Lisätietoliite: Ajankohtaisia esimerkkejä nettihuijauksista ja vinkkejä niiltä suojautumiseen

Kalasteluhuijaukset verkkokaupankäynnissä

Tavaran ostajaa esittävä huijari lähettää verkkokauppa-alustalla myyjälle tekstiviestillä tai WhatsAppilla linkin kuljetuspalvelun tai verkkokaupan maksupalvelun valesivulle. Valesivulla pyydetään myyjän verkkopankkitunnuksia ja maksukortin tietoja, jotta huijari voi maksaa tekemänsä ostoksen.

Suojautuminen:

- Ostaja tai maksupalvelu ei tarvitse myyjän verkkopankkitunnuksia tai maksukortin tietoja. Ostaja tarvitsee ainoastaan myyjän tilinumeron. Verkkopankkitunnuksia tai maksukortin tietoja kyselevä taho on siis todennäköisesti huijari. Ilmoita asiasta poliisille ja pankkiin.
- Jos sinulle lähetetään linkki maksupalveluun, kyseessä on todennäköisesti huijaus. Ilmoita asiasta poliisille ja pankkiin.
- Jos olet luovuttanut verkkopankkitunnukset tai maksukorttisi tiedot tai epäilet maksaneesi huijarille, ole mahdollisimman pian yhteydessä ensin pankkiisi ja sitten poliisiin.

Facebook-huijaukset

Huijari kaappaa henkilön Facebook-tilin, ottaa Messengerillä yhteyttä henkilön Facebook-kavereihin ja ilmoittaa arpajaisvoitosta. Sen jälkeen huijari pyytää uhrin puhelinnumeroa voidakseen lähettää tekstiviestillä linkin huijaussivulle. Huijaussivulla uhrilta pyydetään pankkitunnukset tai maksukortin tiedot voiton lunastamiseksi. Sen seurauksena huijari pääsee tekemään maksuja uhrin tililtä ja tarvittaessa manipuloi uhrin vahvistamaan maksut.

Samaa menetelmää käytetään myös Instagramissa, joten sosiaalisessa mediassa pitää ylipäätään suhtautua varauksella epätavallisiin yhteydenottoihin.

Toisessa Messengerin kautta tapahtuvassa huijauksessa uhrille lähetetään koodi, jonka syöttäessään hänen käyttäjätilinsä päästään kaappaamaan. Sitä ennen keskustelua kuitenkin jatketaan ja kerrotaan mahdollisuudesta osallistua arvontaan tai kilpailuun. Uhrilta pyydetään verkkopankkitunnukset ja hänet huijataan itse vahvistamaan maksuja. Joissain tapauksissa huijarit asentavat itselleen uhrin käyttämän tunnistautumissovelluksen, jolloin he voivat itse käyttää uhrin tiliä.

Ole erityisen varovainen, jos joku tuttusi tiedustelee Messengerin kautta esimerkiksi puhelinnumeroasi tai pyytää lähettämään sinulle tulleen tekstiviestin. Tuttusi sijaan tietojasi kysyy huijari. Jos luovutat ne, huijari pystyy mahdollisesti kaappaamaan Facebook-tilisi.

Suojautuminen:

- Älä luovuta verkkopankkitunnuksia tai maksukortin tietoja kenellekään, älä edes läheisille tai ystäville.
- Maksaja ei tarvitse verkkopankkitunnuksia tai maksukorttisi tietoja. Maksaja tarvitsee ainoastaan tilinumerosi. Verkkopankkitunnuksia tai maksukortin tietoja kyselevä henkilö on siis huijari. Ilmoita asiasta poliisille ja pankkiin.

- Vaikka viesti näyttää tulevan tutulta ihmiseltä, sen lähettäjä voi olla huijari, joka on kaapannut tuttavasi käyttäjätilin.
- Jos olet luovuttanut verkkopankkitunnukset tai maksukortin tiedot tai epäilet maksaneesi huijarille, ole mahdollisimman pian yhteydessä ensin pankkiisi ja sitten poliisiin.

WhatsApp-huijaus

Huijari esittää uhrin aikuista lasta ja kertoo joutuneensa vaihtamaan sekä puhelimen että puhelinnumeron, koska entinen puhelin on mennyt rikki (esim. pesukoneessa). Sen jälkeen huijari ilmoittaa tarvitsevansa heti rahaa ja pyytää sitä uhrilta. Yleensä rahat pyydetään maksamaan ulkomaalaiselle tilille.

Suojautuminen:

- Älä siirrä rahaa tilille ennen kuin olet varma, että viestin lähettäjä on se henkilö, joka hän esittää olevansa.
- Tarkista henkilön aiemmasta puhelinnumerosta, onko hänen puhelinnumeronsa oikeasti vaihtunut ja onko hän lähettänyt sinulle viestin.
- Jos viestissä oleva tilinumero on eri kuin henkilön aiempi tilinumero, varmista myös oikea tilinumero. Jos tilinumeron alussa on muu maakoodi kuin FI (Suomi), varmista maksunsaajalta erityisen huolellisesti, onko tilinumero oikea. Varmista tilinumero jotakin muuta kautta kuin siitä puhelinnumerosta, josta rahaa pyydetään.
- Jos henkilö ei vastaa aiemmasta puhelinnumerosta, varmista viestin aitous kasvokkaisessa tapaamisessa, jos se on mahdollista.
- Jos olet luovuttanut verkkopankkitunnukset tai maksukorttisi tiedot tai epäilet maksaneesi huijarille, ole mahdollisimman pian yhteydessä ensin pankkiisi ja sitten poliisiin.

Flubot-huijausviestit

Etenkin Android-puhelimen käyttäjille lähetettiin kevään 2022 aikana huijausviestejä, joiden tarkoitus oli saada viestin vastaanottaja lataamaan haittaohjelma puhelimeensa. Haittaohjelman avulla rikolliset pääsevät käsiksi puhelimen sisältöön, yhteystietoihin ja viesteihin. He käyttävät saamiaan tietoja tunkeutuakseen käyttäjän sosiaalisen median tileille ja saadakseen muuta taloudellista hyötyä.

Europol sai hajotettua huijauksia tehneen rikollisjärjestön toukokuun lopussa.

Valepoliisit ja valepankit

Uhrille soitetaan puhelimella. Hänelle kerrotaan, että hänen pankkitilinsä on kaapattu ja että poliisi tai pankki tarvitsee verkkopankkitunnukset ja mahdollisesti myös maksukortin tiedot rikoksen estämiseksi.

Poliisia esittävät huijarit toimivat myös verkon ulkopuolella. He voivat tulla uhrin kotiovelle pyytämään verkkopankkitunnuksia ja maksukorttia.

Suojautuminen:

- Poliisi tai pankki ei koskaan soita tai käy kotiovella pyytämässä verkkopankkitunnuksia tai maksukortin tietoja. Jos näin tapahtuu, kyseessä on huijaus. Lopeta puhelu tai sulje ovi välittömästi. Ilmoita asiasta pankkiin ja poliisille.
- Jos olet luovuttanut verkkopankkitunnukset tai maksukortin tiedot tai epäilet maksaneesi huijarille, ole mahdollisimman pian yhteydessä ensin pankkiisi ja sitten poliisiin.

Tekstiviestillä saapuvat pyynnöt

Suhtaudu varauksella kaikkiin tekstiviesteihin, jossa sinua pyydetään avaamaan linkki tai liitetiedosto, asentamaan ohjelma tai luovuttamaan tietojasi. Huijarit voivat lähettää viestejä myös pankkien, kuljetusyritysten ja suurten yritysten nimissä.

Puhelinnumeroiden väärentäminen

Rikolliset pystyvät myös väärentämään puhelinnumeroita. Jos saat puhelun suomalaisesta numerosta ja epäilet puhelun jälkeen sen aitoutta tai olet muuten huolissasi puhelusta, voit soittaa takaisin kyseiseen numeroon tarkistaaksesi asian. Ulkomaalaisiin puhelinnumeroihin ei kannata soittaa takaisin, koska niihin on saatettu kytkeä erilaisia laskutushuijauksia.

Traficomin Kyberturvallisuuskeskus ja teleoperaattorit ovat valmistelleet erilaisia teknisiä ratkaisuja numeronväärennyksen estämiseksi. Jos suomalaiselta näyttävästä numerosta saapuva puhelu tulee tosiasiassa ulkomailta, numeron näkyminen pystytään jatkossa estämään.

QR-koodihuijaukset

Viime aikoina on havaittu väärennettyjä QR-koodeja myyntipisteiden, kuten huoltoasemien, yhteydessä. Kun koodin lukee, päätyy väärennetylle verkkosivustolle. Ole tarkkana, jos käytät maksamisessa QR-koodeja.

Toimi näin, jos epäilet maksutietojesi päätyneen huijareille

Hyödynnä Digi- ja väestötietoviraston ohjetta: Henkilötietojani on viety tai vuotanut – Suomi.fi