

FINANCIËLE FRAUDE EN ONDERNEMINGEN



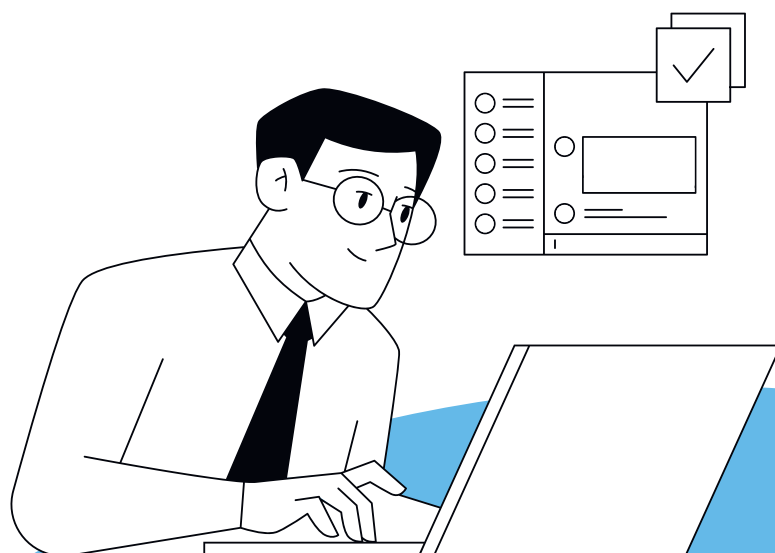
Hoe fraude
voorkomen en
herkennen?

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

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

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

Ontdek in deze brochure 3 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 financiële fraude. 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.

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.
- 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.



— 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 op meldpunt.belgie.be (optie “vervalste factuur”). Op het einde van je melding krijg je meteen advies over welke stappen je nog kan ondernemen, en wie je daarbij kan helpen.



REAGEER SNEL

Als je fraude vaststelt nadat een overschrijving is uitgevoerd, breng dan onmiddellijk je bank op de hoogte. Een overzicht van alle contactpunten kan je terugvinden op www.cardstop.be/content/cardstop-be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html.

Als je de bank snel verwittigt, is de kans groter dat het gestolen geld teruggevonden wordt. Je moet eventueel ook andere formaliteiten vervullen bij de bevoegde instanties (klacht indienen 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.
- 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.

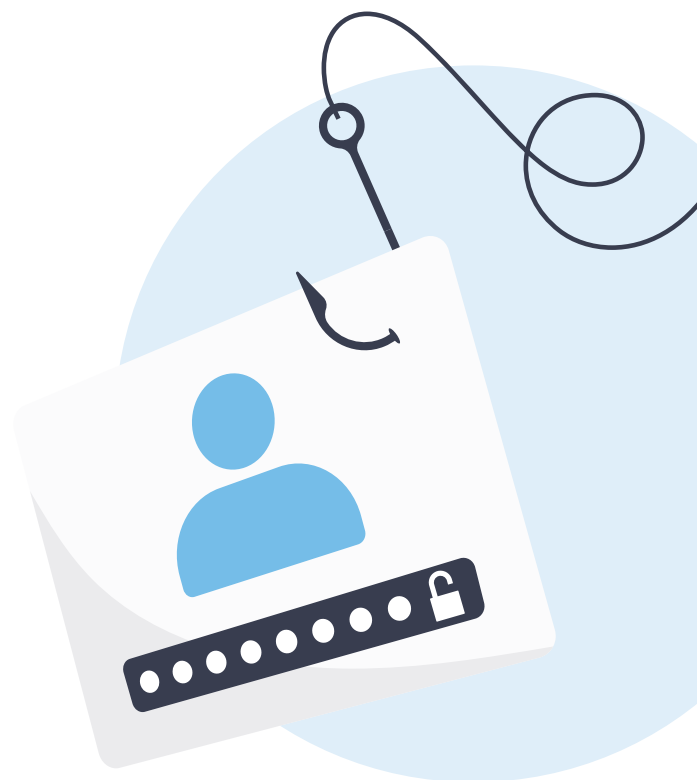


TIPS OM ZICH TE WAPENEN TEGEN CEO-FRAUDE

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. Laat de dubbele handtekening nooit over aan dezelfde persoon (kaarten en pincodes)
5. 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 terecht kunnen 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 waarbij oplichters proberen te hengelen naar je persoonlijke codes, die toegang geven tot je online bankomgeving. De inhoud van phishingberichten kan sterk verschillen. Het kan gaan om een vals bericht (e-mail, WhatsApp, SMS...) van je bank om je bankkaart te vernieuwen, je telefoonoperator over een probleem met

de betaling van je abonnement, van de FOD Financiën die je een premie belooft, 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 internet-bankieren (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.

— 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. Een overzicht van alle contactpunten kan je terugvinden op www.cardstop.be/content/cardstop-be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html/
- Heb je je kaartgegevens doorgegeven, verwittig dan Card Stop (www.cardstop.be of 078 170 170).
- Verander je codes.
- Dien klacht in bij de politie.

Nog 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. Laat beide handtekeningen nooit over aan dezelfde persoon en controleer alles wat u ondertekent.

— 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, 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.

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.



Disclaimer: Deze brochure is louter informatief en Febelfin kan niet aansprakelijk worden gesteld voor schade die voortvloeit uit het raadplegen of het gebruik van de verstrekte informatie.



Koning Albert II-laan 19, 1210 Brussel

www.febelfin.be