



Turvallisesti netissä

- Pankit ja maksukortit
- Verkkokaupat
- Sosiaalinen media
- Tunnista huijarit
- Suojaudu indentiteettivarkaudelta

KODIN TURVAOPAS
Ohjeita digitaaliseen arkeen
Turvallisuuskomitea

Porvoon Kansalliset Seniorit
Olli Holopainen kevät 2024



PANKIT JA MAKSUKORTIT

Verkkopankkien käyttö on turvallista, jos olet huolehtinut tietokoneesi tietoturvasta.

Tunnista pankkitietojen urkinta

- Haittaohjelmat
- Pankkien valesivut
- Tietojenkalastelu
- Pankkitietoja kysytään puhelimesta



Käytä verkkopankkia turvallisesti

Älä koskaan mene verkkopankkiin painamalla linkkiä, jota sinulle lähetetään esimerkiksi sähköpostissa tai tekstiviestissä.

Lukko ja s-kirjain tarkoittavat, että tietokoneen ja pankin välinen yhteys on salattu.



Tästä tunnistat salatun yhteyden

https:// salattu yhteys.

http:// salaamaton yhteys.



Haittaohjelmat

Tietokoneellesi voi tulla haittaohjelmia. Niitä voit saada esimerkiksi sähköpostin liitetiedostoista ja videoista, kuvista ja ohjelmista, joita lataat netistä. Windowsin suojaus on tehokas tarkistustyökalu, joka etsii ja poistaa haittaohjelmia tietokoneesta (ks. Asetus).

Vakoiluohjelma puolestaan tallentaa kaikki näppäinten painallukset koneellasi (keylogger, ks s. x). Niin verkkopankkisi salasana päättyy huijareille.

The screenshot shows a survey page from Op.fi. At the top, it says "Virallinen kysely: Op.fi" and "vannontai, marraskuu 2, 2014". Below this, it says "Arvon Op.fi kävijä." and "Sinut tässä". A pop-up window titled "Congratulations!" is overlaid on the page. The pop-up contains the text: "Arvon Op.fi kävijä, Sinut on valittu anonyymiin tutkimukseen: **sunnuntai, marraskuu 2, 2014**. Tee 30 sekunnin tutkimus ja saat kiitoksena erikoistarjouksen." There is an "Ok" button at the bottom of the pop-up. At the bottom of the survey page, there is a copyright notice: "Copyright © 2014 – Kaikki oikeudet pidätetään." and a disclaimer: "Yksityisyytesi on meille tärkeää. Emme kerää tietojasi tästä kyselystä. Tarkistathan Yksityisyyssehtomme ja sääntömme. Emme ole yhteistyössä minkään kolmannen tahon kanssa, emme myöskään Op.fin. Op.fi Ei ole missään. Tarkistathan myyjän verkkosivut täysii käyttöehtoja ja sääntöjä varten ennen kuin tilaat mitään. Pidäthän mielessä, että nämä tuotteet ovat kolmansien osapuolien tarjoamia, eivätkä liity mitenkään oursite.comiin."



Pankkien valesivut

Voit joutua pankin valesivuille. Saat sähköpostin tai tekstiviestin, joka kertoo esimerkiksi, että olet voittanut jotakin, sinulle on viesti pankiltasi tai sinun on päivitettävä verkkopankkisi. Viestissä on linkki, jota sinun halutaan painaa.

Lähetetty: Danske Verkkopankki [mailto:elisabete.pereira@cprm.gov.br]

Lähetetty: 1. kesäkuuta 2016 10:45

Aihe: Verkkopankin Päivittää

Hyvä asiakas,

Pankki- turvallisuusosasto Suorittaa päivityksiä kaikkien asiakkaiden tileille , tämä päivitys on kriittinen , ja se täyttääturvallisuusvaatimukset Suomen lain edellyttämänä.

Klikkaa alla olevaa linkkiä, seuraa ohjeita ja asiakaspalvelumme ottaa sinuun yhteyttä seuraavan 48h aikana.

[Klikkaa tästä](#)

Noudattamatta jättäminen voi johtaa tukkeutumiseen verkkopankissa.

Asiakaspalvelu

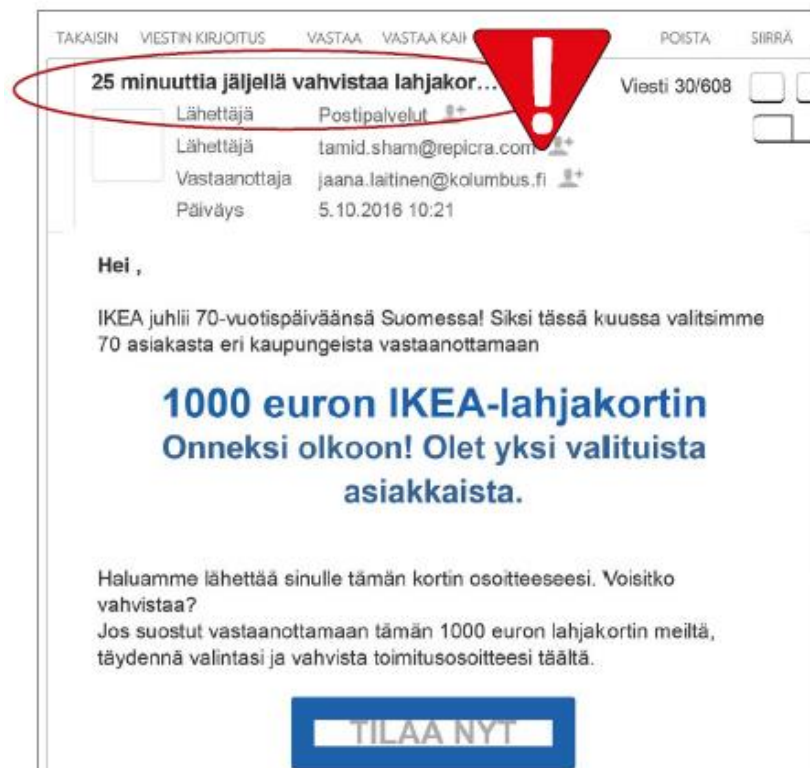
Danske Verkkopankki



Tietojenkalastelu (phishing)

Saat tietojenkalasteluviestin (phishing). Se houkuttelee sinut antamaan verkkopankin ja maksukorttien tietoja sekä muita henkilökohtaisia tietoja. Tunnukset avaavat pääsyn tilillesi ja käyttämään luottokorttiasi.

Tietoja kalastellaan monin kekseliäin keinoin.





Pankkitietoja kysytään puhelimessa

Tietojesi kalastelija voi myös soittaa ja kaupittelee sinulle jotakin tai kertoo tarkastavansa tietojasi. Huijari saattaa esiintyä verotoimiston tai Kelan virkailijana pankkivirkailijana, poliisina tai muuna viranomaisena.

Jos joku kysyy henkilökohtaisia tietojasi puhelimessa, lopeta puhelu. Älä ikinä kerro pankkitunnuksia tai maksukortin tietoja puhelimessa kenellekään.

Pankit eivät soita ja kysy asiakkaan henkilökohtaisia tietoja, verkkopankkitunnuksia tai maksukortin tietoja. Niitä ei pyydetä myöskään sähköpostilla tai tekstiviestillä.



Mitä teen, jos epäilen, että tietokoneessani on verkkopankkiin hyökkäävä haittaohjelma:

Kirjaudu ulos verkkopankista.

Avaa virustorjuntaohjelma ja laita se tarkastamaan ja puhdistamaan kone.

Jos oma virustorjuntaohjelma ei löydä haittaohjelmaa, voit käyttää internetissä toimivia virustutkia. Niitä ovat esimerkiksi F-Securen Online Scanner (löydät sen sivulta www.f-secure.fi).

Ota yhteyttä pankkiin ja tarkasta, onko tililtäsi tehty laittomia siirtoja.

Varminta on viedä tietokone ammattilaisen puhdistettavaksi.



Aseta maksukortille turvarajat

Voit laittaa esimerkiksi nämä rajoitukset maksukortillesi:

Nostorajoitus	Valitse summa, jonka kortilla voi korkeintaan nostaa pankkiautomaatista: <ul style="list-style-type: none">▪ yhdellä nostokerralla▪ vuorokauden aikana
Maksurajoitus:	Valitse summa, jonka kortilla voi korkeintaan maksaa <ul style="list-style-type: none">▪ yhdellä maksukerralla▪ vuorokauden aikana yhteensä
Maarajoitus (geoblocking):	Määritä maa, jossa korttiasi voi käyttää, esimerkiksi vain: <ul style="list-style-type: none">▪ Suomi▪ Pohjoismaat▪ Eurooppa
Internet-käytön rajoitus:	Määritä, saako luottokortillasi tehdä ostoksia internetissä vai ei.



Käytä maksunvälittäjiä

Jotkut verkkokaupat tarjoavat mahdollisuutta maksaa esimerkiksi Checkoutin tai PayPalin kautta. Kun käytät niitä, korttisi tiedot jäävät vain maksunvälittäjän haltuun. Et joudu antamaan niitä monelle eri verkkokaupalle.

Voit käyttää maksamiseen myös laskutuspalvelu Klarnaa, jos nettikauppa sitä vaihtoehtoa tarjoaa. Kun käytät Klarnaa, et joudu antamaan luottokorttisi tietoja.



Mitä teen, jos maksukorttini katoaa tai sen tiedot päätyivät väärin käsiin

Soita heti pankin sulkupalveluun. Vastuusi maksukortin käytöstä päättyy siihen.

Jos tililtäsi katoaa rahaa, etkä ole tehnyt siirtoja itse, ilmoita siitä pankille.

Tee rikosilmoitus poliisille.

Maksukorttien sulkupalvelu

Puh. 020 333

Puh. ulkomailta +358 20 333

- Voit sulkea palvelun kautta suurimman osan kotimaisista maksukorteista.
- Palvelu toimii 24 h.
- Joillakin korteilla on oma sulkunumeronsa. Löydät ne täältä: <https://www.korttiturvallisuus.fi/Apua/>



Mitä teen, jos maksukorttini katoaa tai sen tiedot päätyivät väärin käsiin

Soita heti pankin sulkupalveluun. Vastuusi maksukortin käytöstä päättyy siihen.

Jos tililtäsi katoaa rahaa, etkä ole tehnyt siirtoja itse, ilmoita siitä pankille.

Tee rikosilmoitus poliisille.

Maksukorttien sulkupalvelu

Puh. 020 333

Puh. ulkomailta +358 20 333

- Voit sulkea palvelun kautta suurimman osan kotimaisista maksukorteista.
- Palvelu toimii 24 h.
- Joillakin korteilla on oma sulkunumeronsa. Löydät ne täältä: <https://www.korttiturvallisuus.fi/Apua/>



VERKKOKAUPAT

- Suurin osa verkkokaupoista toimii yhtä luotettavasti kuin fyysiset kaupat.
- Huijareita ja käärmeöljykauppiaita oli ennen internetin kauttakkin. Netti kuitenkin tarjoaa rikollisille uusia väyliä huijata.
- Tavara voi jäädä tulematta, paketissa on väärä tuote tai tuotteen laatu on huono. Siksi kannattaa harkita, millaisessa verkkokaupassa asioit.

Ennen kuin ostat, tee nämä:

- Lue muiden antama palaute.
- Tarkasta, mitä tietoja verkkokauppa antaa itsestään. Kertooko se avoimesti yhteystietonsa eli osoitteen, sähköpostiosoitteen ja asiakaspalvelun tiedot.
- **Varmista, että voit ostaa luottokortilla. Jos tavara ei tulekaan tai siinä on vikaa, voit vaatia hyvitystä luottokorttiyhtiöltä.**



Käytä turvallisen maksamisen palvelua

Turvallisen maksamisen palveluja ovat Verified by Visa ja MasterCard SecureCode.

Turvallisen maksamisen palvelu on kaksiosainen. Ensin teet ostokset ja siirryt maksamaan.

Valitse maksutavaksi Visa tai MasterCard. Anna luottokortin tiedot. Paina maksa-painiketta, minkä jälkeen siirryt verkkopankkiisi.

Kuittaa ostokset verkkopankkitunnuksilla tai pankin antamalla tunnusluvulla.



OTA SOME HALTUUN

Toimi fiksusti somessa

- Suojaa yksityisyyttäsi
- Harkitse mitä sanot tai jaat



Suojaa yksityisyyttäsi

- Älä kerro henkilökohtaisia tietoja.
- Älä julkaise kuvia, joissa näkyy lapsesi, autosi tai kotisi sisältä tai ulkoa.
- Julkaise muiden ihmisten kuvia vain, jos he antavat luvan.
- Älä julkaise kuvia lentolipuista tai lomareissulta tai kerro, milloin olet lomalla.
- Älä levitä intiimejä kuvia verkossa tai viestintäpalveluissa.
- Vältä työnantajan arvostelua ja älä kerro liikaa työhösi liittyviä asioita muutenkaan.



Muista nämä asiat, kun osallistut keskusteluun

- Harkitse mitä kirjoitat.
- Jos kommenttisi koskee toista ihmistä, muista, että sanasi voivat satuttaa häntä pahasti.
- Internet on julkinen kanava. Siitä jää todiste, sillä somessa kerran sanomaasi et enää saa pois.
- Olet kuitenkin aina vastuussa siitä, mitä sanot.
- Älä provosoidu. Jätä provosoivat kommentit huomiotta, äläkä jaa niitä eteenpäin.



Ilkeät kommentit ja viestit voivat olla rikos

- Kunnianloukkaus
- Törkeä kunnianloukkaus
- Yksityiselämää loukkaavan tiedon levittäminen



TUNNISTA HUIJARIT

- Rahapyyntö
- Onnenpotku
- Lainatarjous
- Romanssi

Jos kohtasit huijarin, toimi näin:

- Älä kerro hänelle yksityisasiota, esimerkiksi osoitetta ja tietoa perheestäsi.
- Älä siirry keskustelemaan hänen kanssaan kahden kesken.
- Katkaise yhteydenpito heti, jos hän alkaa pyytää rahaa.
- Poista valeprofiili kaverilistalta.
- Älä lähetä huijarille rahaa tai intiimejä kuvia.



SUOJAUDU IDENTITEETTIVARKAUDELTA

- Älä vie jätekatokseen papereita, joista henkilötietosi voi nähdä.
- Osta lukittava postilaatikko.
- Pidä huoli lompakostasi.
- Älä levitä henkilötietoja huolettomasti netissä.
- Älä jaa sosiaalisessa mediassa kuvia, joissa henkilötunnuksesi näkyy.
- Yhteystietojen luovutuskielto Digi- ja väestötietovirastolle. Silloin identiteettivarkas ei saa sieltä osoitettasi.



Tietoturvaloukkauksen tapauksessa

- Tunnista tilanne
- Estä ennalta tietomurto
- Estä mahdolliset vahingot
- Tee aina poliisille rikosilmoitus tietomurrosta.
- Ota omaehtoinen luottokielto (Asiakastieto, Dan & Bradstreet).
- Yhteystietojen luovutuskielto teleoperaattorille
- Estä muuttoilmoitus Digi- ja väestötietoviraston väestötietojärjestelmään ja Postille
- Tee rekisteröintikielto PRH:n rekistereihin



Ohjeita tietoturvaloukkauksen sattuessa

- Tietosuojavaltuutetun toimiston ohjeistusta tietoturvaloukkauksen kohteeksi joutuneelle:
(<https://tietosuoja.fi/jos-joudut-tietoturvaloukkauksen%20kohteeksi>)
- Poliisin ohjeistusta tietomurron kohteeksi joutuneelle:
(<https://poliisi.fi/tietomurrot>)
- Digi- ja väestötietoviraston ohjeistusta henkilöille, joiden henkilötietoja on vuotanut:
(<https://www.suomi.fi/oppaat/tietovuoto/vaiheet?a=bada&a=552a&a=878b&mun=091>)