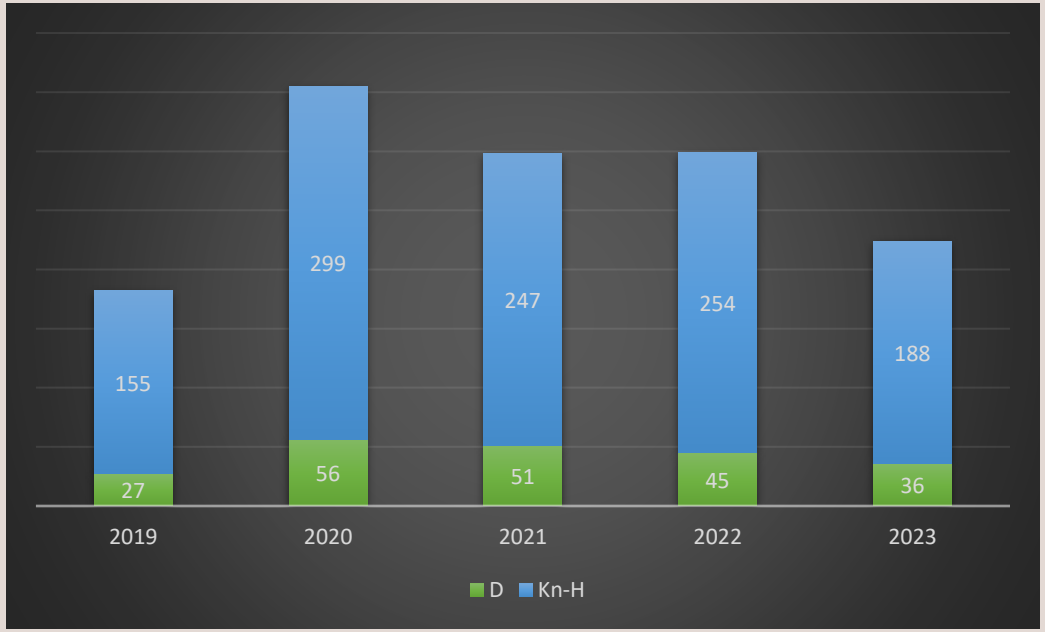
DAMME
KNOKKE-HEIST

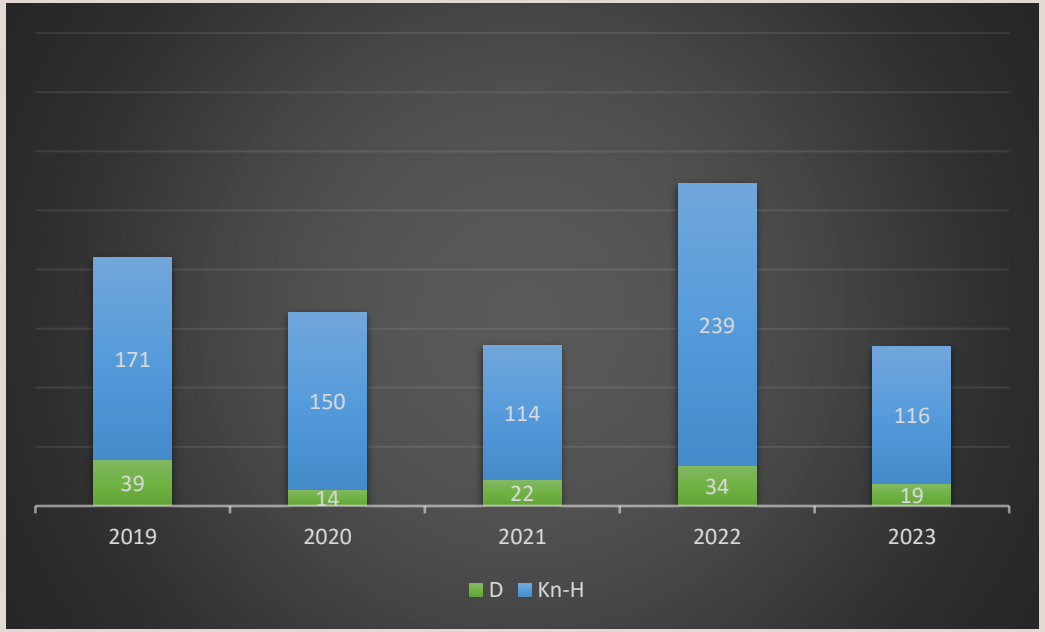
JOUW CYBERCRIME PREVENTIE

CYBERCRIME IN CIJFERS: evolutie

EVOLUTIE AANGIFTES CYBERCRIME BIJ PZ DKH



TER VERGELIJKING: DIEFSTAL MET BRAAK



CYBERCRIME IN CIJFERS: dark number

RESULTATEN 'VEILIGHEIDSMONITOR' OKTOBER 2021

	SLACHTOFFERSCHAP			AANGIFTEPERCENTAGE		
	Federaal	WVL	PZ	Federaal	WVL	PZ
Oplichting via internet	40,1	41,35	40,67	6,61	8,53	12,6
Phishing	33,27	32,28	31,61	10,08	12,76	18,2
Hacking	8,31	7,37	7,14	9,48	10,96	12,93

CYBERCRIME IN CIJFERS: nadeel

GECOMBINEERD NADEEL VAN ALLE AANGIFTES IN 2022 BIJ PZ DAMME/KNOKKE-HEIST

	INFORMATICA BEDROG	OPLICHTING MET INTERNET	VALSHEID IN INFORMATICA	HACKING
Aantal feiten	204	94	15	19
Beoogd nadeel	1 122 066,77€ + 1 673,39 $	1 002 205,18 € + 2 495 £ + 1 voertuig	16 562,41 €	20 591,60 € + 51 844,21 $
Gerecupereerde buit (= 17 %)	325 755,96 € + 1 673,39 $	45 436,03 €	0 €	314,18 €

DE GEVAREN VAN HET INTERNET

JE VOLLEDIGE LEVEN ONLINE ?

JOUW CYBERCRIME PREVENTIE

DE GEVAREN VAN HET INTERNET

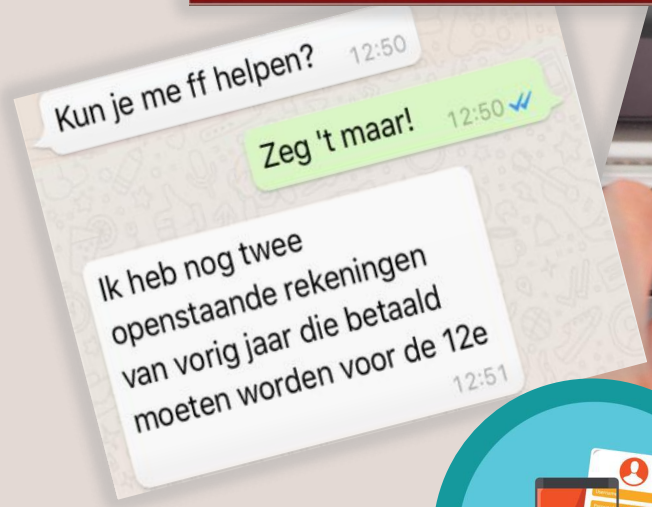
WAT ONTHOUDEN WE ?

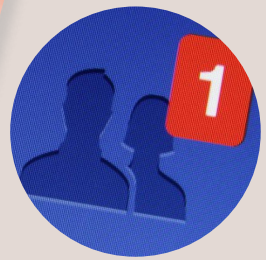
- ✓ Denk niet te snel “mij overkomt het niet!”
- ✓ Geloof ook online niet, wat je in het echte leven niet zou geloven.
- ✓ Wees waakzaam op sociale media en let op met wat je online zet.
- ✓ Is het te mooi om waar te zijn? Dubbelcheck!

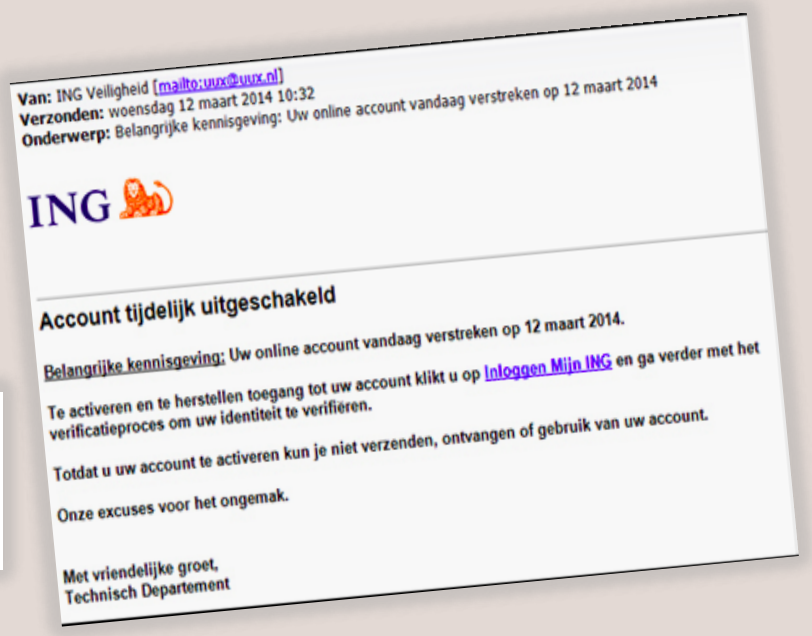
Maar… Wat kunnen jullie er tegen doen ?

HERKEN DE OPLICHTING!

Aan de hand van voorbeelden uit de praktijk







FRAUDE BIJ ONLINE AAN- EN VERKOPEN

OPLICHTING MET INTERNET

Art 496 Sw.


FINANCIËLE BUITENKANS
OF FINANCIËLE KATER?

FRAUDE BIJ ONLINE AAN- & VERKOPEN

NIET-LEVERING VAN (GEDEELTELIJK) BETAALDE GOEDEREN

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

In deze vorm van oplichting komt het slachtoffer in contact met de oplichter via :

- ✓ een **valse advertentie** op een legitieme veilingsite (2dehands.be, Autoscout, Immoweb, AirBnB, enz.)
- ✓ of een **valse verkoopsite** die volledig frauduleus is opgezet

FRAUDE BIJ ONLINE AAN- & VERKOPEN

PHISHING?

In veel gevallen word je via online aan-en verkopen geleid naar een valse website waar men zal pogen je persoonlijke (bank)gegevens te ontfutselen.

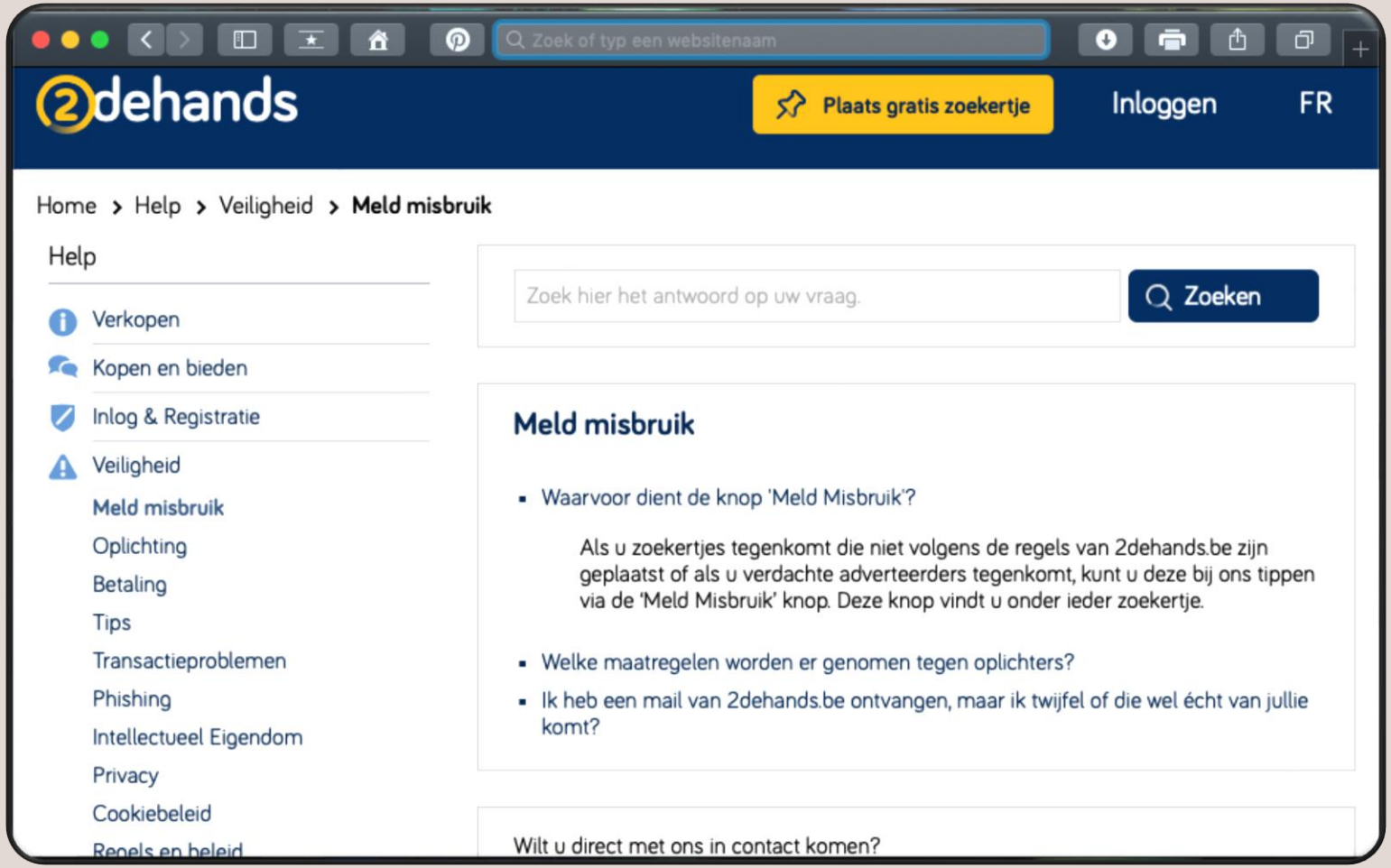
FRAUDE BIJ ONLINE AAN- & VERKOPEN

WAT KAN JE DOEN ?

- ✓ Als het te mooi is om waar te zijn, **dan is het dat meestal ook**!
- ✓ Vermijd aan de oplichters **persoonlijke informatie** vrij te geven, zoals identiteits-documenten of bankgegevens. De oplichters kunnen 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.

FRAUDE BIJ ONLINE AAN- & VERKOPEN

MELD MISBRUIK



FRAUDE BIJ ONLINE AAN- & VERKOPEN

MELD MISBRUIK

FRAUDE BIJ ONLINE AAN- & VERKOPEN

HOE WEET JE OF EEN WEBSHOP BETROUWBAAR IS ?

Betrouwbare webshops bevatten :

- ✓ 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
- ✓ Belgische webshops? Kijk uit naar het BeCommerce-label.

Nagaan of een website in België werd aangemeld als frauduleus :

https://temooiomwaartezijn.be/#check-een-site-op-fraude

CRYPTOMUNTEN & BELEGGINGSFRAUDE

OPLICHTING MET INTERNET

Art 496 Sw.


BELFOE McSTRATTON
fraudulent investments

CRYPTOMUNTEN & BELEGGINGSFRAUDE

WAT IS HET ?

Via een internet-advertentie kom je terecht bij een bedrijf dat belooft je te helpen beleggen in cryptomunten en snel grote winsten beloofd.

Ofwel helpen ze je een effectieve account aan te maken bij een crypto-trader, ontfutselen daarbij je paswoord en laten je (meestal grote) bedragen investeren.

Op een onbewaakt moment wordt je volledige investering via meerdere wallets en cryptomunten doorgestort en verduisterd.

In andere gevallen wordt je naar een nagemaakte en/of valse website geleid en investeer je eigenlijk in ‘lucht’…

CRYPTOMUNTEN & BELEGGINGSFRAUDE

EEN GREEP UIT DE VARIANTEN

BOILER ROOM-FRAUDE

Een vorm van oplichting waarbij fraudeurs je fictieve of waardeloze aandelen of financiële producten aanbieden. De “verkopers” zetten je zwaar onder druk, zodat je steeds meer geld zou storten (vandaar de Engelse benaming ‘boiler room’).

RECOVERY ROOM-FRAUDE

Bij ‘recovery room’-fraude worden beleggers die eerder al werden opgelicht (bv. boilerroom fraude), ongevraagd gecontacteerd met het voorstel om hen te helpen hun geld terug te krijgen.

CRYPTOMUNTEN & BELEGGINGSFRAUDE

WAT KAN JE DOEN ?

- ✓ 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.
- ✓ Ken je wel iets van cryptomunten? Laat je enkel begeleiden door een persoon die je ook **in het echt** kent en vertrouwt.
- ✓ Herken de oplichting!

SOCIAL ENGINEERING

VRIENDSCHAPSFRAUDE

VALSE LIEFDADIGHEID / ERFENIS / HULP

VALSE BOETES / FACTUREN

SEXTORTION


OPRECHTE LIEFDE
OF OPRECHT BEDROG?

VRIENDSCHAPSFRAUDE

SOCIAL ENGINEERING

Via het internet (een spammail, via een datingsite, via sociale media, via de chatbox, enz.) komt je in contact met de oplichter.

Nadat een **vertrouwensband** werd opgebouwd, vraagt de ‘geliefde’ of ‘vriend’ om **geld,** eerst kleine bedragen maar stelselmatig meer en grotere sommen.

Na het incasseren blijft het plots stil aan de andere kant. In werkelijkheid heeft de geliefde/vriend/... nooit bestaan.


DIW
canvas
Ik zal de rest wel doen. Voilà.

VRIENDSCHAPSFRAUDE

WAT KAN JE DOEN?

- ✓ Als het **te mooi is om waar te zijn**, dan is het dat meestal ook!
- ✓ Zorg ervoor dat je weet met wie je te doen hebt. Ken je die persoon **in het echt**?
- ✓ Herken de oplichting!

PHISHING

PHISHING / SMISHING / VISHING

MICROSOFT SCAM

VALSE HELPDESK

PHISHING

WAT IS HET ?

Phishing is een vorm van **internetfraude**.

Het slachtoffer wordt via een e-mailbericht naar een **valse website** gelokt die sterk lijkt op de site van een bank of een commerciële site.

Het kan gaan om een email, sms, whatsapp, messenger, … maar ook berichten verstuurd via een verkoopplatform zoals 2dehands & facebook marketplace.

Wanneer het slachtoffer zijn gebruikersnaam en paswoord ingeeft, zal de fraudeur deze **onderscheppen** en zelf gebruiken om transacties of aankopen uit te voeren.

Soms vragen ze software op de computer te installeren waarmee ze vanop afstand de **computer kunnen overnemen of de toetsaanslagen zien** om zo inloggegevens te stelen.

PHISHING

VARIANTEN

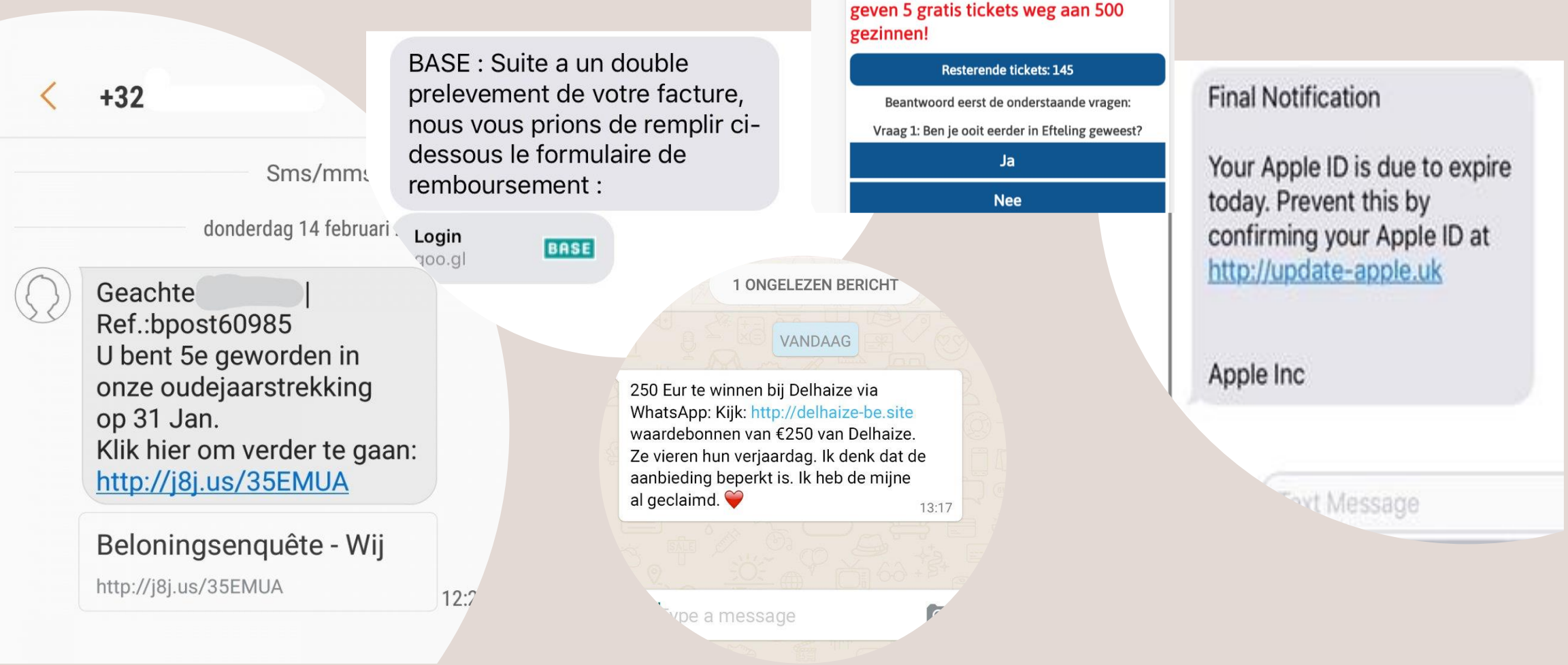
SMISHING

Het slachtoffer wordt via sms, met daarin een link, naar een valse website gelokt waarop gehengeld wordt naar de login- en/of bankgegevens van het slachtoffer.

VISHING

Het slachtoffer wordt telefonisch gecontacteerd en gevraagd om bepaalde handelingen te stellen. (bv. Microsoft Scam)

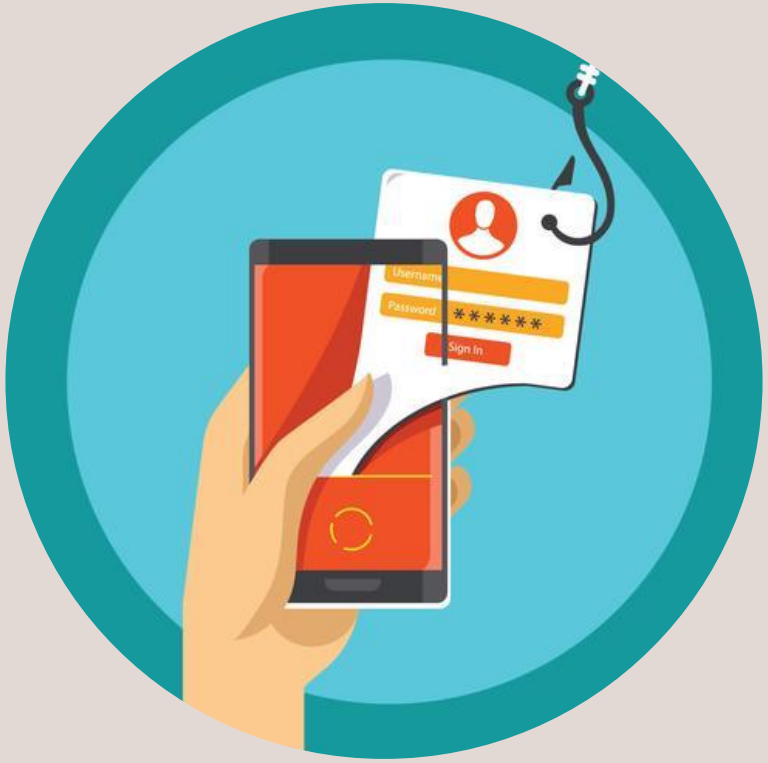
PHISHING


+32
Sms/mms
donderdag 14 februari
Geachte |
Ref.:bpost60985
U bent 5e geworden in onze oudejaarstrekking op 31 Jan.
Klik hier om verder te gaan:
http://j8j.us/35EMUA
Beloningsenquête - Wij
http://j8j.us/35EMUA
BASE : Suite a un double prelevement de votre facture, nous vous prions de remplir ci-dessous le formulaire de remboursement :
Login
BASE
efteling
Wednesday, 30. Mai 2018
We vieren ons 47-jarig jubileum en geven 5 gratis tickets weg aan 500 gezinnen!
Resterende tickets: 145
Beantwoord eerst de onderstaande vragen:
Vraag 1: Ben je ooit eerder in Efteling geweest?
Ja
Nee
1 ONGELEZEN BERICHT
VANDAAG
250 Eur te winnen bij Delhaize via WhatsApp: Kijk: http://delhaize-be.site waardebonnen van €250 van Delhaize. Ze vieren hun verjaardag. Ik denk dat de aanbieding beperkt is. Ik heb de mijne al geclaimd. ❤️
13:17
Final Notification
Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at http://update-apple.uk
Apple Inc

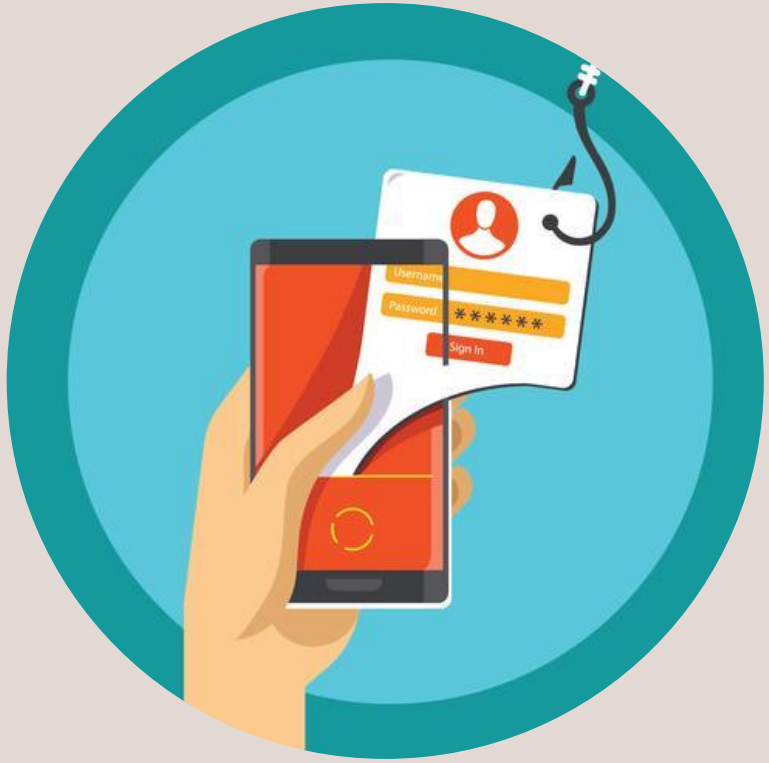
PHISHING

EERST EN VOORAL

Uw bank zal u nooit via e-mail, sms, pop-up bericht of telefoon vragen om vertrouwelijke gegevens door te geven of uw bankkaart op te sturen.
Zo'n bericht is dan ook per definitie een phishingbericht.



PHISHING



WAT KAN JE DOEN

Leer verdachte e-mails en phishing websites te **herkennen**.

Klik niet op de link in het bericht. Toch geklikt?
Vul dan zeker geen velden in en breek elke interactie af.

Een verdacht bericht ontvangen? **Stuur het door** naar:

verdacht@safeonweb.be


DIW
canvas
PHISH ME UP

PREVENTIETIPS

5 EENVOUDIGE STAPPEN VOOR EEN BETERE ONLINE VEILIGHEID

JOUW CYBERCRIME PREVENTIE

JEZELF

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

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

Als ze je wachtwoord, creditcard of controle over jouw computer willen,
zullen ze proberen je 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.

UPDATES & PATCHES

De laatste patches en upgrades toepassen is een belangrijke stap om jouw toestellen te **beschermen**.

Dit geldt niet alleen voor jouw computers of mobiele toestellen, maar **alles wat met het internet kan verbinden** zoals spelconsoles, thermostaten of zelfs luidsprekers en lichten.

Schakel **automatische updates** in waar mogelijk, dit is de makkelijkste manier om al jouw toestellen bij te werken.

ANTIVIRUS

Mensen maken fouten, soms klikken we op of installeren we zaken die we beter niet doen omdat ze het systeem infecteren.
Antivirus is er om je te helpen bij fouten.

Antivirus kan echter niet alle malware stoppen, maar het 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.

Windows 10 heeft standaard een antivirus aan boord in de vorm van Windows Defender.

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**.


Wachtwoorden zijn
niet meer van deze tijd.
Bescherm je online accounts
met tweestapsverificatie.
Check safeonweb.be
Safeonweb.be
CENTRE FOR
CYBER SECURITY
BELGIUM
CYBER SECURITY
COALITION
.be

WACHTWOORDBELEID

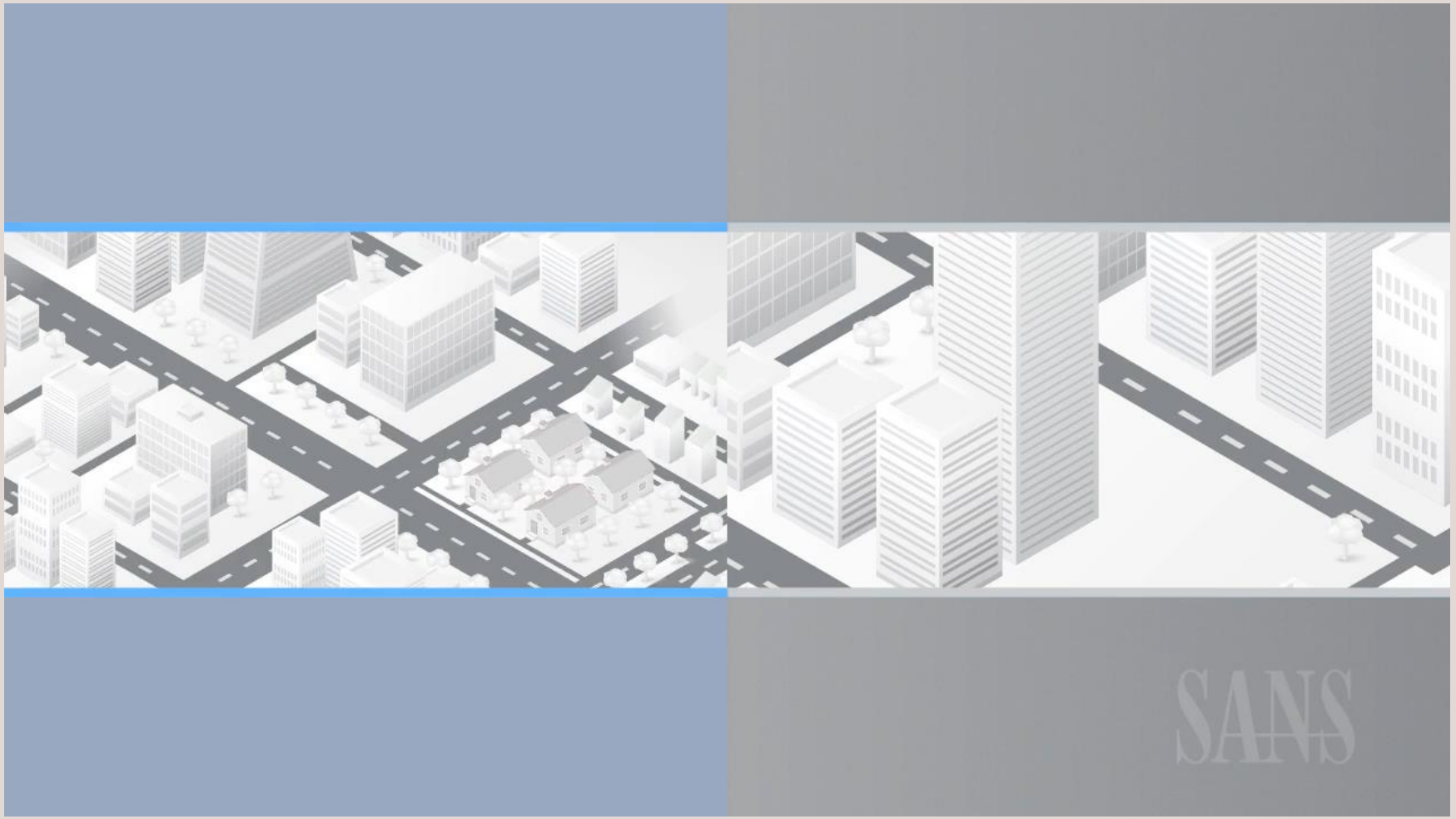
Sterke wachtwoorden zijn de sleutel tot het beschermen van toestellen en online accounts.

Wachtzinnen zijn als wachtwoorden maar zijn gebaseerd op een zin.

Twee-staps-verificatie, ook wel twee-factor-authenticatie 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.

Het enige wat een cyberaanvaller hoeft te doen is een website die je gebruikt te hacken, alle wachtwoorden te stelen, inclusief die van jou, en vervolgens je wachtwoord te gebruiken om in te loggen op al je andere accounts. Kijk op de website


SANS

VEILIGHEID VAN MIJN TELEFOON

VEILIGHEID VAN MIJN TELEFOON

WAT KAN JE DOEN ?

Stel een **uniek wachtwoord** en **pincode** in

Schrijf je **IMEI-nummer** op (*#06#)

Maak ook regelmatig een **back-up** van je gegevens

Beveilig je smartphone in 5 stappen

STAP 1

Download enkel apps uit officiële app winkels

De officiële app winkels zijn de **App Store** als je een iPhone gebruikt en de **Google Play Store** als je een ander merk toestel gebruikt. Voordat je een app downloadt, is het dus belangrijk dat je goed kijkt wie deze app aanbiedt.

STAP 2

Kijk uit voor verdachte berichten

Wees altijd **heel voorzichtig** als je een e-mail of een sms'je ontvangt waarin gevraagd wordt om een app te downloaden. De kans is groot dat je via een **minder veilige app winkel** een **gevaarlijke app** of zelfs een **virus** installeert.

STAP 3

Negeer veiligheids-waarschuwingen niet

Krijg je een **waarschuwing** dat je een onbetrouwbare app wil installeren? Stop onmiddellijk met het installeren van de app.

STAP 4

Geef alleen minimale toegang aan apps

Als je een app installeert wordt er vaak **toegang** gevraagd **tot andere gegevens:** bv. je foto's, je contacten of je locatie. Geef **enkel toestemming** als dat nodig en nuttig is voor het gebruik van de app. Een rekenmachine-app heeft echt geen toegang nodig tot je contacten, foto's of locatie.

STAP 5

Zorg dat je smartphone en apps steeds up-to-date zijn

Krijg je de vraag om **updates** uit te voeren? Doe het zo snel mogelijk. Zet je smartphone regelmatig eens uit. Bij het opnieuw opstarten gebeuren sommige updates automatisch.

Download alleen van erkende app stores

VEILIGHEID BIJ ONLINE BANKIEREN

WAT KAN JE DOEN ?

Spreid het risico: Werk met 1 bank waar je voldoende geld op beschikbaar hebt voor de dagdagelijkse transacties. Maak gebruik van andere banken voor je spaargeld/beleggingen.

Uw bank zal u nooit via e-mail, sms, pop-up bericht of telefoon vragen om vertrouwelijke gegevens door te geven of uw bankkaart op te sturen.

Uw bank zal u nooit vragen om software te installeren om uw toestel te kunnen overnemen.

HERKEN DE OPLICHTING

7 VRAGEN OM ZELF TE BEOORDELEN OF HET OM EEN VALS BERICHT GAAT

1. Heeft de e-mail, het bericht of telefoongesprek **een persoonlijke aanhef** (correcte naam & voornaam)?
2. Lijkt het bericht **foutloos** geschreven? Wordt het gesprek in correct Nederlands gevoerd?
3. Ben je klant bij het genoemde bedrijf?
4. Is de e-mail verstuurd vanuit een e-mailadres **van het bedrijf zelf** (@naambedrijf.be)? Is het telefoonnummer van de oproeper gekoppeld aan het bedrijf?

EUROPEES POLITIEBUREAU (EUROPOL)
Opgericht: 1 juli 1999
Hoofdkantoor: Eisenhowerlaan 73, Den Haag
Coördinaten: 52° 05 34' N, 4° 16 53 E
Werknemers: 1065 (december 2016)1
Jaarlijks budget: 116,4 miljoen euro (2017)2
Verantwoordelijk minister Belgische vlag¬ Catherine De Bolle (directeur)

Police Fédérale

CONVOCATIE

Op verzoek van mevrouw Catherine DE BOLLE,

In opdracht van **mevrouw Catherine DE BOLLE**, directeur-generaal van Europol en hoofd van de brigade voor de bescherming van minderjarigen, referentie **N* 160422900879**.
Naar aanleiding van analyses en werkzaamheden van onze **Brigade voor de bescherming van minderjarigen (BPM)** op het computernetwerk zijn bepaalde sporen van uw identificatiegegevens geïdentificeerd en maakt u het voorwerp uit van verschillende lopende gerechtelijke procedures:

*** KINDERPORNO**

*** PORNOGRAFISCHE SITES**

*** CYBERPORNOGRAFIE**

*** PEDOPHILIA**

*** EXHIBITIONISME**

Ter informatie. **De wet van maart 2007** verhoogt de straffen wanneer pogingen op minderjarigen, aanranding of verkrachting mogelijk zijn gepleegd via het internet.
Gelieve ons in antwoord op deze e-mail binnen 72 uur een verklaring te geven om de straffen te kunnen vaststellen;

Na deze termijn zullen wij verplicht zijn ons verslag over te maken aan de procureur des Konings **Patrick VANDENBRUWAENE**, teneinde een arrestatiebevel tegen u op te stellen en dit over te maken aan de Politie die het dichtst bij uw woonplaats is gevestigd voor uw arrestatie.

U zult ook worden geregistreerd als zedendelinquent en uw dossier zal worden gepubliceerd bij verschillende tv-stations voor uitzending, waar uw familie, geliefden en de hele wereld zullen zien wat u voor uw computer doet.

Nu ben je gewaarschuwd.

HERKEN DE OPLICHTING

VIND JE EEN MAIL VERDACHT? BEANTWOORD DAN DEZE VRAGEN.

5. Is de toon van het bericht **vriendelijk** en krijg je voldoende tijd om te reageren?
6. Verwijst het bericht naar een **betrouwbare** website? (plaats de muis boven de link ZONDER te klikken. Werk je met een tablet? Houd dan de link langer ingedrukt)
7. Wat zegt je **gevoel**? Is het bericht echt/betrouwbaar?

TOCH SLACHTOFFER ?

Bel onmiddellijk Cardstop op het nummer **078 170 170**

Contacteer zo vlug mogelijk je bank om eventueel de laatste betalingen te blokkeren.

Doe aangifte bij de politie (op afspraak).

Breng nuttige bewijzen mee
(zoekertjes, screenshots, berichten, e-mails,…)

JOUW POLITIE.

www.trapnietindeval.be
www.safeonweb.be

PZ.DKH@police.belgium.eu
www.politie.be/5446

Bel voor dringende politiehulp **101**
Geen spoed, wel politie?
Bel **050 619 619**