

Cyberpreventie ADVISEURS



ALGEMENE KENNIS & CIJFERS • BELGIE

Meest voorkomende feiten

PHISHING



**AAN / VERKOOP
FRAUDE**



**BETAALVERZOEK
FRAUDE**



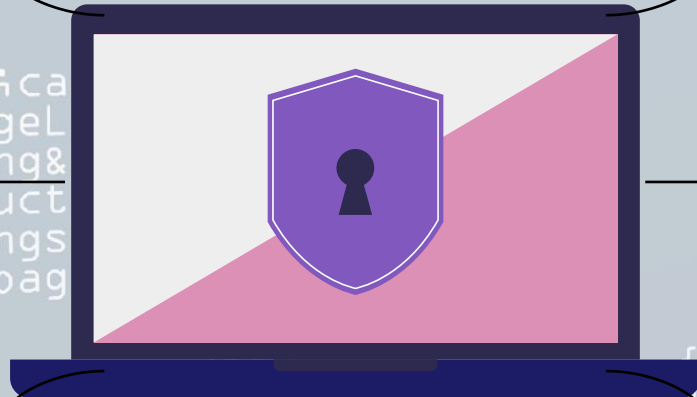
**VRIENDSCHAPS
FRAUDE**



**HELPDESK
FRAUDE**



**RANSOMWARE /
HACKING**



Wachtwoorden

1

Wachtwoordkluizen zijn een goed idee.

2

Gebruik wachtwoordzinnen.

3

2 stapverificatie een must.

4

Gebruik een wachtwoordboekje,

Check je email op [datalekken](https://datalekken.be).

5

Gebruik wachtwoordzinnen of cijferletters. Paswoord testen kan op www.passwordmonster.com

6



Wat is een URL?



Een link naar een website adres.
www.kortrijk.be



.be is een landencode.
.NL .FR .COM .EU
Kan ook .vlaanderen .business



Website adressen zijn proper.
www.argenta-dxl-spot.ng



Hoe check ik een link?



Een link in een website of email is een verwijzing naar een pagina op het internet.



Hover over de tekstlink om het adres te zien. **Testlink**
Op smartphone blijf drukken op de link.



Check verdachte linkjes op **www.scamadviser.com**



Wat is een protocol?



Is het eerste deel van de URL



HTTP versus HTTPS, met de S van security



Er is een beveiligde verbinding tussen jou en de site. **Maar de site zelf kan zo corrupt zijn als wat.**



Wat is een subdomein?



Een link naar een onderdeel van een website.
<https://financien.belgium.be>



Domeinnaam kiezen en gecheckt bij DNS.
Subdomein kan je zelf aanmaken.



www is een deel van het protocol.
Je kan het ook weglaten bij opzoeken.

Check het adres



Check voor je een email opent het afzenderadres.



Email van een firma en twijfel. Zoek het telefoonnummer op en bel de firma.



Denk kritisch na, boetes, politionele onderzoeken, belastingvoordeel via email?



TERMINOLOGIE



PHISHING



VERKOOPS
FRAUDE



VRIENDSCHAPS
FRAUDE



SMISHING



WHATS APP
FRAUDE



SPOOFING/
VISHING /
HELPDESK
FRAUDE

PHISHING

1

Bij phishing proberen criminelen je door e-mails naar een valse website te lokken.

Daar stelen ze jouw gegevens of geld. Klik nooit op links in een phishing e-mail.

2

De oproep is **steeds dringend**, meestal onpersoonlijk en onverwacht.

3

NIETS op het internet is zo dringend dat het niet even kan wachten.

Check de zeggende afzender via de URL of neem zelf contact op met de instantie.



(VER)KOOPSFRAUDE

1

Je betaalt voor iets dat je niet ontvangt of je levert iets maar krijgt er geen betaling voor. Jongeren en vrouwen zijn vaker het slachtoffer. Slechts 10% doet aangifte.

2

Vaak wordt een betaling geregeld via een fraudeleuze link. Het storten van 0,1 € gebeurt op een spiegelsite waarbij men dus je gegevens verkrijgt.

3

Betaling gebeuren het best face to face. Koop je zelf iets op het net. Vraag het rekeningnr en identiteitsgegevens en doe de betaling via je **eigen bankapp**. Vraag bij grotere sommen ook een identiteitsbewijs.



WHATSAPP FRAUDE

1

Via spoofing doet men zich voor als een bekende vriend. Steeds op dezelfde wijze worden mensen aangemaand om te betalen. GSM in het water gevallen, nieuwe meubels... toch lopen nog steeds mensen in de val

2

Vaak wordt een betaling geregeld via een fraudeleuze link. Betaal dus NOOIT via deze link.

3

Neem printscreens en lever die af bij de politie.
Verwijder de persoon en blokker hem op jouw telefoon.



VRIENDSCHAPSFRAUDE

1

Hierbij worden mensen opgelicht door iemand die ze online leren kennen. Slachtoffers geloven dat ze een vriendschap hebben opgebouwd met de oplichter, waardoor ze deze persoon uiteindelijk geld geven.

2

Er wordt vooral op de emoties van het slachtoffer gespeeld. Vaak heeft de **“vriend”** tijdelijke tegenslagen, of financiële problemen.

3

Maak NOOIT geld over. Google de naam even, vaak kom je gelijkaardige verhalen op het internet tegen. Geef ook zeker geen persoonlijke informatie door, deze kan tegen u worden gebruikt.



SMISHING

1

Smishing of sms-spam is een type phishing-aanval waarbij criminelen smsjes sturen om slachtoffers te verleiden hun persoonlijke informatie te delen of malware op hun apparaten te installeren.

2

Vaak gaat het hier over SMS die zogezegd van een overheidsdienst komen. Vaak gaat het ook over een **tegoed of een dringende vraag voor verificatie**.

3

De overheid, politie, belastingen... communiceren niet via SMS. De meeste overheidsdiensten werken nog steeds met papier of kiezen voor een online service zoals doccle.



SPOOFING / HELPDESKFRAUDE / VISHING



1

Het is een combinatie van 'voice' en 'phishing'. Oplichters **bellen je op** en vragen persoonlijke, financiële of veiligheidsinformatie, of ze vragen om geld over te maken.

2

De oproep is vaak in het Engels of gebrekkig Nederlands. Oproepen komen zogezegd van de helpdesk van je **bank of Microsoft**.

3

Let op het telefoonnummer kan gespoofd zijn.
Verbreek de verbinding. Laat u zeker niet dwingen handeling via de computer uit te voeren.

10 TIPS OM MEE TEGEVEN

WACHTWOORDEN

Complexe of wachtwoordzinnen.
Verander regelmatig



2 STAPSVERIFICATIE

Indien mogelijk
DOEN!



SOFTWARE / UPDATES

Kies off. software en
update die !



ANTIVIRUS

Installeer antivirus
op al jouw
apparaten.



WEES WANTROUWIG

Open geen berichten of
bestanden die je niet
vertrouwt of verwacht.



APPS

Installeer enkel
apps van off
applicatiewinkels



CHECK

Controleer het adres
van webpagina's



HELPDESK

Verbreek het contact
met ongevraagde
helpdeskmedewerkers.



PRIVACY

Privacyinstellingen
zo hoog mogelijk.



WIFI

Maak enkel contact met
betrouwbare wifi
netwerken, liefst niet
publieke.

HOE JE REKENING BLOKKEREN

1

Een betaalmiddel blokkeren via Card Stop gaat makkelijk en snel. Bel naar het nummer **+32 (0)78 170 170**. Neem ook contact op met 24/24 helpdesk van je bank om de apps te blokkeren zoals payconiq, apple pay...

2

Je kiest **de taal** waarin je het gesprek wil voeren. Een stemcomputer zal je vragen om je bankrekening of kaartnummer in te toetsen. Je wordt vervolgens doorverbonden met een van **onze Card Stop assistenten** die alle verdere stappen onderneemt om je betaalmiddelen te blokkeren.

3

Tot slot zal de stemcomputer je informatie geven over de vervanging van je betaalmiddel en zal je **de referentie** van dit gesprek krijgen. Noteer deze zorgvuldig. Deze kan je worden opgevraagd door je bank of de politie bij aangifte. **PAS OP : card stop blokkeert je kaart NIET jouw rekening.**



ONZE PARTNERS

