SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

DATA

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 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.

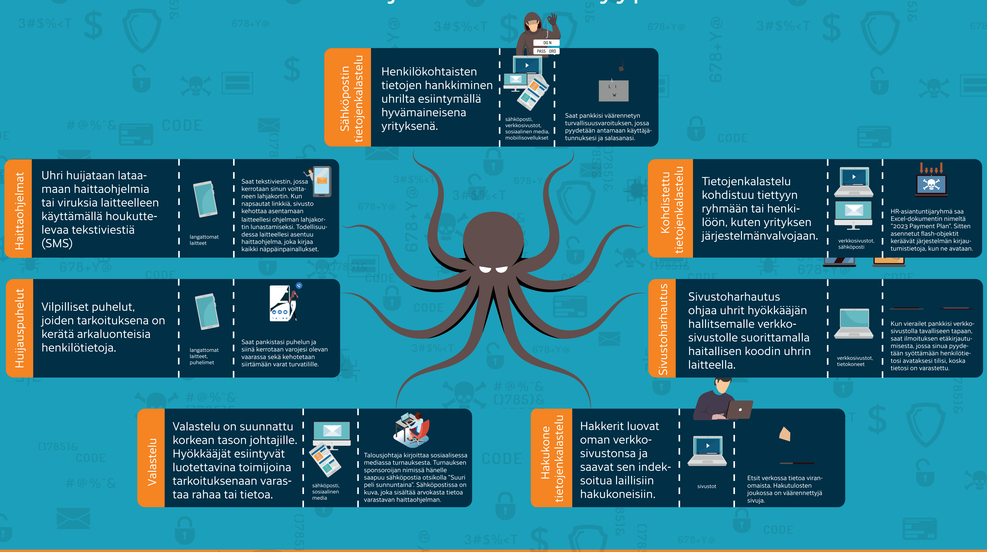
Tämä identiteettivarkaustapa on Suomessa harvinainen.

Rikollinen identiteettivarkaus

Rikollisella identiteettivarkaudella tarkoitetaan tilanteita, joissa pidätystilanteessa henkilö käyttää vääriä henkilötietoja, esimerkiksi näyttämällä väärennetyn ajokortin poliisille.

Lue lisää identiteettirikoksista Rikosuhripäivystyksen sivuilta.

Tietojenkalastelun tyypit



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.

Bonusvinkki: Käytä salasanahallintaohjelmistoa salasanojen muistamiseen ja suojaamiseen.

Älä koskaan käytä nimeäsi tai syntymäpäivääsi salasanana. Vaihda salasana aina, kun epäilet, että tili on vaarassa.

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 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 epäilyttäviltä sähköposteissa tai tekstiviesteissä. Tietojenkalastelijat käyttävät sähköposteja ja verkkosivustoja, jotka näyttävät tuleva pankilta, luottokorttiyhtiöstä, luotonantajalta tai muusta rahoituslaitoksesta huijatakseen sinua syöttämään tilitietojasi tai muita yksityisiä tietoja tietojenkalasteluun.

Nämä sähköpostit voivat pyytää sinua avaamaan liitetiedoston, joka asentaa haitalliset haittaohjelmat laitteeseen.

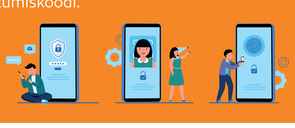
Suojaa yksityiset dokumentit

Myös fyysiset asiakirjat voivat aiheuttaa turvallisuusriskin, jos niitä käsitellään väärin. Sosiaaliturvatunnuksesi 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 tunnistautumista

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.



SaferInternet4Kids.gr · safeline.gr · helpline · ITE · INHOPE · insafe
Co-funded by the European Union