

# Henkilön manipulointi (Social engineering)

## 1. Mitä on henkilön manipulointi?

Kun puhutaan henkilön manipuloinnista silloin, on kyseessä tilanne, jossa henkilöä yritetään manipuloinnin avulla saada luovuttamaan tietoja tai dataa. Tapoja on useita erilaisia, mutta yleisimmät tavat on, kun huijari tekeytyy esimerkiksi IT-tuen edustajaksi tai työkaveriksi. Huijaukset voivat tapahtua verkossa, puhelimitse tai kasvotusten. Manipuloinneista vaarallista tekee se, että ne ovat tarkasti suunniteltuja. Yleensä huijaaja kerää taustatietoa uhristaan, jotta yhteydenotto olisi mahdollisimman uskottava. Sen jälkeen huijaaja ottaa yhteyttä uhriin ja yrittää luoda uskottavan tuntuksen kanssa käymisen. Lopuksi kun uhri on saatu tekemään toivottu toimenpide, huijaaja tekee petoksen. Tärkeintä on tiedostaa, että pienikin määrä tietoa huijarille voi olla tarpeeksi yhdistää tiedon olemassa olevaan tietoon, jonka seurauksena huijari voi päästä käsiksi sisäverkkoon tai käyttäjätileille.

## 2. Mitkä ovat tyypillisiä piirteitä manipuloinnille?

Yleisimmät manipuloinnin piirteet ovat suostuttelu ja luotettavuus, jota käytetään lähestymis- taktiikkana. Sen avulla saadaan uhri antamaan tietoa, jota muuten et luovuttaisi. Myös tunteiden manipuloinnilla yritetään saada uhri tuntemaan sääliä, syyllisyyttä, pelkoa tai innostusta. Kuten aikaisemmin mainittu hyökkääjä on suunnitellut yhteydenottoa, joten heidän yhteydenottonsa voi kuulostaa uskottavalta tiedon saamisen perusteeksi.

## 3. Käyttäjän manipulointi tapoja

### Houkuttelu

- Houkuttelu tapahtuu siten, että huijari yhteydenotossa houkutellaan sinut tekemään, jotain esimerkiksi klikkaamaan sinua kiinnostavaa linkkiä tai liittämään kirjekuoressa saadun USB-muistitkun tietokoneeseesi, jossa voisi olla haittaohjelma.

### Peitetarina

- Tällaisessa hyökkäyksessä uhrit yritetään kerätä tietoa peitetarinan varjolla, kuten Internet-kyselyn. "Vastaa kuinka suuri hiilijalanjälki sinulla on?"

### Tietojenkalastelu

- Tietoja voidaan pyytää sähköpostitse, tekstiviestillä tai puhelinsoitolla, tekeytymällä aidolta vaikuttavalta lähteeltä, kuten pankilta, kuriiriyritykseltä tai johtoryhmän jäseneltä.

## 4. Torjuntakeinot

### Rauhoita tilanne

- Jos tilanne vaikuttaa kiireelliseltä tai sinua painostetaan on tärkeää pysähtyä hetkeksi harkitsemaan seuraavaa toimenpidettä. Huijarit pyrkivät kiireellisyyteen, jotta sinulla ei olisi aikaa miettiä asiaa perusteellisesti.

### Tarkista oikeinkirjoitus

- Suurin osa kalasteluviesteistä, jotka ovat suomen kielellä on käännetty käännös ohjelman avulla. Silloin tekstistä löytyy kirjoitusvirheitä tai viesti on kirjoitettu huonosti, joka voi viitata huijaukseen.

### Mitä tietoa yhteydenottajalla on sinusta?

- Yhteydenotossa on hyvä huomioda, mitä tietoa yhteydenottajalla on sinusta. Jos yhteydenottajalla puuttuu tieto, joka hänellä ehdottomasti pitäisi olla voi kyseessä olla tekaistu yhteydenotto, joka voi olla sähköpostitse, puhelimitse tai tekstiviestitse.

### Pyydä yhteydenottajaa todistamaan henkilöllisyytensä

- Kuten mainittu sosiaalinen manipulointi voi tapahtua kasvotusten. Jos tuntematon henkilö yrittää rakennukseen sisään vaikka kantaen tikkaita, on häneltäkin varmistettava henkilöllisyys. Kantaen, jotain tavaraa hämätään uhria avaamaan lukittu ovi huijarille. Sama pätee muihin yhteydenottoihin, pyydä esimiehen nimeä sekä puhelinnumeroa ja varmista tietojen paikkansapitävyys.

### Onko tilanne realistinen?

- Realistisella ajattelulla tarkoitetaan sitä, että ymmärrät mikä voisi oikeasti olla mahdollista ja miksi se tapahtuisi. Jos saat sähköpostin, jonka liitteenä "Palkkatiedot" Word-tiedosto ja et käsittele työssäsi kenenkään palkkatietoja on tärkeää miettiä, miksi kyseinen tiedosto lähetettäisiin minulle? Sama pätee, jos esimiehesi soittaa pyytää sinua tekemään, jotain yllättävää. Tekisikö esimieheni näin? Tilanteen realismisuuden pohtiminen voi auttaa torjumaan monia tällaisia hyökkäyksiä.