# BEC-HUIJAUS (BUSINESS EMAIL COMPROMISE)

BEC-huijauksessa yrityksen rahaliikenteestä huolehtiva työntekijä huijataan maksamaan valelasku tai tekemään muu siirto yrityksen varoista.

## KUINKA BEC-HUIJAUS TOIMII?

Huijari soittaa tai lähettää sähköpostia, jossa esiintyy yrityksen korkea-arvoisena henkilönä, kuten toimitusjohtajana.

Huijarilla on paljon tietoa yrityksestä, jonka nimissä esiintyy.

Huijari kertoo tarvitsevansa kiireellisen maksusuorituksen.

Huijari vetoaa esimerkiksi salassapitoon, uhrin luotettavuuteen, tai siihen ettei itse juuri nyt pysty hoitamaan asiaa.


Varoja pyydetään usein Euroopan ulkopuoliseen pankkiin.

Jos huijaus onnistuu, työntekijä siirtää varat huijarin hallitsemalle tilille.

Toimintaohjeet saatetaan antaa myöhemmin sähköpostitse tai kolmannen henkilön toimesta.

Työntekijää pyydetään ohittamaan tavanomaiset valtuutuskäytännöt.

Huijari voi vedota arkaluontoiseen tilanteeseen, kuten yrityskauppoihin tai tilintarkastukseen.

## TUNNUSMERKIT

- Pyytämättä saatu sähköposti/puhelinsoitto
- Suora yhteydenotto korkea-arvoiselta henkilöltä, johon uhri ei normaalisti ole yhteydessä
- Pyyntö luottamuksellisuudesta
- Kiireen tuntu, painostus
- Epätavallinen pyyntö, joka on ristiriidassa yrityksen sisäisten käytäntöjen kanssa
- Puhetta ylimääräisistä korvauksista, imartelua tai uhkailua

## MITÄ VOIT TEHDÄ?

### YRITYKSENÄ

Olkaa tietoisia riskeistä, ja varmistakaa että **työntekijät ovat myös.**

Kannustakaa työntekijöitä s**uhtautumaan maksupyyntöihin varauksella.**

**Noudattakaa vakiintuneita käytäntöjä laskutukseen ja maksuihin liittyen.**

**Laatikaa tarkistuskäytännöt,** joilla varmistetaan sähköpostitse saapuvien maksujen oikeellisuus.

Laatikaa raportointikäytännöt petosten ehkäisemiseksi.

Tarkastakaa yrityksen sivuilla näkyvät tiedot, ja rajoittakaa liian yksityiskohtaisen tiedon levittämistä, etenkin somessa.

**Pitäkää yrityksenne laitteisto ja tietoturva ajan tasalla.**

Ottakaa petostapauksissa aina yhteyttä poliisiin, vaikka välttäisittekin huijauksen.

### TYÖNTEKIJÄNÄ

Noudata aina yrityksesi maksamiseen liittyviä ohjeita. **Älä ohita mitään vaiheita painostuksesta huolimatta.**

**Tarkista sähköpostiosoitteet huolellisesti aina,** kun kyseessä on rahojen siirto tai arkaluonteinen tieto.

Mikäli epäilyksiä herää, **keskustele asiasta pätevän kollegan kanssa.**

**Älä avaa epäilyttäviä linkkejä tai liitetiedostoja sähköpostista.** Ole erityisen varovainen kun katsot yksityistä sähköpostiasi yrityksen tietokoneilla.

**Rajoita tarpeetonta tiedon leviämistä** somessa.

**Älä jaa ulkopuolisille tietoa** yrityksen hierarkiasta, tietoturvasta tai menettelytavoista.

Jos saat epäilyttävän sähköpostin tai puhelinsoiton, ota yhteyttä yrityksesi IT-osastoon.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLIISI POLICE OF FINLAND | FINANSSIALA | Finnish Communications Regulatory Authority National Cyber Security Centre

#CyberScams