



TIETOJENKALASTELU JA IDENTITEETTIVARKAUDET VERKOSSA

Mitä ne ovat, miten niiltä suojaudutaan?
Varoitusmerkit ja vinkit

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

Mikä on identiteettivarkaus?

Taloudellisen hyödyn tavoittelu Tämä on yleisin identiteettivarkauden muoto. Identiteettivaras voi avata luottokortin käyttämällä sinun sosiaaliturvatunnustasi tai pankkitietojasi, tarkoituksena varastaa rahaa tai tehdä hankintoja.	Sosiaaliturvatunnuksen väärinkäyttö Sosiaaliturvatunnustasi voidaan väärinkäyttää luottokorttien ja lainojen haettaessa ja sitten käyttää välttyäkseen maksamasta takaisin olemassa olevia lainoja. Huijarit voivat mahdollisesti käyttää tunnustasi haettaessa vakuutusta tai sosiaalietuuksia.	Sairausvakuutuksen luvaton käyttö Toisen henkilön sairausvakuutusta käytetään luvatta, etuuden nostaa henkilö, jolla ei ole sairausvakuutusta. Tämä identiteettivarkautapa on Suomessa harvinainen.	Rikollinen identiteettivarkaus Rikollisella identiteettivarkaudella tarkoitetaan tilanteita, joissa pidätystilanteessa henkilö käyttää väärä henkilö-tietoja, esimerkiksi näyttämällä väärennetyn ajokortin poliisille.
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Lue lisää identiteettirikoksista Rikosuhripäivystyksen sivuilta.



Tietojenkalastelun tyypit

Sähköpostin tietojenkalastelu
Henkilökohtaisten tietojen hankkiminen uhriin esiintymällä hyvämaineisena yrityksenä.
Sähköposti, verkkosivustot, sosiaalinen media, mobiilisovellukset.
Saat pankiksi väärennetyn turvallisuusvaroituksen, jossa pyydetään antamaan käyttäjätunnuksesi ja salasanasi.

Haittaohjelmat
Uhri huijataan lataamaan haittaohjelmia tai viruksia laitteelleen käyttämällä houkuttelevaa tekstiviestiä (SMS).
langattomat laitteet.
Saat tekstiviestin, jossa kerrotaan sinun voittaneen lahjakortin. Kun napsautat linkkiä, sivusto kehottaa asentamaan laitteellesi ohjelman lahjakortin lunastamiseksi. Todellisuudessa laitteellesi asennuu haittaohjelma, joka kirjaa kaikki näppäinpainallukset.

Huijauspuhelut
Viipilliset puhelut, joiden tarkoituksena on kerätä arkaluonteisia henkilötietoja.
langattomat laitteet, puhelimet.
Saat pankistasi puhelun ja siinä kerrotaan varojesi olevan vaarassa sekä kehoitetaan siirtämään varat turvalliselle.

Kohdistettu tietojenkalastelu
Tietojenkalastelu kohdistuu tiettyyn ryhmään tai henkilöön, kuten yrityksen järjestelmänvalvojaan.
verkkosivustot, sähköposti.
HR-asiantuntijaryhmä saa Excel-dokumentin nimeltä "2023 Payment Plan". Sitten asennetut flash-objektit keräävät järjestelmän kirjautumistietoja, kun ne avataan.

Sivustoharhautus
Sivustoharhautus ohjaa uhrit hyökkääjän hallitsemalle verkkosivustolle suorittamalla haitallisen koodin uhriin laitteella.
verkkosivustot, tietokoneet.
Kun vieraillet pankiksi verkkosivustolla tavalliseen tapaan, saat ilmoituksen etäkirjautumisesta, jossa sinua pyydetään syöttämään henkilötietoja arvokkaille tilille, koska tietosi on varastettu.

Valastelu
Valastelu on suunnattu korkean tason johtajille. Hyökkääjät esiintyvät luotettavina toimijoina tarkoituksenaan varastaa rahaa tai tietoa.
sähköposti, sosiaalinen media.
Tilousjohtaja kirjottaa sosiaalisessa mediassa tumauksesta. Tumauksen sponsorijan nimissä hänelle saapuu sähköpostia otsikolla "Suuri peli sunnuntai". Sähköpostissa on kuva, joka sisältää arvokasta tietoa varastavan haittaohjelman.

Hakukone tietojenkalastelu
Hakkerit luovat oman verkkosivustonsa ja saavat sen indeksoitua laillisiin hakukoneisiin.
sivustot.
Etsit verkossa tietoa viranomaisista. Hakukoneiden joukossa on väärennettyjä sivuja.

Näin suojat tietosi verkossa tietojenkalastelulta

Käytä vahvoja salasanajoja

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 salasananä. Vaihda salasana aina, kun epäilet, että tili on vaarassa.

Bonusvinkki: Käytä salasana-hallintaohjelmistoa salasanojen muistamiseen ja suojaamiseen.

Tarkista tiliotteesi usein

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

Bonusvinkki: Jos laskun tilitiedoissa tai summassa on jotakin epätavallista, ota yhteys laskun lähittäjään 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.

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 suoja sinua kaikilta hyökkäyksiltä tai huijauksilta.

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

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 huijatakseen sinua syöttämään tilitietojasi tai muita yksityisiä tietojasi 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 kotiin saapuneet arkaluonteisia tietoja sisältävät asiakirjat.

Postilaatikot on hyvä lukita, jotta ulkopuoliset eivät pääse niihin käsiksi.

Käytä monivaiheista tunnistautumista

Monivaiheinen tunnistautuminen (englanniksi multi-factor authentication, MFA) on ylimääräinen turvatoimenpide, käytetään käyttäjätileille 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.

