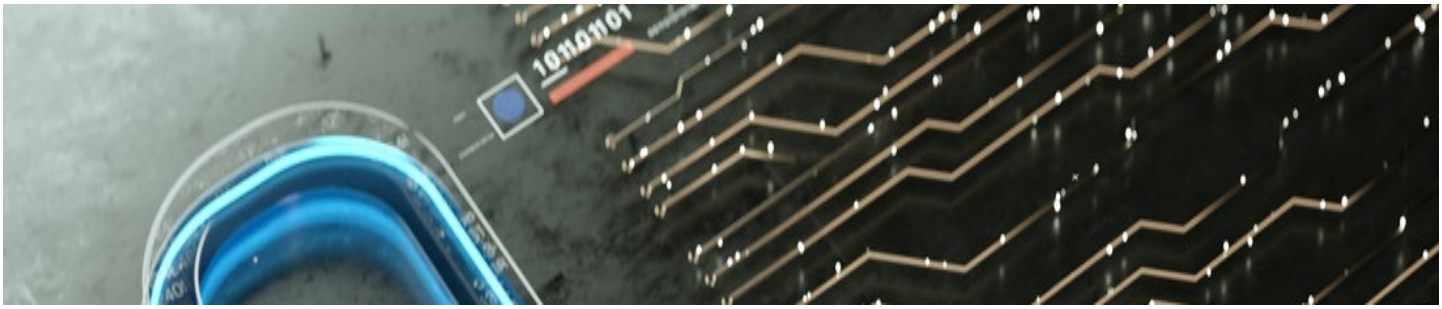

CEO/BEC-fraude

PDF Versie

Wat is CEO/BEC-fraude ?

Een personeelslid van een bedrijf (bv. de secretaresse van de baas, de boekhouder, enz.) wordt telefonisch of via e-mail benaderd door een persoon die zich voordoet als een van de managers of werknemers van het bedrijf, met het verzoek namens hen een dringende financiële transactie uit te voeren.

CEO-fraude, ook wel whaling genoemd, is een vorm van spear-phishing, wat gericht phishing betekent.

De oplichter geeft zich uit als CEO, CFO of een andere vertrouwenspersoon van het bedrijf, en probeert in contact te komen met een medewerker die betalingen mag uitvoeren. Hij zal deze medewerker proberen misleiden en vragen om een belangrijke en dringende betaling vanaf de bedrijfsrekening uit te voeren.

Bij dergelijke feiten wordt de mailbox van de CEO *gespooft* (vervalst) of gehackt, of maakt men een vals e-mailadres aan dat bijna niet te onderscheiden is van het echte. Er is dan bijvoorbeeld één lettertje anders.

Medewerkers die in de val trappen, doen geen betaling voor de echte CEO maar schrijven, zonder het zelf te beseffen, geld over naar rekeningen gebruikt door de criminelen.

Wat heb je nodig om klacht neer te leggen?

Wat de communicatie met de dader(s) betreft:

- Gedetailleerde en chronologische beschrijving van de gesprekken en handelingen uitgevoerd op verzoek van de oplichter.
    - **Wat betreft de e-mails:**
        - E-mailadres gebruikt door de oplichter;
        - Uw e-mailadres;
        - Datum en tijdstip van ontvangst van de verdachte e-mails;
        - Inhoud van de uitgewisselde e-mails (af te drukken en bij uw verklaring te voegen) en technische header van de e-mails (https://mxtoolbox.com/public/content/emailheaders/);
        - URL (internetadres) van alle links in de e-mail van de oplichter, indien aanwezig.
    - **Wat de telefoontjes betreft:**
        - Het oproepnummer gebruikt door de oplichter;
        - Indien het oproepnummer niet bekend is: noteer de tijd en het oproepnummer waarop u werd gecontacteerd;
        - Uw telefoonnummer;
        - Datum en tijd van telefoongesprek(en);
        - Mogelijke opnames van telefoongesprekken;

Wat betreft banktransacties:

- Alle beschikbare informatie over verrichte betalingen
    - Bankrekeningnummer waarop de betaling werd verricht
    - Datum en tijdstip van de transactie(s)
    - Betaald bedrag
    - Documenten met betrekking tot de betaling (facturen, betalingsopdracht, mandaat...)

Wat kan je nog doen?

Heeft er reeds een betaling/transactie plaatsgevonden? Neem onmiddellijk contact op met uw bank om de transactie te onderscheppen, als dat nog mogelijk is.

Waarschuw al uw werknemers, zodat niemand anders in de val loopt. Fraudeurs beperken zich immers niet altijd tot één enkel contact en één enkele transactie.

Neem altijd contact op met de politie in geval van een poging tot oplichting, ook als u niet in de val bent gelopen.

Hoe vermijd je om opnieuw slachtoffer te worden?

Preventie en voorzichtigheid zijn de meest doeltreffende manieren om dit soort misdrijven te bestrijden.

Als onderneming:

- Zorg ervoor dat medewerkers op de hoogte en bewust zijn van de risico's.
- Moedig je personeel aan om voorzichtig te zijn met betalingsverzoeken.
- Voer interne protocollen in voor betalingen.
- Voer een controleprocedure in voor per e-mail ontvangen betalingsverzoeken.
- Controleer informatie op je bedrijfswebsite, beperk de informatie en wees voorzichtig met sociale media.

Als medewerker:

- Volg strikt de bestaande beveiligingsprocedures voor betalingen en aanbestedingen. Sla geen stappen over en geef niet toe aan druk.

- Controleer e-mailadressen altijd zorgvuldig bij gevoelige informatie/overschrijvingen.

- Als u twijfelt over een betalingsopdracht, neem dan contact op met de persoon die de opdracht geeft op zijn gebruikelijke nummer. Bij voorkeur probeert u fysiek in contact te komen. Lukt dat niet, opteer dan voor een videogesprek. Is dat ook niet mogelijk, ga dan voor een telefonisch contact.

- Neem via video/telefonisch contact op met de dienst of organisatie en controleer of de communicatie legitiem is alvorens te antwoorden.

- Open geen verdachte, onverwachte of ongevraagde e-mails (en de koppelingen, bijlagen die ze bevatten) van een onbekende afzender of van een bekende afzender, maar waarvan de berichtenstructuur ongebruikelijk lijkt.

- Beperk het delen van informatie over je werkgever en wees voorzichtig met sociale media.

- Deel geen informatie over de hiërarchie, veiligheid of procedures van het bedrijf.

- Ontvang je een verdachte mail of telefoonoproep, verwittig dan altijd je IT-afdeling.

Waar vind je meer informatie?

https://www.safeonweb.be/nl/actueel/opnieuw-meer-ceo-fraude