chat-box, datingapplicatie,...	Weblinks, mail (phishing), sms (smishing), whatsapp, sociale media,...	Zoekertjessites, sociale media, e-mail, chat-box, datingapplicatie,...	Hacking, gijzelvirus, helpdeskfraude,...
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.	Via valse weblinks of profielen ontfutselen 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.	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,...	Met gegevens die ze online vinden, trachten oplichters in te breken in je computer. 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	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.	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.	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.	Microsoft, Apple of andere computerbedrijven zullen je niet ongevraagd contacteren om een probleem te melden. Wees voorzichtig met 'interessante' maar valse e-mails die vissen naar je gegevens.
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.	Taalfouten, een vreemd web- of mailadres, ze zetten je onder druk ("Doe het snel of..."),... allemaal signalen die alarmbellen zouden moeten doen afgaan.	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.	Wantrouw altijd telefoons van bedrijven die je vragen om een aantal acties uit te voeren op je computer.
TRAINING	* Zorg ervoor dat je zicht hebt op de identiteit van je gesprekspartner: naam, gsm, mailadres, rekeningnummer,... * Verzamel nuttige documentatie: zoekertje, berichten, mailverkeer, screenshots,...	* 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.	* 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.	* Installeer een goede virusscanner. * Gebruik sterke wachtwoorden. * Gebruik verificatie in 2 stappen (2FA). * Doe regelmatig updates. * Back-up je bestanden regelmatig.