VIJF TIPS VOOR ONLINE VEILIGHEID.

JEZELF

Aanvallers richten zich liever op **jou**, in plaats van op jouw computer of andere apparaten.

Als ze je wachtwoord, creditcard of controle over jouw computer willen, zullen ze je proberen te **verleiden** om het aan hen te geven. Vaak door een gevoel van urgentie te creëren.

Uiteindelijk ben **jij** de grootste verdediging tegen aanvallers. Door gebruik te maken van **gezond verstand** kun je veel aanvallen herkennen en stoppen.

Vertrouw niet uitsluitend de technologie om je te beschermen,
jij bent jouw beste verdediging.

UPDATES & PATCHES

Bescherm jouw computer en mobiele toestellen door steeds de laatste updates te installeren.

Installeer alleen apps en updates uit de **erkende app-stores**.

Schakel **automatische updates** in waar mogelijk.

ANTIVIRUS

Kan niet alle malware stoppen, maar helpt om de meest voorkomende aanvallen te detecteren en stoppen.

Zorg ervoor dat jouw computers thuis **één antivirus** hebben en dat deze **up-to-date** en **actief** is. Een smartphone heeft in principe geen antivirus nodig.

RESERVEKOPIE

Back-ups zijn vaak de laatste oplossing om fouten te herstellen, zoals het per ongeluk verwijderen van bestanden of cyberaanvallen zoals ransomware.

Zorg ervoor dat familie en vrienden een **automatisch back-up**systeem hebben. Vaak zijn de eenvoudigste oplossingen deze in de **Cloud**.

WACHTWOORDBELEID

Sterke wachtwoorden zijn de sleutel tot het beschermen van toestellen en online accounts. **Wachtzinnen** zijn als wachtwoorden, maar zijn gebaseerd op een zin.

Twee-staps-verificatie, ook wel twee-factor-authentificatie genoemd, is één van de beste maatregelen die je kan nemen om een account te beveiligen.

Je hebt een **uniek** wachtwoord nodig voor elk account.

MEER WETEN?

Kijk ook eens op www.safeonweb.be

Lokale politie Damme/Knokke-Heist
Van Steenestraat 10, 8300 Knokke-Heist
050 619 619 of noodnummer 101
PZ.DKH.Safe@police.belgium.eu
www.politie.be/5446

JOUW POLITIE.

SAMEN VOOR EEN VEILIGER INTERNET.

CYBERCRIME

DAMME KNOKKE-HEIST

WAT IS HET?

Cybercrime of computercriminaliteit is een vorm van oplichting waarbij gebruik gemaakt wordt van computers, smartphones en/ of het internet. Ook een klassieke bankkaart is vatbaar voor misbruik als die gestolen wordt.
In veel gevallen wordt een IT-systeem gemanipuleerd om:

- Een onrechtmatig voordeel te bekomen,
- valse gegevens in te voeren,
- onrechtmatig toegang te krijgen,
- de normale werking van het systeem te wijzigen.

Leer hoe je de oplichting kan herkennen en voorkomen dat cybercriminelen aan de haal gaan met jouw zuurverdiende centen.

NIET-LEVERING VAN (GEDEELTELIJK) BETAALDE GOEDEREN

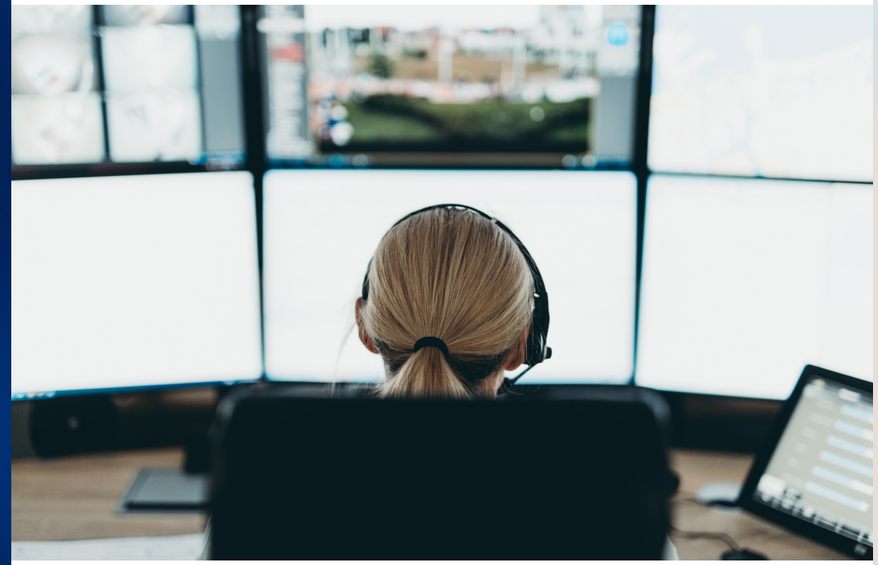
De oplichter doet zich voor als **verkoper** en biedt objecten te koop aan tegen een abnormaal lage prijs.

NIET-BETALING VAN GELEVERDE GOEDEREN

Je wordt bij het te koop aanbieden van een goed (bv. Autoscout, Immoweb, 2deHands, Facebook Market...) gecontacteerd door oplichters, die zich voor doen als **koper**. Er wordt zelden gediscussieerd over de prijs en men belooft het gevraagde bedrag te betalen. Vervolgens zijn er diverse mogelijkheden die de oplichter zal gebruiken:

- De oplichter stuurt een vals betalingsbewijs door en vraagt of je het goed al kan versturen.
- De oplichter betaalt met een valse of vervalste cheque van een buitenlandse bank.
- In veel gevallen word je via online aan- en verkopen naar een valse website geleid waar men zal pogen je persoonlijke (bank)gegevens te ontfutselen (= **phishing**).

HERKEN DE OPLICHTING.



WAT IS EEN PHISHINGBERICHT?

- Het bericht is **plots en onverwachts** toegestuurd.
- Het **afzendadres** van de e-mail kan er raar uitzien. Indien je twijfelt, contacteer de bank.
- De toon is **dringend en dwingend**.
- Let op **spelling- en grammaticale** fouten.
- **Controleer de link** in de e-mail door er met je cursor over te zweven, maar niet te klikken. Hierdoor zie je de URL waar je naartoe geleid wordt. Als deze niet naar de officiële website leidt, of een verkorte link is, is het hoogstwaarschijnlijk een phishingmail.
- De link in een phishingbericht leidt naar een website die eruitziet als de echte website (=**spoofing**).
- De spamfilter geeft aan dat het bericht **spam** is.

WAT KAN JE DOEN?

- Als het te mooi is om waar te zijn, **dan is het dat meestal ook!**
- Vermijd aan de oplichter **persoonlijke informatie** vrij te geven, zoals een kopie van identiteitsdocumenten of bankgegevens. De oplichter kan ze gebruiken voor het plegen van andere criminele feiten.
- Wanneer je goederen verkoopt, **controleer** steeds of het bedrag op je bankrekening staat voordat je het goed verzendt.
- Stel je vast dat een zoekertje vals is, **meld** dit op de website van de adverteerder.

HOE HERKEN JE...

VALSE FACTUREN

- Het rekeningnummer wijkt af van vorige betalingen.
- Het gaat om een buitenlands rekeningnummer.

EEN BETROUWBARE WEBSHOP

Een betrouwbare webshop bevat:

- de **ondubbelzinnige identiteit** van de verkoper,
- een **duidelijke prijs** voor de producten,
- informatie over waar je de spullen kan **terugsturen** en
- wie je kan **contacteren** bij problemen.

VALSE BOETES

- Het bericht is **dwingend** en er is geen vermelding van **nummerplaat**, noch gegevens van de eigenaar van de nummerplaat.
- De **exacte locatie** van de overtreding wordt niet aangegeven.
- E-mailadressen van de politie eindigen op **@police.belgium.eu**
- De politie vraagt nooit om te betalen met **alternatieve betaalmogelijkheden** zoals Bitcoins, 3G Payment, Ukash of andere pre-paid kaartensystemen.

Alles met betrekking tot boetes:
https://justonweb.be/fines of 02/278 55 60

VRIENDSCHAPSFRAUDE

- Zorg ervoor dat je weet met wie je te doen hebt. Ken je die persoon **in het echt**?
- Indien je een mail krijgt van een kennis of vriend in nood die vraagt om hem te helpen, antwoord niet en probeer de rechtmatige eigenaar via een andere weg te bereiken.

ONLINE BELEGGEN & CRYPTOMUNTEN

- Als het te mooi is om waar te zijn, **dan is het dat meestal ook!**
- Ken je niets van cryptomunten? Blijf er zo ver mogelijk van weg.
- Wil je toch aan de slag met cryptomunten? Laat je enkel begeleiden door een persoon die je ook **in het echt** kent en vertrouwt.

EEN VALS LIEFDADIGHEIDSPLATFORM

- Maak alleen geld over aan een organisatie waarmee je vertrouwd bent.
- Ga na of de **organisatie geregistreerd** is.