CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

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

HOE WERKT HET?

De fraudeur belt of mailt en doet zich voor als hooggeplaatst persoon binnen het bedrijf (bv. CEO, CFO).

Ze kennen de organisatie goed.

Ze willen een dringende betaling.

Zij gebruiken taal zoals: 'Vertrouwelijkheid', 'Het bedrijf vertrouwt je', 'Momenteel niet beschikbaar'.

Vaak wordt er gevraagd om internationale betalingen aan banken buiten Europa.

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

Instructies over de verdere stappen kunnen later worden gegeven, door een derde persoon of via e-mail.

De werknemer wordt gevraagd de gewone toelatingsprocedures niet te volgen.

Ze verwijzen naar een gevoelige situatie (bijvoorbeeld belastingcontrole, fusie, overname).

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 gevoel van 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 ook op de hoogte en bewust zijn.**

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.

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

Controleer informatie op je bedrijfswebsite, **beperk de informatie 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 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.

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