Yleisimmät huijaukset ja parhaat toimintatavat niiden välttämiseen

Verkkosivuhuijaukset:

Verkkosivuhuijauksia tehdään pankkien, yritysten ja viranomaisten nimissä. Hakukoneiden (esimerkiksi Google tai Bing) hakutuloksissa saattaa olla linkkejä, jotka vievät huijaussivulle. Huijaussivu saattaa näyttää pankin tai viranomaisen verkkosivulta. Huijaussivulle syötetyt pankkitunnukset tai muut henkilötiedot päätyvät vääriin käsiin.

Toimi näin:

- Kirjoita selaimen osoiteriville pankin tai viranomaisen verkkosivun koko osoite, esimerkiksi www.op.fi, www.nordea.fi tai www.kela.fi.
  Tarkista sivun osoite ennen kirjautumista.
  Tallenna tärkeät verkkosivut selaimesi kirjanmerkkeihin tai suosikkeihin. Pääset näin sivulle jatkossa suoraan käyttämättä hakukoneita.
- Pankit tarjoavat yleensä mobiilisovelluksen, jonka kautta pankkiasioiden hoitaminen on turvallista.
- Jos syötät henkilötietojasi tai pankkitunnuksesi epäilyttävälle sivulle, ole välittömästi yhteydessä pankkiisi ja poliisiin. Ilmoita huijauksesta myös organisaatiolle, jonka nimissä huijaussivusto esiintyy.

Puhelimitse tapahtuvat huijaukset:

IT-tukihuijaukset

IT-tukihuijauksessa uhri saa puhelun, jossa soittaja väittää olevansa teknologiayrityksen, usein Microsoftin tuesta. Hän sanoo tietokoneesi olevan hyökkäyksen kohteena ja pyytää sinua toimimaan antamiensa ohjeiden mukaan. Esimerkiksi Microsoft ei koskaan soita suoraan henkilöasiakkaille ilman että asiakas on ensin itse ollut Microsoftiin yhteydessä. Microsoft ei koskaan pyydä henkilötunnusta, pankkitunnuksia tai kuvia ajokortista, passista tai muusta henkilöllisyystodistuksesta.

Toimi näin:

- Jos saat yllättäen puhelun, jonka soittaja väittää olevansa IT-tuesta, lopeta puhelu heti.
- Jos annat huijarille tietojasi, ole välittömästi yhteydessä pankkiisi ja poliisiin.
- Lue Microsoftin sivuilta tietoa teknisen tuen huijauksilta suojautumisesta.

Kalastelupuhelut viranomaisten ja pankkien nimissä

Poliisin, Kelan tai pankkien nimissä tehdyt huijaussoitot ovat olleet jo vuosien ajan yleisiä. Soittaja esittäytyy esimerkiksi poliisiksi tai pankin turvallisuusyksikön työntekijäksi ja kertoo, että omaisuutesi on vaarassa tai tililläsi on epätavallisia tapahtumia. Hän pyytää sinua toimimaan ohjeistamallaan tavalla, jotta rahasi saadaan suojattua ja rikolliset otettua kiinni.

Soittajan tavoitteena on saada sinulta verkkopankkitunnukset tai korttitiedot. Näiden tietojen avulla rikolliset siirtävät uhrin tililtä rahaa omille tileilleen.

Pankit, Kela, Poliisi tai muutkaan viranomaiset eivät koskaan pyydä pankkitunnuksia tai muita tietoja, joilla kirjaudut palveluihin.

Toimi näin:

- Jos saat puhelun pankin, poliisin tai muun viranomaisen nimissä ja soittaja pyytää sinua kertomaan verkkopankkitunnuksesi ja/tai antamaan korttitietosi puhelimitse, lopeta puhelu.
- Varmista aina, että puhelu tulee siltä organisaatiolta, jonka nimissä soittaja esittäytyy. Voit esimerkiksi kysyä asiakkuudestasi jotain sellaista, johon vain organisaation virallinen edustaja osaa vastata tai kysyä, voitko soittaa takaisin organisaation puhelinvaihteen kautta.
- Jos annat huijarille tietojasi, ole välittömästi yhteydessä pankkiisi ja poliisiin.

Tietojenkalastelu sähköpostiviestillä ja tekstiviestillä

Pankin tai viranomaisen, kuten Veron, nimissä tulevat huijausviestit voivat tulla sähköpostilla, tekstiviestillä, WhatsAppilla tai sosiaalisen median palvelun yksityisviestillä. Huijausviestissä on yleensä linkki, jonka kautta sinua kehotetaan kirjautumaan. Linkki ohjaa huijaussivulle, jonka tarkoituksena on saada henkilötietojasi, maksukorttisi tietoja tai pankkitunnuksesi.

Viestissä on usein painostava sävy. Viestin saajaa kehotetaan toimimaan nopeasti ja tekemään pakolliset toimenpiteet tai palveluiden käyttö voidaan katkaista.

Viesti voi olla virheetöntä suomen tai ruotsin kieltä ja se saattaa tulla samaan viestiketjuun, jossa on virallisen tahon aikaisemmin sinulle lähettämiä viestejä.

Toimi näin:

- Jos saat tekstiviestin tai sähköpostin viranomaiselta tai pankiltasi, älä klikkaa viestissä olevia linkkejä.
- Älä vastaa saamiisi viesteihin.
- Voit tarkastaa pankin tai viranomaisen sinulle laittamat viestit kirjautumalla organisaation verkkopalveluun turvallisesti organisaation omilta verkkosivuilta.
- Ilmoita epäilyttävistä viesteistä poliisille ja organisaatiolle, jonka nimissä viestejä on lähetetty.
- Jos syötät henkilötietojasi tai pankkitunnuksesi epäilyttävälle sivulle, ole välittömästi yhteydessä pankkiisi ja poliisiin. Ilmoita huijauksesta myös organisaatiolle, jonka nimissä huijaussivusto esiintyy.

Sijoitushuijaukset

Sijoitushuijaukset lähtevät liikkeelle yleensä sosiaalisen median, sähköpostin tai puhelun välityksellä. Rikolliset mainostavat sijoituskohdetta jonka tuottojen luvataan olevan

”tähtitieteellisiä”. Yleisimpiä viime aikoina liikkeellä olleita sijoitushuijauksia ovat huijaukset, joissa mainostetaan vilpillisesti julkisuuden henkilön nimissä jotain pettämätöntä sijoituskohdetta, esimerkiksi kryptovaluuttaa. Nyrkkisääntönä on, että jos joku sijoituskohde kuulostaa liian hyvältä ollakseen totta niin silloin kyseessä on hyvin suurella todennäköisyydellä huijaus. On olemassa myös teknisesti kehittyneempiä sijoitushuijauksia, joissa rikollistaho on tehnyt uskottavan näköisen verkkosivun josta asiakas voi ikään kuin seurata sijoituksiaan, mutta todellisuudessa sivusto on tekaistu ja rahat menevät rikollisille.

Toimi näin:

- Epäile aina kun some-kanaviisi tai sähköpostiisi ilmestyy sijoituksiin liittyvä ”huipputarjous” jossa luvataan ruhtinaallisia tuottoja.
- Älä klikkaa linkkiä jos se vaikuttaa sinusta epäilyttävältä tai lähestyvä taho ei ole tuttu.
- Epäile aina jos tuntematon sijoitusneuvojaksi esittäytyvä henkilö on sinuun yhteydessä puhelimen, sosiaalisen median tai sähköpostin välityksellä. Tarkista henkilön ja hänen edustamansa yrityksen taustat netistä. Mikäli yrityksestä ei ole helposti tietoa saatavilla tai tieto on vajavaista niin usein kyseessä on huijausyritys.

Toimitusjohtajahuijaukset

Toimitusjohtajahuijauksesta puhutaan esim. silloin, kun rikollinen lähettää yrityksen toimitusjohtajan (tai muun johtohenkilön) nimissä sähköpostiviestillä yrityksen maksuliikenteestä vastaavalle henkilölle pyynnön suorittaa kiireellinen maksu. Rikollinen on yleensä luonut sähköpostitilin joka eroaa toimitusjohtajan sähköpostiosoitteesta mahdollisimman vähän, usein vain yhden merkin tai kirjaimen verran, jolloin sähköpostiosoitteen eroa on hyvin vaikea havaita. On myös mahdollista, että rikolliset ovat onnistuneet kaappaamaan toimitusjohtajan oikean sähköpostitilin, jolloin huijaus on entistäkin uskottavampi.

Toimi näin:

- Pelkän sähköpostiviestin perusteella ei kannat suorittaa maksuja varsinkaan silloin kun saaja on uusi tai saajan tilinumero on vaihtunut
- Yrityksen maksuista vastaavan henkilön on syytä aina varmistaa maksupyynnön oikeellisuus esimerkiksi soittamalla henkilölle jolta maksupyyntö näyttää tulleen.

Lisätietoja, kampanjamateriaaleja ja linkkejä aikaisempiin ohjeisiin ja tutkimuksiin löytyy osoitteesta huijausinfo.fi

Lisätietoja medialle:

Finanssiala ry: Niko Saxholm, niko.saxholm@finanssiala.fi, 020 793 4235

Poliisi: Tuomas Pöyhönen tuomas.poyhonen@poliisi.fi

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus: kyberturvallisuuskeskus@traficom.fi

Kela: Henri Burtsov, henri.burtsov@kela.fi

Digi- ja väestötietovirasto: Kimmo Rousku, kimmo.rousku@dvv.fi, 0295 553 5120

Kuluttajaliitto: Tapani Veija, tapani.veija@kuluttajaliitto.fi

Aktia: Henri Heinonen, henri.heinonen@aktia.fi

Handelsbanken: Harri Hautala, harri.hautala@handelsbanken.fi, 050 323 0637

Nordea: Annukka Multanen, annukka.multanen@nordea.com, 050 302 7815

Oma Säästöpankki: Markku Luova, markku.luova@omasp.fi

OP Ryhmä: Kim Sirén, kim.siren@op.fi

POP Pankki: Guoxi Yu, guoxi.yu@poppankki.fi F

S-Pankki: Juha Nieminen, juha.a.nieminen@s-pankki.fi 050 599 1882.

Säästöpankki: Vesa Pyyluoma, vesa.pyyluoma@saastopankki.fi, 040 647 1900

Microsoft: Marja Laitinen, marja.laitinen@microsoft.com