



TIETOJENKALASTELU JA IDENTITEETTIVARKAUDET VERKOSSA

Mitä ne ovat, miten niiltä suojaudutaan? Varoitusmerkit ja vinkit

Digitaalisten palvelujen yleistymisen myötä on tullut yhä tärkeämmäksi, että verkkopalveluihin kirjaudutaan turvallisesti ja että kirjautumistiedot eivät ole verkkorikollisten helposti saatavilla tai arvattavissa. Verkossa käsitellään niin arkaluonteisia terveystietoja kuin raha-asioita. Näiden menetys tai vaarantuminen voi aiheuttaa merkittävää henkistä ja taloudellista haittaa.

Mikä on identiteettivarkaus?

Lue lisää identiteettirikoksista Rikosuhrripäivystyksen sivuilta.

Identiteettivarkauudessa

on kyse tilanteesta, jossa esiinnyttäen toisen henkilöllisyydellä. Rikoksen tekijä erehdyttää tarkoituksellisesti kolmatta osapuolta käyttämällä jonkun muun henkilön henkilötietoja,

tunnistautumistietoja

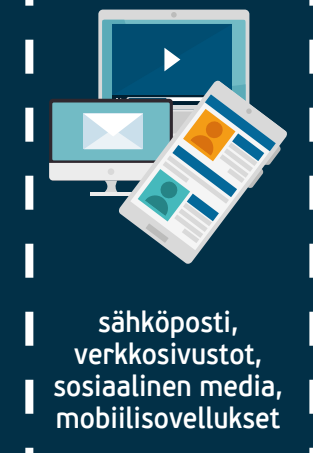
tai muuta vastaavaa toisen henkilön yksilöivää tietoa. Tämä voi tarkoittaa esimerkiksi toisena ihmisenä esiintymistä sosiaalisessa mediassa, toisen ihmisen nimissä tehtyä osamaksukauppaa tai verkkokauppa- tai lehtitilautusta.



Tietojenkalastelun tyypit

Sähköpostin tietojenkalastelu

Henkilökohtaisten tietojen hankkiminen uhrilta esiintymällä hyvämaineisena yrityksenä.



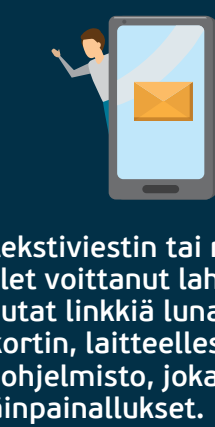
Saati pankiksi väärennetyt turvallisuusvaroitukset, jossa pyydetään antamaan käyttäjätunnukset ja salasanasasi.

SMS-kalastelu

Käytäntö huijata käyttäjää lataamaan haittaohjelmia tai viruksia käyttämällä syötti- ja kytkintekstiviestiä (SMS).



langattomat laitteet



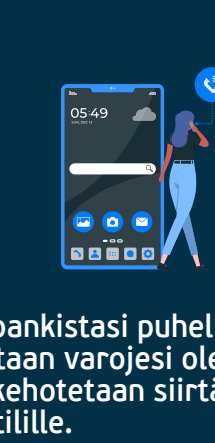
Saati tekstiviestin tai muun viestin, että olet voittanut lahjoituksen. Kun napsautat linkkiä luvustaaksesi lahjakortin, luittelee asentuu haittaohjelma, joka kirjaa kaikki näppäinpainallukset.

Huijauspuhelut

Viipilliset puhelut, joiden tarkoituksena on kerätä arkaluonteisia henkilötietoja.



langattomat laitteet, puhelimet



Saati pankistasi puhelun ja siinä kerrotaan varojesi olevan vaarassa sekä kehoitetaan siirtämään varot turvapaikalle.

Valastelu

Valastelu on suunnattu korkean tason johtajille. Hyökkääjät esiintyvät luotettavina toimijoina tarkoituksenaan varastaa rahaa tai tietoa.



sähköposti, sosiaalinen media

Talusojohtaja kirjoittaa sosiaalisessa mediassa turnuksesta. Turnuksen sponsorin nimissä hänelle saapuu sähköpostia otsikolla "Suuri peli sunnuntaina". Sähköpostissa on kuva, joka sisältää erittäin tervettä tietoa varastavan haittaohjelman.

Hakukone tietojenkalastelu

Hakkerit luovat oman verkkosivustonsa ja saavat sen indeksoitua laillisiin hakukoneisiin.

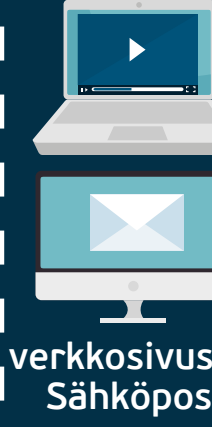


sivustot

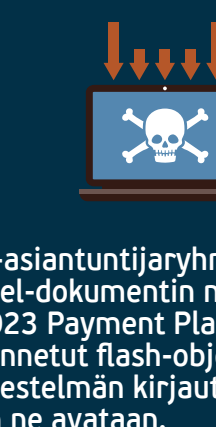
Etsit verkossa tietoa viranomaisista. Hakutulosten joukossa on väärennetyjä sivuja.

Kohdistettu tietojenkalastelu

Tietojenkalastelu kohdistuu tietyyn ryhmään tai henkilöön, kuten yrityksen



verkkosivustot, sähköposti



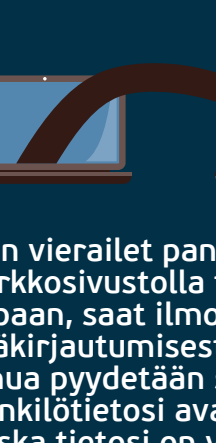
HR-asiantuntijaryhmä saa Excel-dokumentin nimeltä "2023 Payment Plan". Siinä asennetut flash-objektit keräävät kirjotettua kirjautumistietoja, kun ne avataan.

Sivustoharhautus

Sivustoharhautus ohjaa uhrit hyökkääjän hallitsemalle verkkosivustolle suorittamalla haitallisen koodin uhrin laitteella.



verkkosivustot, tietokoneet



Kun vieraillet pankiksi verkkosivustolla tavalliseen tapaan, saat ilmoituksen etäkirjautumisesta, jossa sinua pyydetään syöttämään henkilötietosi avataksesi tilisi, koska tietosi on varastettu.

Näin suojaat tietosi verkossa tietojenkalastelulta

Käytä vahvoja salasanoja.

Merkittävä tietoturvariski syntyy käyttämällä samaa salasanaa kaikissa sähköisissä laitteissa ja tärkeissä käyttäjätileissä, joista on pääsy pankki- tai luottokorttitietoihisi. Jos käytät samaa salasanaa, huijari tarvitsee vain yhden salasanan päästäkseen kaikkiin tileihisi. Älä koskaan käytä nimeäsi tai syntymäpäivääsi salasanana. Vaihda salasana aina, kun epäilet, että tili on vaarassa.

Bonusvinkki: Käytä salasanaohjelmistoa salasanojen muistamiseen ja suojaamiseen.

Tarkista tiliotteesi usein.

Tilisi toiminta, mukaan lukien viimeksi ilmoitetut saldot, näkyy tiliotteessasi. Luottotilisi tapahtumien säännöllinen tarkistaminen on hyvä tapa havaita väärinkäytöksiä.

Bonusvinkki: Jos laskun tilitiedoissa tai summassa on jotakin epätavallista, ota yhteys laskun lähettäjään ja tarkista, että tiedot ovat oikein.

Käytä virtuaalista yksityisverkkoa.

Jos mahdollista, vältä julkisen wi-fi-verkon käyttöä kirjautuaksesi pankki- tai maksutileille tai syöttääksesi maksutietoja. Jopa verkot, joilla on salasanasuojaus, esimerkiksi kahviloiden maksuttomat internetverkot, voivat olla riskialttiita, jos salasana on helposti saatavilla.

Bonusvinkki: Muista, että jos kotiverkossasi ei vielä ole salasanaa, lisää se heti.

VPN-sovellusta käyttämällä voit muodostaa salatun yhteyden tietokoneesi tai mobiililaitteesi ja VPN-palvelimen välille, jos käytät julkista wi-fi-yhteyttä. VPN:n käyttö voi vähentää todennäköisyyttä, että joku varastaa tietosi, mutta se ei suojaa sinua kaikilta hyökkäyksiltä tai huijauksilta.

Älä klikkaa sähköpostien epäilyttäviä linkkejä.

Älä koskaan klikkaa linkkejä, jotka näyttävät epäilyttävilta sähköposteissa tai tekstiviesteissä. Tietojenkalastelijat käyttävät sähköposteja ja verkkosivustoja, jotka näyttävät tuleva pankilta, luottokorttiyhtiöstä, luotonantajalta tai muusta rahoituslaitoksesta huijataksesi sinua syöttämään tilitietojasi tai muita yksityisiä tietoja tietojenkalasteluun. Nämä sähköpostit voivat pyytää sinua avaamaan liitetiedoston, joka asentaa haitalliset haittaohjelmat laitteeseen.

Suojaa yksityiset dokumentit.

Myös fyysiset asiakirjat voivat aiheuttaa turvallisuusrisikin, jos niitä käsitellään väärin. Sosiaaliturvatunnukseksi ja pankkitilisi tiedot löytyvät useista asiakirjoista. Nämä asiakirjat voivat olla arvokkaita myös varkaille. Hävitä asianmukaisesti kotiisi saapuneet arkaluonteisia tietoja sisältävät asiakirjat. Postilaatikot on hyvä lukita, jotta ulkopuoliset eivät pääse niihin käsiksi.



Käytä monivaiheista tunnistautuminen.

Monivaiheinen tunnistautuminen (englanniksi multi-factor authentication, MFA) on ylimääräinen turvatoimenpide, käytetään käyttäjätilille kirjautumisessa. Käyttäjän on ensin syötettävä käyttäjätunnus ja salasana. Pääsy myönnetään tilille vasta sitten kun lisävarmistus on syötetty onnistuneesti. Sellainen voi olla esimerkiksi puhelimeen toimitettava kertakäyttöinen kirjautumiskoodi.

