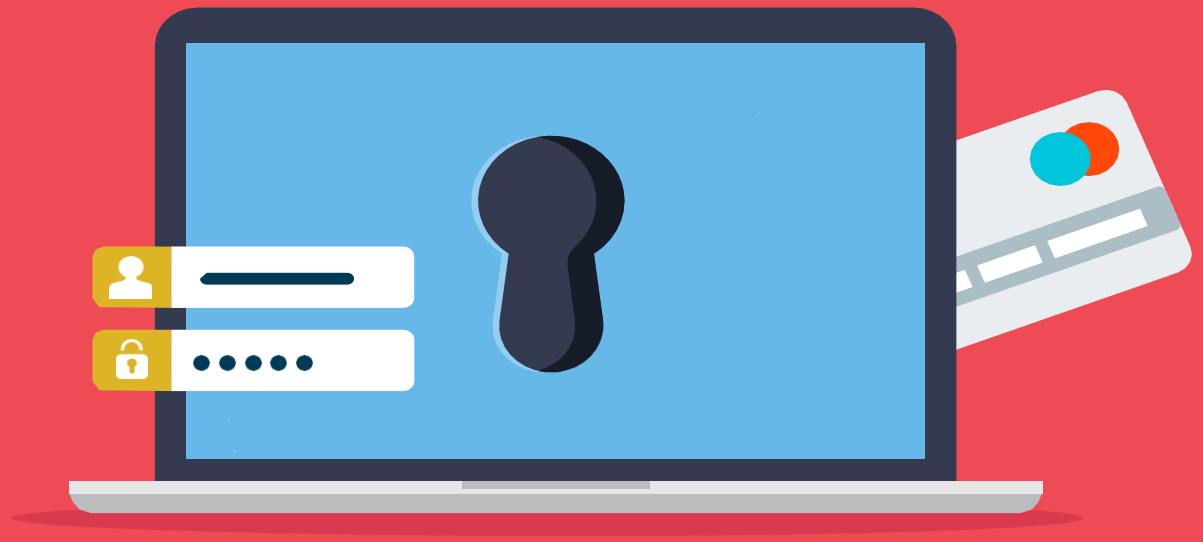


Veilig bankieren

Bin-event Zandhoven 14/9

febelfin

Traditionele misdaad neemt af, digitale misdaad stijgt

- Cijfers Federale Politie: **over de laatste 5 jaren** zijn online fraudegevallen met **175% gestegen**.
- 2020: gezondheidscrisis & economische crisis maar ook een '**phishingcrisis.**
- Fraudepraktijken aangepast aan **nieuwe levensstijl**:
  - Inspelen op emotie, angst & onwetendheid
  - Voordoen als betrouwbare organisaties (cfr. gezondheidsorganisaties, overheidsdiensten, banken, …).
  - Toename van online winkelen & thuiswerk → fraudeurs doen zich voor als pakketbezorgers, e-commerceplatformen of netwerkproviders.
- **Drempel** om over te gaan tot digitale fraude werd alsmaar kleiner:
  - Phishing kits zijn beschikbaar op het "surface web" aan zeer lage prijzen
  - Snel geld verdienen voor weinig inspanning
  - Via diverse kanalen: mail/sms/sociale media/telefoon/zoekmachines
- In 2021 verschuiving naar fraudevormen waarbij de klant zelf een overschrijving doet.
- Daarom is aandacht voor **digitale weerbaarheid en het herkennen van fraudevormen nodig.**
- Want voorkomen is beter dan genezen en elk slachtoffer is er 1 te veel!

Online fraudevormen: Phishing

Phishing in cijfers

Fraudeurs konden in 2021 voor meer dan **€25.000.000 buitmaken**

12% van de bevolking, en zelfs 30% van de jongeren heeft nog nooit van phishing gehoord.

3% van de bevolking zou zijn pincode geven als zijn bank daarom vraagt.

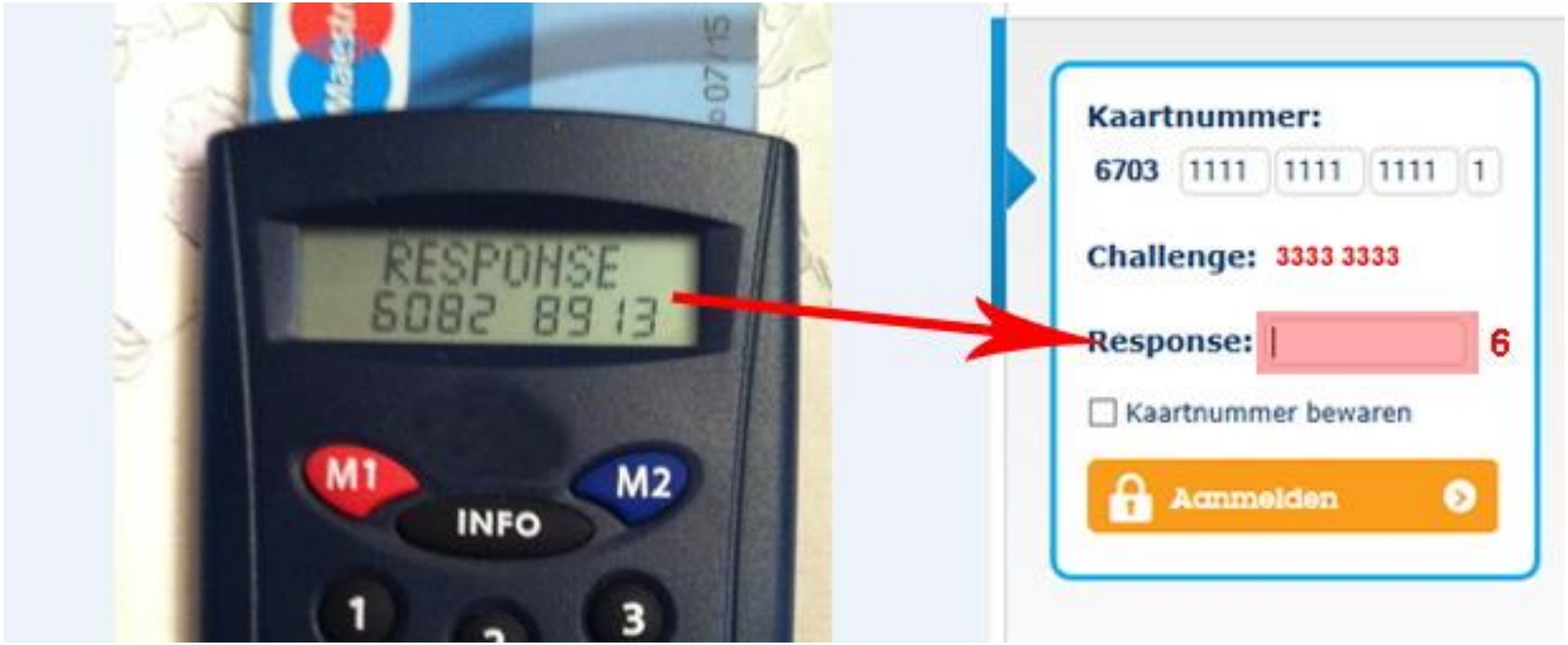
In **2021** zien we een verschuiving naar **andere fraudevormen** waarbij het **slachtoffer zelf geld overschrijft.**

Wat is phishing?

- **Meest voorkomende** fraudevorm
- **Phishing:**
  - vorm van oplichting waarbij de fraudeur een bericht via sms, email of sociale media stuurt die een link naar een valse website bevat.
  - Als je je persoonlijke informatie ingeeft (zoals je codes), hebben ze toegang tot je bankrekening. Gebeurt ook telefonisch.
- **Smishing** = phishing via sms.

De link kan ook bedoeld zijn om bepaalde software of een app te installeren. Dat gaat dan over een **virus of over 'malware'.**

Geef nooit je pincode & responsecode!



Hoe kan je phishing/oplichting herkennen?

- Geloofwaardigheid
  - men gebruikt de identiteit van gekende personen, overheid of instellingen waardoor het slachtoffer veronderstelt met een legitieme persoon te handelen
- Tijdsdruk:
  - men simuleert een acute/dringende situatie
- Angst:
  - fear of missing out of angst om niet te handelen
- Aanspreking is zelden of nooit persoonlijk:
  - Je wordt aangesproken met ‘Beste’ of ‘Geachte’ maar met nooit je naam
- Afwezigheid van details:
  - Bijvoorbeeld PV-politie bevat geen details; factuur dat nog moet worden betaald is algemeen (geen details)
- Onrealistische voorstellen
  - Bijvoorbeeld een spaarrekening met 8% opbrengst → als het te mooi is om waar te zijn, is het meestal ook zo!

Hoe kan je een phishingmail herkennen?

Hoe kan je een phishingmail herkennen?

Beweeg met je muis over de link zonder erop te klikken. Zo kan je de domeinnaam die onder de link verborgen is, controleren.

Van: "Febelfin" <info@terbergspecials.be>
Aan: "johan vansteenwegen" <johan.vansteenwegen@telenet.be>
Verzonden: Zondag 29 oktober 2017 13:23:27
Onderwerp: Bericht

Geachte klant,

Uit onze administratie is naar voren gekomen dat u nog geen gebruik maakt van onze nieuwe kaart. De nieuwe kaart is beter beveiligd tegen fraude-activiteiten en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankierzaken.

Belangrijkste aanpassing: Banken moeten klanten verzekeren tegen financiële schade bij eventuele fraude-activiteiten. Als gevolg hiervan introduceren wij de nieuwe beter beveiligde kaart.

Vanwege de veiligheid van onze klanten verplicht ING het gebruik van de nieuwe kaart. Het gebruik van uw huidige product vervalt per 10 november 2017 voor gebruik.

Uit vei http://www.ing.be.fcnnbfn.info/aanvragen ail uit naam van Febelfin
Click or tap to follow link.

Vraag hier kosteloos uw nieuwe kaart aan.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groeten,

Pascale Jacobs
ING
Afdeling personeelszaken

Smishing

Proximus : Votre facture est PAYEE 2 fois par erreur, rendez-vous sur https://bit.ly/Proximus20

[Cardstop]

WAARSCHUWING: Wij hebben uw rekening tijdelijk geblokkeerd. U dient uw rekening zo snel mogelijk te verifieren om blokkade te voorkomen. Ga naar:

https://cardstop-heractiveren.me/cardstop.html

[LETOP]
De Nationale Veiligheidsraad heeft beslist dat elke burger een bedrag terugkrijgt als compensatie voor zijn/haar facturen tijdens de crisis, meld u aan via. -> https://mijn-compensatie.co
---
[FAITES ATTENTION]
Le Conseil national de sécurité a décidé que pendant la crise chaque citoyen doit recevoir un montant pour rembourser ses factures, Inscrivez-vous via. -> https://mijn-compensatie.co

[INGApp]: Votre compte est bloquée suite à plusieurs tentatives de connexion. Pour réactiver votre compte cliquez ici: https://ltsme-auth.web.do?login

[Postnl.be] Uw pakket heeft ons detacheringcentrum bereikt gelieve eenmalige kosten te voldoen via : https://bom.so/7lgWRa

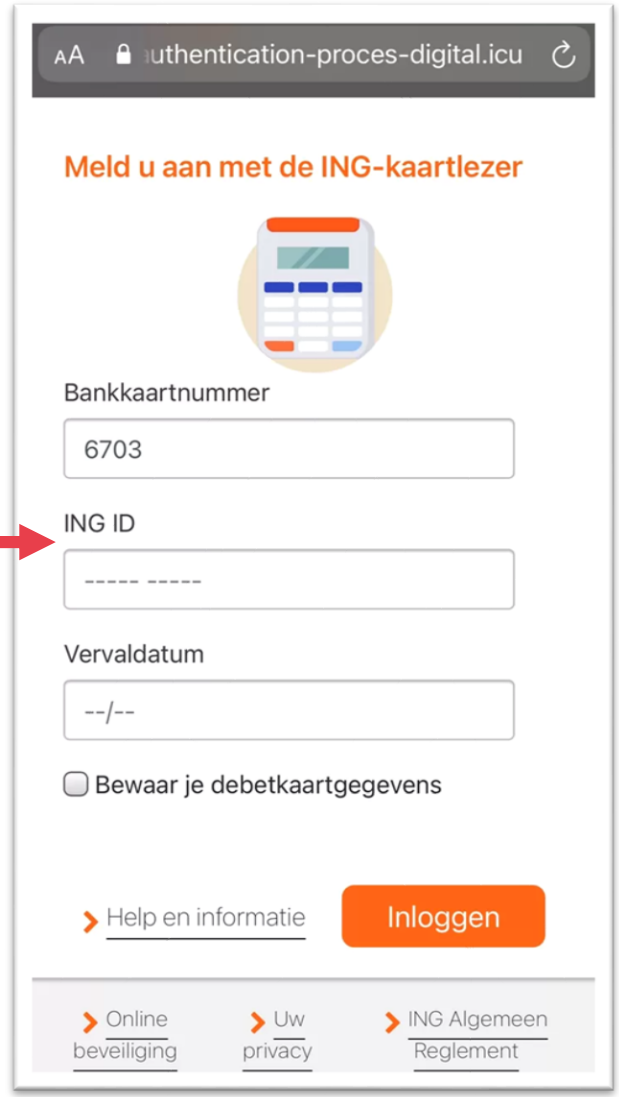
[Postnl.be] Votre colis est arrivé à notre centre de dépôt, merci de régler les frais de dédouanement ponctuels imposés par les douanes via : https://bom.so/7lgWRa

Afgeleverd

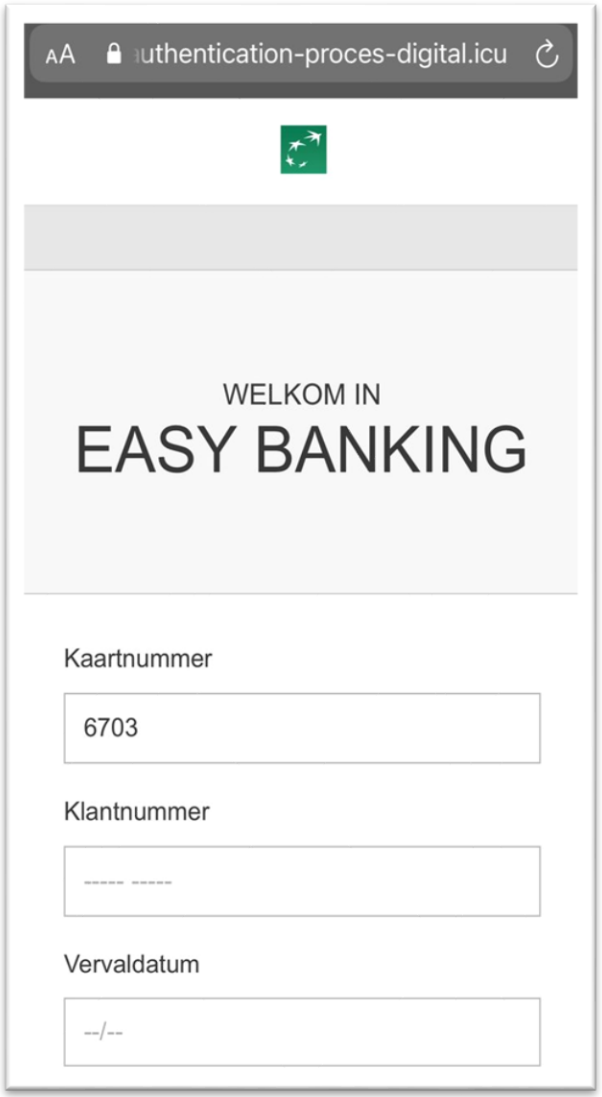
Uw teruggave hebben wij opnieuw berekend.
Bevestig het bedrag wat u nog hoort te krijgen van ons via:
Bevestig voor 29-8-21

gaven-herstel.info

Voorbeelden van valse websites



Valse pagina lijkt op webpagina ING



Valse pagina lijkt op webpagina BNP Paribas Fortis

Voorbeeld van ‘malware’

Bankkaart phishing

Vrouw stuurt doorgeknipte bankkaart naar oplichters en raakt duizenden euro's kwijt

NEDERLAND **Een Nederlandse vrouw (28) is duizenden euro's kwijtgeraakt door bankkaartfraude. De vrouw stuurde haar doorgeknipte kaart op naar een adres in Wijchen in de oostelijke provincie Gelderland. Ze reageerde op een mailtje dat ze eind juli 2019 ontving waarin stond dat haar pas was verlopen.**

Hai Voeten 03-02-20, 16:53 **Bron:** De Gelderlander

De man die met de bankkaart van het slachtoffer duizenden euro's opnam, onder meer in het Nederlandse Tiel (provincie Gelderland). © Nederlandse politie

Bankkaart phishing aan huis

- **Oplichters doen zich voor als een medewerker van je bank en bellen je** op om je bijvoorbeeld te waarschuwen voor verdachte transacties die zouden uitgevoerd zijn met jouw bankkaart. Plots zijn er problemen met de verbinding en stellen ze voor om bij je thuis te komen en samen het probleem op te lossen.

- **Bankbedienden zullen je nooit om jouw persoonlijke codes (pincodes of response codes) vragen. Zij zullen ook nooit tot bij je thuis komen om jouw bankkaart door te knippen of op te halen of om betalingsproblemen op te lossen.**

Permanente waakzaamheid is noodzakelijk

Campagnemateriaal: www.safeonweb.be/nl/campagnemateriaal

Andere vormen van fraude

Kluisrekeningfraude

- Oplichters benaderen je meestal in 2 stappen:

    1. Eerst sturen ze een phishingbericht om je persoonlijke bankcodes te ontfutselen (proberen zo toegang te krijgen tot je rekening).
    2. Daarna bellen ze je op waarbij ze zich voordoen als medewerker van je bank (stap 1 kan ook overgeslaan worden).
    3. Ze vragen je om geld over te schrijven naar een nieuwe, veilige rekening.

    Filmpje: [Kluisrekeningfraude - Laat je niet vangen - YouTube]

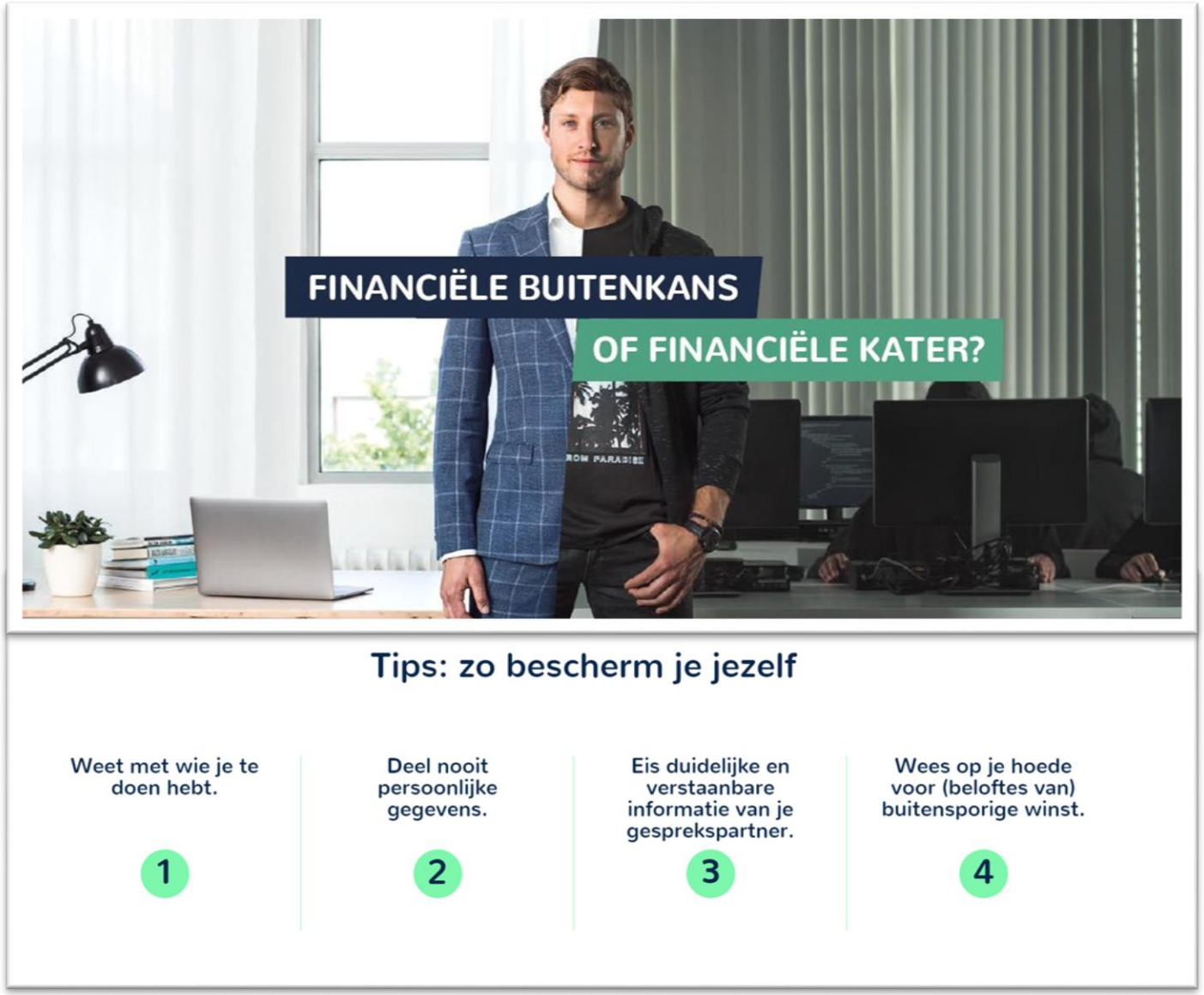
Hulpvraagfraude

- Fraudeurs doen zich via e-mail, sms of appberichten voor als een van jouw dierbaren.
- Of omgekeerd: ze schrijven je dierbaren aan in jouw naam.
- Ze vragen om dringende financiële hulp, en dus om een overschrijving te maken.

Gouden tip: bel de afzender van het bericht eerst zelf op, of stel wat controlevragen waarvan de antwoorden niet in eerdere e-mails, chatberichten of op social media staan.

Blokkeer het telefoonnummer.

Beleggingsfraude



Vriendschapsfraude

- **Tips:**
  - Aanvaard niet zomaar vriendschapsverzoeken
  - Ga de echtheid van het profile na
  - Vertrouw niet zomaar iedereen
  - Wees op je hoede voor ‘zielige’ verhalen
  - Maak nooit zomaar geld over!

Meer info: https://temooiomwaartezijn.be

Vraag naar ons gratis digitaal materiaal

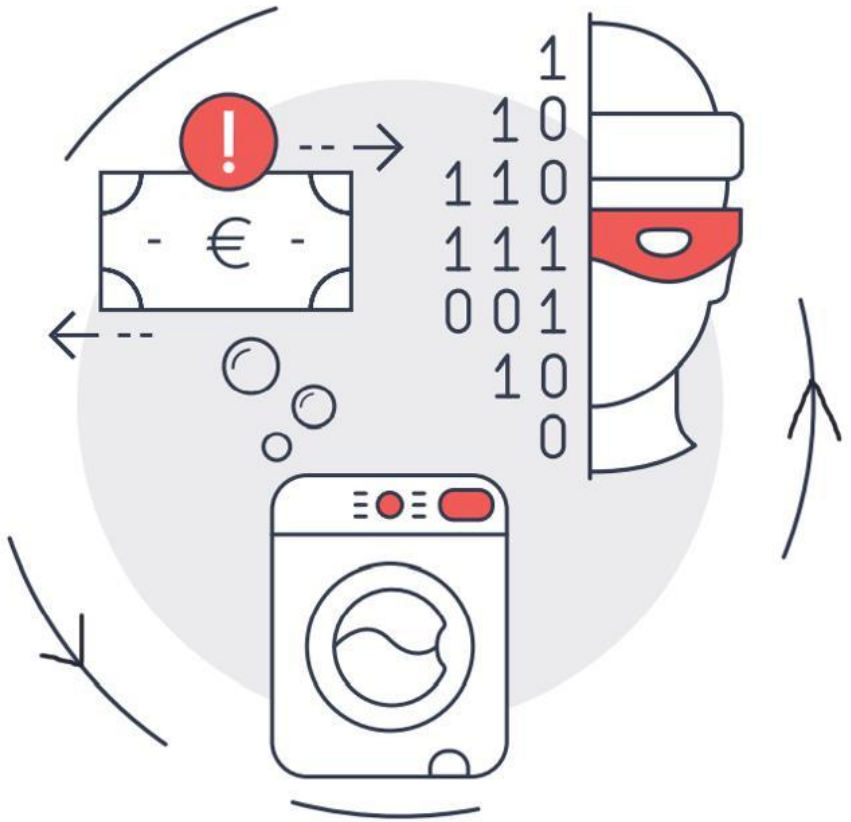
Op te vragen bij: info@febelfin.be

Geldezels

febelfin

Gestolen geld gaat nooit rechtstreeks naar de crimineel…

Klant (rekening)



Criminele organisatie

Geldezel

De rol van de geldezel

Wat ?

- Geldezels stelt zijn bankrekening en/of bankkaart en codes te beschikking van criminelen. Vaak zijn het mensen met financiële moeilijkheden die op een eenvoudige en snelle manier iets willen bijverdienen.

Wie ?

- Doelgroep zijn dikwijls jongeren. Meer dan 1 op 10 zou in ruil voor een vergoeding hun bankaart + codes uitlenen.

Hoe?

- Ronselaars zoeken geldezels online (bijv. via sociale media) of in het echte leven (uitgaansleven, stations of in de buurt van scholen).
- De ‘opdracht’ wordt voorgesteld als volledig veilig, legaal of een ‘vriendendienst’. In de praktijk stelt de vergoeding voor de geldezel amper iets voor en blijft die vaak achter met een geplunderde bankrekening.


Ik ben met pensioen
wisten jullie dat niet?
@mango-mano
Bonker heeft goed gegeten
@Genoemd


Belgium F game
2 subscribers
BEFgame
Username
Wij vullen alles.🏦 Hoge% 🔌🔋en alles strak vol! 🇧🇪BE & NL🇳🇱
Bio
Notifications


Kijkennietpraten
Su geleden door Blackghost uit Foto's
De grootste oplichter van ANTWERPEN
@wauw777 wauw niet horen
Bankoe maal 6
Verstuur een chat

Geldezels zijn strafbaar

Gevolgen?

- Fysieke bedreigingen en geweld door criminelen
- Strafbaar - gerechtelijke vervolging (geldboete/werkstraf)
- Minderjarige geldezel: ouders kunnen aansprakelijk worden gesteld (terugbetaling)
- Je bank kan weigeren om je nog een bankrekening, bankkaart en/of lening te geven

Wat als je je toch hebt laten verleiden?

- Contacteer zo snel mogelijk je bank
- Laat je kaart blokkeren bij Card Stop
- Ga langs bij de politie

Sensibilisering is nodig!

Alle materiaal beschikbaar op: www.febelfin.be

Veilige banksystemen

Veilige banksystemen

Boodschappen ATM
'laat u niet afleiden'

Beveiligde verbinding
internetbankieren (https://)

Verplicht aanmelden

Kaartlezer: pin-code
en responscode

Betaalopdrachten
digitaal ondertekenen

Betaallimieten

Automatische afmelding

Experts die gedrag van
internetcriminelen volgen

febelfin

Is mobiel bankieren minder veilig?

Veilig online bankieren

- Dezelfde hyperbeveiligde technologie zowel bij pc banking als mobile bankieren
- Registratie via identificatie (kaartlezer, vingerafdruk, aanmeldcode, …)
- Persoonlijke codes om verrichtingen te doen
- Aanmelden met vingerafdruk mogelijk
- Geen bankgegevens op uw smartphone bewaard

Sterke veiligheidssystemen = evenwicht zoeken

- Banken doen veel inspanningen om phishing te voorkomen:
  - '**tweestapsauthenticatie**' = klant identificeert zichzelf aan de hand van 2 elementen (kaart/telefoon & pincode/vingerafdruk/gezichtsscan) om e-betalingen te initiëren.
  - Intensieve monitoring van transacties: 75% van alle frauduleuze overschrijvingen wordt gedetecteerd of gerecupereerd
  - Nauwe samenwerking met telecom (ikv smishing & spoofing), parket, justitie, politie,…
- Evenwicht is cruciaal: klant wil **vlotte, snelle betalingen (instant payments)** en **efficiënte fraudedetectie (heeft tijd nodig)**.
- MAAR: **33% van de Belgen** vindt deze **extra beveiligingsstappen overbodig → voelt als een belemmering**

Tips voor een goede cyberhygiëne

febelfin

Om nooit meer te vergeten: Geef nooit je persoonlijke codes door!!!

Tips voor een goede cyberhygiëne

- Wachtwoorden:
  - Neem lange wachtwoorden/wachtwoordzinnen
  - Gebruik nooit hetzelfde wachtwoord op meerdere plekken
  - Sla je wachtwoorden op een praktische manier op
    (bv. Wachtwoordmanager op je PC of smartphone, etc.)
  - Kijk naar de mogelijkheid om twee-staps-verificatie in te stellen (vingerafdruk, …)
- Updates:
  - Updates zijn verbeteringen van kwetsbaarheden in je computer of telefoon.
  - Wanneer een update beschikbaar is, zorg ervoor dat je deze uitvoert. Zo zorg je dat er zo min mogelijk kwetsbaarheden in jouw apparaten zitten.
- Klikgedrag:
  - Klik nooit zomaar op linkjes of bijlagen
  - Ga liever zelf naar een website dan via een link in een mail of sms
- Ten slotte: Gebruik je gezond verstand
  - Handel nooit gehaast en laat je nooit opjagen.
  - Check altijd of de inhoud van het bericht wel kan.
  - Vertrouw je het niet? Stop het contact/verrichting.

Toch in de val getrapt?

1. **Blokkeer onmiddellijk je bankkaarten.**
   Bel Card Stop.

2. **Contacteer zo snel mogelijk je bank.**
   De contactgegevens van de banken vind je terug op Blokkeer via de uitgever (cardstop.be)

3. **Verander zo snel mogelijk je codes**.

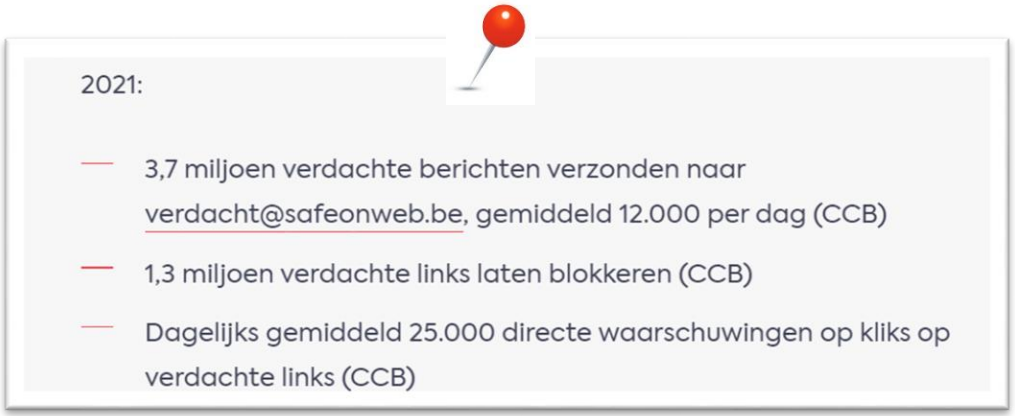
4. **Dien klacht in bij de politie.**

Opgelet: Nieuw Card Stop nummer!

Ook bereikbaar in het buitenland!

Help anderen door verdachte berichten te melden

- **Stuur het door naar verdacht@safeonweb.be**
- Indien het een phishingbericht is in naam van een bank → naambank@phishing.be



Door deze berichten te melden, kan je phishingwebsites laten **blokkeren** en voorkomen dat anderen **in de val lopen**.

Blijf op de hoogte met de SafeonWeb app:

- Deze app waarschuwt je voor cyberdreigingen en nieuwe phishingberichten
- Download de Safeonweb-app via www.safeonweb.be

Volg Febelfin voor meer info

- **Website**: https://www.febelfin.be
- **Brochure over digitale inclusie** (hoofdstuk over online veiligheid): https://www.febelfin.be/nl/artikel/febelfins-brochure-digitale-inclusie-helpt-je-op-weg
- **Social media:** Facebook – Instagram – LinkedIn – Twitter

Coming soon…

- Najaar 2022: launch **gratis** **e-learning veilig bankieren met bijhorend certificaat**
- Doelgroep: **professionelen en vrijwilligers**
- E-learning als **referentiewerk** voor mensen die werken rond **online veiligheid**:
  - de meest relevante en actuele fraudevormen
  - Overzicht van alle bestaande tools en sensibiliseringsmateriaal
  - Guidelines voor het omgaan met digistarters
  - Tips en tricks om veilig te bankieren
  - Mogelijkheid tot vraagstelling aan Febelfin experten
  - …
- Voor meer info contacteer info@febelfin.be

Belgian Financial Sector Federation

www.febelfin.be