BEC-HUIJAUS (BUSINESS EMAIL COMPROMISE)

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

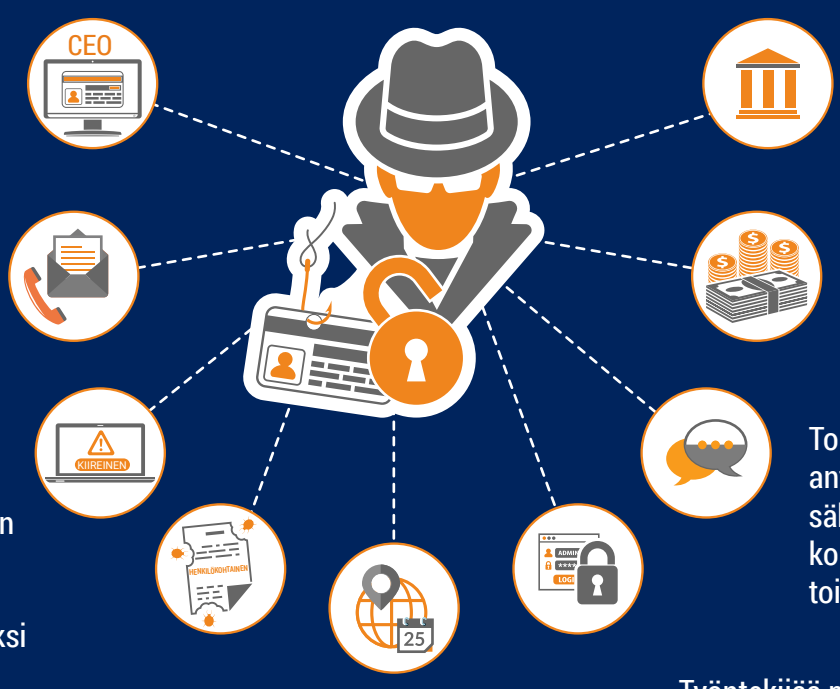
KUINKA BEC-HUIJAUS TOIMII?

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.

Huijari voi vedota arkaluontoiseen tilanteeseen, kuten yrityskauppoihin tai tilintarkastukseen.

Työntekijää pyydetään ohittamaan tavanomaiset valtuutuskäytännöt.

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 **suhtautumaan 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

SIJOITUSHUIJAUKSET

Sijoitushuijaus voi olla houkutteleva sijoitustarjous esimerkiksi osakkeisiin, joukkolainoihin, kryptovaluuttaan, metalleihin tai vaihtoehtoisiin energiamuotoihin.

TUNNUSMERKIT

- Sinulle lupaillaan nopeita tuottoja turvallisilla sijoituksilla.
- Tarjous on voimassa vain vähän aikaa.
- Sinuun otetaan pyytämättä yhteyttä, usein toistuvasti.
- Tarjous on vain sinulle, ja sinua pyydetään olemaan jakamatta sitä.

MITÄ VOIT TEHDÄ?

- **Pyydä aina puolueetonta neuvoa** ennen kuin teet sijoituksia tai muuten luovutat rahaa.
- **Torju sijoitustarjoukset** ennestään tuntemattomilta tahoilta.
- **Suhtaudu varauksella tarjouksiin, joissa luvataan** turvallinen sijoitus sekä varmat ja suuret tuotot.
- **Jos olet aiemmin joutunut huijatuksi, varo tulevia huijauksia.** Huijarit voivat yrittää uudestaan ja myydä tietosi muille huijareille.
- **Ota yhteyttä poliisiin** jos olet epävarma.

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

HUIJAUSLASKUT

MITEN LASKUHUIJAUKSET TOIMIVAT?

- Yritykseen tulee yhteydenotto, joka on olevinaan tavarantoimittajalta/palveluntarjoajalta/lainanantajalta.
- Yhteydenotto voi tulla useammallakin tavalla (puhelin, sähköposti, kirje, ym.).
- Huijari pyytää muutosta jonkin toistuvan maksun tietoihin mm. maksunsaajan osalta. Uusi tili on huijarin hallitsema.

MITÄ VOIT TEHDÄ?

YRITYKSENÄ

Varmistakaa, että **työntekijänne ovat tietoisia** tällaisista huijauksista.

Ohjeistakaa laskuja käsitteleviä henkilöitä **aina tarkistamaan, ettei laskuissa ole mitään epätavallista.**

Ottakaa käyttöön **laskun aitouden vahvistavat menettelyt.**

Käykää läpi yrityksenne nettisivuilla näkyvät tiedot, etenkin tavarantoimittajat ja sopimukset. Varmistakaa, etteivät työntekijänne jaa yrityksen tietoja tarpeettomasti somessa.

TYÖNTEKIJÄNÄ

Tarkista kaikki laskuttajilta saapuvat muutospyynnöt, etenkin jos ne koskevat maksutietoja.

Määrittele maksuille raja, jonka ylittyessä vastaanottaja ja pankki on vahvistettava tiettyä menettelyä noudattaen (esimerkiksi tapaamisella).

Älä käytä muutosta pyytävässä kirjeessä/sähköpostissa olleita yhteystietoja, vaan käytä aiempia, vahvistettuja yhteystietoja viesteistä, jotka tiedät aidoiksi.

Kun lasku on maksettu, **lähetä vastaanottajalle tiedonanto sähköpostitse**. Sisällytä siihen vastaanottajan pankin nimi ja tilin neljä viimeistä numeroa.

Käytä **vakituista yhteyshenkilöä/-tahoa** sellaisten yritysten kanssa, joille lähetät toistuvia maksuja.

Rajoita yrityksestä somessa jakamaasi tietoa.

Tee petosyrityksestä aina ilmoitus poliisille, vaikket olisikaan joutunut sen uhriksi.

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

#CyberScams

NETTIKAUPPAHUIJAUKSET

Netistä saa usein hyviä tarjouksia, mutta varo huijauksia.

MITÄ VOIT TEHDÄ?

- **Käytä kotimaisia vähittäismyyjiä** jos voit – mahdolliset ongelmatilanteet on helpompi ratkaista.
- **Tarkista muiden käyttäjien arviot** ja niiden aitous ennen ostamista.
- **Käytä luottokorttia –** voit saada rahasi takaisin helpommin.
- **Maksa vain turvallisen maksupalvelun kautta.** Harkitse uudemman kerran jos myyjä esimerkiksi pyytää tilisiirtoa.
- **Maksa vain turvallisella internet-yhteydellä** – älä maksa avoimien verkkojen kautta.
- Maksa vain turvallisilla laitteilla – **pidä käyttöjärjestelmäsi ja tietoturvasi ajan tasalla.**

- Varo suuria lupauksia – **jos tarjous kuulostaa liian hyvältä ollakseen totta, se luultavasti on.**
- Mainos, jonka mukaan voitit juuri jonkin palkinnon? **Älä klikkaa,** voit voittaa korkeintaan haittaohjelmia.
- Jos tilaamasi tuote ei saavu perille, ota yhteyttä myyjään. Jos myyjä ei vastaa, ota yhteyttä pankkiisi.

! Tee petosyrityksestä aina ilmoitus poliisille, vaikket olisikaan joutunut sen uhriksi.

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

#CyberScams

(TIETOJEN)KALASTELUVIESTIT

Kalasteluviestit ovat sähköposteja, joilla pyritään saamaan vastaanottajalta käyttäjätunnuksia, pankkitietoja tai muita henkilökohtaisia tietoja.

MITEN KALASTELUVIESTIT TOIMIVAT?

Kalasteluviestit voivat:

Näyttää samanlaisilta kuin oikeiden pankkien viestit.

kopioida pankkien logoja ja sähköpostien sanamuotoja.

pyytää sinua avaamaan linkin tai liitetiedoston.

antaa ymmärtää, että tilanne on kiireellinen.

MITÄ VOIT TEHDÄ?

- **Pidä ohjelmistosi päivitettynä** – niin selain, virustorjunta kuin käyttöjärjestelmäkin.
- **Ole erityisen tarkkana** jos "pankki" kysyy sähköpostitse yksityisiä tietoja kuten salasanaa.
- **Tarkista lähettäjän osoite huolella.** Epämääräinen osoite ja huono suomen kieli ovat huijauksen merkkejä.
- **Älä vastaa epäilyttävään viestiin.** Voit lähettää sen pankille tiedoksi kirjoittamalla pankin osoitteen itse.
- **Älä avaa sähköpostista linkkejä tai liitetiedostoja.** Käytä pankin sivuja omista kirjanmerkeistäsi tai kirjoittamalla osoite itse.
- Epäselvissä tapauksissa **voit kysyä** asiaa pankistasi tai hakea tietoa pankin sivuilta.

Nettihuijaus perustuu siihen, että ihmiset ovat kiireisiä. Viestit voivat vaikuttaa aidoilta jos niitä vilkaisee vain pikaisesti.

Ole tarkkana käyttäessäsi mobiililaitteita. Huijauksen huomaaminen saattaa olla niillä hankalampaa.

#CyberScams

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

DEITTIHUIJAUS

Huijarit etsivät uhreja yleensä seuranhakupalveluista, mutta voivat ottaa yhteyttä myös somessa tai sähköpostitse.

TUNNUSMERKIT

Hiljattain netissä tapaamasi henkilö kertoo olevansa hyvin kiinnostunut ja haluaa yhteystietosi.

Viestit ovat usein huonosti kirjoitettuja ja epämääräisiä.

Henkilön profiili ei täsmää siihen, mitä hän kertoo itsestään.

Sinulta voidaan pyytää intiimejä valokuvia tai videoita.

Huijari pyrkii ensin saamaan uhrinsa luottamuksen, ja vasta sen jälkeen rahaa, lahjoja tai pankkitietoja.

Jos et lähetä rahaa, huijari saattaa yrittää kiristää sitä sinulta. Jos lähetät, hän pyytää myöhemmin lisää.

OLETKO UHRI?

Älä pelkää nolostumista!
Lopeta kaikki yhteydenpito välittömästi.
Jos mahdollista, säilytä kopio kaikesta viestittelystä.
Ota yhteys poliisiin.
Raportoi tapaus sivustolle, jonka kautta huijari otti sinuun yhteyttä.
Jos olet antanut pankkitietoja, ota yhteys pankkiisi.

MITÄ VOIT TEHDÄ?

- **Harkitse tarkasti** kuinka paljon henkilökohtaista tietoa jaat somessa ja seuranhakupalveluissa.
- **Huomioi aina riskit.** Huijareita on myös hyvämaineisilla sivustoilla.
- **Etene rauhallisesti** ja esitä kysymyksiä.
- **Tarkista** onko henkilön valokuvia tai profiilissa olevia tietoja käytetty muualla.
- **Ole valppaana** mikäli näet paljon kirjoitusvirheitä, epäjohdonmukaisuuksia, tai tekosyitä, kuten "kamera ei toimi".
- **Älä jaa arkaluonteista tietoa tai aineistoa,** jota voitaisiin käyttää kiristystarkoituksessa.
- Jos suostut tapaamiseen, **kerro perheellesi ja ystävillesi** mihin olet menossa.
- **Kieltädy rahapyynnöistä.** Älä milloinkaan lähetä rahaa, korttitietoja tai kopioita henkilötodistuksista tai muista asiakirjoista.
- **Vältä etukäteismaksuja.**
- **Älä avusta varojen siirrossa henkilöltä toiselle.** Rahanpesu on rikos.

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

#CyberScams

KALASTELUTEKSTIVIESTIT

Kalastelutekstiviestit (smishing) tarkoittaa yritystä saada pankkitietoja tai henkilökohtaisia tietoja tekstiviestitse.

MITEN KALASTELUTEKSTIVIESTIT TOIMIVAT?

Yleensä viestissä pyydetään avaamaan linkki tai soittamaan tiettyyn puhelinnumeroon, jotta jokin tilisi voitaisiin esimerkiksi vahvistaa, päivittää tai uudelleenaktivoida. Linkki kuitenkin johtaa huijaussivustolle ja puhelinnumero huijarille.

MITÄ VOIT TEHDÄ?

- **Älä avaa linkkejä, liitetiedostoa ja tai kuvia** joita saat pyytämättä tekstiviestitse.
- **Älä hätiköi.** Tarkista lähettäjän aitous kaikessa rauhassa ennen kuin harkitset vastaamista tai sisällön avaamista.
- **Älä koskaan vastaa sellaiseen viestiin,** joka pyytää PIN-koodiasi, salasanaasi tai muita yksityisiä tietoja.
- Jos epäilet antaneesi huijarille pankkitietojasi, **ota välittömästi yhteys pankkiisi.**

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

HUIJAUSSIVUSTOT

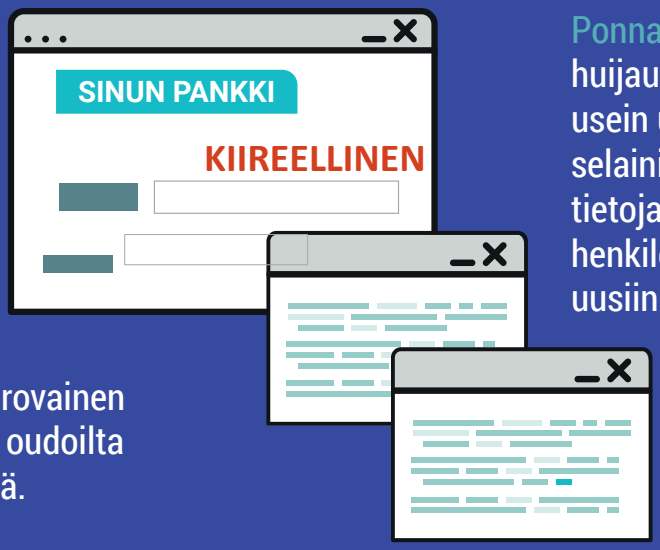
Kalasteluviestit sisältävät usein linkin väärennetylle, pankin sivun näköiselle nettisivulle, jossa käyttäjältä pyritään saamaan pankkitietoja ja henkilökohtaisia tietoja.

TUNNUSMERKIT

Huijaussivustot voivat olla ulkoasultaan lähes identtisiä pankin todellisten nettisivujen kanssa.

Huijaussivustoilla näkyy usein:

Viesti kiireellisyydestä: oikeat pankin nettisivut eivät pyydä sinua toimimaan kiireessä.



Ponnahdusikkunat: huijaussivustot avaavat usein uusia selainikkunoita, joilla onkia tietoja. Älä kirjoita henkilökohtaisia tietoja uusiin selainikkunoihin.

Huonoa suunnittelua: ole varovainen nettisivuilla, jotka näyttävät oudoilta tai sisältävät kirjoitusvirheitä.

MITÄ VOIT TEHDÄ?

Älä avaa sähköpostissa olevia linkkejä pankkien nettisivuille.

Kirjoita pankin osoite itse tai käytä omia kirjanmerkkejäsi.

Käytä selainta, jolla voit **estää ponnahdusikkunat.**

Jos oikealla pankillasi on sinulle tärkeää asiaa, **saat siitä tiedon kirjautuessasi pankkiisi.**

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

#CyberScams

KALASTELUSOITOT

Kalastelusoitot ovat puhelinsoittoja, joilla huijari pyrkii saamaan uhriltaan rahaa, pankkitietoja tai muita henkilökohtaisia tietoja.

MITÄ VOIT TEHDÄ?

- **Varo** pyytämättä saamiasi puhelinsoittoja.
- **Ota soittajan numero ylös** ja kerro soittavasi takaisin.
- **Etsi yrityksen puhelinnumero luotettavasta lähteestä** ja soita siihen suoraan.
- **Älä pyri vahvistamaan soittajan aitoutta soittamalla hänen antamaansa numeroon.** Numero voi olla tekaistu tai maksullinen.
- Huijarit voivat saada perustietojasi internetistä. **Älä oleta, että soittaja on aito vain koska hänellä on tietosi.**
- **Älä anna korttinumeroita, PIN-koodeja, salasanoja tai muita yksityisiä tietoja puhelimitse.** Pankki ei koskaan kysy tällaisia tietoja puhelimitse.
- **Älä lähetä rahaa puhelinsoiton perusteella.** Pankkisi ei koskaan pyydä toimimaan niin.
- Jos epäilet kyseessä olevan huijaus, **ota yhteys pankkiisi.**

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

#CyberScams