DIREKTØRSVINDEL

Direktørsvindel, også kalt CEO-svindel eller BEC-svindel (Business Email Compromise), innebærer at en ansatt med myndighet til å foreta betalinger lures til å betale en falsk faktura eller foreta en uautorisert overføring fra bedriftens konto.

HVORDAN FUNGERER DET?

En svindler ringer eller sender en e-post og utgir seg for å være en person i ledelsen (f.eks. administrerende direktør eller økonomidirektøren).

Vedkommende har god kjennskap til organisasjonen.

Den ansatte bes om å foreta en hastebetaling.

Svindleren bruker ord som "konfidensielt", "bedriften stoler på deg" og "jeg er ikke tilgjengelig akkurat nå".

Det vises til en sensitiv situasjon (f.eks. skattekontroll, sammenslåing eller oppkjøp).

Forespørselen gjelder ofte betaling til banker utenfor Europa.

Den ansatte overfører pengene til en konto svindleren kontrollerer.

Instruksjoner om hvordan betalingen skal gjøres, kommer kanskje senere, fra en tredjeperson eller på e-post.

Den ansatte bes om ikke å følge de vanlige godkjenningsrutinene.

FARESIGNALER

- Du får en uventet e-post eller oppringning.
- En leder du vanligvis ikke har kontakt med, tar direkte kontakt med deg.
- Personen ber deg om absolutt fortrolighet.
- Du opplever press og at det haster.
- Forespørselen er uvanlig og ikke i tråd med bedriftens rutiner.
- Du mottar trusler, utsettes for uvanlig smiger eller får løfter om belønning.

HVA KAN DU GJØRE?

SOM VIRKSOMHET

Vær oppmerksom på risikoen, og sørg for at **de ansatte også er informert og på vakt.**

Oppfordre de ansatte til å **håndtere betalingsforespørsler med aktsomhet.**

Iverksett interne prosedyrer som skal følges ved betalinger.

Iverksett en rutine for å kontrollere at betalingsforespørsler som sendes på e-post, er ekte.

Få på plass **rutiner for å rapportere** om svindel.

Vurder hvilken informasjon som ligger på virksomhetens nettsider. **Begrens hva som deles, og vær bevisst** ved bruk av sosiale medier.

Oppgrader og oppdater den tekniske sikkerheten.

Kontakt alltid politiet ved svindelforsøk, også når du ikke lot deg lure.

SOM ANSATT

Følg sikkerhetsrutinene for betalinger og innkjøp til punkt og prikke. **Ikke hopp over noen trinn, og ikke gi etter for press.**

Sjekk alltid e-postadresser nøye når det dreier seg om sensitive opplysninger eller pengeoverføringer.

Er du i tvil om en bestemt forespørsel, **rådfør deg med en erfaren kollega.**

Åpne aldri mistenkelige lenker eller vedlegg du har fått på e-post. Vær spesielt forsiktig når du sjekker privat e-post på arbeidsgivers datamaskiner.

Begrens hva som deles, og vær bevisst ved bruk av sosiale medier.

Unngå å dele informasjon om hvordan virksomheten er organisert, sikkerhetstiltakog rutiner.

Informer IT-avdelingen om du mottar en mistenkelig e-post eller telefonoppringning.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIET KRIPOS | NorSIS Norsk senter for informasjonssikring | mnemonic SECURING YOUR BUSINESS | #CyberScams