BETAALFRAUDE EN ONDERNEMINGEN

Hoe fraude voorkomen en herkennen?

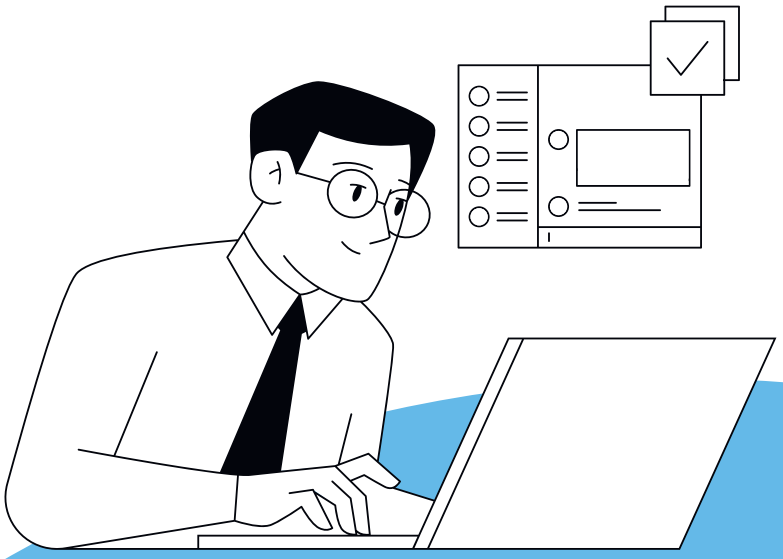
febelfin

Niet alleen consumenten, maar ook ondernemingen worden in toenemende mate een doelwit voor verschillende vormen van betaalfraude.

Er bestaan tegenwoordig verschillende fraudevormen die zich in het bijzonder richten op ondernemingen en die mogelijks tot grote financiële verliezen kunnen leiden. Denk maar aan CEO-fraude, factuurfraude, phishing, enz.
Banken investeren voortdurend in fraudedetectiesystemen en monitoring maar het is helaas niet mogelijk om alle fraudepogingen te detecteren.

Maar ook ondernemingen kunnen zelf initiatieven opzetten om de waakzaamheid te verhogen en daarbij eigen beveiligingssystemen uitwerken. Want alleen samen kunnen wij de fraudeurs een halt toeroepen..

Ontdek in deze brochure 5 fraudevormen die vaak voorkomen in het bedrijfsleven. We leggen uit hoe fraudeurs proberen te misleiden en hoe je jezelf, je medewerkers en jouw onderneming hiertegen kan beschermen. Je vindt in de brochure ook nuttige tips om dergelijke fraude binnen je onderneming op te sporen of – nog beter – te voorkomen.



Leid je financiële medewerkers op

De medewerkers van de boekhoudafdeling zijn de eerste verdedigingslinie tegen betaalfraude. Het zijn zij die fraude kunnen opsporen en financiële verliezen kunnen voorkomen. Wij raden je aan om dit document te verspreiden in je bedrijf. Spoor de directieleden en alle medewerkers die een volmacht hebben op de bedrijfsrekeningen aan om deze brochure te lezen.

FACTUURFRAUDE

— Wat is factuurfraude?

De naam zegt het zelf: bij factuurfraude vervalsen oplichters een factuur. Fraudeurs onderscheppen een echte factuur, vervangen de bankgegevens van de begunstigde door hun eigen bankgegevens en versturen de aangepaste factuur. Een onderneming kan een valse factuur ontvangen, of zelf een factuur versturen die hierna vervalst wordt.

— Hoe gaat factuurfraude in zijn werk?

Eerst onderscheppen fraudeurs een factuur. Dit kan op verschillende manieren:

- Vanuit het postcircuit: de fraudeurs halen de facturen uit de rode brievenbussen of sorteercentra van bpost.
- Ze halen die bij particulieren of ondernemingen zelf uit brievenbussen.
- Ze dringen het informaticasysteem binnen van een leverancier. Hier onderscheppen ze facturatiemails of passen het rekeningnummer aan. Wees dus ook op je hoede bij facturen die je elektronisch ontvangt.

Daarna wijzigen de oplichters het rekeningnummer van de begunstigde.

- Vaak scannen ze de originele factuur in en passen de gegevens (rekeningnummer en soms telefoonnummer) van de leverancier/verkoper aan met speciale software.
- Of ze voegen een brief bij de factuur die vermeldt dat het rekeningnummer is gewijzigd. Soms plakken ze een sticker op de enveloppe of de factuur zelf met “Opgelet, gewijzigd rekeningnummer”.

Daarna versturen ze de aangepaste factuur.

Ze stellen zelf ook soms volledig uitgevonden facturen op.

TIPS OM FACTUURFRAUDE TE VOORKOMEN

- Vergelijk het rekeningnummer op de factuur met het rekeningnummer op de bestelbon of officiële website van de verkoper of leverancier.
- Wanneer je een overschrijving uitvoert, controleer dan ook of de naam van de begunstigde overeenkomt met het rekeningnummer (IBAN). Als jouw bank een waarschuwing toont, neem dan de tijd om alles te controleren voordat je de betaling bevestigt.
- Wees extra waakzaam als een factuur een nieuw rekeningnummer vermeldt of als er een sticker “Opgelet, gewijzigd rekeningnummer” op de enveloppe of factuur kleeft. Ook als het de eerste factuur is die je ontvangt van een verkoper of leverancier. Neem even de tijd om het rekeningnummer te checken vooraleer over te gaan tot betaling.
- Twijfel je? Bel dan het bedrijf op via het nummer dat al bestaat in je database, niet naar het nummer dat op de factuur vermeld staat (dat zelf ook vervalst kan zijn).
- Bewaar de gegevens en het bankrekeningnummer van je leveranciers, ook als je via e-banking betaalt. Indien je dan een nieuwe factuur ontvangt, kan je makkelijk nagaan of het rekeningnummer overeenkomt met de opgeslagen gegevens.
- Betaal nooit een factuur of rekening die er verdacht uitziet zonder dat je goed hebt gecontroleerd of je wel degelijk klant bent bij dit bedrijf, of je iets hebt besteld.
- Ontvang je de factuur via e-mail, controleer of het e-mailadres correct is.
- Sinds 1 januari 2026 moeten facturen tussen bedrijven (B2B) verplicht via Peppol worden verzonden. De aanbevelingen blijven ook voor deze facturen gelden.

VERIFICATIE VAN DE NAAM VAN DE BEGUNSTIGDE

Wanneer je een overschrijving doet, controleert je bank of de naam van de begunstigde overeenkomt met het rekeningnummer (IBAN) dat je hebt ingevoerd.

Als de naam niet of slechts gedeeltelijk klopt, kan er een waarschuwing verschijnen voordat je de betaling bevestigt.

Dit systeem zorgt voor extra bescherming tegen fouten en bepaalde vormen van fraude, zoals factuurfraude.

— Ik heb toch een valse factuur betaald. Wat nu?

- Contacteer zo snel mogelijk de bank van jouw onderneming om de fraude te melden. Je bank zal aan de bank van de begunstigde vragen om het geld terug te storten. Deze bank zal ook de overschrijving of de rekening proberen te blokkeren zodat geldafhalingen door de fraudeurs niet meer mogelijk zijn.
- Dien klacht in bij de politie.
- Meld het fraudegeval via ConsumerConnect. Daar vindt je een antwoord op je vragen en advies over welke stappen je best kunt ondernemen.

REAGEER SNEL

Als je fraude vaststelt nadat een overschrijving is uitgevoerd, breng dan onmiddellijk je bank op de hoogte.

Als je de bank snel verwittigt, is de kans groter dat het gestolen geld teruggevonden wordt. Eventueel zijn er nog bijkomende formaliteiten nodig bij de bevoegde instanties, zoals een klacht bij de politie.
De experts bij de banken kunnen je advies geven over de te volgen stappen.

CEO-FRAUDE

— Wat is CEO-fraude?

Bij CEO-fraude of *social engineering* geven fraudeurs zich uit voor de CEO (of een andere interne of externe vertrouwenspersoon) van een bedrijf om een interne medewerker van dat bedrijf te manipuleren zodat hij of zij een handeling verricht (vaak een betaling) of vertrouwelijke informatie onthult.

— Hoe gaat CEO-fraude te werk?

- Fraudeurs **verzamelen eerst informatie** over de interne betalingsprocedures en de medewerkers van een onderneming die gemachtigd zijn om grote betalingstransacties te verrichten. Ze doen dit door contact op te nemen via e-mail of telefoon en zich uit te geven voor auditors, bedrijfsrevisoren of een overheidsdienst.

- Wanneer de fraudeurs over genoeg informatie beschikken **nemen ze contact op met één of meerdere medewerkers die verantwoordelijk zijn voor betalingen** (bv. de boekhouding) en geven zich uit als CEO. Daarvoor kraken ze meestal de mailbox van de CEO of creëren ze een vals adres dat bijna niet te onderscheiden is van het echte adres van de CEO. Vaak is er dan bijvoorbeeld één lettertje veranderd tegenover het officiële adres. Fraudeurs verzinnen een verhaal waarvoor een grote som geld dringend – en in het grootste geheim – overgeschreven moet worden.

- Soms gaan de fraudeurs nog een stap verder door een consultancybureau of een advocaat (waarvan ze de identiteit hebben aangenomen) te laten tussenkomen. Het bureau of de advocaat gaat de verrichting bevestigen en opnieuw benadrukken dat de betaling dringend en geheim is.

- Fraudeurs maken steeds vaker gebruik van kunstmatige intelligentie om een stem of beeld na te bootsen (telefoongesprek, spraakbericht, videocall) en zich voor te doen als CEO of een andere bertrouwbare persoon.

- Medewerkers die in de val trappen, doen geen betaling voor de echte CEO maar schrijven – zonder het zelf te beseffen – grote sommen geld over naar rekeningen van geldezels. Vanop die rekeningen wordt het geld dan doorgesluisd naar de rekening van de fraudeurs.

TIPS OM ZICH TE WAPENEN TEGEN CEO-FRAUDE

1. Check altijd de domeinnaam in het emailadres van de afzender.
2. Wees waakzaam bij "vertrouwelijke" opdrachten om dringend grote sommen geld over te schrijven.
3. Ontvang je zo'n dringende vraag, bel dan de aanvrager altijd terug op een telefoonnummer dat je kent.
4. Ook al lijkt het verzoek echt te zijn, controleer het altijd via een vertrouwd kanaal. Met AI kan tegenwoordig zelfs een CEO worden geïmiteerd.
5. Laat de dubbele handtekening nooit over aan dezelfde persoon (kaarten en pincodes).
6. Bouw voldoende controlestappen in:
   - Afspreken dat – en al zeker grote - betalingen niet enkel via mail worden doorgegeven maar ook bevestigd worden via een SMS, een WhatsApp-bericht, via telefoon...
   - Een andere persoon aanstellen binnen de onderneming (niet de CEO) bij wie de medewerkers terechtkunnen als er een vertrouwelijke of dringende aanvraag binnenkomt. De aangestelde persoon kan dan bij de CEO nagaan of de aanvraag echt is. Opgelet: niemand buiten de onderneming moet weten wie de aangestelde persoon is.

— Ik ben in de val getrapt. Wat nu?

- Contacteer zo snel mogelijk de bank van uw onderneming.
- Dien een klacht in bij de politie.
- Informeer het ICT-departement van je onderneming indien de mailbox van de CEO gehackt is. Waarschijnlijk hebben de fraudeurs toegang tot heel wat informatie dankzij die mailbox. Paswoorden zullen bv. aangepast moeten worden.

PHISHING

— Wat is phishing?

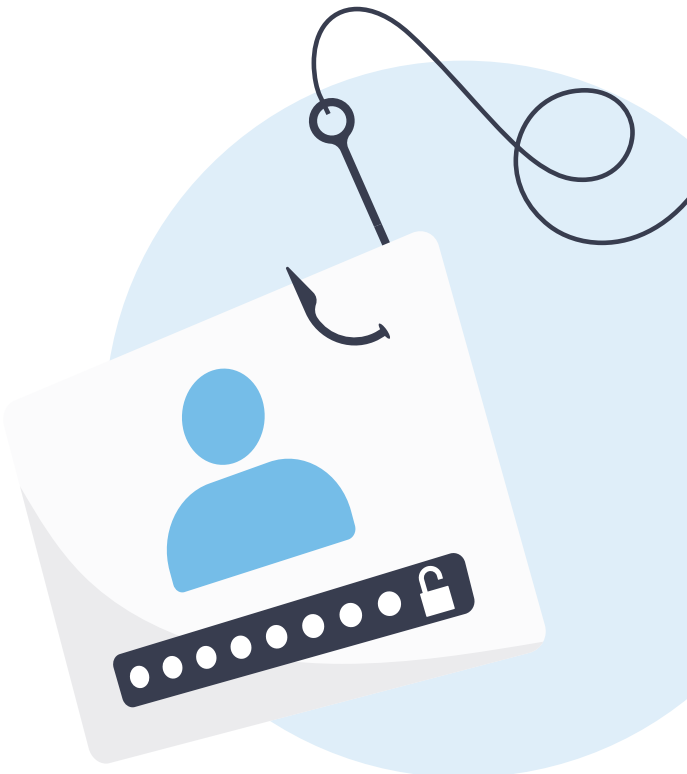
Phishing is een techniek waarmee oplichters jouw persoonlijke codes proberen te bemachtigen, om toegang te krijgen tot jouw online bankomgeving, of om je bepaalde handelingen te laten uitvoeren (via itsme®, een kaartlezer, enz.).
De inhoud van phishingberichten kan sterk variëren. Het kan gaan om een vals bericht (e-mail, WhatsApp, sms, enz.) van je bank, Card Stop, je telefoonprovider, je energieleverancier, de federale overheidsdiensten, enz. Wel omvat dit bericht altijd een link naar een valse website. Klik je hierop en geef je op de valse website de bankgegevens en geheime code van je onderneming in, dan geef je de fraudeurs toegang tot de rekeningen van je onderneming.

TIPS OM JE ONDERNEMING TE BESCHERMEN TEGEN PHISHING

- Geef nooit de codes om te internetbankieren (codes gegenereerd door je kaartlezer) via e-mail, sociale media, sms of telefoon. De codes van je onderneming om te internetbankieren zijn even geheim als de pincode van je bankkaart!
- Ga nooit via een link naar de betaalsite of mobiele app van je bank. Je bank vraagt je nooit naar de codes via een link.
- Typ altijd zélf het adres van de bankwebsite van je onderneming in je browser. Je kan ook het adres (URL) opslaan in je favorietenlijst van je browser. Of open zelf de mobiele app van de bank.
- Als je twijfelt, kan je beter stoppen. Kreeg je dus een vreemd bericht en weet je niet wat gedaan, neem dan het zekere voor het onzekere en stop alles.
- Bekijk zeker eens de gratis module 'Kijk waar je naartoe gaat!' van 'Surfen zonder zorgen' via Safeonweb.be.

— Toch in de val getrapt?

- Neem zo snel mogelijk contact op met de bank van je onderneming. Via speciale fraudenummers is de bank 24/7 bereikbaar om online fraude te melden.
- Heb je je kaartgegeven doorgegeven, verwittig dan Card Stop (www.cardstop.be of 078 170 170).
- Verander je codes.
- Dien klacht in bij de politie.



KLUISREKENINGFRAUDE

Een andere vorm van fraude die in opmars is bij bedrijven, is kluisrekeningfraude. Een schijnbaar betrouwbare afzender (zoals een sociaal secretariaat, de bank, de post, een telefoonoperator...) belt de onderneming of zelfstandige om te waarschuwen dat er verdachte banktransacties op de bedrijfsrekening gebeuren. Schade kan voorkomen worden indien men 'snel' handelt en de gelden overschrijft naar een 'veilige kluisrekening'. Alleen blijkt achteraf dat zo'n 'kluisrekening' niet bestaat en de bedrijfsleider blijft achter met een groot financieel verlies...

Bij deze fraudevorm handelen de oplichters vaak in twee stappen. Ze sturen eerst een phishingbericht om toegang te krijgen tot de bankrekening van de onderneming of zelfstandige. Daarna bellen ze een medewerker van de onderneming of de zelfstandige op en overtuigen hem/haar om geld over te schrijven naar een zogezegd 'veilige kluisrekening.'

— Hoe werkt het?

Kluisrekeningfraude begint vaak met een phishingbericht dat cybercriminelen per e-mail, sms, Whatsapp of sociale media versturen. Dit bericht bevat een link die je naar een valse website brengt. Oplichters gebruiken deze website om persoonlijke informatie te verzamelen zoals bijvoorbeeld contactgegevens of zelfs codes om aan te melden in internetbankieren. Zodra de oplichters over deze gegevens beschikken kunnen ze met hun frauduleuze handelingen beginnen: ze bellen de onderneming of zelfstandige op en doen zich voor als een medewerker van de bank. Ze leggen dan uit dat er verdachte transacties op de rekening zijn verricht.

Vaak slaat men deze stap waarbij men een phishingbericht gebruikt ook over, en bellen oplichters de onderneming of zelfstandige gewoon op met heel veel overtuigingskracht. Ze zullen alles doen om het vertrouwen te winnen.

De oplichters zullen dan aanbieden om het geld over te maken naar een veilige rekening, namelijk de zogenaamde 'kluisrekening'. Maar zo'n type rekening bestaat helemaal niet. En als de medewerker van de onderneming of de zelfstandige toch geld overmaakt naar deze valse 'veilige kluisrekening', komt het terecht op de rekening van een geldezel. Vanaf dan wordt het overgemaakte bedrag in recordtempo doorgesluisd naar de rekening van de cybercriminelen.
Een alternatief scenario is dat de fraudeur de 'annulering van frauduleuze overschrijvingen' laat bevestigen door de gedupeerde terwijl deze in feite net de frauduleuze overschrijvingen tekent.

TIPS OM JE ONDERNEMING TE BESCHERMEN

1. Geef nooit persoonlijke informatie en/of bankcodes van de onderneming (rekeningnummer, pincode, responsecode) door via e-mail, sms, telefoongesprek, een bericht op social media of WhatsApp. De bank - of elke andere organisatie - zal nooit een dergelijk verzoek doen via telefoon, e-mail, sms of sociale media.
2. Evenmin zal de bank adviseren om het geld van de onderneming over te maken naar een rekening van een andere partij. Een veilige 'kluisrekening' bestaat niet!
3. Ook zal de bank je nooit vragen om software (AnyDesk, TeamViewer) te installeren om vanop afstand je computer over te nemen.
4. Ontving je een raar bericht of een vreemde oproep en twijfel je over de echtheid? Neem dan het zekere voor het onzekere ga hier niet op in. Laat je niet onder druk zetten en overhalen om 'snel' te handelen. Wil je meer info? Bel dan zelf naar de bank. Oplichters kunnen die oproep namelijk niet onderscheppen, maar ze kunnen immers wel een nummer van de bank 'spoofen' en je zelf met dat nummer opbellen.

— Toch in de val getrapt?

- Neem zo snel mogelijk contact op met de bank van je onderneming. Via speciale fraudenummers is de bank 24/7 bereikbaar om online fraude te melden.
- Verwittig Card Stop (078 170 170).
- Dien klacht in bij de politie.

BANKHELPDESKFRAUDE

— Wat is bankhelpdeskfraude?

Bij deze vorm van fraude worden ondernemers opgebeld door oplichters die zich voordoen als een bankmedewerker. Ze overtuigen ondernemers om hun computerscherm van op afstand te laten overnemen en vragen hun persoonlijke codes op of verzoeken hen om bepaalde handelingen uit te voeren (bv. via itsme®). Zo slagen de oplichters erin om grote sommen geld te stelen. Deze fraudevorm is in opmars en kan leiden tot grote financiële schade op korte tijd.

— Hoe gaat het in zijn werk?

Meestal krijgt de ondernemer een telefoontje van een zogenaamde medewerker (van de fraudeafdeling) van zijn/haar bank die waarschuwt dat er zopas verdachte transacties op de rekening van de onderneming werden gedetecteerd. De fraudeur overtuigt de ondernemer van de dringende situatie en geeft advies om erger te voorkomen.

Zodra het slachtoffer mee is in het verhaal wordt gevraagd om geld over te maken naar (niet-bestaande) 'veilige rekeningen', ofwel om samen met de zogenaamde 'bankmedewerker' (niet-bestaande) frauduleuze overschrijvingen te annuleren.

Oplichters zullen ook vragen om software te installeren (AnyDesk, TeamViewer...) waarmee de zogenaamde 'bankmedewerker' de ondernemer kan helpen. Op die manier krijgt de fraudeur de volledige controle over de computer of smartphone van het slachtoffer. Hij/zij bepaalt wat de ondernemer kan zien en wat niet en kan dus in naam van de bedrijfsklant online bankieren en overschrijvingen (laten) uitvoeren vanaf de professionele en privérekeningen van het slachtoffer. De ondernemer ondertekent deze overschrijvingen, denkende dat deze naar veilige rekeningen gaan of hij/zij deze overschrijvingen aan het annuleren is.

TIPS OM JEZELF EN JE ONDERNEMING TE BESCHERMEN

1. Wanneer je wordt opgebeld door een bankmedewerker die je vraagt om software te installeren zodat hij/zij je computer kan overnemen, ga hier dan niet op in en beëindig meteen het gesprek!
2. Je kan ook als onderneming beslissen dat jouw medewerkers geen software mogen installeren.
3. Neem de nodige maatregelen: informeer je collega's, vrienden of werknemers hierover zodat ze zich beter kunnen wapenen tegen deze fraudevorm.

— Toch in de val getrapt?

- Neem zo snel mogelijk contact op met de bank van je onderneming. Via speciale fraudenummers is de bank 24/7 bereikbaar om online fraude te melden.
- Verwittig Card Stop (078 170 170).
- Dien klacht in bij de politie.

Enkele best practices op het gebied van online betalen in een onderneming:

— Goed beheer van de dubbele handtekening

De dubbele handtekening is een manier om fraude te voorkomen. De persoon die de tweede handtekening plaatst, staat los van de transactie en zal de fraude sneller opmerken.

— Verstandig gebruik van volmachten op de rekeningen

Elke mandataris moet een eigen toegang tot de bedrijfsrekeningen hebben. Wanneer hij een elektronische toegang tot de bedrijfsrekeningen deelt met een andere persoon, deelt hij immers niet alleen zijn volmachten maar geeft hij ook toegang tot zijn privérekeningen. Een eigen toegang is veiliger voor het bedrijf en ook voor de medewerker zelf, die zo enkel de transacties kan uitvoeren die gekoppeld zijn aan zijn of haar volmachten.

Nog enkele belangrijke tips om jouw onderneming te beschermen:

• Maak je medewerkers bewuster van de risico's
Geef je medewerkers regelmatig opleidingen over de risico's van fraude (phishing, CEO-fraude, factuurfraude, enz.). Medewerkers vormen vaak de eerste verdedigingslinie.

• Zorg voor duidelijke procedures
Stel interne processen op voor betalingen (dubbele validatie, scheiding van taken, controle van wijzigingen in bankgegevens, enz.).

• Controleer gevoelige verzoeken systematisch
Bij dringende of ongebruikelijke verzoeken (betaling, wijziging van rekening, enz.), sporen we je aan om altijd navraag te doen via een bekend kanaal of bij een vertrouwenspersoon.

• Beperk toegangen en beveilig programma's/tools
Beperk de toegang tot gegevens en systemen uitsluitend tot de personen die dit nodig hebben, en gebruik sterke authenticatiemethoden.

• Houd je systemen up-to-date
Installeer regelmatig beveiligingsupdates en gebruik beveiligingsoplossingen (antivirus, firewall, enz.).

• Wees voorbereid om te reageren in geval van een incident
Zorg voor een interne procedure in geval van fraude of een cyberincident (wie te contacteren, welke acties te ondernemen, enz.).

• Maak gebruik van betrouwbare tools en hulpmiddelen
Het Safeonweb@work-platform van het Centrum voor Cybersecurity België biedt gratis tools, advies en waarschuwingen om bedrijven te helpen cyberdreigingen te identificeren en te beperken.

• Beoordeel regelmatig je niveau van cyberbeveiliging
Met zelfbeoordelingstools kun je je zwakke punten opsporen en je beveiligingsmaatregelen verbeteren.

SLOTWOORD

Elke onderneming kan slachtoffer worden van fraude. Fraude kan talloze vormen aannemen maar gelukkig kunnen ook heel wat stappen ondernomen worden om jouw bedrijf en de medewerkers hiertegen te beschermen. Het blijft van essentieel belang om waakzaam te blijven en de gepaste maatregelen te treffen om fraudeurs buitenspel te zetten.

Koning Albert II-laan 19, 1210 Brussel

www.febelfin.be