Online veiligheid: bescherm jezelf tegen fraude

Ontdek onze brochure over online veiligheid.

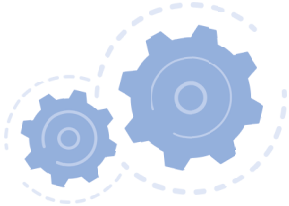
Leer hoe je pogingen tot fraude kan herkennen, hoe je je vertrouwelijke gegevens kan beschermen en hoe je in alle zekerheid gebruik kan maken van bankdiensten. Of je nu een beginnende of ervaren gebruiker bent, neem de controle over je online veiligheid!

BRUSSELS HOOFDSTEDELIJK GEWEST

paradigm .brussels

febelfin

Inhoud



Beveiligde banksystemen

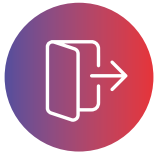
Online bankdiensten bevatten beveiligingsmechanismen en controles om mogelijke fraude te voorkomen en op te sporen.

> Online en mobiel bankieren gebeurt altijd via een **beveiligde verbinding**.

> Om toegang te krijgen tot online bankieren zal **je bank je altijd vragen om je op een veilige manier te identificeren aan de hand van twee of meer elementen uit de volgende categorieën:** iets wat alleen de gebruiker kent (geheime code); iets wat enkel de gebruiker in zijn of haar bezit heeft (bankkaart of gsm); iets wat de gebruiker kenmerkt (gezichtsherkenning of vingerafdruk). Over het algemeen gebruik je een van deze elementen, vaak een wachtwoord, om te bewijzen wie je bent. Maar voor online bankieren is het verplicht om er twee of meer te gebruiken: dit noemen we **'sterke klantauthenticatie'**.

> Je bank past omwille van **veiligheidsredenen betalingslimieten** toe. Dit bedrag kan je zelf aanpassen indien gewenst.

> Wanneer **de bank een verdachte betalingsopdracht opmerkt**, voert ze eerst een aantal extra controles uit voordat ze de overschrijving uitvoert.



> Je wordt **automatisch afgemeld van online bankieren** als je gedurende een bepaalde periode geen activiteiten hebt uitgevoerd.

> **De hyper-beveiligde technologie van bankdiensten via pc** is gelijkwaardig aan die op smartphones en tablets. Bovendien worden er geen bankgegevens opgeslagen op je smartphone.

Hoe bescherm je jezelf tegen online fraude?

Geef nooit je codes door

Over welke codes hebben we het dan?

> **Je pincode** : de code die aan je bankkaart is gekoppeld.

> **De code** om toegang te krijgen tot je **bankapp**.

> **De codes van de kaartlezer** die een sterke authenticatie vormen.

Je bank en andere betrouwbare organisaties zullen je nooit vragen om je codes door te geven.

Onderteken nooit een transactie (via itsme of je kaartlezer) die je niet zelf hebt geïnitieerd.

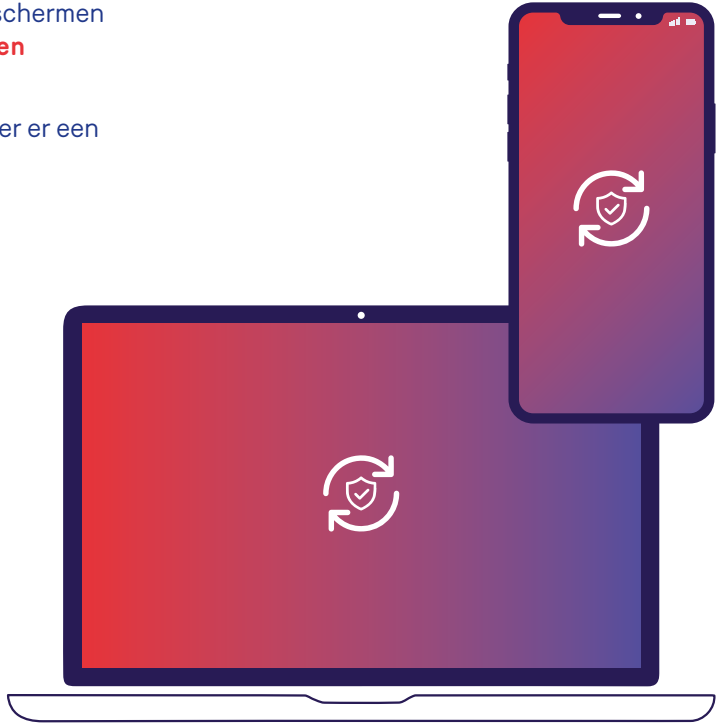
Dit is een bankkaartlezer:

Geef NOOIT je pincode door... Maar deel ook de nooit de 'responsecode' die door je kaartlezer gemaakt wordt met anderen!

Vergeet de updates van al je apparaten niet uit te voeren

Het is belangrijk om je gegevens te beschermen tegen cybercriminelen door **je apparaten regelmatig te updaten**.

Je apparaten melden je meestal wanneer er een beveiligingsupdate beschikbaar is.



Denk na, ga niet overhaast te werk

Wees op je hoede wanneer men je vraagt om ‘dringend’ te handelen.

Deze urgentie is een voorwendsel dat fraudeurs vaak gebruiken om onrust te zaaien bij hun slachtoffers.

Ze proberen je snel te laten handelen, zonder je de tijd te geven om jezelf de juiste vragen te stellen en te beseffen dat er sprake is van oplichting.

Wanneer je vermoedt dat je het slachtoffer bent van een poging tot fraude, neem dan de tijd om het bericht inhoudelijk te analyseren en meer te weten te komen door de gegevens van de organisatie die in het bericht wordt genoemd op te zoeken en zelf contact op te nemen.

Gebruik nooit de telefoonnummers, de e-mailadressen of de webadressen in het bericht.

Zet bij twijfel alle contacten en transacties stop. Meld het bericht aan **verdacht@safeonweb.be** en verwijder het.

Gebruik een beveiligde verbinding bij het invoeren van persoonlijke informatie

> Gebruik een beveiligde verbinding

Neem voorzorgsmaatregelen wanneer je een gratis wifinetwerk buitenshuis gebruikt.

Er zijn gratis wifi-hotspots beschikbaar op tal van openbare plaatsen. Hoewel ze praktisch zijn, zijn deze netwerken voor iedereen toegankelijk, waardoor het risico op cybercriminaliteit toeneemt.

Om dit risico tot een minimum te beperken, moet je een verbinding met je online en mobiel bankieren via openbare wifi vermijden en in plaats daarvan het 3G-, 4G- of 5G-netwerk op je telefoon en je computer of tablet gebruiken.

Thuis kan je je eigen wifi natuurlijk wel in alle veiligheid gebruiken.

> Bezoek beveiligde websites

Controleer ook of de verbinding beveiligd is door naar de URL te kijken, d.w.z. het webadres dat in de navigatiebalk (bovenaan je browser) verschijnt. Het adres moet beginnen met **'https://'**. De **'s'** in 'https' betekent dat de verbinding beveiligd is. Je ziet ook een klein hangslotje links van het adres van de website.

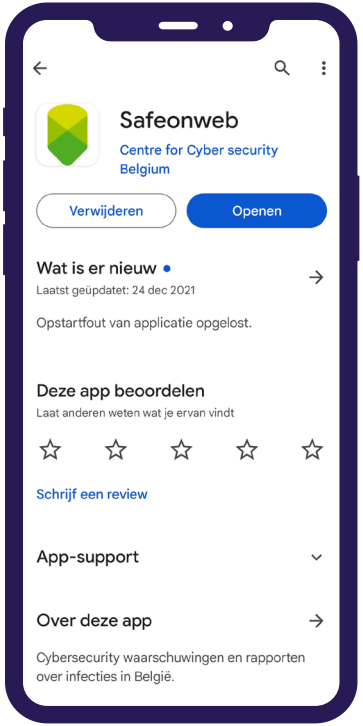
Voer geen banktransacties uit en communiceer je vertrouwelijke gegevens niet op websites zonder hangslot of beginnend met 'http://'.

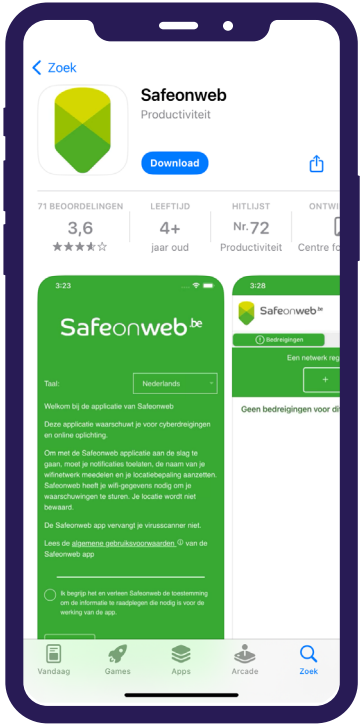
Opgelet! Cybercriminelen kunnen ook beveiligde 'https://'-websites namaken. Wees altijd voorzichtig wanneer je persoonlijke gegevens deelt en controleer altijd of je je op de juiste website bevindt.

Gebruik de Safeonweb-app

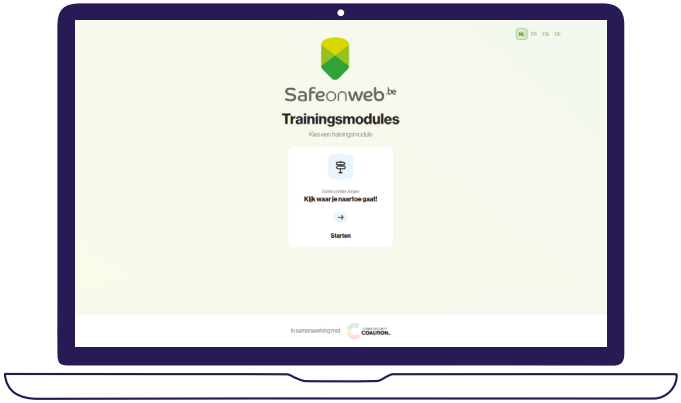
Wanneer je op de hoogte wenst te blijven van de verschillende cyberbedreigingen en nieuwe scams, download dan de Safeonweb-app, die gratis verkrijgbaar is in de App Store en Google Play, of bezoek de website **www.safeonweb.be**.

Safeonweb.be





Gebruik hun module op **https://surfenzonderzorgen.safeonweb.be/nl/modules/1** om te oefenen hoe je een link naar een valse website herkent.



Opgelet, Safeonweb is geen antivirus, maar een informatief platform.

De Safeonweb-browserextensie helpt je bij het beoordelen van de betrouwbaarheid van een website door aan elke site een vertrouwensniveau toe te kennen: hoog (groen), gemiddeld (oranje) of laag (rood). Ga naar https://safeonweb.be/nl/nationale-sensibiliseringscampagne-cyberveiligheid-2023 om de extensie op je internetbrowser te installeren (alleen pc).

Pogingen tot online fraude herkennen

Dit zijn enkele elementen die je helpen om een poging tot fraude te herkennen:

> **Verdachte afzender:** fraudeurs nemen vaak de identiteit aan van een persoon of een instelling die je vertrouwt.

Zo krijg je de indruk dat je met een 'legitieme' persoon communiceert. Cybercriminelen gebruiken geavanceerde technieken om logo's, lettertypes, afbeeldingen en e-mailhandtekeningen van legitieme bedrijven te kopiëren om hun berichten geloofwaardiger te maken. Ze kunnen zich ook aan de telefoon voordoen als deze bedrijven.

> **Noodsituatie:** om je snel in de val te lokken, creëren ze vaak valse noodsituaties, bijvoorbeeld door te zeggen dat de veiligheid van je bankkaart in het gedrang is (er is zogezegd een onveilige transactie gebeurt of je kaart is onveilig).

In stressvolle situaties is de kans groter dat je minder weloverwogen beslissingen neemt.

> **Nieuwsgierigheid:** fraudeurs proberen ook je interesse te wekken door geld-gerelateerde (en onrealistische) voorstellen aan te bieden, zoals een spaarrekening met 10% rente, een wedstrijd om een luxewagen te winnen, de aflossing van je hypotheek, een gratis reis enz.

> **Online fraudeurs** kunnen je zowel via een link of op een andere manier om persoonlijke informatie vragen.

VI. Methodes voor online fraude

Phishing

Phishing is een fraudevorm waarbij fraudeurs naar de bankcodes en de persoonlijke gegevens van hun slachtoffers hengelen. Ze sturen misleidende berichten die de gebruikers aanmoedigen om hun persoonlijke gegevens te delen.

Wanneer deze frauduleuze berichten via sms worden verstuurd, spreken we van smishing.

Phishing kan ook telefonisch gebeuren waarbij fraudeurs potentiële slachtoffers eveneens aanmoedigen om persoonlijke gegevens te geven, een transactie te ondertekenen met itsme of de kaartlezer, of software te installeren.

> Standaard phishing

Laten we eens kijken hoe je een phishingmail herkent:

(A) **Het e-mailadres komt niet overeen met het officiële e-mailadres van de organisatie.** Wanneer je beter kijkt, merk je een extra letter op, een ontbrekende letter, ongebruikelijke tekens enzovoort. Banken en bedrijven hebben geen Gmail-, Yahoo- of Outlook/Hotmail-account. Een e-mailadres van een bedrijf dat eindigt op @gmail, @outlook, @yahoo, @hotmail is daarom mogelijk een frauduleuze e-mail.

(B) De tekst bevat soms (maar niet altijd) **spellings- en grammaticale fouten**.

(C) Meestal is het bericht **niet aan jou persoonlijk gericht**.

(D) Phishing-berichten zetten je aan tot snel handelen door een gevoel van **urgentie te creëren**.

Ⓔ **Het bericht zal je altijd aanmoedigen om op een link te klikken.** Deze link brengt je naar een frauduleuze website waar je wordt gevraagd om je persoonlijke en/of bankgegevens te verstrekken of om een frauduleuze app of software te downloaden.

Opgelet, ingenieuze oplichters slagen er soms wel in om zich tot jou persoonlijk te richten.

Om er zeker van te zijn dat je je op de echte pagina van je bank bevindt, gebruik je je bankapp of typ je zelf het adres van de website van je bank in de navigatiebalk.

Van: RBS Bank <rbsbanke@hotmail.com> Ⓐ
Verzonden: Maandag 8 mei, 2022
Aan : John Doe
Onderwerp: DRINGEND – Ongebruikelijke activiteit op uw account Ⓑ

Ⓒ

Geachte klant,

We hebben onlangs ongebruikelijke activiteit gedetecteerd op uw bankrekening. Om uw account te beschermen en frauduleus gebruik te voorkomen, vragen wij u om onmiddellijk in te loggen op uw account via onderstaande link en uw accountinformatie te controleren.

Indien u uw account niet binnen 48 uur controleert, zien wij ons genoodzaakt uw account om veiligheidsredenen op te schorten. Ⓓ

Klik hier > Ⓔ

Bedankt voor uw medewerking.

Met vriendelijke groet,

Uw bankteam

> Online bankkaart-phishing

Bij een poging tot bankkaart-phishing proberen fraudeurs je bankkaart en de bankcodes rechtstreeks te bemachtigen.

Je krijgt een bericht waarin staat dat je je bankkaart moet vervangen. Dit bericht moedigt je aan om op een link te klikken. Wanneer je erop klikt, kom je op een pagina terecht waar je wordt gevraagd om:

1. Je **persoonlijke gegevens** en je bankkaartnummer **in te vullen**.
2. Je **huidige pincode** in te vullen en een nieuwe pincode te kiezen.
3. Je **debetkaart met de post** op te sturen. Om je nog meer te verwarren, vragen criminelen je soms om je kaart doormidden te knippen, waarbij de chip intact blijft, en ze vervolgens met de post te versturen.

> Bankkaart-phishing aan huis

De fraudeurs kunnen zich ook voordoen als medewerkers van je bank en gedragen zich dan doorgaans als een ware professional, om je vertrouwen te winnen.

1. **Ze bellen je** op om je te vertellen dat er verdachte transacties zijn verricht met je bankkaart.
2. Tijdens het gesprek doen ze alsof de telefoonverbinding slecht is en bieden ze aan **naar je toe te komen** om het probleem op te lossen.
3. Bij jou thuis zullen de fraudeurs **je vragen om verbinding te maken met de online bank** en zich zo plaatsen dat ze je persoonlijke codes kunnen zien. Ze kunnen je ook rechtstreeks om je codes vragen.

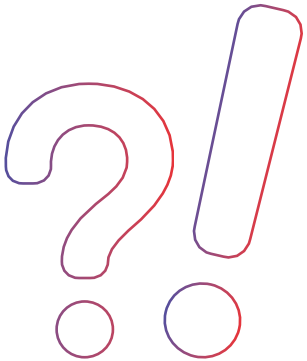
④ De ‘medewerkers’ beweren dat er **problemen zijn met je kaart** en bieden aan om ze mee te nemen zodat je een nieuwe kaart kan ontvangen. Ze kunnen ook aanbieden om je kaart voor je neus te vernietigen. Ze knippen de kaart dan doormidden **zonder de chip te beschadigen**. Wanneer de chip intact is, kunnen ze de kaart gebruiken om geld van je te stelen.

Gouden raad: wanneer je je kaart toch moet afgeven, knip de chip dan doormidden.

Bankpersoneel zal je nooit om je pincode of om de responsecodes van je kaartlezer vragen. Ze komen nooit bij je thuis om je bankkaart te vernietigen of op te halen of om betalingsproblemen op te lossen.

Wat gebeurt er wanneer je op frauduleuze links klikt?

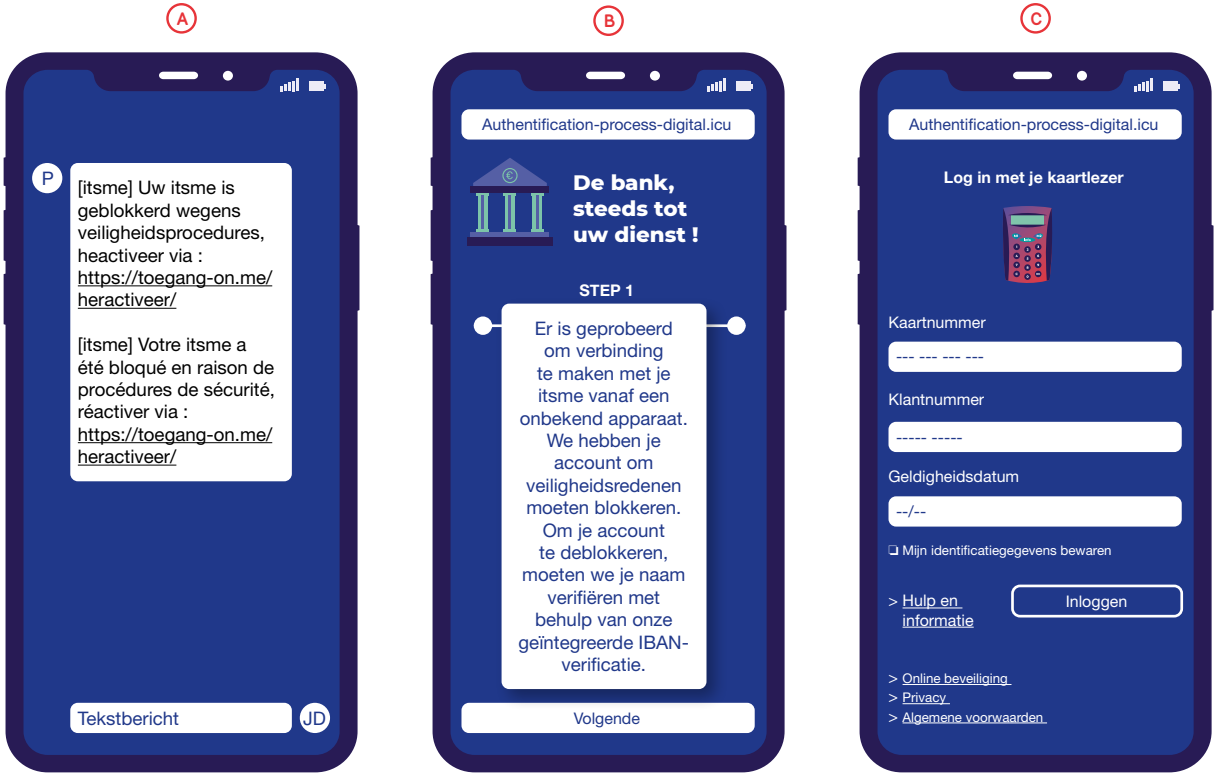
Wanneer je op een frauduleuze link klikt, kom je op een website terecht die door fraudeurs gemaakt is en die vaak een goede imitatie is van de website van je bank. Op deze manier willen ze jouw persoonlijke gegevens en je bankcodes achterhalen.



(A) Op de volgende pagina zie je een voorbeeld van smishing (phishing via sms) in naam van itsme.

(B) Wanneer je op de link klikt, kom je terecht op een pagina waar wordt uitgelegd dat er wordt geprobeerd om verbinding te maken met je itsme-account vanaf een onbekend apparaat. Vervolgens wordt je gevraagd om je bank te kiezen en kom je op een valse inlogpagina van je bank terecht.

(C) Je wordt gevraagd om je bankgegevens in te voeren op een pagina die heel sterk lijkt op de website van je bank: hetzelfde logo, dezelfde kleur, hetzelfde lettertype.


A
P
[itsme] Uw itsme is geblokkerd wegens veiligheidsprocedures, heactiveer via : https://toegang-on.me/heractiveer/
[itsme] Votre itsme a été bloqué en raison de procédures de sécurité, réactiver via : https://toegang-on.me/heractiveer/
Tekstbericht
JD
B
Authentification-process-digital.icu
De bank, steeds tot uw dienst !
STEP 1
Er is geprobeerd om verbinding te maken met je itsme vanaf een onbekend apparaat. We hebben je account om veiligheidsredenen moeten blokkeren. Om je account te deblokkeren, moeten we je naam verifiëren met behulp van onze geïntegreerde IBAN-verificatie.
Volgende
C
Authentification-process-digital.icu
Log in met je kaartlezer
Kaartnummer
--- --- --- ---
Klantnummer
----- -----
Geldigheidsdatum
--/--
❑ Mijn identificatiegegevens bewaren
> Hulp en informatie
Inloggen
> Online beveiliging
> Privacy
> Algemene voorwaarden

Fraude waarbij het slachtoffer wordt gevraagd zelf een overschrijving te doen

Sinds 2021 vindt er een verschuiving naar nieuwe vormen van fraude plaats waarbij slachtoffers worden aangemoedigd om zelf geld over te schrijven.

Opgelet! Alle bankrekeningen hebben een hoog beveiligingsniveau. Een 'kluisrekening' bestaat echter niet.

> Kluisrekeningfraude

Bij kluisrekeningfraude benaderen cybercriminelen je doorgaans in twee of drie stappen:

- **Eerst sturen ze je een bericht** waarin ze vragen naar jouw bankcodes zodat ze toegang kunnen krijgen tot je rekening.
- **Vervolgens bellen ze je op en doen ze alsof ze een medewerker van je bank zijn.** Soms beginnen ze meteen bij deze stap.
- **Ze zeggen dat je rekening in gevaar is.**
- **Tot slot nodigen ze je uit om je geld** over te maken naar een nieuwe zogenaamde 'veilige' kluisrekening.

Onthoud dat je bank je nooit via telefoon, e-mail, sms of sociale netwerken zal vragen om je geld over te maken naar een andere rekening.

> Vriendschapsfraude

Vriendschapsfraude, ook bekend als datingfraude, is een techniek die fraudeurs gebruiken om het vertrouwen van hun slachtoffers te winnen door zich online voor te doen als vrienden of romantische partners.

1. Fraudeurs maken valse profielen aan op datingsites of sociale netwerken en doen zich voor als betrouwbare personen. Ze gebruiken gestolen of vervalste foto's en persoonlijke informatie om zich voor te doen als echte profielen.
2. Vervolgens bouwen ze een relatie op met hun slachtoffer door regelmatig te communiceren via e-mail, telefoon of chat.
3. Na verloop van tijd gebruiken fraudeurs deze relatie om geld of persoonlijke informatie van het slachtoffer te krijgen. Zo kunnen ze geld vragen voor onverwachte uitgaven, zoals medische rekeningen of vliegtickets, of vragen om gevoelige informatie zoals kredietkaartnummers of het nummer van je identiteitskaart of je rijksregisternummer.

Wees voorzichtig en waakzaam bij het aangaan van online relaties. Wanneer je wordt benaderd door iemand die je niet kent of wanneer iets verdacht lijkt, aarzel dan niet om een stap terug te zetten en op onderzoek te gaan om er zeker van te zijn dat de persoon wel degelijk echt en betrouwbaar is. Maak bij de geringste twijfel geen geld over.

> Hulpvraagfraude

Bij hulpvraagfraude:

1. Nemen ze contact met je op via e-mail, sms of de sociale netwerken
2. Doen ze zich voor als een naaste
3. Leggen ze je tot slot uit dat ze met een dringend financieel probleem zitten en vragen ze je om een overschrijving te doen.

Fraudeurs kunnen ook in jouw naam berichten sturen naar je naasten.

Een gouden raad: bel de afzender van het bericht zelf op om zijn of haar identiteit te controleren. Stel persoonlijke vragen die niet werden beantwoord in eerdere e-mails, chats of op de sociale netwerken.


A
Hallo oma dit is mijn nieuwe nummer, ik heb een probleem met mijn gsm. Kan je dit nummer opslaan?
B
Natuurlijk, het is opgeslagen!
A
Ik heb echt geen geluk.. mijn telefoon is in het water gevallen… Bovendien was het mijn nieuwe telefoon. Ik heb hem nu in rijst gelegd om te drogen, en gebruik momenteel een oude telefoon, maar de microfoon is kapot…
B
Ohnee…!
A
Ik kan me voorlopig redden met mijn oude telefoon en je tenminste berichten sturen. Hoe gaat het met je?


B
Heel goed schat :) En met jou, afgezien van je kapotte telefoon?
A
Niet al te best, nee. Alsof dat nog niet genoeg is, heb ik nu nog een ander probleem...
B
Kan ik je ergens mee helpen?
A
Ik moet twee rekeningen betalen, maar nu mijn telefoon kapot is, heb ik geen toegang tot mijn bankingapp. Kan je de rekeningen voor mij betalen alsjeblieft?
A
Ik betaal je morgenochtend alles terug, beloofd.
Tekst bericht
B

> Beleggingsfraude

Bij beleggingsfraude proberen fraudeurs geld af te troggelen van slachtoffers door hen een belegging met een zeer aantrekkelijk rendement aan te bieden. Later blijkt dat de aangeboden belegging niet bestaat of veel minder opbrengt dan verwacht. Werd je benaderd door onbekenden met een beleggingsaanbod? Wees extra waakzaam bij volgende situaties:

- Je wordt ongevraagd telefonisch of via e-mail benaderd zonder dat je weet hoe de aanbieders aan je gegevens komen.
- De aanbieders identificeren zichzelf niet en weigeren hun adres te geven ‘om vertrouwelijkheidsredenen’.
- Ze beloven je uitzonderlijk hoge rendementen of winsten.
- Je krijgt geen verdere details over de belegging, zelfs niet wanneer je er expliciet om vraagt.
- De aanbieders zijn gevestigd in een ander land.
- Je wordt gevraagd om het geld over te maken naar een buitenlandse bankrekening (het rekeningnummer begint niet met ‘BE’).
- Je wordt onder druk gezet om snel een beslissing te nemen.

Wanneer je bent benaderd door onbekenden die je een aanbod deden om te beleggen:

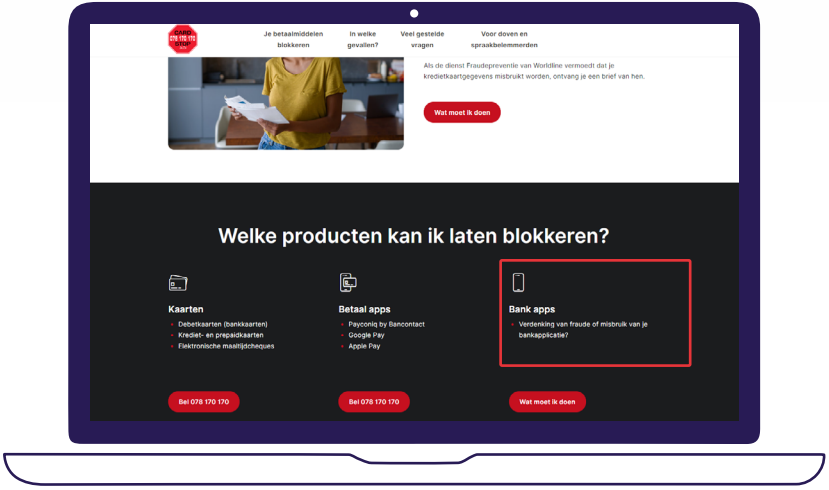
1. Check eerst met wie je te maken hebt: controleer steeds de identiteit van de aanbieders en wees kritisch met de informatie die je op het internet vindt. Geen duidelijke en betrouwbare informatie? Accepteer het aanbod niet.
2. Deel nooit je persoonlijke gegevens: fraudeurs vragen vaak om een kopie van je identiteitskaart, een foto, een bankkaart- of kredietkaartnummer enzovoort. Ga hier niet op in!
3. Eis duidelijke en begrijpelijke informatie en probeer zoveel mogelijk te weten te komen over het aanbod. Wanneer je het aanbod niet begrijpt, negeer het dan.
4. Wees op je hoede voor de belofte van buitensporige winsten: wanneer een rendement te mooi lijkt om waar te zijn, is het dat meestal ook. Gegarandeerde winsten bestaan niet.

Met wie moet je contact opnemen in geval van fraude?

Wanneer je toch het slachtoffer bent geworden van fraude, moet je:

1. Zo snel mogelijk contact opnemen met je bank zodat ze de toegang tot je bankrekening kan blokkeren. Elke bank heeft een fraudeafdeling die 24 uur op 24 en 7 dagen op 7 bereikbaar is.

Op de website van je bank of van Card Stop (zie hieronder) vind je een pagina met de contactgegevens van je bank zodat je contact kan opnemen wanneer je het slachtoffer bent geworden van fraude of phishing.



② Neem ook contact op met Card Stop via het nummer 078 170 170 om je kaart te blokkeren. Dit nummer is ook vanuit het buitenland te bereiken via +32 78 170 170.

③ Dien een klacht in bij de politie.

CARD
078 170 170
STOP
24/24

Politie

Oefeningen: om welk type fraude gaat het?

Duidt alle zaken aan waaraan je fraude kan herkennen

Oefening 1

e-mail

Betreft: DRINGEND - Bijwerking van de gegevens van uw bankkaart

Beste klant,

We schrijven u om u te informeren dat het tijd is om de gegevens van uw bankkaart bij te werken. We hebben onlangs extra veiligheidsmaatregelen ingevoerd om uw transacties te beschermen en we hebben uw medewerking nodig om deze maatregelen te implementeren.

We vragen u vriendelijk om uw persoonlijke gegevens in te vullen en uw volledige bankkaartnummer te vermelden. We vragen u ook om uw huidige pincode in te voeren en een nieuwe pincode te kiezen voor uw eigen veiligheid.

Naam:

Voornaam:

Telefoonnummer:

Bankkaartnummer:

Pincode:

Om veiligheidsredenen willen we u ook informeren dat u uw debetkaart per post moet terugsturen naar het volgende adres: Fraudestraat, 12 – 23145 Cyber, België.

We hechten het grootste belang aan de veiligheid van onze klanten en daarom vragen we om uw medewerking bij het bijwerken van de gegevens van uw bankkaart.

Alvast bedankt.

Met vriendelijke groeten,

Het team van MijnBank

Oefening 2

e-mail

Proximus: Beste Proximus-klant, u heeft een openstaande factuur. Voorkom afsluiting, betaal via: https//proximus.e-factuur.digital/openstaand/HC3065DER?id: 9adeudhuh4 https://bit.ly/Proximus20

Oefening 3

sms

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

Oefening 4

Message Whatsapp

Marie Christine, Ik zou je graag komen opzoeken, maar ik heb veel financiële problemen.

Mijn moeder is ernstig ziek en ik heb veel ziekenhuiskosten. Het is heel moeilijk voor me omdat je de vrouw van mijn leven bent en ik wil zo graag bij je zijn :(

Misschien kun je me helpen? Ik zou 200€ nodig hebben :(

Aantekeningen

Deze brochure werd gemaakt door **Paradigm** in samenwerking met de **Belgische Federatie van de Financiële Sector (Febelfin)** in het kader van het **Plan voor Digitale Toegankelijkheid 2021 – 2024**.

Contact : inclusie@paradigm.brussels

BRUSSELS HOOFDSTEDELIJK GEWEST

paradigm .brussels

febelfin

VU : Paradigm - Nicolas Locoge - Kunstlaan, 21 - 1000 Brussels. Gooi niet op de openbare weg.