Näin tunnistat digihuijauksen

KULUTTAJALIITTO
KONSUMENTFÖRBUNDET

huijausinfo.fi

Tämän koulutuspaketin avulla voit oppia lisää digihuijauksista. Koulutuspaketin läpikäytyäsi tunnet yleisimmät huijaustyypit, osaat tunnistaa huijauksia ja tiedät, miten toimia, jos joudut huijatuksi. Koulutuspaketin tavoitteena on tukea ja kannustaa turvalliseen netin käyttämiseen.

Koulutuspakettia voi käyttää itseopiskeluun tai neuvoa sen avulla muita. Pakettia saa jakaa eteenpäin myös omille verkostoille.

Tämä koulutuspaketti on toteutettu osana Kuluttajaliiton Huijarit kuriin! –hanketta (STEA 2019-2021). Lisätietoja hankkeesta ja huijauksista löydät osoitteesta www.huijausinfo.fi

Tämä koulutuspaketti on päivitetty joulukuussa 2021.

Kuluttajaliitto – Konsumentförbundet ry on Suomen ainoa yleinen ja kaikille avoin kuluttajien ja julkisten palveluiden käyttäjien edunvalvonta-, koulutus- ja neuvontajärjestö. Puolustamme kuluttajan ja julkisten palveluiden käyttäjien oikeuksia yhteiskunnallisessa päätöksenteossa.

Lue lisää ja liity jäseneksi verkossa: www.kuluttajaliitto.fi/liity.

Sisältö

1. Yleistä digihuijauksista

Digihuijaukset ovat rikollisten tekemiä erityyppisiä petoksia, joissa hyödynnetään digilaitteita (esim. tietokone, tabletti, kännykkä) ja joissa menetetään rahaa, henkilötietoja tai käyttäjätunnuksia ja salasanoja.

Huijausten taustalla on usein kansainvälinen järjestäytynyt rikollisuus. Vaikka huijauksessa käytettäisiin suomen kieltä, ei se tarkoita, että se olisi tehty Suomessa. Iso osa huijauksista toteutetaan Suomen rajojen ulkopuolella.

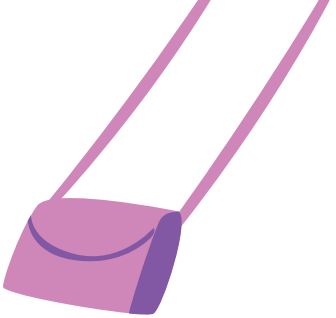
Huijausten tavoitteena on saada taloudellista hyötyä joko heti tai hyödyntämällä huijatulta saatuja tietoja myöhemmin.

Digihuijauksia voidaan jaotella seuraavalla tavalla:

- Nettikauppahuijaukset
- Huijausviestit
- It-tukihuijaukset
- Romanssihuijaukset
- Sijoitushuijaukset
- Toimitusjohtajahuijaukset (koskevat yritysten lisäksi yhdistyksiä ja järjestöjä)

Pelisäännöt turvalliseen netinkäyttämiseen

- Ole tarkka ja huolellinen, mieti aina mitä teet.
- Älä tee päätöksiä kiireessä. Huijarit painostavat yleensä kiireellä ja uhkauksilla toimimaan huolimattomasti.
- Ole kriittinen äläkä usko kaikkea mitä netissä kirjoitetaan. Jos jokin vaikuttaa liian hyvältä ollakseen totta, se ei yleensä ole totta!
- Tarkista asioita: sivuston luotettavuus, viestin lähettäjä, linkkien osoitteet.
- Etsi lisätietoa ja opettele tunnistamaan erilaisia huijauksia.
- Kysy apua, jos et tiedä. Apua saa esimerkiksi kirjastoista ja digitukijoilta.
- Älä mene verkkopankkiin tai viranomaisten verkkoasiointiin hakukoneen tai sähköpostiin tulleen linkin kautta!
- Älä avaa oudosta numerosta tai osoitteesta tullutta linkkiä!



2. Nettikauppahuijaukset ja tilausansat

Nettikauppahuijaukset

Nykyisin netistä voi ostaa lähes mitä tahansa. Luotettavien nettikauppojen lisäksi netissä on kuitenkin myös huijaussivuja ja -mainoksia. Myös netin kirpputoreilla, kuten Tori.fi-palvelussa ja Facebookissa on huijareita, jotka saattavat esiintyä käytetyn tavaran ostajana tai myyjänä.

Älä tee ostopäätöstä kiireellä! Harkitse ja tarkista verkkokaupan luotettavuus esim. hakukoneen avulla.

Nettikauppahuijauksissa rikolliset luovat aidon nettikaupan näköisiä sivuja verkkoon huijatakseen ihmisiltä rahaa. Nettikirpputoreilla huijarit esiintyvät keksityillä henkilötiedoilla.

Huijausnettikaupoissa kaupataan mitä tahansa palveluita ja tavaroita, joita ihmiset hankkivat muutenkin (esim. vaatteet, lomaosakkeet, vuokramökit, puhelimet).

Näin vältät nettikauppahuijauksen

- Muista, ettei mikään netissä ole ilmaista! Myyntitilanteessa huijari yrittää hämätä uskomattoman hyvillä tarjouksilla ja ohjata nopeaan ostopäätökseen kiireellä painostaen.

- Tee ostoksia tuttujen yritysten sivuilla tai varmista verkkokaupan luotettavuus ja maine: etsi hakukoneella (esim. google) keskustelupalstoilta muiden käyttäjien kommentteja yrityksestä ja tarkista, että verkkokaupan sivulla annetaan riittävästi tietoa yrityksestä.

- Älä osta, jos olet epävarma nettikaupan luotettavuudesta.

- Maksa aina luottokortilla, jos mahdollista. Luottokortilla maksettuasi voit kääntyä luottokortin myöntäneen pankin puoleen, jos joudut huijatuksi, eikä asian selvittely verkkokaupan kanssa onnistu.

- Säilytä tilausvahvistukset, kaikki viestinvaihto myyjän kanssa ja kauppiaan kuittaus maksun hyväksynnän jälkeen.

- Lue tilausehdot huolellisesti, aina myös pienellä kirjoitettu teksti.

Huijauksissa voidaan esiintyä tuttuina suomalaisina yrityksinä. Lisäksi nykyisin varsinkin Instagramissa on paljon huijaustilejä, jotka väittävät henkilön voittaneen arvonnassa ja voivan tilata tai ostaa jonkin tuotteen.

ESIMERKKI

Kuvassa on kauppaketju Gigantin nimissä tehty huijausmainos, jossa väitetään, että henkilö on voittanut sähköpotkulaudan. Mainoksessa oleva linkki palkinnon lunastamiseen ohjaa huijaussivulle.

Kuvassa on sosiaalisen median kanava Instagramissa ollut huijaustili ja sen julkaisu, jossa väitettiin, että kuvaan merkityt käyttäjät olisivat voittaneet hiustenkuivaajan. Huijauksen tavoitteena oli ohjata käyttäjä huijaussivulle, jonka avulla henkilöltä olisi saatu luottokorttitiedot.

Tarkista aina ennen ostamista, että yritys antaa verkkosivuillaan selkeästi seuraavat tiedot, varsinkin jos kyseessä on sinulle aiemmin tuntematon verkkokauppa

- Yrityksen tiedot ja yhteystiedot (yrityksen nimi, postiosoite, puhelinnumero ja sähköpostiosoite)
- Tuotteen tai palvelun sisältö ja hinta (myös toimituskulut)
- Toimitusehdot ja niissä mahdollisesti mainittavat tuotteeseen liittyvät rajoitukset tai yllättävät ehdot
- Tavaran tai palvelun toimitustapa ja toimitusaikataulu
- Onko kyseessä kertatilaus vai sitoutuuko ostaessa kestotilaukseen
- Miten maksu tapahtuu ja millä ehdoilla
- Miten tilauksen voi peruuttaa tai palvelun sulkea ostamisen jälkeen
- Minkälaiset takuu- ja huoltoehdot tilatulla tuotteella on.

Tilausansat

Tilausansalla tarkoitetaan sitä, kun kuluttaja huijataan sitoutumaan tietämättään kestotilaukseen joko puhelimessa, verkkokaupassa tai esimerkiksi huijausviestillä.

Huijarit saattavat väittää tarjoavansa ilmaista näytettä, maksutonta tutustumistarjousta tai nettiarvontaan osallistumista, mutta tosiasiassa uhri joutuu tilausansaan. Puhelimella soittaja saattaa kertoa kyseessä olevan markkinatutkimus, josta kiitoksena voi saada jonkin tuotteen pelkällä postimaksulla.

Myytävän tuotteen varjolla kuluttaja huijataan sitoutumaan pitkään määräaikaiseen sopimukseen, jolla tilaa tavaran tai palvelun ilman, että kuluttaja ymmärtää tai tietää asiaa itse.

Myös esimerkiksi Postin nimissä lähetettyjen huijausviestien myötä ihmisiä on joutunut tilausansaan, kun he ovat luulleet maksavansa tilauksen toimitusmaksun. Tosiasiassa henkilö on tietämättään sitoutunut ”tilaukseen”, jonka myötä hänen tililtään veloitetaan kuukausittain tietty summa.

Tilausansassa myyjän asiakaspalveluun ei yleensä saa yhteyttä, jotta saisi selvitettyä asian. Tämän takia tilausansan peruuttaminen ei yleensä onnistu ja veloitusten lopettaminen voi olla vaikeaa.

Ohjeet tilausansaan joutuneelle

- Maksa vain siitä, mitä olet tilannut! Veloitukset omalta tililtä kannattaa tarkistaa säännöllisesti.

- Tilaamatta toimitetusta tuotteesta tai näytteestä ei voi vaatia kuluttajalta maksua, tuotteen palauttamista tai säilyttämistä.

- Tilaamatta lähetetystä tuotteesta ja laskusta tulee tehdä reklamaatio lähettäjälle.

- Ole yhteydessä tililtäsi tai luottokortiltasi tehdyistä oudoista suoraveloituksista pankkiisi.

- Kilpailu- ja kuluttajaviraston (KKV, www.kkv.fi) verkkosivuilla annetaan ohjeita reklamaation tekemiseen. KKV:n Kuluttajaneuvonta auttaa reklamoinnissa. KKV:n reklamaatioapurilla voit tehdä reklamoinnin myös itse (www.reklamaatioapuri.fi).

3. Huijausviestit ja tietojenkalastelu

Huijausviestit ovat yleisin huijauksen muoto. Lähes jokainen saa huijausviestejä. Huijausviestejä lähetellään sähköpostitse, tekstiviesteillä, sosiaalisen median kanavissa ja muissa sovelluksissa.

Rikolliset pyrkivät kalastelemaan huijausviesteillä vastaanottajan pankki- ja luottokorttitietoja, henkilötietoja sekä käyttäjätietoja (esim. sähköpostin tunnus ja salasana).

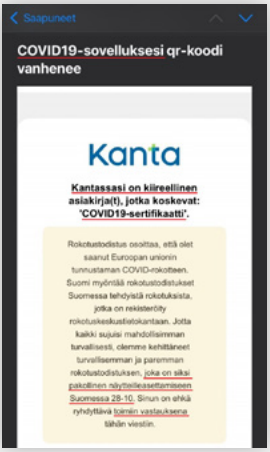
Huijausviestien mukana lähetetään lähes aina linkki, jonka kautta uhri ohjataan toimimaan. Yllättävän viestin mukana tullutta linkkiä ei kannata avata!

Tekstiviestillä lähetetty huijausviesti saattaa mennä älypuhelimessa samaan ketjuun aitojen viestien kanssa (esim. Postin viestit). Huijausviestiä voi siis olla vaikea erottaa aidosta viestistä.

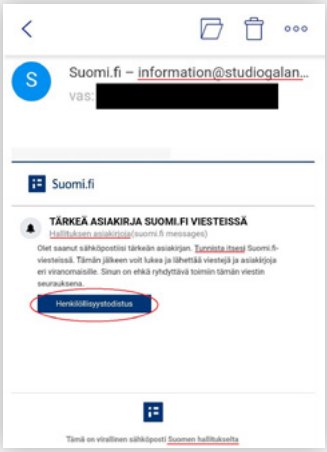
Huijausviestejä saatetaan lähettää myös viranomaisten nimissä. Näissä viesteissä väitetään, että esimerkiksi suomi.fi-palvelussa, Kanta-palvelussa tai Verohallinnon palvelussa on asiakirja, joka pitää lukea viestin mukana tulleen linkin kautta.

Myös kaikkien suomalaisten pankkien nimissä lähetellään viestejä, joilla uhataan esimerkiksi pankkikortin tai verkkopankin sulkemisella, jos ei päivitä tietojaan viestin mukana tulleella linkillä.

ESIMERKKI



Kanta-palvelun nimissä lähetettiin huijausviestejä, kun Suomessa otettiin käyttöön koronapassi. Viestin saaja yritettiin ohjata viestin mukana tulleen linkin kautta huijaussivulle, jonka avulla rikolliset yrittivät saada uhrin verkkopankkitunnukset. Viestissä on useita kirjoitusvirheitä ja epätavallisia termejä.



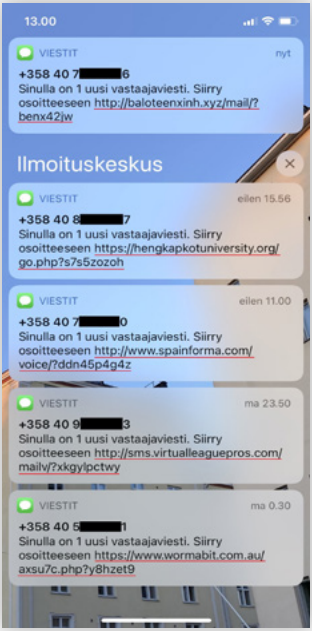
Suomi.fi-palvelun nimissä lähetellään huijausviestejä, joissa väitetään, että viestin saajalla on tärkeä asiakirja palvelussa ja se pitää lukea viestin mukana tulleen linkin kautta tunnistautumalla pankkitunnuksilla. Viestin avulla levitetään huijaussivua, jonka kautta rikolliset saavat uhrin verkkopankkitunnukset. Viestissä on kirjoitusvirheitä, useita epätavallisia termejä ja epäilystä herättäviä väitteitä lähettäjästä.

Lisäksi huijausviestejä voidaan lähettää esimerkiksi Postin, kuljetusyritysten, kauppojen ja operaattoreiden nimissä. Viesteissä painostetaan aina kiireellä ja uhataan joillain seurauksilla.

Kaikkien pankkien nimissä lähetellään huijausviestejä. Viesteissä uhkaillaan tai pelotellaan esimerkiksi tilin tai kortin sulkemisella, jotta uhri saataisiin toimimaan nopeasti ja harkitsemattomasti. Viesteissä on aina linkki, joka johtaa verkkopankilta näyttävälle huijaussivulle. Tekstit voivat olla huonoa suomen kieltä. Esimerkiksi Nordean nimissä lähetetyssä viestissä oli useita kirjoitusvirheitä ja siinä uhkailtiin tilin sulkemisella.

- **Pankit eivät pyydä tavallisella sähköpostilla asiakkaitaan päivittämään mitään tietoja – huijarit pyytävät!**
- **Pankin lähettämät viestit ovat aina verkkopankissa kohdassa ”viestit”. Jos saat pankin nimissä viestin, jossa pyydetään tekemään jotain verkkopankissa, mene verkkopankkiin aina ainoastaan kirjoittamalla verkkopankin osoite selaimeen (esim. www.pankki.fi) tai käyttämällä pankin omaa mobiilisovellusta.**
- **Älä ikinä avaa sähköposti- tai tekstiviestin mukana tullutta linkkiä, lataa outoa viestin liitettä tai annan tietojasi, jos et ole täysin varma, ettei kyseessä ole huijausviesti.**

ESIMERKKI



Huijausviestejä saattaa tulla useita peräkkäin. Huijausviesteissä, joissa väitetään, että henkilöllä on uusi vastaajaviesti tai paketti allekirjoitettavana, on usein outo pitkä linkki, joka ohjaa huijaussivulle. Viesti näyttää tulevan suomalaisesta numerosta. Linkin avaamalla saattaa ladata laitteelleen haittaohjelman.

Postin nimissä tekstiviestinä lähetetyssä huijausviestissä väitetään, että vastaanottajalla on paketti, joka pitää allekirjoittaa viestin mukana olevan linkin kautta.

Kiristyshuijausviestit

Huijausviesteillä voidaan yrittää myös kiristää viestin saajaa. Usein lähettäjä väittää kaapanneensa uhrin tietokoneen tai sähköpostitilin ja salakuvanneensa uhria koneen kameralla.

Viestillä huijari yrittää kiristää rahaa (yleensä kryptovaluuttaa, kuten bitcoineja) ja uhkaa julkaista ”arkaluontoisia” kuvia uhrin työkavereille ja muulle lähipiirille.

Kyseessä on huijaus, eikä konetta (yleensä) ole hakkeroitu tai kaapattu. Älä ikinä maksa kiristysviesteissä vaadittuja rahoja. Tee kiristysviestistä rikosilmoitus poliisille.

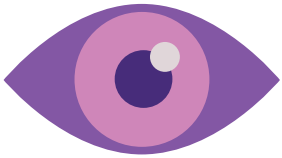
Huijausviestin tunnistaminen

Ennen kuin reagoit saamaasi viestiin, mieti seuraavia asioita:

- Painostetaanko sinua kiireellä ja uhataanko seurauksilla, jos et toimi niin kuin viestissä käsketään?
- Tunnetko viestin lähettäjän?
- Onko viestin mukana linkki, jonka kautta asia pitää hoitaa?
- Onko viestissä kirjoitusvirheitä?
- Onko viestin sisältö muuten epäilyttävä?
- Onko mahdollinen linkki oudon näköinen?
- Lähestyisikö kyseinen organisaatio sinua viestin sisällön mukaisesti?
- Kuulostaako viestissä oleva tarjous tai arvonta liian hyvältä ollakseen totta tai viestissä mainitut seuraukset liian pahoilta ollakseen totta?

Toimi näin, jos sait epäilyttävän viestin

1. Älä avaa viestissä olevaa oudon näköistä linkkiä.
2. Älä kirjaudu verkkopankkiin tai viranomaisten palveluihin viestien mukana tulleiden linkkien kautta.
3. Mene viestissä väitettyyn palveluun kirjoittamalla palvelun osoite selaimen osoiteriville (esim. verkkopankkiin osoitteella www.pankki.fi).
4. Jos et tiedä onko viesti huijausta vai ei, voit kysyä asiasta soittamalla viestin lähettäneen yrityksen asiakaspalveluun. Älä kuitenkaan vastaa viestiin suoraan, vaan etsi erikseen asiakaspalvelun yhteystiedot. Yritykset kertovat arvonnoista ja kilpailuista yleensä nettisivuillaan. Kannattaa tarkistaa onko viestissä väitetty kilpailu tai arvonta todellinen.



4. It-tukihuijaukset

It-tukihuijauksessa on kyse siitä, että rikollinen soittaa ja esiintyy it-tukihenkilönä ja väittää, että henkilön tietokone on uhattuna. Yleensä englantia puhuva huijari sanoo soittavansa Microsoftin it-tuesta ja väittää, että:

1. hän soittaa Microsoftin pääkonttorilta, jossa henkilön konetta on tarkkailtu
2. uhrin kone lähettää jotain signaalia viasta, joka pitää korjata
3. tietokone on saastunut haittaohjelmilla ja mahdollisesti tilit on kaapattu
4. on kiire ja vain hän voi auttaa pelastamaan henkilön koneen

Soittaja haluaa antaa vaikutelman, että kyseessä on erittäin kiireellinen asia ja, että hänen ohjeitaan on välttämätöntä kuunnella ja noudattaa.

Yleensä huijari pyytää uhria lataamaan laitteelleen etähallintaohjelman, jonka avulla soittaja voi auttaa koneen pelastamisessa.

Jos saat it-tukihuijauspuhelun

1. Lopeta puhelu välittömästi. **Microsoft tai mikään muukaan taho ei valvo kuluttajien laitteita ja tarjoa yleistä it-tukea.** It-tuki on palvelu, joka on käytössä esimerkiksi yrityksillä, mutta Microsoft ei tällaista palvelua tarjoa.

2. Älä lataa ikinä etähallintaohjelmia tai muita sovelluksia laitteellesi, jos et ole aivan varma ohjelman käytöstä. Yllättäen soittanut henkilö, joka vaatii ohjelman lataamista laitteelle on aina huijari.

3. Älä usko soittajaa, vaikka hän väittäisi tietävänsä laitteesi tietoja.

4. Jos latasit etähallintaohjelman tai toimit muuten it-tukihuijarin ohjeistamalla tavalla, ilmoita asiasta välittömästä pankkiisi ja anna ammattilaisen tarkistaa laitteesi haittaohjelmien varalta.

5. Romanssihuijaukset

Romanssihuijauksessa huijari esiintyy kuviteltuna henkilönä tavoitteenaan luoda romanssi tai ystävyyssuhde tämän olemattoman hahmon ja uhrin välille. Aikaansaatua romanssia hyödyntämällä huijarin tarkoituksena on saada uhrilta rahaa.

Rikoksen tekijät ovat erittäin taitavia ihmistuntijoita ja tietoverkon hyödyntäjiä. He käyttävät häikäilemättömästi hyväksi ihmisten luonnollista tarvetta löytää seuraa tai elämänkumppani.

Taitavasti tunteisiin vetoamalla voidaan saada huijattua suuriakin summia rahaa. Moni romanssihuijauksen uhri menettää kymmeniä tai jopa satoja tuhansia euroja.

Romanssihuijaus saattaa kestää jopa vuosia ja ihmiseltä saatetaan saada kaikki säästöt ja saada uhri ottamaan jopa lainaa.

Romanssihuijauksen kulku

1. Huijari lähestyy uhria yleensä sosiaalisen median (esim. Facebook tai Instagram) tai deittisovellusten (esim. Tinder) kautta.

2. Yhteyttä pidetään pääsääntöisesti eri viestisovellusten kautta (WhatsApp, Hangouts, Messenger).

3. Huijari saattaa kertoa työskentelevänsä jossain kriisialueella tai öljynporauslautalla.

4. Huijarin sosiaalisessa mediassa oleva profiili esittää usein komeaa ja varakasta upseeria tai kaunista näyttelijää esimerkiksi Amerikasta tai itä-Euroopasta. Kuvat, henkilön nimi ja titteli elämäntarinoineen on joko keksitty tai varastettu toisen ihmisen sometileiltä netistä.

5. Huijari kertoo usein tietävänsä paljon Suomesta ja haluavansa tulla käymään. Matkat Suomeen peruuntuvat kuitenkin aina erilaisten epäonnisten sattumien vuoksi.

6. Yleensä videokeskustelut eivät onnistu ja puheluitakin soitetaan vain satunnaisesti.

7. Usein huijari kertoo saaneen hiljattain perinnön tai suuren summan rahaa muusta syystä tai on valmiiksi rikas. Huijari on kuitenkin jostain syystä estynyt käyttämään rahojaan ja pyytää uhria sen takia ”lainaamaan” rahaa.

8. Usein rahasiirtoja pyydetään tekemään jonkun toisen tilille, ei huijarille itselleen. Rahapyynnöt saattavat liittyä myös johonkin hätään, kuten sairaalakuluihin, palkkojen maksamiseen, tullimaksuihin, työttömyyteen, eroon tai läheisen kuolemaan.

9. Huijari saattaa syyllistää tai uhkailla uhria, jos hän ei suostu tai pysty tekemään pyydettyjä rahasiirtoja ja jos rahaa pyytäneen luotettavuutta epäilee, saattaa huijari esittää loukkaantunutta ja suuttua.

10. Huijari todistelee omaa luotettavuuttaan ja aitouttaan esimerkiksi lähettämällä kuvia itsestään, joissa hän on eläinten tai lasten kanssa tai luottamusta herättävässä työssä. Huijari saattaa esitellä myös linkkejä yrityksensä verkkosivuille. Yleensä hän kertoo olevansa varakas, hyvässä työssä ja hyvässä fyysisessä kunnossa.

Jos epäilet nettituttavasi luotettavuutta, kysy itseltäsi nämä kysymykset

- Miksi juuri minua lähestytään?
- Tiedänkö oikeasti, kuka nettirakkaani on?
- Olenko koskaan tavannut nettirakastani?
- Onnistuuko hänen kanssaan yhteydenpito puhelimitse tai videon välityksellä?
- Pyytääkö hän minulta rahaa vedoten mahdollisiin matkakuluihin, passi-hankintaan tai erilaisiin dramaattisiin tapahtumiin ja tarinoihin?
- Onko rahanpyynnöissä painostuksen, kiireen tai kiristyksen maku?

Jos asia vaikuttaa liian hyvältä tai liian pahalta ollakseen totta, se ei yleensä ole totta!

Näin voit välttyä romanssihuijaukselta

- Ole varovainen tutustuessasi uusiin ihmisiin netissä. Varsinkin jos täysin vieras henkilö lähettää yllättäen viestin. Älä usko liian helposti kaikkiin tarinoihin, joita uusi tuttavasi kertoo.

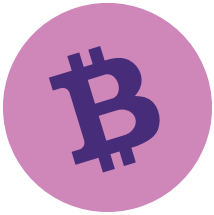
- Tarkista nettituttavan taustat hakemalla esimerkiksi hänen nimeänsä Googlesta ja käyttämällä Googlen käänteistä kuvahakua. Pyri varmistamaan tuttavan henkilöllisyys.

- Älä lähetä uudelle tuttavalle rahaa tai kuvia passistasi.

- Vaadi tapaamista ja sitä, että henkilö kustantaa itse matkansa luoksesi.

- Keskustele henkilön kanssa eri kanavissa. Tänä päivänä jokaisella on mahdollisuus videopuheluihin ja tavallisiin puheluihin.

- Puhu läheisesi kanssa uudesta tuttavastasi.



6. Sijoitushuijaukset

Sijoitushuijauksessa houkutellaan huipputuottavan sijoitustarjouksen varjolla hankkimaan esimerkiksi osakkeita, joukkolainoja tai kryptovaluuttaa.

Usein ainutlaatuista huippusijoitusta tarjotaan erikoistarjouksena juuri sinulle. Tarjouksen kerrotaan olevan voimassa lyhyen ajan ja luvataan äkkirikastumista.

Huijarit tehtailevat nettiin erilaisia valeuutisia ja -mainoksia, joissa käytetään suomalaisten luotettaviksi koettujen julkkisten kuvia ja väitetään heidän rikastuneen virtuaalivaluuttaan sijoittamalla tai suosittelevan Bitcoin-sijoituksia (esim. Matti Rönkä, Mika Anttonen, Sauli Niinistö ja Sanna Marin, Ville Haapasalo).

Sijoitushuijarit mainostavat myös Tinderissä ja hakukoneissa, kuten Googlessa.

Sijoitushuijauksissa uhrien rahanmenetykset ovat usein suuria, jopa kymmeniä ja satoja tuhansia euroja.

Sijoitushuijauksen kulku

1. Sijoitushuijaus käynnistyy yleensä sosiaalisessa mediassa nähdystä valemainoksesta, jossa mainostetaan hyvin tuottavista sijoituskohteista, joihin kannattaa sijoittaa heti, sillä tilaisuus on voimassa vain hetken.

2. Mainos johtaa huijaussivulle, joka voi olla tehty näyttämään esimerkiksi Yle uutisten nettisivulta. Sivulla ohjeistetaan tarkasti, miten sijoitus tapahtuu. Kun uhri antaa yhteystietonsa, alkaa huijareiden painostavat yhteydenotot, joiden tavoitteena on saada uhrilta mahdollisimman paljon rahaa.

3. Uhri huijataan sijoittamaan rahaa kohteeseen, jota ei todellisuudessa ole olemassa.

4. Tämän jälkeen uhrille soitellaan ja lähetellään sähköpostia ja pyydetään lisäsijoitusta ulkomaiselle pankkitilille tai virtuaalivaluutan vaihtopalveluun.

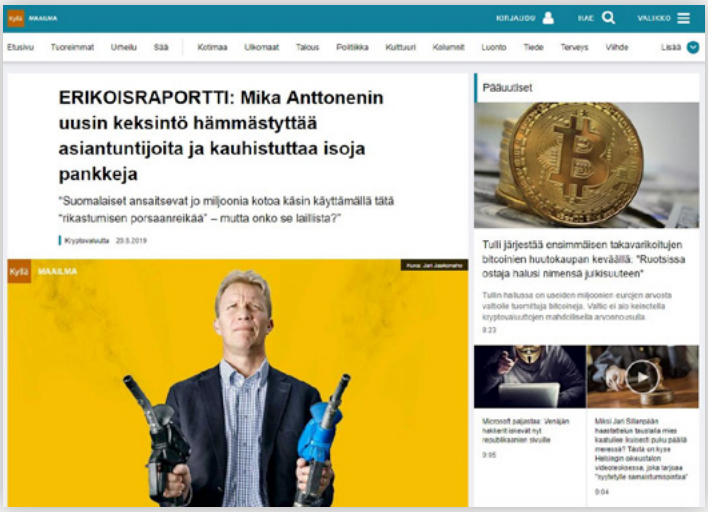
5. Uhrille tarjotaan aina isompia voittoja ja ”todisteeksi” näytetään kuvia tekaistuista pörssikaavioista tai verkkosivuista, joiden mukaan sijoituksilla menee hyvin.

6. Uhria saatetaan pyytää asentamaan tietokoneeseen etähallintaohjelma, jolla sijoitusmyyjä vakuuttaa pystyvänsä antamaan parempaa palvelua. Todellisuudessa huijari tekee uhrin pankkitililtä luvattomia siirtoja tyhjentäen mahdollisesti uhrin koko tilin.

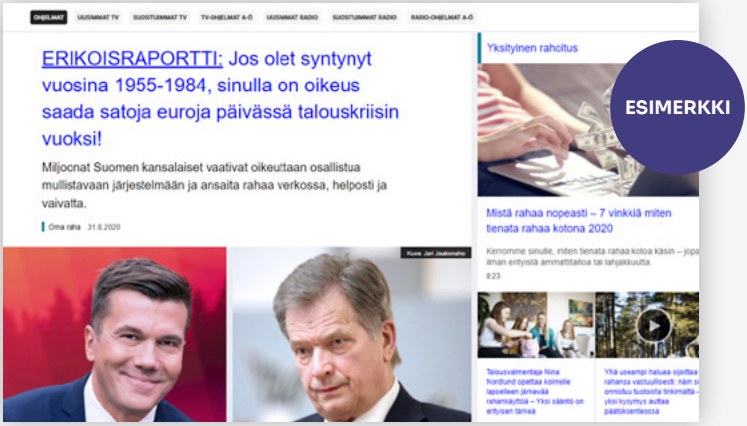
7. Yhteydenpito voi olla hyvin tiivistä ja aggressiivista eikä omia rahoja saa pois vaikka haluaisi nostaa sijoituksensa tai saamansa ”voitot”.

Sijoitushuijauksia varten tehdään usein uutissivu, jolla mainostetaan tutun suomalaisen julkkiksen kasvoilla huijausta. Sivut on usein naamioitu näyttämään esimerkiksi Yle uutisten sivuilta ja niissä on tarkat ohjeet sijoituksen tekemiseen ja mainoksia kryptovaluutoista. Usein sivuilla on kirjoitusvirheitä ja sivuilla olevat linkit muihin artikkeleihin ei yleensä toimi. Huijaussivuja mainostetaan esimerkiksi Facebookissa ja Googlessa.

ESIMERKKI



Sijoitushuijausta varten tehdään usein huijaussivu, jota mainostetaan sosiaalisessa mediassa. Esimerkkisivulla pyritään luomaan luottamusta kryptovaluuttoja ja huijarin palvelua kohtaan sekä annetaan yksityiskohtaiset tiedot sijoittamisesta. Huijaussivulla käytettiin yritysjohtaja Mika Anttosen nimeä ja kuvaa.



Huijauksissa on käytetty myös presidentti Sauli Niinistön kuvaa ja nimeä markkinoimaan olematonta sijoituskohdetta. Yle uutisten sivuksi naamioidulla huijaussivulla väitetään, että tietyn ikäisillä suomalaisilla olisi erityinen oikeus sijoittaa mainostettuun kryptovaluuttaan, joka on tosiasiassa huijausta.

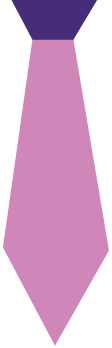
Jos epäilet sijoitushuijausta

- Muista, ettei kukaan tarjoa ilmaiseksi hyvin tuottavia sijoituskohteita tai sijoitusvinkkejä tavalliselle ihmiselle puhelimitse. Ainoastaan huijarit soittavat ja tarjoavat sijoituskohdetta.

- Älä sijoita rahojasi netissä (esim. Facebookissa) nähdyn mainoksen perusteella.

- Varmista sijoituskohteen ja sitä hoitavan yrityksen tausta ja luotettavuus. Apua voit kysyä esimerkiksi omasta pankistasi, jos et itse tiedä onko kohde aito vai huijausta.

- Älä sijoita kohteisiin, joita et ymmärrä. Varsinkin kryptovaluuttoihin sijoittamisessa kannattaa olla varovainen, sillä niihin liittyy paljon huijauksia ja riskejä.



7. Toimitusjohtaja-huijaukset

Toimitusjohtaja huijaus kohdistuu yritykseen, yhdistykseen, järjestöön tai sen työntekijään.

Huijauksessa rikollinen esiintyy oman organisaatiosi johtohenkilönä, joka pyytää siirtämään rahaa ulkomaille jollakin verukkeella tai kysyy ensin organisaation pankkitilin saldoa ja pyytää sen jälkeen tekemään siirron.

Huijari voi vedota asian kiireellisyyteen tai arkaluonteisuuteen ja eri tavoin painostaa uhria toteuttamaan maksun.

Yleensä huijari lähettää sähköpostiviestin johtotehtävissä olevan henkilön nimissä. Sähköpostiviesti saattaa näyttää tulevan johtajan sähköpostiosoitteesta, vaikka hän ei olisikaan sitä lähettänyt itse. Jos viesti epäilyttää vähäänkään tai jos se on hyvin epätavallinen, kysy ja varmista asia soittamalla tai lähettämällä sähköposti henkilölle, jonka nimissä viesti on tullut.

Älä kuitenkaan koskaan vastaa suoraan lähetettyyn viestiin vaan lähetä uusi viesti, jotta kysymyksesi menee varmasti haluamallesi ihmiselle eikä huijarille!

8. Toimintaohjeet huijatulle

Jos olet menettänyt rahaa, henkilötietoja tai pankkitunnukset

1. Ole mahdollisimman nopeasti yhteydessä oman pankkisi asiakaspalveluun ja kerro huijauksesta. Pankki voi sulkea pankkitilisi ja pankki- ja luottokorttisi, jos tiedot ovat päätyneet huijarille.
2. Tee rikosilmoitus poliisille, www.poliisi.fi

Hae apua muualta

- Älä jää yksin! Puhu huijauksesta läheistesi kanssa. Lisäksi voit keskustella huijauksesta soittamalla Rikosuhripäivystykseen (www.riku.fi).
- Huijauksen selvittämisessä auttaa Kilpailu- ja kuluttajavirasto, jos kotimainen yritys on huijannut (www.kkv.fi/kuluttajaneuvonta/).

- Rajat ylittävässä kaupassa EU:ssa auttaa Euroopan kuluttajakeskus Suomessa (www.ecc.fi).

Oma luottokielto ja markkinoinnin esto puhelimeen

Jos olet menettänyt henkilötietosi rikollisille huijauksen seurauksena, voit ottaa maksullisen omaehtoisen luottokiellon 2 vuodeksi

- Oma luottokielto estää tekemästä mitään luotollisia ostoksia.
- Oman luottokiellon voi itse keskeyttää tarvittaessa
- Suomessa on kaksi palveluntarjoajaa, Suomen Asiakastieto Oy ja Bisnode

Suoramarkkinoinnin esto puhelimeen

- Suoramarkkinointia voi rajoittaa ilmoittautumalla suoramarkkinoinnin rajoituspalveluun. Palvelut voivat olla maksullisia.
- Lisätietoa saa mm. Kilpailu- ja kuluttajaviraston sivuilta osoitteesta www.kkv.fi.

Huijatun kokeman häpeän käsittely ja huijauksen uhrin auttaminen

Huijattu on petosrikoksen uhri, eikä huijatuksi joutumista tarvitse hävetä.

Huijatuksi tulemista voidaan verrata hyväksikäyttökokemukseen, sillä hyväksikäytön uhriksi joutuneet kokevat häpeää. Yleensä huijauksen uhri syyttää itseään huijauksesta.

Häpeän käsittelyssä tärkeintä on puhua huijauksesta ja hakea tarvittaessa ammattiapua. Kun ihminen kokee valmiiksi häpeää, häntä kannattaa kohdella silkkihansikkain.

9. Lisätietoja huijauksista

Kuluttajaliiton tietopankki huijauksista
www.huijausinfo.fi

Poliisi
www.poliisi.fi/petosrikokset

Rikosuhripäivystys
www.riku.fi/erilaisia-rikoksia/nettihuijaus/

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
www.kyberturvallisuuskeskus.fi

Kilpailu- ja kuluttajaviraston kuluttajaneuvonta
www.kkv.fi/kuluttajaneuvonta

Euroopan kuluttajakeskus Suomessa
www.ecc.fi

Digi- ja väestötietoviraston kansalaisneuvonta
puh. 0295 000

Huijauksista varoitetaan esimerkiksi Huijausinfon ja Kyberturvallisuuskeskuksen sekä poliisin sosiaalisen median kanavissa ja nettisivuilla

Huijausinfo
Twitterissä ja Facebookissa @huijausinfo

Kyberturvallisuuskeskus
Twitterissä @CERTFI ja Facebookissa @NCSC-FI

Poliisi
Twitterissä ja Facebookissa @Suomenpoliisi

Huijauksista varoitetaan myös esimerkiksi
112 Suomi-sovelluksessa

Yle Oppimisen Digitreenien materiaalit huijauksista

Huijausvisa: https://yle.fi/aihe/artikkeli/2019/05/17/digitreenit-testaa-parjaatko-nettiajan-huijareille

Tunnistatko luotettavan nettikaupan: https://yle.fi/aihe/artikkeli/2021/01/30/digitreenit-tunnistatko-luotettavan-nettikaupan-testaa-9-kysymyksella

Kuluttajaliiton nettisivuilla ja YouTube-kanavalla on useita huijauksiin liittyviä koulutusvideoita

www.huijausinfo.fi tai
www.youtube.com, hakusanalla ”huijausinfo”

Lue lisää huijauksista huijausinfo.fi

huijausinfo.fi

KULUTTAJALIITTO
KONSUMENTFÖRBUNDET