CEO-FRAUDE

Bij CEO-fraude wordt een medewerker die betalingen mag verrichten, door fraudeurs misleid om een valse factuur te betalen of ongeoorloofd geld van de bedrijfsrekening over te schrijven.

HOE WERKT HET?

De fraudeur belt of mailt en doet zich voor als iemand met een hoge functie binnen het bedrijf (bv. CEO, CFO).

De fraudeur kent de organisatie goed.

Hij vraagt een dringende betaling.

Hij gebruikt taal zoals: 'Dit is vertrouwelijk', 'Het bedrijf vertrouwt je', 'De CEO/ CFO is momenteel niet beschikbaar'.

Hij verwijst naar een gevoelige situatie (bijvoorbeeld belastingcontrole, fusie, overname).

De werknemer wordt gevraagd de gewone toelatingsprocedures niet te volgen.

Een derde persoon kan later nog eens bellen of mailen met verdere instructies.

De werknemer schrijft het geld over op een rekening die de fraudeur beheert.

Vaak worden er internationale betalingen gevraagd aan banken buiten Europa.

HOE HERKEN JE HET?

- Ongevraagde e-mail/telefoonoproep
- Rechtstreeks contact met een hooggeplaatst persoon met wie je normaal geen contact hebt
- Vraag om absolute geheimhouding
- Druk en klemtoon op dringendheid
- Ongewone vraag in strijd met interne procedures
- Bedreigingen of ongewone vleierij/beloften

WAT KAN JE DOEN?

ALS BEDRIJF

Ken de risico's en zorg ervoor dat **medewerkers zich daar ook bewust van zijn.**

Moedig je personeel aan om **voorzichtig te zijn met betalingsverzoeken.**

Voer interne protocollen in voor betalingen.

Voer een controleprocedure voor betalingsverzoeken die per e-mail toekomen.

Stel **meldingsroutines** vast om fraude te bestrijden.

Controleer en beperk de informatie op je bedrijfswebsite en **wees voorzichtig** met sociale media.

Upgrade en update je technische beveiliging.

Contacteer steeds de politie bij fraudepogingen, zelfs als je niet in de val bent getrapt.

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.

Bij twijfel over een betalingsopdracht, **raadpleeg een bevoegde collega.**

Open nooit verdachte links of bijlagen in e-mails. Wees vooral voorzichtig wanneer je je persoonlijke e-mail nakijkt op de bedrijfscomputers.

Beperk informatie over je bedrijf en wees voorzichtig met sociale media.

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

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

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Politie Police | febelfin | Cyber Security Coalition | #CyberScams