VERKOSSA TAPAHTUVAT TALOUSPETOKSET JA -HUIJAUKSET JA TEKOÄLY

PYSY VALPPAANA JA SUOJAA ITSESI

Verkossa tapahtuvat talouspetokset ja -huijaukset eivät ole uusia ilmiöitä, mutta tekoäly (Artificial Intelligence, AI) on tehnyt niistä entistäkin älykkäämpiä ja vaikeammin havaittavia. Rikolliset käyttävät nyt väärennettyjä viestejä ja verkkosivustoja, tekaistuja tunnettujen henkilöiden profiileja sekä jopa tekoälyn luomaa ääntä tai videoita, jotka näyttävät pankkivirkailijaltasi, ystäviltäsi tai perheenjäseniltäsi huijatakseen sinua.

He voivat ottaa sinuun yhteyttä vaikuttaen luotettavalta sosiaalisen median, odottamattomien puheluiden tai viestintäsovellusten kautta tai sähköpostitse.

Sinulle saattaa aiheutua riskejä, kuten taloudellisia menetyksiä, identiteettivarkauksia tai henkistä kuormitusta ja ahdistusta. Ole varovainen ja noudata näitä vinkkejä pysyäksesi turvassa:

Pysy valppaana verkossa tapahtuvista talouspetoksista ja -huijauksista, joissa on voitu hyödyntää tekoälyä, kuten väärennetyt henkilöllisyydet, tietojenkalastelu, sijoitus- ja vakuutushuijaukset sekä rakkauspetokset ja -huijaukset. Saat lisätietoa eri petos- ja huijaustyypeistä sivuilta 5, 6 ja 7.

Saat lisätietoa kryptovaluuttoihin liittyvistä petoksista ja huijauksista *erillisestä kryptopetoksia ja -huijauksia koskevasta tietopaketista* ( ).

Tunnista varoitusmerkit:
Opi tunnistamaan *epäilyttävä käyttäytyminen, viestit tai tarjoukset* (lisätietoja sivulla 2);

Suojaa itsesi:
Suojaa *henkilökohtaiset tietosi* (lisätietoja sivulla 3); ja

Tiedä, mitä tehdä, jos joudut petoksen tai huijauksen uhriksi
(lisätietoja sivulla 4).

Varoitusmerkit

Lupaus, joka kuulostaa liian hyvältä ollakseen totta.

Odottamaton puhelu tuntemattomasta numerosta.

Kiireellinen pyyntö lähettää rahaa tai henkilötietoja, myös henkilöltä, joka teeskentelee olevansa perheenjäsen, ystävä tai joku tunnettu henkilö.

Pyyntö ottaa laitteesi hallintaan, ladata sovellus, skannata QR-koodi tai klikata linkkiä.

Pyyntö saada henkilökohtaisia tietoja tai pankkitietoja (esim. salasanat, luottokorttinumerot, verkkopankkitunnukset tai turvakoodit).

Pyyntö tehdä maksu jäljittämättömällä menetelmällä (esim. kryptot, lahjakortit, tilisiirrot tai prepaid-kortit).

Epäilyttävä tai virheellinen sähköpostiosoite tai linkki (esim. kirjoitusvirheitä URL-osoitteessa tai epätavallisia verkko-osoitteita tai -tunnuksia).

Liite tuntemattomasta lähteestä, erityisesti .exe, .scr, .zip tai makroilla varustettu Office-tiedosto (.docm, .xlsm).

Huono kielioppi tai muotoilu viralliselta näyttävässä asiakirjassa, joskin tekoäly auttaa huijareita peittämään tällaiset virheet aiempaa paremmin.

Verkkosivusto, joka näyttää ammattimaiselta, mutta josta puuttuu vahvistetut yhteystiedot tai yrityksen rekisteröintitiedot.

Puhe, joka kuulostaa epäluonnolliselta, jossa ei ole taukoja, tai joka kuulostaa liian sujuvalta tai robottimaiselta. Kiinnitä huomiota ”äänen kloonaukseen”, vaikka tekoälyllä tuotettu puhe voi myös kuulostaa hyvin luonnolliselta.

Videot, joissa ääni saattaa kuulostaa robottimaiselta tai liian tasaiselta, huulten liikkeet tai kasvojen ilmeet eivät vastaa puhetta, tai tausta, valaistus tai varjot voivat olla epätavallisia. Nämä voivat usein olla tekoälyn tuottamia videoita (syvävääreennös, deepfake).

Miten suojautua

1 **Älä koskaan jaa henkilökohtaisia tietoja tai pankkitietoja:**

Luotettavat yritykset eivät koskaan pyydä sinulta PIN-koodeja, salasanoja, verkkopankkitunnuksia tai turvakoodeja sähköpostitse, tekstiviestillä, sosiaalisessa mediassa tai puhelimitse.

2 **Pysähdy ja mieti, ennen kuin toimit:**

Älä kiirehdi lähettämään rahaa, jakamaan tietoja tai klikkaamaan linkkejä. Huijarit luovat tarkoituksella kiireen tuntua (esim. IT-ongelmat pankin kanssa, hätäpuhelut, jotka koskevat ystäviä tai perheenjäseniä, uhkaava kieli jne.). Jos sinulle herää pieninkin epäilys, älä toimi; lopeta puhelu ja tarkista lähde tai henkilöllisyys huolellisesti.

3 **Tarkista lähde tai henkilöllisyys huolellisesti:**

- Varmista aina, mistä viestit, puhelut, sähköpostit tai linkit tulevat, vaikka ne näyttäisivät virallisilta tai vaikuttaisivat tulevan ystävältäsi tai perheenjäseneltäsi tai tunnetulta henkilöltä. Voit esimerkiksi soittaa tai lähettää tekstiviestin perheenjäsenellesi tai ystävällesi luotettavan kanavan kautta käyttämällä tuntemaasi numeroa, etsiä kirjoitusvirheitä, outoja URL-osoitteita tai puuttuvia turvaindikaattoreita (esim. tarkista, että verkkosivuston linkissä on kirjain ”s” kohdassa ”HTTPS”, joka kertoo verkkosivuston turvallisuudesta, ja tarkista, ettei yrityksen nimessä ole lisättyjä tai puuttuvia kirjaimia).

- Älä avaa linkkejä ei-toivotuista viesteistä, asenna vain virallisia sovelluksia luotettavien sovelluskauppojen kautta äläkä skannaa tuntemattomia QR-koodeja.

- Sovi perheesi kanssa “turvasana” eli esimerkiksi salainen lause, jolla voitte vahvistaa toistenne henkilöllisyyden, jos joku soittaa sinulle tutulla äänellä ja esittää kiireellisen rahapyynnön väittäen olevansa perheenjäsen (esim. vanhemmat, sisarus, lapsi).

- Varmista itse yhteystiedot ottaessasi yhteyttä suoraan yritykseen tai henkilöön, äläkä koskaan luota epäillyn huijarin sinulle antamiin yhteystietoihin (esim. etsi itse yrityksen nimellä, käytä vahvistettuja yrityshakemistoja tai aiemmin vahvistettuja yhteydenottotapoja). Huijarit voivat väittää olevansa valtuutettuja toimimaan yrityksen puolesta tai jäljitellä yrityksen verkkosivustoa. Tarkista, onko kansallinen finanssialaa valvova viranomainen antanut varoituksia tai onko yritys IOSCOn I-SCAN-listalla (iosco.org/i-scan/). Kryptopalveluntarjoajien osalta tarkista, onko niillä toimilupa toimia EU:ssa (esim. tarkista ESMA:n rekisteri ( )).

4 **Kiinnitä huomiota mahdollisiin tekoälyhuijauksiin:**

Tekoälyteknologian kehittyessä huijaukset ovat entistä vakuuttavampia – jopa parhaista tietoturvavinkeistä huolimatta. Jos jokin vaikuttaa epätavalliselta tai havaitset yllä mainittuja varoitusmerkkejä, pysähdy ja arvioi tilanne uudelleen.

5 **Älä koskaan asenna etähallintaohjelmistoa tai jaa näyttöäsi:**

Pankit tai luottolaitokset eivät koskaan pyydä sinua tekemään niin.

6 **Pidä laitteesi ja tilisi turvassa:**

Käytä vahvoja ja yksilöllisiä salasanoja, pidä ne salassa, äläkä käytä samoja tunnuksia eri alustoilla. Ota käyttöön monivaiheinen todennus aina kun mahdollista. Katso lisää salasanavinkkejä täältä (https://shorturl.at/4zp4U). Pidä ohjelmistot ja virustorjunta ajan tasalla ja aktivoituna.

7 **Ole varovainen odottamattomien ja vain rajoitetun ajan voimassa olevien sijoitusmahdollisuuksien kanssa:**

Jos se kuulostaa liian hyvältä ollakseen totta, se todennäköisesti on.

8 **Mieti, ennen kuin jaat tietoja sosiaalisessa mediassa:**

Keskusteluryhmät, foorumit, sosiaalisen median postaukset ja valokuvat voivat olla arvokkaita tietolähteitä huijareille. Liian henkilökohtaisten tietojen tai sijoituksia koskevien tietojen paljastaminen voi tehdä sinusta helpon kohteen.

Mitä tehdä, jos joudut petoksen tai huijauksen uhriksi

Keskeytä tapahtumat välittömästi

Estääksesi lisäsiirrot epäilyttäville tileille ja välttääksesi lisätappiot. Lopeta kaikki yhteydenpito huijareihin: älä vastaa heidän puheluihinsa tai sähköposteihinsa ja estä lähettäjä.

Ota yhteyttä pankkiin tai rahoitusyhtiöön:

Ilmoita tapahtuneesta pankkiisi tai rahoitusyhtiöön välittömästi virallisten yhteyskanavien kautta, jotta voidaan selvittää mahdollisuudet jäädyttää tai peruuttaa tapahtumat.

Vaihda salasanasi kaikissa laitteissasi ja sovelluksissa/verkkosivustoilla.

Huijarit ostavat vuotaneita salasanoja verkossa ja kokeilevat niitä useilla eri tileillä. Yhden salasanan vaihtaminen ei riitä. Varmista, että vaihdat kaikki salasanasi, jotta huijarit eivät voi käyttää niitä uudelleen.

Ilmoita ja varoita:

Ilmoita tapauksesta poliisille tai kansalliselle finanssialaa valvovalle viranomaiselle (↖) ja kerro asiasta verkostossasi (esim. ystäville ja perheelle) tietoisuuden lisäämiseksi. Nämä toimet voivat auttaa suojaamaan itseäsi ja muita.

Varo ”jatkohuijauksia”:

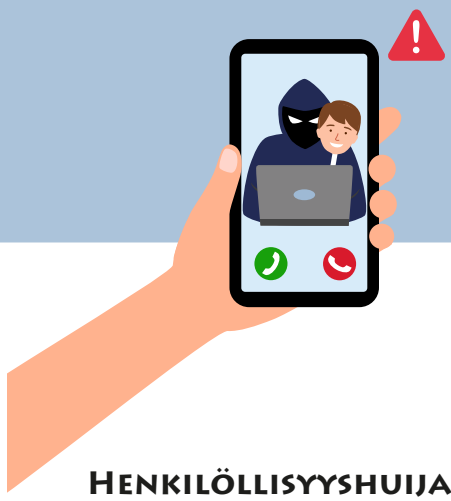
Huijari voi ottaa sinuun yhteyttä tietäen, että olet joutunut aiemmin huijauksen uhriksi, väittäen olevasi viranomainen (esim. poliisi, veroviranomainen tai Finanssivalvonta jne.) ja tarjoten apua menettämiesi rahojen palauttamiseksi maksua vastaan. Tämä on usein uusi huijausyritys. Muista, kerran huijatuksi joutuminen ei estä sinua joutumasta huijatuksi uudelleen.

Euroopan pankkiviranomainen, Euroopan vakuutus- ja lisäeläkeviranomainen, Euroopan arvopaperimarkkinaviranomainen, 2025

Luxemburg: Euroopan unionin julkaisutoimisto, 2025

PDF ISBN 978-92-9407-278-8 doi:10.2853/2980291 DZ-01-25-166-FI-N

Verkossa tapahtuvat talouspetokset ja -huijaukset, joissa hyödynnetään tekoälyä



Henkilöllisyyshuijaus ja deepfake-teknologian käyttäminen

Saat odottamattoman puhelun henkilöltä, joka väittää olevansa pankkivirkailijasi, viranomaisen (esim. poliisi, veroviranomainen tai Finanssivalvonta) tai vakuutusyhtiön edustaja, IT-yritys tai jopa perheenjäsenesi. Soittaja voi painostaa sinua siirtämään varoja “turvaan” vedoten epäilyttävään toimintaan tililläsi tai vakuutuksessasi. Hän voi myös pyytää sinulta pankkitietojasi (esim. maksukortin numero, verkkopankkitunnukset tai salasanat), klikkaamaan linkkiä tai asentamaan ohjelmiston väittäen sen ratkaisevan ongelman nopeasti. Soittaja voi käyttää väärennettyä numeroa, joka näyttää pankkisi viralliselta puhelinnumerolta (spoofing).

Huijarit voivat käyttää tekoälyä luodakseen väärennettyjä videoita, kuvia tai ääntä, jotka jäljittelevät jonkun ääntä (esim. pankkivirkailija tai perheenjäsen), kasvoja (esim. julkisuuden henkilö) tai liikkeitä. **Tätä kutsutaan deepfakeksi.**

Mitä voi tapahtua:

Luomalla kiireen tuntua ja käyttämällä henkilökohtaisia tietoja huijari yrittää saada sinut toteuttamaan toimenpiteitä, joita et aikonut toteuttaa, kuten siirtämään rahaa, klikkaamaan haitallista linkkiä tai asentamaan haittaohjelman laitteellesi. Näin huijari voi saada pääsyn pankkitunnuksiisi, joiden avulla hän voi vaihtaa salasanasi, käyttää pankkitiliäsi ja varastaa rahasi. Muista: vaikka soittaja tietää henkilökohtaisia tietojasi, ei se tee hänestä luotettavaa.

Tietojenkalastelu ja sosiaalinen manipulointi (social engineering)

Saat sähköpostin tai viestin, joka näyttää tulevan pankiltasi tai rahoitusyhtiöltäsi, jossa sinua varoitetaan ”epäilyttävästä toiminnasta” tililläsi. Logo, ulkoasu ja kieli näyttävät ammattimaisilta, ja viesti voi esiintyä samassa ketjussa aiempien pankkiviestiesi kanssa. Viestissä kehotetaan klikkaamaan linkkiä tilin vahvistamiseksi tai salasanan vaihtamiseksi. Linkki johtaa kuitenkin väärennetylle verkkosivustolle, joka näyttää identtiseltä verkkopankkisi kanssa. Huomaamattasi syötät tietosi verkkosivustolle, joka on luotu varastamaan tietosi.

Huijarit käyttävät tekoälyä luodakseen uskottavia tietojenkalasteluviestejä analysoimalla sosiaalisen median tietoja ja räätälöimällä sisällön kohteelle.

Mitä voi tapahtua:

Huijari saa pääsyn pankkitilillesi ja varastaa rahasi tai luo väärennetyn profiilin tiedoillasi tehdäkseen petoksia.

Sijoitus- tai vakuutushuijaus

Näet sosiaalisessa mediassa tai verkkosivustolla mainoksen, jossa tarjotaan ”sijoitusmahdollisuutta pienellä riskillä vain rajoitetun ajan” tai ”rajoitetun ajan voimassa olevaa alennusta” vakuutuksesta tunnetulta yritykseltä. Mainos sisältää tunnetun henkilön kuvan ja suosituksia, jotka ovat usein väärennettyjä. Kun olet ilmaissut kiinnostuksesi klikkaamalla linkkiä tai täyttämällä lomakkeen, sinuun otetaan yhteyttä ja ohjataan alustalle tai viestintäkanavalle, jossa saat ammattimaiselta näyttäviä neuvoja ja asiakirjoja. Sinua rohkaistaan sijoittamaan ensin pieni summa, jota seuraa suurempia summia, tai maksamaan vakuutusmaksu näennäisesti turvalliselle tilille.

Huijarit hyödyntävät tekoälytyökaluja luodakseen erittäin uskottavan näköisiä väärennettyjä ehdotuksia tai sähköposteja, joita on vaikea havaita huijauksiksi. He käyttävät myös tekoälypohjaisia sosiaalisen median botteja luodakseen väärennettyjä tilejä, jotka ovat vuorovaikutuksessa kanssasi, levittävät väärää tietoa ja simuloivat todellista käyttäytymistä luottamuksen rakentamiseksi ja vaikuttaakseen päätöksiisi.

Mitä voi tapahtua:

Kun yrität nostaa rahasi tai tehdä korvausvaatimuksen, yhteydenpito lakkaa. Huomaat, ettei yritystä ole olemassa tai ettei vakuuttamasi riski kuulu vakuutusturvan piiriin. Rahasi on lähetetty suoraan huijarille osana huijausjärjestelmää, eikä niitä voi saada takaisin. Lisäksi henkilökohtaisia ja taloudellisia tietojasi voidaan käyttää lisäpetoksiin (esim. allekirjoittamalla sopimuksia nimissäsi, mikä voi johtaa lisätappioihin).

Rakkauspetokset ja -huijaukset

Sinuun ottaa yhteyttä sosiaalisessa mediassa, deittisovelluksissa tai puhelimitse tai tekstiviestillä henkilö, jota et ole tavannut. Hän käy kanssasi henkilökohtaisia ja romanttisia keskusteluja usein rakentaen luottamusta väärennetyn profiilin avulla. Ajan myötä keskustelu siirtyy rahaan tai sijoitusmahdollisuuksiin, kuten kryptosijoituksiin, joissa luvataan korkeita tuottoja pienellä riskillä. Henkilö pyytää sinua siirtämään rahaa tilille tai opastaa sinua tilin perustamisessa ja pienen alkusijoituksen tekemisessä, jolla saa järjestelmän näyttämään lailliselta ennen kuin rohkaisee sinua sijoittamaan enemmän.

Huijarit käyttävät tekoälyä luodakseen väärennettyjä profiileja, tunnistaakseen uhreja sosiaalisessa mediassa tai deittisovelluksissa antamiesi tietojen avulla tai luodakseen viestejä chatbottien avulla.

Mitä voi tapahtua:

Huijari vie mahdollisimman paljon rahaa ennen kuin katkaisee kaiken yhteyden ja katoaa. Väärennetty sijoitussivusto tai -sovellus poistetaan tai ajetaan alas, jolloin et pääse käsiksi “sijoituksiisi”. Taloudellisten tappioiden lisäksi jakamiasi henkilötietoja voidaan käyttää huijausten kohdistamiseksi ystäviisi tai perheenjäseniisi tai identiteettivarkauksiin, joilla voi olla taloudellisia tai oikeudellisia seurauksia sinulle (esim. huijari voi tehdä ostoksia tai ottaa lainoja nimissäsi, tai sinua voidaan pitää vastuullisena veloista tai rikoksista, jotka on tehty nimissäsi, kunnes toisin todistetaan).

Ostohuijaus

Törmäät houkuttelevaan tarjoukseen verkkomarkkinapaikalla. Yritys pyytää maksua virallisen alustan ulkopuolella väittäen käyttävänsä ”turvallista maksujärjestelmää” ja lähettää sinulle linkin ostoksen suorittamiseksi. Linkki ohjaa sinut väärennetylle pankin tunnistautumissivulle, joka jäljittelee pankin virallista verkkosivustoa ja käyttää sen logoa ja ulkoasua, joten syötät verkkopankkitietosi maksua varten.

Huijarit käyttävät tekoälyä luodakseen erittäin uskottavan näköisiä väärennettyjä pankkisivustoja, tilausvahvistuksia ja laskuja. Tekoäly auttaa heitä jäljittelemään oikeiden yritysten kieliasua, brändiä ja tyyliä. Joissakin tapauksissa he käyttävät tekoälychatbotteja vastaamaan kysymyksiin saaden kaupasta entistä uskottavamman.

Mitä voi tapahtua:

Maksu kolmannen osapuolen linkin kautta ohittaa markkinapaikan suojan. Huijari saa verkkopankkitunnuksesi ja varastaa rahasi.