CEO/BUSINESS EMAIL COMPROMISE (BEC) SVINDEL

CEO/BEC svindel opstår, når en medarbejder, bliver narret til at betale en falsk faktura eller foretage en uautoriseret overførsel med virksomhedskontoen.

HVORDAN FOREGÅR DET?

En bedrager ringer eller mail'er og udgiver sig for at være en højtstående person inden for virksomheden (fx CEO eller CFO).

De har et godt kendskab til organisationen.

De kræver en hasteoverførsel.

De bruger sprog som: "Fortrolighed", "Virksomheden stoler på dig", "Jeg er i øjeblikket utilgængelig".

Ofte er anmodningen om internationale betalinger til banker uden for Europa.

Medarbejderen overfører pengene til en konto, der kontrolleres af svindleren.

Instruktioner om det videre forløb kan gives senere af en tredje person eller via e-mail.

Medarbejderen anmodes om ikke at følge de almindelige godkendelsesprocedurer.

De henviser til en følsom situation (fx skattekontrol, fusion, virksomhedsovertagelse).

HVAD ER FARESIGNALERNE?

- Uopfordret e-mail/telefonopkald
- Presserende og hastende karakter
- Direkte kontakt fra en person i den øverste ledelse, du normalt ikke er i kontakt med
- Usædvanlig anmodning i strid med interne procedurer
- Anmodning om absolut fortrolighed
- Trusler eller usædvanlig smiger/løfter om belønning

HVAD KAN DU GØRE?

SOM EN VIRKSOMHED

Vær opmærksom på risiciene og sørg for, at **medarbejderne også er informerede og opmærksomme.**

Opfordre dine medarbejdere til at **håndtere betalingsanmodninger med forsigtighed.**

Implementer interne forretningsgange vedrørende betalinger.

Implementer en procedure for kontrol af legitimiteten af betalingsanmodninger modtaget via e-mail.

Etabler **rapporteringsrutiner** til håndtering af bedrageri.

Gennemgå informationer, der er publiceret på din virksomheds hjemmeside, **begræns informationer og vær forsigtig med hensyn til sociale medier.**

Opgrader og opdater teknisk sikkerhed.

Kontakt altid politiet i alle tilfælde af forsøg på svindel, også selvom du ikke blev offer for svindel.

SOM MEDARBEJDER

Overhold de foreskrevne sikkerhedsprocedurer for betalinger og indkøb. **Spring ikke over nogle trin, og giv ikke efter for pres.**

Kontroller altid e-mail adresser grundigt, når du håndterer følsomme oplysninger/pengeoverførsler.

I tilfælde af tvivl om en overførselsordre, **inddrag altid en kompetent kollega.**

Åben aldrig mistænkelige links eller vedhæftede filer modtaget via e-mail. Vær særlig forsigtig, når du åbner dine private e-mails på virksomhedens computere.

Vær forsigtig, hvis du deler oplysninger på sociale medier.

Undgå at dele oplysninger om virksomhedens hierarki, sikkerhed eller procedurer.

Hvis du modtager en mistænkelig e-mail eller et opkald, skal du altid informere din it-afdeling.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITI | FINANS DANMARK

#CyberScams