Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

KODIN KYBEROPAS

Ohjeita digitaaliseen arkeen

Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

Turvallisuuskomitean sihteeristö
Eteläinen Makasiinikatu 8
PL 31, 00131 Helsinki

www.turvallisuuskomitea.fi

Kirjoittanut: toimittaja Jaana Laitinen
Taitto: Tiina Takala, puolustusministeriö
Kannen grafiikkakuva: Freepik.com

ISBN: 978-951-25-2906-3 (pdf)
ISBN: 978-951-25-2907-0 (print)

Paino: Lönnberg Print, 2017

Esipuhe

Digitaaliseen arkeemme kuuluu tiedon ja palveluiden hyödyntäminen ilman sitoutumista aikaan tai paikkaan. Pankkiasiointi, viranomaispalvelut, ajanvaraukset, tilaukset, ostokset ja monet muut arkiset toimet hoituvat vaikkapa tietokoneella omalta kotisohvalta tai kännykällä kesken työmatkan. Yhteiskunnan palvelut tarjotaan sähköisinä, ja ne rakentuvat digitaalisista verkoista. Tämä muutos, digitalisaatio, on avannut rajattomasti mahdollisuuksia monien ammattien ja arjen toimintojen käytännöllisempään ja nopeampaan hoitamiseen.

Digitalisaation hyödyt ovat luotettavasti käytettävissämme vain, jos huolehdimme samalla tieto- ja kyberturvallisuudesta. Tiedotusvälineet viestivät jatkuvasti erilaisista tieto- ja kyberturvallisuusuhkista sekä -rikollisista, jotka tuntuvat suorastaan vaanivan tavallista verkonkäyttäjää. Valitettavasti haitat, väärinkäyttöyritykset ja rikollinen toiminta ovat osa verkon arkea. Toki kotikäytössä harvemmin kohtaa tietokoneviruksia ja haittaohjelmia laajempia ongelmia. Nekin syntyvät valitettavan usein käyttäjän itse aiheuttamina, eli seurauksena tietoturvallisuuden perusasioiden laiminlyömisestä.

Tämä opas neuvoo huolehtimaan niistä perusasioista, jotka auttavat toimimaan turvallisesti internetissä ja ymmärtämään kyberturvallisuutta. Opas sisältää runsaasti esimerkkejä, jotka avaavat kybermaailman riskejä ja mahdollisuuksia. Niissä meillä nykypäivän digikansalaisilla ja päätöksillämme on ratkaisevan tärkeä rooli. Myös medialukutaito, internetin valtavan tietomäärän lähdekriittinen hyödyntäminen, on tärkeä digiajan kansalaistaito.

Oppaan julkaisulla toivomme, että lukija rohkaistuu ottamaan digitalisaation ystäväkseen ja uskaltaa luovia turvallisesti bittien virrassa. Riskit on tärkeä tiedostaa, mutta vielä tärkeämpää on nauttia digitaalisten palveluiden hyödyistä ja iloista. Turvallisuuskomitea kiittää oppaan laatijaa, toimittaja Jaana Laitista, erinomaisesti kootusta ja havainnollisesta tietopaketista.

Turvallisuuden tekevät ihmiset, myös kybertoimintaympäristössä. Osaava yksilö on suomalaisen varautumisen yhteistoimintamallin, kokonaisturvallisuuden, kivijalka. Huolehtimalla omasta ja läheistemme kyberturvallisuudesta parannamme koko yhteiskunnan turvallisuutta. Siten jokainen meistä voi olla turvallisuustoimija digitaalisessa Suomessa ja maailmassa.

Turvallisuuskomitean pääsihteeri
Vesa Valtonen

Mitä on kyberturvallisuus?

Kyberturvallisuus tarkoittaa tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Mitä on tietoturvallisuus?

Tietoturvallisuudella tarkoitetaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. Tässä oppaassa kyberturvallisuudella tarkoitetaan edellisen lisäksi laajempaa tietojärjestelmien kokonaisuutta kuin yksittäistä tietokonetta. Kyberturvallisuuden voidaan ajatella olevan sama kuin digitaalisen maailman turvallisuus.

KODIN KYBEROPAS

Sisältö

1 SUOJAA TIETOKONE JA LÄHIVERKKO

Jos sinulla on tietokone tai älypuhelin ja niissä internetyhteys, pääset liikkumaan maailman laajuisessa tietoverkossa. Voit tehdä ja kokea siellä asioita, jotka vielä muutama vuosikymmen sitten kuulostivat mahdottomilta.

Voit käväistä kierroksella museossa maassa, jossa et ole ikinä käynyt. Voit tilata ruokaa kaupasta ja ostaa vaatteista putiikeista eri puolilta maailmaa. Voit lähettää ystävällesi viestin, jonka hän voi lukea saman tien, olipa hän missä tahansa. Monet arjen asiat hoituvat tietokoneella.

Tietoverkkojen käyttöön liittyy myös riskejä. Tietoverkkojen kautta tulevat uhkat ovat osin samoja, joita kohtaat fyysisessä maailmassa. Rosvo voi viedä käsilaukkusi, jossa ovat juuri pankista nostamasi rahat. Tietoverkossa varas voi siirtää rahaa tililtäsi, jos hän saa tietää pankkitunnuksesi. Riskit ovat osin samoja, mutta teon keinot erilaisia. Internetin hyödyt ovat kuitenkin suurempia kuin sen riskit. Uhkia ei pidä liioitella eikä pelätä, mutta niiltä pitää osata suojautua.

Tietoverkoissa liikkumista voi verrata liikenteeseen. Uskallat liikkua muiden joukossa, koska tunnet liikennesäännöt. Pääsääntöisesti voit luottaa siihen, että muutkin niitä noudattavat. Samalla kuitenkin on viisasta pitää mielessä, että aina on joku, joka ei niitä noudata.

Kun huolehdit laitteidesi ja internetyhteytesi tietoturvasta, riski saada haittaohjelmia vähenee. Voit opetella tästä tärkeimmät keinot, joilla pidät koneesi ja verkkosi turvassa.

Yhtä tärkeää on, että osaat itse toimia niin, että laitteesi ja tietosi pysyvät turvassa. Ohjeet löydät luvusta 2.

Suojaa tietokoneesi, verkkosi ja tietosi. Opettele fiksut turvatavat, niin pärjäät digitalisoituvassa maailmassa.

Opettele tekemään nämä:

- Pidä käyttöjärjestelmä, selain ja selaimen liitännäiset päivitettyinä
- Pidä palomuuri päällä
- Käytä pääkäyttäjän oikeuksia vain, kun niitä tarvitaan
- Suojaa kodin lähiverkko
- Pidä modeemi tai reititin päivitettynä ja niiden palomuuri käytössä
- Suojaa älykodinlaitteet (esineiden internet, IoT)
- Hanki hyvä tietoturvaohjelma

Kuva: Freepik.com

Pidä käyttöjärjestelmä, selain ja liitännäiset päivitettyinä

Tärkein keino suojata tietokone on se, että pidät käyttöjärjestelmän, selaimen ja laajennusosat aina päivitettynä. Niihin tulee päivityksiä usein. Niistä tulee myös uusia versioita silloin tällöin. Päivitykset korjaavat ohjelmassa olleita haavoittuvaisuuksia. Ne ovat heikkoja kohtia, joita hakkerit ja rikolliset käyttävät hyväkseen. Kun päivität ohjelmat, vähennät riskiä, että haittaohjelmia pääsee koneellesi.
Käyttöjärjestelmiä, selaimia ja liitännäisiä ja niiden eri versioita on paljon. Siksi tässä on mahdoton antaa tarkkoja ohjeita niiden päivittämisestä. Paras ohje kotikäyttäjälle onkin se, että laitat ohjelmat päivittämään itse itsensä.

Näin saat päivityksen päälle:

- Kun ostat tietokoneen, pyydä, että myyjä asentaa siihen valmiiksi haluamasi käyttöjärjestelmän, selaimen ja muut ohjelmat. Pyydä, että myyjä laittaa automaattisen päivityksen päälle kaikkiin ohjelmiin.
- Katso ohjelman valmistajan nettisivuilta ohjeet, miten ohjelma päivitetään ja miten automaattinen päivitys otetaan käyttöön.
- Vie tietokone ammattilaiselle ja pyydä, että automaattinen päivitys otetaan käyttöön.

Pidä palomuuri päällä

Palomuuri tarkkailee tietoliikennettä koneesi ja modeemisi sekä tietoverkkojen välillä. Se auttaa estämään haittaohjelmien ja luvattomien käyttäjien pääsyn tietokoneellesi verkkoyhteyden kautta.
Käyttöjärjestelmän palomuuri kannattaa pitää siksi päällä. Tarkasta, onko palomuuri päällä ja jos ei ole, laita se päälle.
Myös langattoman verkon modeemin tai reitittimen palomuuri kannattaa pitää käytössä (ks. ohje s. 7).

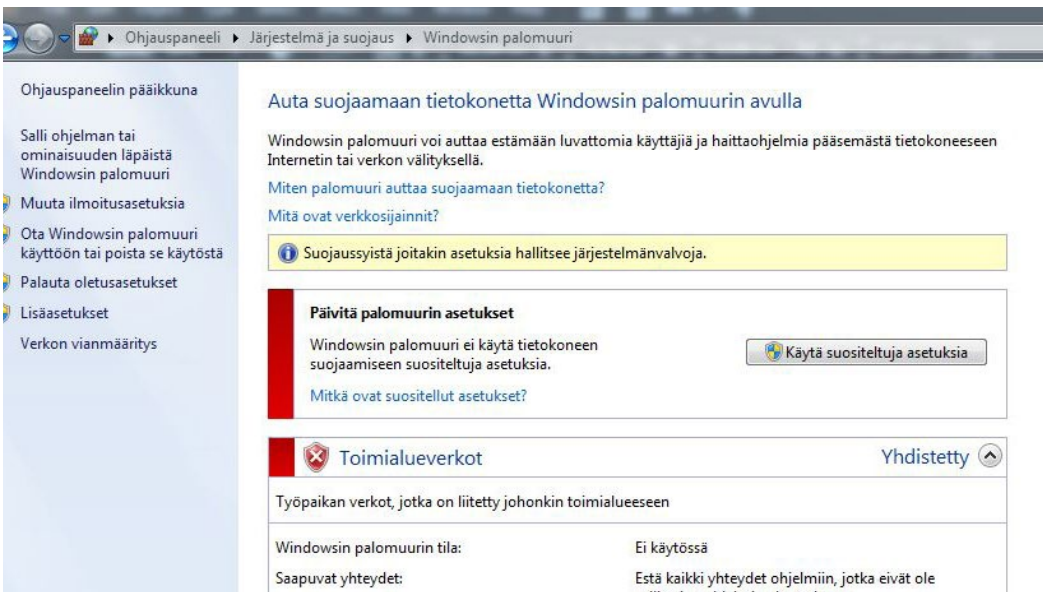
Näin tarkastat käyttöjärjestelmän palomuurin tilan:

- Kirjoita hakuun palomuuri. Pääset ikkunaan, jonka kautta palomuuria voi hallita.
- Etsi kohta, josta palomuurin voi ottaa käyttöön ja poistaa se käytöstä.
- Klikkaa palomuuri päälle.

VINKKI

Näin teet hakuja tietokoneeltasi

Etsi tietokoneeltasi symboli, joka näyttää suurennuslasilta. Klikkaa sitä. Kirjoita avautuvalle riville, mitä etsit. Hakutulos näyttää listan tiedostoista, sovelluksista ja asetuksista, joissa hakusanasi esiintyy.



Tämän oppaan ohjeet on tarkoitettu Windows-käyttöjärjestelmälle. Samat toiminnot löytyvät myös muista käyttöjärjestelmistä.

Esimerkiksi tältä näyttää sivu, josta Windowsin käyttäjä voi muuttaa palomuurin asetuksia. Tee kuten suositus neuvoo eli klikkaa päälle yksityisen ja julkisen verkon palomuuri. Etsi omasta selaimesta vastaava toiminto.

Käytä pääkäyttäjän oikeuksia vain, kun niitä tarvitaan.

Voit tehdä tietokoneeseen eri käyttäjille omat käyttäjätilit. Niin tietokone tietää, kenellä on oikeus käyttää sitä. Voit lisätä tai poistaa käyttäjätilejä tarpeen mukaan. Jokainen käyttäjä kirjautuu käyttäjätililleen omalla salasanalla.

Yksi käyttäjätileistä on pääkäyttäjätili. Pääkäyttäjällä on suurimmat oikeudet muokata tietokonetta. Pääkäyttäjä voi esimerkiksi ladata ja poistaa ohjelmia, tehdä päivityksiä ja muuttaa tietokoneen asetuksia. Tee siksi itsestäsi pääkäyttäjä.

Tee itsellesi myös toinen, tavallinen käyttäjätili. Käytä yleensä sitä tiliä. Kirjaudu koneelle pääkäyttäjänä vain silloin, kun tietokone vaatii pääkäyttäjän oikeuksia. Tietokone ilmoittaa, jos niitä tarvitaan.

Kun olet tehnyt loppuun toiminnon, joka vaatii pääkäyttäjän valtuuksia, kirjaudu ulos pääkäyttäjän tililtä. Mene takaisin tavallisen käyttäjätilisi kautta ja jatka tietokoneen käyttöä.

Näin kannattaa tehdä, sillä jos tietokoneellesi pääsee haittaohjelma, se pystyy tekemään vähemmän vahinkoa tavallisen käyttäjätilin oikeuksilla. Jos tunkeutuja saa pääkäyttäjän valtuudet, se pystyy ottamaan tietokoneesi haltuunsa kokonaan.

Anna ulkopuolisen käyttää tietokonetta oman käyttäjätilisi kautta vain, jos luotat häneen ja hänen osaamiseensa tietokoneen ja internetin käyttäjänä.

Tämän tietokoneen pääkäyttäjä on Mikko. Mikolla on lisäksi tavallisen käyttäjän tili nimellä Iskä. Tietokonetta käyttävät myös lapset Siiri, Henri ja Santtu, joilla on omat käyttäjätilit.

Suojaa kodin lähiverkko

Jos käytät internetiä, kotonasi on modeemi tai reititin. Se yhdistää kotiverkkosi internetiin eli erilaisiin tietoverkkoihin kodin ulkopuolella. Kaikki kodin laitteet, joista on yhteys modeemiin tai reitittimeen, muodostavat kodin lähiverkon. Siihen voi kuulua yksi tai useita tietokoneita, matkapuhelimia ja kodinkoneita, joissa on verkkoyhteys.

Nykyisin lähiverkot ovat yleensä langattomia. Se tarkoittaa, että laitteita ei yhdistetä verkkoon johdoilla. Sen sijaan tieto laitteiden ja modeemin tai reitittimen välillä kulkee langattomasti radioaalloilla.

Radiosignaali voi yltää jopa sadan metrin päähän. Se tarkoittaa, että jos lähiverkkoa ei ole suojattu, esimerkiksi naapuri voi käyttää internetiä lähiverkkosi kautta. Se voi hidastaa oman verkkoyhteytesi nopeutta.

Kuka tahansa voi lähettää oikeita tai väärennettyjä viestejä suojaamattomaan lähiverkkoon, jos hän on tarpeeksi lähellä. Suojaamatonta lähiverkkoasi voidaan käyttää esimerkiksi rikosten tekoon. Sitä kautta voidaan myös ladata laitonta materiaalia. Hakkerit tai rikolliset pystyvät urkkimaan tietojasi ja seuraamaan, mitä teet verkossasi.

Et voi mistään tietää, käyttääkö joku suojaamatonta lähiverkkoa. Siksi on tärkeä suojata oma lähiverkko ulkopuolisilta. Suojaaminen tapahtuu laittamalla verkolle salasana. Hakkerit etsivät verkosta suojaamattomia verkkoja, joiden modeemeissa on yhä tehtaalla laitettu oletussalasana.

Näin suojaat lähiverkkosi:

- Modeemissasi on tarra, jossa on kerrottu laitteen tiedot ja internetsivu, jossa laitteen asetuksia voi muuttaa. Mene tietokoneella annettuun osoitteeseen. Reittimen osoitteen näet käyttöohjeesta.
- Etsi kohta, jossa voit vaihtaa käyttäjätunnuksen (username) ja salasanan (password).
- Näet siellä laitteen valmistajan antaman oletussalasanan. Se voi olla esimerkiksi admin.
- Anna laitteelle oma salasana. Kirjoita käyttäjätunnus ja salasana talteen.

Kuva modeemin takana olevasta tarrasta. Siinä näkyy nettiosoite, jossa voit vaihtaa oletussalasanat. Tässä oletussalasanana on admin.

Älä mene verkkopankkiin kahvilan avoimessa verkossa.

Monet kahvilat, kirjastot, junat ja muut palvelut antavat nykyään asiakkaiden käyttöön internetyhteyden. Niillä on oma, suojaamaton eli avoin langaton verkkonsa. Siihen pääsee kirjautumaan sisälle kuka tahansa verkon alueella oleva asiakas. Kahvila, kirjasto jne. antaa tarvittavan käyttäjätunnuksen ja salasanan.

Voit kirjautua verkkoon omalla tabletilla tai kannettavalla tietokoneella.

Koska samassa verkossa on muitakin, älä tee siellä mitään henkilökohtaista. Lue kahvilassa lehtiä, käväise somessa tai etsi vaikka aukioloaikoja. Älä mene palveluihin, joissa pitää antaa salasana, käyttäjätunnus tai esimerkiksi maksukortin tietoja.

VINKKI

Tyhjennä selaushistoria vieraalta koneelta

Voit käyttää vierasta tietokonetta esimerkiksi kylässä, kirjastossa tai internetkahvilassa. Putsaa tietokoneelta aina käytön jälkeen käyntisi jäljet. Silloin kukaan ei voi katsoa, millä sivuilla kävit.

Jäljet poistuvat, kun tyhjennät tietokoneen selaushistorian. Mene selaimen hakuun ja kirjoita sinne: poista selaushistoria. Päädyt ohjauspaneelin kohtaan, josta voit tyhjentää selaustiedot.

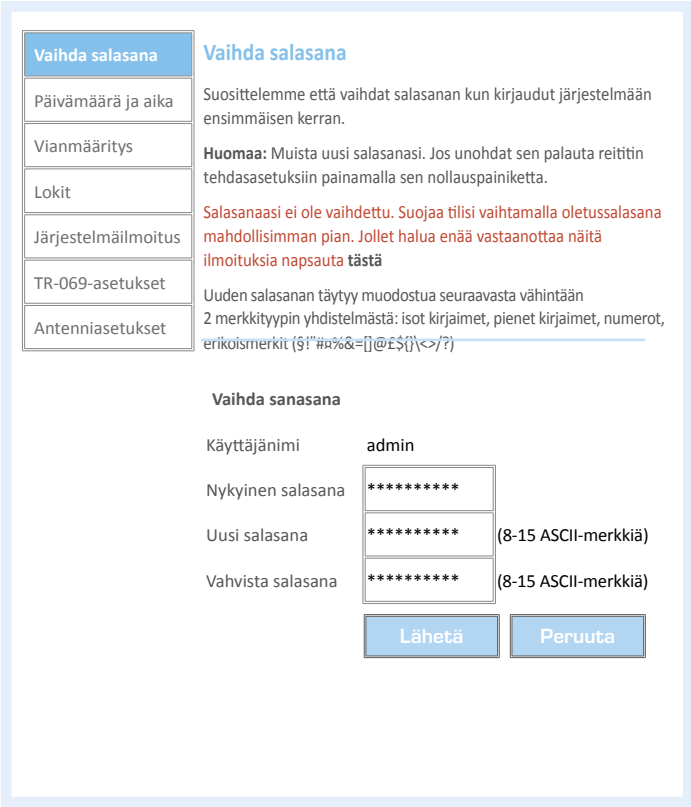
Kuva: Freepik.com

Pidä modeemi päivitettynä ja sen palomuuri käytössä

Myös modeemin ohjelmisto pitää päivittää ja sen palomuuri pitää käytössä.

Näin päivität modeemin ohjelmiston:

- Mene modeemin hallintaohjelmaan tietokoneellasi kuten aiemmin on neuvottu (ks. Näin suojaat lähiverkkosi, ks. s. 5).
- Etsi kohta, josta voit päivittää ohjelmiston. Päivitä. Jos on mahdollista ottaa käyttöön automaattinen ohjelmiston päivitys, tee se.
- Etsi kohta, jossa voit ottaa modeemin palomuurin käyttöön. Jos palomuuri on käytössä, kaikki hyvin. Jos ei ole, laita palomuuri päälle.



Kuva erään modeemin hallintaohjelmasta, josta voi muuttaa oletussalasanan.

Suojaa älykodinkoneet

Yhä useammissa kodinkoneissa on verkkoyhteys. Puhutaan esineiden internetistä eli IoT:stä (Internet of Things). Internetyhteys voi olla televisiossa, jääkaapissa, kiukaassa, turvakamerassa, silitysraudassa tai vaikka pölyimurissa.

Nettiyhteydellä varustetun laitteen voi kytkeä kodin langattomaan tietoverkkoon. Laitteella voi olla myös oma internetyhteys, joka ei käytä kodin verkkoa. Se on yhteydessä suoraan laitteen valmistajan verkkoon. Se voi lähettää valmistajalle esimerkiksi tietoja laitteen käytöstä ilman että tiedät asiasta mitään.

Kodinkoneiden nettiyhteydestä on hyötyä. Jos kiuas on kytketty kodin verkkoon, voit laittaa saunan lämpiämään kännykällä kotimatkalla. Kaupassa voit kurkistaa jääkaappiisi ja katsoa, mitä ruokaa pitää ostaa. Voit ladata älytelevisioon lisäohjelmistoja kuten tablettiin tai matkapuhelimeen.

Esineiden internetin ongelma on, että useiden kodinkoneiden ja laitteiden tietoturva on huono. Kaikissa laitteissa sitä ei ole ollenkaan. Etenkin halpojen mallien tietoturvassa on heikkouksia.

Tunkeutuja saattaa kaapata kodinkoneesi

Jos tietoturvasta ei ole huolehdittu, tunkeutuja pystyy valjastamaan kodinkoneitasi osaksi palvelunestohyökkäystä. Hän voi myös ohjata kodinkoneiden toimintaa.

Hyökkääjä rakentaa ensin ison ns. bottiverkon hallintaansa ottamistaan laitteista. Sitten hän määrää laitteet lähettämään yhtä aikaa liikennettä hyökkäyksen kohteeksi joutuneille nettisivuille tai muihin palveluihin. Ne menevät tukkoon, eikä niitä voi silloin käyttää.

Palvelunestohyökkäyksen kohteena eivät ole tavalliset ihmiset vaan yleensä yritykset ja julkisen palvelun verkkosivut. Hyökkäys voi silti häiritä omistamaasi laitetta, jota on liitetty mukaan hyökkäykseen.

Harva haluaa tarjota rikollisille välineen hyökätä esimerkiksi viranomaisten sivuille. Hyökkäys aiheuttaa haittaa palvelujen käyttäjille, kun nettisivuille ei pääsekään. Ei ole syytä antaa omia laitteita palvelunestohyökkäysten käyttöön. Siksi on tärkeää pitää huolta myös älykodinkoneiden tietoturvasta.

Mistä tiedän, että kodinkoneeni lähettää tietoa kotini ulkopuolelle?

- Et välttämättä mistään. Jos tunkeutuja käyttää laitettasi, hän haluaa, ettet huomaakaan sitä.
- Verkko-operaattorisi ottaa yhteyttä ja kertoo, että koneeltasi lähtee epätavallisen paljon liikennettä.
- Laite muuttuu hitaaksi tai toimii oudosti. Televisio temppuilee tai tietokone jumiutuu.
- Verkkoyhteys muuttuu hitaaksi, tai se toimii epäluotettavasti.

Katso ohjeet palveluhyökkäykseen valjastetun tietokoneen puhdistamisesta, katso luku 3.

Mitä teen, jos en halua, että kodinkoneeni on yhteydessä internetiin?

- Kun ostat kodinkonetta, kysy kaupassa, onko siinä langaton WiFi-yhteys. Jos et tarvitse yhteyttä, osta laite, jossa sitä ei ole.
- Haluat ehkä laitteen muttet halua käyttää sen nettiyhteyttä. Kysy silloin myyjältä ohjeet, miten yhteyden saa pois päältä.
- Laita kotona langaton verkkoyhteys pois päältä näin:
  - Laitteessa tai laitteen ohjekirjassa on kerrottu internetosoite. Siellä pääset hallinnoimaan laitteen internetyhteyttä. Voit kysyä osoitetta myös laitteen valmistajalta.
  - Mene tietokoneellasi nettiosoitteeseen ja kirjaudu palveluun laitteen tai ohjekirjan antamilla tiedoilla.
  - Etsi kohta, jossa internetyhteyden voi laittaa pois päältä. Se tosin ei aina ole mahdollista. Esimerkiksi jos haluat käyttää television puheohjausta, internetyhteys täytyy pitää päällä.

Näin käytät kodinkoneen internetyhteyttä turvallisesti:

- Kirjaudu laitteen tai ohjekirjan kertomille internetsivuille ja yhdistä laite kodin verkkoon.
- Vaihda laitteen salasana ja käyttäjätunnus. Rikolliset etsivät verkosta laitteita, joissa on valmistajan alkuperäiset tunnukset, esimerkiksi admin tai root. Älä käytä laitetta, jonka salasanoja ja käyttäjätunnuksia ei voi muuttaa.
- Jos laitteessa on palomuuri, laita se päälle. Päivitä palomuuri silloin tällöin.
- Laita päälle ohjelmien automaattinen päivitys. Laitteessa on silloin aina uusin versio ohjelmasta. Se vähentää riskiä, että ulkopuolinen pääsee kotiverkkoosi ja laitteellesi.

VINKKI

Voit kokeilla ilmaisella skannerilla, onko tietokoneesi yhteydessä verkkoon kiinnitettyihin laitteisiin. Skannerin tarjoaa Tietoturvayhtiö Bullguard.

http://iotscanner.bullguard.com/

Hyökkääjä löysi leivänpaahtimen 40 minuutissa

Yhdysvaltalainen toimittaja kokeili, kuinka nopeasti hakkerit löytävät verkosta suojaamattoman kodin laitteen. Hän käytti apunaan internetpalvelinta, jonka hän muutti muistuttamaan suojaamatonta, nettiin kytkettyä älyleivänpaahdinta. Hän suunnitteli kokeen niin, että hakkerit eivät pääse palvelimelle. Sen sijaan järjestelmä tallentaa hakkerien tietokoneiden IP-osoitteet ja heidän syöttämänsä komennot. Jokaisella tietokoneella on oma IP-osoite, josta ne voi tunnistaa.

Toimittaja aloitti kokeen eräänä päivänä kello 13.12. Ensimmäinen hyökkäys ”leivänpaahtimelle” tuli noin 40 minuutin kuluttua. Hyökkääjä yritti kirjautua valejärjestelmään salasanalla ja käyttäjätunnuksella root. Sitä käytetään oletussalasanana monissa laitteissa.

Seuraava hyökkäys tuli muutama minuuttia myöhemmin eri IP-osoitteesta. Vuorokauden vaihtuessa järjestelmän käyttäjänimeä ja salasanaa oli yritetty arvata jo 300:sta eri IP-osoitteesta.

Monet hyökkäyksistä yrittivät käyttää salasanaa ”xc3511”. Se on yleinen oletussalasana vanhoissa valvontakameroissa, joita on käytetty palvelunestohyökkäyksissä. Testi osoittaa, miten tärkeää on vaihtaa oletussalasana kaikkiin internetiin kytkettyihin laitteisiin.

Lähde: Tekniikka & Talous 29.10.2016

Valtava verkkohyökkäys tehtiin tavallisten ihmisten laitteilla

Perjantaina alkanut yksi maailman pahimmista palvelunestohyökkäyksistä tehtiin esineiden internetin kautta. Hyökkäyksessä käytettiin satoja tuhansia tavallisten ihmisten kodeista löytyviä suojaamattomia laitteita.

Kodeissa on nykyisin paljon nettiin kytkettyjä laitteita, esimerkiksi reitittimiä, nettikameroita ja älytelevisioita. Laitteiden tietoturva ei ole samalla tasolla kuin perinteisten tietokoneiden suojaus. Se ei ole jäänyt huomaamatta hakkereiltakaan.

Verkkoyritys Dyn joutui perjantaina kolmen laajan palvelunestohyökkäyksen kohteeksi. Hyökkäyksen vuoksi esimerkiksi Netflixissä, Twitterissä ja Spotifyssa oli häiriöitä useiden tuntien ajan. Epäillään, että hyökkäykset tehtiin Mirai-haittaohjelman avulla. Se ottaa haltuunsa kotien suojaamattomia laitteita. Mirai pääsee käsiksi laitteisiin, joihin ei ole asetettu salasanaa tai joissa on käytössä tehtaalta tullut oletussalasana. Yksinkertaisin keino suojata omat laitteet on vaihtaa oletussalasanat.

Lähde: Iltalehti 24.10.2016

Kuva: Rodeo

Hanki hyvä tietoturvaohjelma

Hanki tietokoneeseesi hyvä ja kattava virustorjuntaohjelma. Sen tehtävä on suojata tietokonetta viruksilta ja muilta haittaohjelmilta.

Voit ladata internetistä ilmaisen virusturvaohjelman. Asiaan perehtymättömän on vaikea tietää, mikä ilmaisohjelma on luotettava. Saatat jopa törmätä netissä virustorjuntaohjelmaan, joka kertoo, että koneessasi on virus ja voit poistaa sen tämän tietoturvaohjelman kautta. Käykin niin, että tietoturvaohjelma lataa koneellesi viruksen.

Voit myös ostaa koneellesi virustorjuntaohjelman joltakin tunnetulta tietoturvayhtiöltä. Maksullisissa ohjelmissa on enemmän ominaisuuksia. Niissä on mukana yleensä myös palomuuri, roskapostisuojaus ja varmuuskopiointisovellus. Se voi myös varoittaa, jos olet menossa huijaussivustolle.

Sovellus voi tarjota myös lapsilukon, jolla voit estää lapsia pääsemästä sopimattomille sivuille.

Pimeä internet on rosvojen kauppapaikka

Tiesitkö, että internetissä on salainen pimeä puolensa? Sitä kutsutaan nimellä Dark Web, pimeä internet.

Koko internetin sisällöstä 0,1 prosenttia eli tuhannesosa on pimeää puolta. Siellä on tietoa, joka halutaan pitää piilossa. Siellä rikolliset myyvät esimerkiksi huumeita ja kaapattuja luottokorttitietoja. On arvioitu, että puolet pimeän internetin sisällöstä on laitonta.

Dark Webiä on vaikea valvoa. Sen käyttäjät voivat toimia anonyymisti eli heidän henkilöllisyytensä pysyy salassa. Myös toiminta pimeällä puolella on salattu erilaisilla tekniikoilla.

On myös Deep Web eli syvä internet. Se tarkoittaa internetin sisältöä, jonne halukoneet eivät ulotu. Se kattaa yli 90 prosenttia kaikesta internetin sisällöstä.

Kannattaako ostaa käytetty tietokone?

Osta halvalla käytetty, toimiva tietokone. Tekisi mieli, kun tuttava myy tai netissä on houkutteleva tarjous, mutta kannattaako? Harkitse hetki.

Et voi tietää, onko koneella haittaohjelmia. Virustorjuntaohjelmat eivät aina löydä kaikkia niitä.

Ei riitä, että poistat käytetystä tietokoneesta ohjelmat ja tiedostot. Tietokone kannattaa alustaa eli formatoida uudelleen. Alustus tarkoittaa sitä, että tietokone valmistellaan uudelleen tiedon tallentamista varten.

Alustuksen jälkeen tietokoneelle asennetaan uudelleen ohjelmat. Sitten vanhankin tietokoneen voi ottaa käyttöön.

Jos ostat vanhan koneen, käytä se alustettavana ammattilaisella tai merkkivalmistajan huollossa.

Kuva: Freepik.com

Bottiverkko on palvelunestohyökkäystä varten tehty verkko, johon liitetään jopa miljoonia tietokoneita ja muita älylaitteita, esimerkiksi internetillä varustettuja kodin laitteita.

Esineiden internet (Internet of Things, IoT) tarkoittaa sitä, että useilla kodinkoneilla ja muilla vastaavilla laitteilla (esimerkiksi valvontakameroilla, autoilla jne) on internetyhteys. Se mahdollistaa muun muassa laitteiden etäkäytön.

Hakkeri tarkoittaa innokasta tietokonealan harrastajaa. Hakkereiksi kutsutaan usein myös tietojärjestelmiin murtautujia.

Käyttäjätunnus on käyttölupa, jonka avulla käyttämäsi tietokoneohjelma tunnistaa sinut. Saat käyttäjätunnuksen palvelun tarjoajalta tai voit tehdä sen itse, kun rekisteröidyt palveluun.

Käyttöjärjestelmä on ohjelmisto, joka mahdollistaa tietokoneen toiminnan. Se tarjoaa muille ohjelmistoille niiden tarvitsemia palveluja. Käyttöjärjestelmä myös jakaa tietokoneen resursseja, kun käytät tietokonetta.

Laajennukset ja liitännäiset ovat eräänlaisia tietokoneohjelmien apuohjelma. Niitä tarvitaan esimerkiksi kuvien ja videoiden katsomiseen.

Langaton lähiverkko on lähiverkko, jossa eri laitteita ei ole yhdistetty verkkoon kaapelilla vaan langattomasti radioaaltojen avulla.

Modeemi on laite, joka siirtää tietoa lähiverkosta internetiin ja internetistä lähiverkkoon. Se muuttaa lähiverkosta lähtevää tietoa internetin ymmärtämään muotoon ja päinvastoin.

Ohjauspaneelissa voit muuttaa tietokoneen käyttöjärjestelmän asetuksia.

Oletussalasana on salasana, joka laitteelle annetaan tehtaalla. Laitteen käyttäjä muuttaa oletussalasanan tilalle oman salasanan.

Palomuuri on ohjelma, joka seuraa verkosta tietokoneellesi tulevaa ja sieltä lähtevää tietoa. Se toimii kuin puomi joka estää ajamisen väärään suuntaan tai paikkaan.

Pääkäyttäjä on tietokoneen käyttäjä, jolla suurimmat oikeudet tehdä muutoksia tietokoneelle.

Roskapostit ovat sähköpostilla tulevia massapostituksia, joista ei ole sovittu vastaanottajan kanssa. Usein roskapostit ovat mainoksia.

Salasana on kirjaimista, numeroista ja erikoismerkeistä koostuva avain, jonka avulla pääset käyttämään käyttäjätunnustasi.

Selain on ohjelma, jolla käytät internetiä.

Selaushistoriaan tietokone tallentaa, millä internetsivuilla olet viimeksi käynyt.

Some tarkoittaa sosiaalista mediaa.

Verkkopankki on pankin internetissä tarjoama palvelu, jonka kautta voit hoitaa pankkiasioita tietokoneella.

WiFi on WLAN-tuotteista käytetty kaupallinen nimitys.

WLAN (Wireless Local Area Network) on langaton lähiverkko. Se tarjoaa mahdollisuuden muodostaa internetyhteys ilman, että koneesta menee verkkopiuha nettirasiaan.

2 TÄRKEIN TIETOSUOJA OLET SINÄ ITSE

Tietoturvan ammattilaiset sanovat, että suurin tietoturvariski on ihminen itse. Mikään tekniikka ei pysty suojaamaan laitteita ja verkkoa, jos tietokoneen käyttäjä on varomaton ja huolimaton.

Joskus kyse on myös osaamisen puutteesta. Avaat sähköpostien liitteitä tuosta vain, vaikka niistä voi tulla haittaohjelmia. Lataat materiaalia netistä tietämättä, että kaikkien sivujen materiaaleihin ei voi luottaa. Liitteistä ja ladattavista tiedostoista voi tulla haittaohjelmia, joita virusturvaohjelmatkaan eivät vielä tunnista.

Tärkeimmät tietoturvataidot ovat nämä: tee vahvoja salasanoja, käytä sähköpostia ja internettiä harkiten ja pidä omat tiedostot tallessa ja turvassa. On tärkeä myös tunnistaa huijausviestit ja huijarit, joita tietoverkoissa liikkuu. Lue huijausviesteistä enemmän luvusta 3 ja huijareista luvusta 9. Maalaisjärki auttaa tässäkin pitkälle.

”Tietoturvasta 20 prosenttia on tekniikkaa ja 80 % ihmisen käytöstä.”

Panu Moilanen
lehtori
Kyberturvallisuus, Jyväskylän yliopisto

Etkö keksi hyvää salasanaa?

Kysy koneelta. Salasanageneraattori arpoo sinulle satunnaisia, vahvoja salasanoja.
http://www.xorbin.com/tools/password-generator

Opettele nämä asiat:

- Satsaa salasanoihin
- Opettele sähköpostin turvallinen käyttö
- Pidä tietosi turvassa

Satsaa salasanoihin

Kun käytät internetin eri palveluita, joudut keksimään niihin salasanoja. Salasanojen tarkoitus on varmistaa, että juuri sinä haluat käyttää palvelua.

Salasanoilla on väliä. Hyvä salasana on tärkein keino pitää käyttämäsi palvelu turvassa.

Salasanoja eivät yritä selvittää ihmiset vaan tehokkaat tietokoneet. Ne tuntevat yleisimmät salasanat ja tunnistavat jo kikkoja, joita salasanojen teossa käytetään. Murto-ohjelmat käyvät läpi miljoonia jo käytettyjä salasanoja ja plaraavat läpi sanakirjoja.

Huono salasana paljastuu näille ohjelmille nopeasti. Päihität koneet, kun opettelet tekemään hyviä salasanoja ja pidät ne turvassa.

Kaikki salasanat eivät ole yhtä tärkeitä. Ehkä tärkein salasana on sähköpostisi salasana. Näin on, koska jos joku ulkopuolinen pääsee sähköpostiisi, hän voi sen avulla muuttaa muiden palveluiden salasanoja.

Hän menee palveluun ja pyytää lähettämään uuden salasanan sähköpostiisi. Hän nappaa uuden salasanan sähköpostistasi ja ottaa palvelun haltuunsa.

Tärkeitä salasanoja ovat myös tietokoneesi salasana sekä pääsalasanat, joiden taakse voit tallettaa muut salasanat omalle koneelle tai pilvipalveluun.

Tee tärkeimmistä salasanoista vahvoja ja pidä ne parhaimmassa tallessa.

Tee jokaiselle palvelulle eri salasana. Jos yhden palvelun salasana päätyy ulkopuolisen tietoon, hän ei pääse sillä muihin palveluihin. Vahinko jää pienemmäksi.

Älä käytä yleisesti tunnettuja salasanoja. Rikolliset tietävät, että salasanat muistuttavat toisiaan. Siksi murtaminen aloitetaan salasanoista, jotka ovat jo tiedossa.

Hyvä salasana

- ☑ on pitkä. Siinä on 15–20 merkkiä. Salasanoja murtavat tietokoneet saavat selville 8 kirjainta sisältävän salasanan nopeasti.
- ☑ ei ole sana vaan lause, runo tai laulun pätkä. Voit kirjoittaa sen yhteen tai muunneltuna niin, että koostat salasanan esimerkiksi sanojen ensimmäisistä kirjaimista. Esimerkiksi lause ”Joulupukki tulee meille jo jouluaaton iltana, mutta muualla maailmassa usein vasta joulukuun 25. päivän vastaisena yönä!” muuntuu salasanaksi ”Jtmjjimmmuvj25vy!”
- ☑ sisältää pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä.
- ☑ on suomen kieltä ja sisältää taivutettuja sanoja.

Huono salasana

- ☒ on lyhyt.
- ☒ on yleinen salasana, esimerkiksi salasana, salasana 123 tai 12345678. Näitä salasanoja murtavat koneet kokeilevat ensimmäiseksi.
- ☒ on geometrinen kuvio, jonka näppäimistöllä voi muodostaa.
- ☒ on muokattu sanoista käyttämällä yleisesti tunnettuja kirjaimen ja numeron vaihtoja. Esimerkiksi i-kirjain on korvattu numerolla 1 ja o-kirjain numerolla 0. Hakkerit tuntevat jo tämän tempun.
- ☒ on oikea, yleisesti käytetty sana, esimerkiksi kissa. Murto-ohjelmat käyvät läpi sanakirjoja.
- ☒ sisältää henkilökohtaisia tietoja, esimerkiksi lemmikin, lapsen tai asuinpaikan nimi, ikä, syntymäaika tai -vuosi.
- ☒ sisältää vain pieniä kirjaimia. Erikoismerkit, numerot ja isot kirjaimet teettävät hakkereilla enemmän töitä.

Näin säilytät salasanat:

- Opettele ulkoa tärkeimmät salasanasi. Niitä ovat esimerkiksi sähköpostin ja tietokoneen salasana.
- Kirjoita salasanat lunttilapulle, ja pidä se hyvässä tallessa kotona. Älä kirjoita lapulle, mihin palveluun kukin salasana kuuluu. Jos joku ulkopuolinen löytää lapun, vahinko voi olla suuri.
- Tallenna salasanat salasanapalveluun. Niitä tarjoavat tunnetut tietoturvayhtiöt. Salasanapalvelut tallentavat salasanasi yleensä pilveen. Tarvitset myös pilveen salasanan, jonka takana salasanasi ovat tallessa. Opettele pääsalasana ulkoa, laita se lapulle kotiin tai tallenna esimerkiksi matkapuhelimeen tai USB-tikulle.
- Tallenna salasanat omalle tietokoneelle ja matkapuhelimeen salasanaohjelman avulla. Lataa tietokoneelle ensin salasanaohjelma. Tee sinne pääsalasana ja opettele se ulkoa tai laita lunttilapulle. Kirjoita sinne myös muut käyttämäsi salasanat. Tallenna salasanat ohjelman avulla ainakin kahdelle laitteelle. Silloin ne ovat turvassa, jos jompikumpi laite katoaa tai menee rikki. Salasanaohjelmia ovat esimerkiksi Password Safe, KeyPass free ja F-Secure Key.

VINKKI

Valehtele turvakysymyksissä

Kun pyydät unohtunutta salasanaa takaisin, joudut joskus vastaamaan turvakysymykseen.

Sinulta on kysytty aiemmin esimerkiksi, mikä oli ensimmäisen autosi merkki tai minkä niminen on lemmikkisi. Olet antanut vastaukset, kun rekisteröidyit palveluun.

Turvakysymyksiin ei pidä vastata rehellisesti. Jos joku tuntee sinut, hän tietää vastauksen ja voi käyttää tietoa hyväkseen. Lisäksi urkkija voi löytää lemmikkisi nimen esimerkiksi somesta.

Valehtele surutta turvakysymysten vastaukset. Tärkeintä on, että muistat, mitä vastasit. Säilytä turvakysymysten vastaukset hyvässä tallessa.

Älä kerro salasanaa kenellekään

Sinut saatetaan huijata paljastamaan salasanasi. Voit saada sähköpostiisi tietojenkalasteluviestin (ks. s. 20), jossa pyydetään salasanaa ja muita tietojasi.

Sinulle voidaan myös soittaa ja kysyä salasanaa (ks. s. 25). Soittaja kertoo olevansa esimerkiksi poliisi tai pankin virkailija. Voit myös joutua internetissä valesivuille (ks. s.24). Luulet, että kirjaudut pankkiin, mutta annatkin tietosi huijareille. Älä anna salasanojasi puhelimessa tai sähköpostissa tulleeseen kyselyyn.

Suosituimmat salasanat 2015

Tietoturvayhtiö SpashData julkaisee vuosittain listan suosituimmista salasanoista. Listan kärjessä ovat samat tutut salasanat kuin edellisinä vuosina. Jotkut numerosarjat ovat pidentyneet.

Pituus ei kuitenkaan niissä auta. Tietokoneet, joilla salasanoja yritetään murtaa, tunnistavat nopeasti numero- tai kirjainjonot. Heikkoja salasanoja ovat myös tutut sanat password (salasana), football (jalkapallo), baseball ja welcome (tervetuloa).

Testaa salasanoja

Kokeile, miten turvallisia salasanoja keksit. Älä kuitenkaan testaa oikeita salasanojasi. Salasanatestin löydät osoitteesta https://howsecureismypassword.net/ Palvelu on tehty opetuskäyttöön. Sen tulokset ovat viitteellisiä.

Palvelun mukaan salasanat murtuvat näin nopeasti:

password	välittömästi
1234567890	välittömästi
salasana	välittömästi
k01ra	2 millisekuntia eli sekunnin tuhannesosaa
k1i2s3s4a5	1 päivä
1F408B15C23	1 kuukausi
Pääsiäisyö	vuosia
MustanKissanPaksutPosket	vuosia
Nytpä_Lähden+Tästä-Pelistä!Pois	vuosia

15 yleisintä salasanaa vuonna 2015

qwerty
(näppäimistön ylin kirjainrivi alkaen vasemmalta)

123456789

1234

password

111111

football

welcome

1234567

12345678

123456

12345

baseball

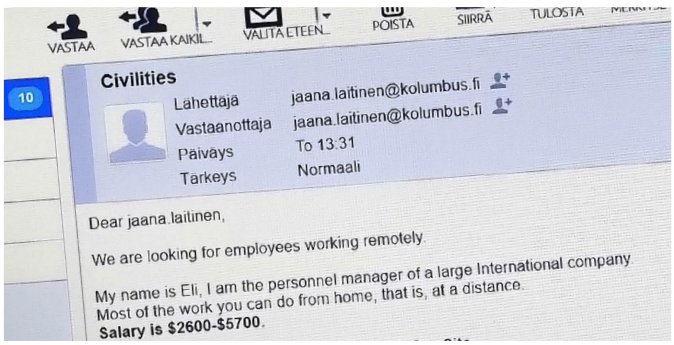
1234567890

1qaz2wsx
(näppäimistön kaksi ensimmäistä pystyriviä vasemmalta)

Opettele sähköpostin turvallinen käyttö

Sähköpostista on tullut monille arjen yhteydenpidon tärkeä väline. Tavoitat sen avulla ihmisiä läheltä ja kaukaa. Sähköposti tavoittaa myös kiireiset ihmiset, jotka eivät aina ehdi vastata puhelimeen.

Alla on kerrottu tärkeimmät sähköpostin käyttöön liittyvät turvataidot. On hyvä opetella ne, sillä sähköpostin kautta leviää myös haittaohjelmia, roskapostia ja huijauksia. Kun osaat toimia harkiten ja tiedät, mitä ei kannata tehdä, suojaat laitteitasi haittaohjelmilta.



Voit saada roskapostia jopa itseltäsi, kuten tässä viestissä. Viestin lähettäjätieto on helppo väärentää.

Näin käytät sähköpostia turvallisesti

- Tarkasta sähköpostin lähettäjä
- Älä avaa tai lataa harkitsematta tuntemattoman lähettäjän liitteitä
- Älä klikkaa sähköpostissa annettua linkkiä
- Älä lähetä tärkeitä henkilökohtaisia tietoja sähköpostissa

Tarkasta sähköpostin lähettäjä

Kun näet saapuneet-kansiossa uuden viestin, älä avaa sitä tuosta vain. Arvioi hetki, onko avaaminen turvallista.

Sähköpostin lähettäjän nimi on helppo väärentää viestikenttään. Tarkasta siksi sähköpostin lähettäjän sähköpostiosoite. Vie hiiren nuoli lähettäjän sähköpostiosoitteen päälle. Älä kuitenkaan klikkaa. Ruudulle avautuu ikkuna tai rivi, joka kertoo, mistä sähköpostiosoitteesta viesti on oikeasti lähetetty.

Lähettäjän nimi voi olla tunnetun yrityksen nimi tai yleinen suomalainen henkilön nimi. Sähköpostiosoite kuitenkin paljastaa, jos se tuleekin huijausmassapostituksia tekevästä osoitteesta ulkomailta.

Älä luota edes tuttavasi nimissä lähetettyyn sähköpostiin, jos et odottanut viestiä häneltä. Joskus lähettäjäksi on väärennetty ystäväsi nimi, jotta avaat sähköpostin epäröimättä. Tarkasta silloinkin lähettäjän sähköpostisoite.

VIESTI	VIESTIN LÄHETTÄJÄ	LÄHETTÄJÄN SÄHKÖPOSTIOSOITE
Your Package	FedEx Post	joao.branco@ci.sc.gov.br
Your Package	FedEx Delivery	bevisko@tpg.com.au
Viitenumerosi on: 3135	Gigantti.fi	newsletter@mailer.bigmailer.eu
Sadat miehet vahvistavat p...	Asiakaspalvelu: Apteekkari	info@supernovaglobal.info
Testaa iPhone 7 meille	Gigantti	myinboxdaily1@consumernews99.com
Prøv Finasavisen i 2 uker f...	Kundesupport: Avisttilbud	info@supernovaglobal.info
Tule Giganttiin ja voita henki...	Gigantti	noreply@gigantti.fi
Sinut on valittu vastaanottamaan...	Gigantti	newsletter@mailer.bigmailer.eu
Ota meihin yhteyttä mahdollis...	Verkkokauppa.com	newsletter@mailer.bigmailer.eu
jaana.laitinen@kolumbus.fi	Lahjakortti	Lahjakortti8654127@sprekengekomen.eu
Onnittelut, olet voittanut mei	IKEA	newsletter@mailer.bigmailer.eu
Vain sinulle, iPhone 6s vain	GIGANTTI	newsletter@mailer.bigmailer.eu
Ota meihin yhteyttä mahdollisim	Verkkokauppa.com	newsletter@mailer.bigmailer.eu
Markkinoiden edistyksellisin...	Parranajotuotteet	info@supernovaglobal.info
Shell	Puolen vuoden polltoaineet ilmaiseksi	martinreplyto@mail.com
Apple Shop	Apple TV	mail@appleshop.fi
RE: Samsung Galaxy S7 E...	GIGANTTI	newsletter@mailer.bigmailer.eu
Lainaa 20000€ ilman vakuuksia	Matti Mäkinen	info@supernovaglobal.info

Vertaa viestin lähettäjien nimiä ja sähköpostiosoitteita. Huomaat, että Gigantin nimissä tulee huijausviestejä useasta osoitteesta. Gigantin oikea osoite, josta se lähettää mainosviestejä, on noreply@gigantti.fi. Myös esimerkiksi Ikean nimissä tulee paljon huijausviestejä.

Listan alimmassa viestissä lähettäjällä on suomalainen nimi. Lähettäjän sähköpostiosoite kuitenkin paljastaa massapostien lähettäjän.

Älä avaa tai lataa tuntemattoman lähettäjän liitetiedostoja

Sähköpostin kautta levitettävät haittaohjelmat on usein piilotettu liitetiedostoihin ja ladattaviin tiedostoihin. Älä avaa niitä suin päin. Virustorjuntaohjelmat eivät löydä kaikkia haittaohjelmia. Avaa liite vasta kun tiedät, että se on tullut luotettavalta lähettäjältä. Tarvittaessa varmista lähettäjältä, että hän on lähettänyt sinulle viestin ja liitteet.

Epäile varsinkin liitteitä, joiden tiedostopäätteet ovat .COM, .EXE, SHS, .PIF ja .VBS. Ne ovat yleisiä sähköpostin kautta leviävissä haittaohjelmissa. Joissakin huijareiden liitteissä voi olla kaksi tiedostopäätettä peräkkäin, esimerkiksi kuva.jpg.VBS tai teksti.rtf.EXE.

Mene palvelun internesivuille ja hoida asia sitä kautta turvallisesti. Muista, että esimerkiksi pankki tai poliisi eivät koskaan ota yhteyttä sähköpostilla.

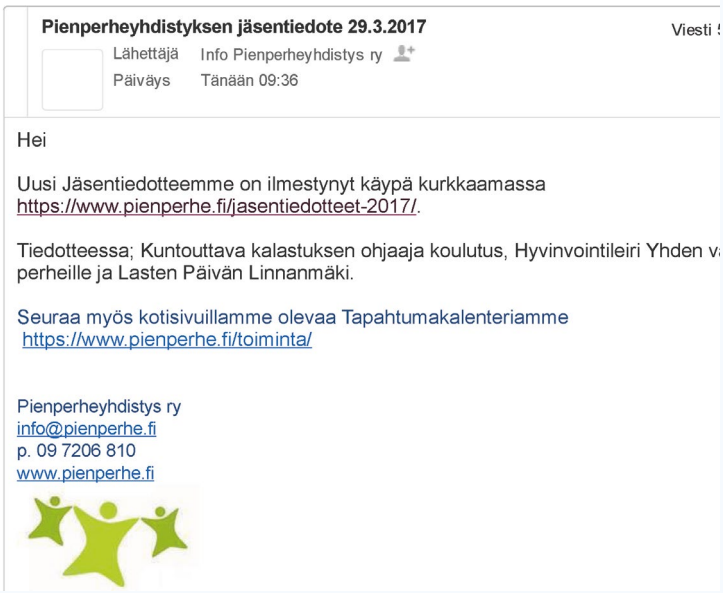
Älä klikkaa sähköpostin linkkiä

Sait tuntemattomalta lähettäjältä sähköpostiviestin, jossa sinulle annetaan linkki. Painat linkkiä ja päädyt esimerkiksi verkkopankin tai jonkin muun palvelun etusivulle. Siellä sinua pyydetään antamaan henkilökohtaisia tietoja.

Linkki saattoi viedä sinut valesivulle, joka muistuttaa pankin oikeita nettisivuja. Kun syötät sinne tietosi, ne päätyvät ulkopuolisten tietoon. Älä suin päin klikkaa viestissä tullutta linkkiä.

Voit tarkastaa, mille sivuille linkki sinut vie. Vie hiiri linkin päälle mutta älä klikkaa. Ruudulle avautuu ikkuna tai rivi, jossa näkyy internetsivujen osoite, jonne linkki johtaa. Katso, onko se sama kuin linkissä kerrottu osoite.

Jos vieläkin epäilyttää, mene palvelun oikeille nettisivuille ja vertaa sitä linkissä olevaan osoitteeseen. Älä kopioi sähköpostissa tarjottua linkkiä selaimen osoitekenttään. Linkki voi viedä sinut valesivuille myös sitä kautta.



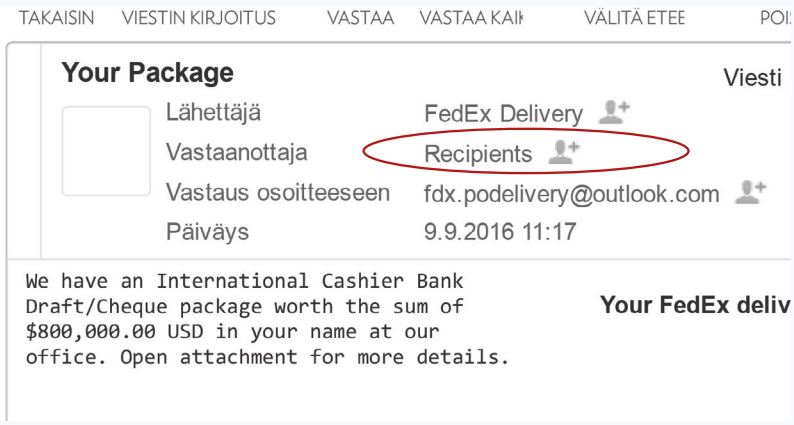
Näin arvioit, onko saamasi sähköposti luotettava

Katso, kuka tai mikä on lähettäjä. Laita sitten kursori lähettäjän tiedon päälle mutta älä klikkaa. Lähettäjän nimen alle avautuu ikkuna, jossa näkyy, mistä sähköpostiosoitteesta viesti on tullut. Vastaavatko ne toisiaan?

Laita kursori viestissä olevan linkin päälle, älä taaskaan klikkaa. Viereen aukeaa ikkuna, jossa näkyy, mihin internetosoitteeseen linkki johtaa. Vertaa osoitteita. Jos ikkunaan avautuva linkki ei ole sama kuin annettu linkki, älä klikkaa.

Viestin allekirjoittaja on yhdistys. Mene nettiin ja googlaa, onko sellainen yhdistys olemassa. Voit googlata myös esimerkiksi lähettäjän nimeä, jos se on annettu.

Tässä viestissä kaikki on hyvin. Vastaanottaja tuntee yhdistyksen, josta sähköposti tuli. Samasta osoitteesta tulevat muutkin jäsenkirjeet. Linkit johtavat oikeisiin osoitteisiin.



Sähköposti kertoo, että sinulle on lähetetty 800 000 dollarin arvoinen shekki pikakuljetuspalvelu FedExin kautta. Viestin lähettäjäksi on kirjoitettu FedEx Delivery. Kun sen päälle laittaa kursorin, avautuu ikkuna, joka paljastaa, että viesti on lähetetty osoitteesta bevisko@tpg.com.eu. Tarkoitus on saada sinut avaamaan liitetiedosto ja antamaan sinne henkilökohtaisia tietoja. Kyse on tietojenkalastelusta. Huomaat sen muun muassa siitä, että viestiä ei ole lähetetty nimelläsi vaan useille vastaanottajia (recipients).

Tunnetun kuljetuspalvelun FedExin nimeä käytetään monissa huijauksissa. Yritys antaa ohjeita huijausten tunnistamiseen sivuillaan.

Pidä tietosi turvassa

Kirjoitat tietokoneella tekstejä, ja laitat ne talteen. Siirrät koneellesi myös hauskat lomakuvat. Saatat tallettaa sinne myös tekemiäsi videopätkiä, opinnäytetöitä, esitelmiä tai pankin tiliotteita ja veroilmoituksen kopioita. Haluat, että ne pysyvät tallessa ja saat ne käyttöösi, kun haluat. Et halua, että joku muu katsoo niitä tai tekee niihin muutoksia luvatta. Et halua sitäkään, että joku muu kopioi niitä käyttöönsä.

On hyvä ymmärtää, että kaikki tieto, jonka olet tallentanut tietokoneelle, voi periaatteessa joutua rikollisen silmiin tai käsiin. Se on mahdollista, jos tietokoneeseesi on internetyhteys.

Mieti siksi, mitkä tietosi ovat niin yksityisiä, ettet missään tilanteessa halua vieraiden näkevän niitä. Jaa tiedostosi suojassa pidettäviin ja vähemmän tärkeisiin. Jos vähemmän tärkeät tiedot joutuvat tietomurron kohteeksi, se harmittaa muttei aiheuta suurta vahinkoa. Esimerkiksi henkilökohtaisia tietoja sisältävät asiakirjat haluat ehkä pitää suojassa. Lomakuvat tai syntymäpäivien kutsulistat saattavat olla vähemmän kriittisiä tietoja. Sinä päätät.

Tietosi voivat vaarantua, jos:

- joku ulkopuolinen käyttää konettasi.
- koneesi menee rikki, katoaa tai se varastetaan.
- koneellesi pääsee haittaohjelma, joka lukitsee koneesi.
- koneellesi pääsee esimerkiksi vakoiluohjelma, joka kopioi tietojasi murtautujan käyttöön.

Näin pidät tietosi turvassa ja eheinä:

- Päästä tietokoneellesi vain ihmisiä, joihin luotat.
- Jos omistat kaksi tietokonetta, pidä vain toinen yhdistettynä internetiin. Tee toisella koneella tärkeät työt, joita et halua missään tilanteessa muiden silmiin. Internetiin yhdistetyllä koneella lähetät sähköpostit, hoidat pankkiasiat ja liikut netissä.
- Ota tiedostoistasi varmuuskopiot. Voit tehdä kopiot USB-tikulle, ulkoiselle kovalevylle tai toiselle tietokoneelle. Voit myös kopioida ne ns. pilveen. Pilvipalveluja ovat esimerkiksi iCloud ja DrobBox tai OneDrive.
- Pilvi on pilvipalveluja tarjoavan yrityksen omistama tehokas tietokone, palvelin. Voit tallentaa sinne tietojasi salasanan ja käyttäjätunnuksen taakse. Pilvipalvelu voi sisältyä yrityksen palvelupakettiin tai voit ostaa tilaa pilvestä.

Kumpaa tallennustapaa käytät:

- **Muistitikku tai ulkoinen kovalevy**
  Kotona tikulla tai ulkoisella kovalevyllä tiedot säilyvät tallessa, jos laitteetkin ovat tallessa ja ehjiä. Hakkerit ja tietoverkkojen murtautujat eivät pääse niihin käsiksi.
- **Pilvipalvelu**
  Pilvestä saat tietosi käyttöön missä tahansa. Voit tallentaa sinne kuvat ja katsoa niitä kotoa, kylässä, työpaikalla tai vaikka lomamatkalla. Pääset pilveen millä tahansa tietokoneella, tabletilla tai älypuhelimella.
  Pilven avulla voit myös jakaa tietojasi. Jos annat käyttäjätunnuksen ja salasanan esimerkiksi sukulaiselle tai työkaverille, hänkin pääsee näkemään kuvasi ja muut tietosi missä onkaan.
  Tietosi ovat turvassa pilvessä myös silloin, jos kotona syttyy esimerkiksi tulipalo tai tietokoneesi ja muistitikkusi päätyvät varkaan käsiin.
  Isojen yritysten pilvipalvelut ovat yleensä turvallisia. Yhteydet kotikoneeltasi pilveen ovat salattuja. Osa pilvipalvelujen tarjoajista salaa myös pilvessä olevat tietosi. Kaikki eivät niin kuitenkaan tee. On olemassa pieni mahdollisuus, että taitava rikollinen murtautuu pilveen ja näkee sieltä tietosi.

VINKKI

Varmuuskopioi ahkerasti

Ota tavaksi tallentaa varmuuskopiot säännöllisesti. Jos teet tärkeää työtä, ota varmuuskopiot vaikka työpäivän päätteeksi. Tilanteen ja tietokoneen käytön mukaan voit kopioida tietosi talteen myös esimerkiksi kerran viikossa.

Helpointa on laittaa tietokone tallentamaan varmuuskopiot automaattisesti.

Tärkeää on, että otat varmuuskopiot säännöllisesti. Se voi tuntua turhalta, jos mitään pahaa ei tapahdu.

Sitten eräänä päivänä tietokone menee rikki tai kiristysohjelma lukitsee koneesi. Jos tiedoista ei ole kopioita, on vaara, että menetät ne.

Älä laita vierasta USB-tikkua koneeseesi

No, mutta tuossahan lojuu joutava muistitikku. Sujautan sen taskuun ja työnnän koneeseen kotona. Kannattaahan se ottaa, kun löytää tai ilmaiseksi saa.
Ei kannata! Muistitikku on yksi keino, joilla tietokoneille ujutetaan haittaohjelmia. Älä siis laita tietokoneeseesi vierasta muistitikkua.

Haittaohjelma saastutti satoja Helsingin kaupungin tietokoneita

Helsingin kaupungin sosiaali- ja terveysviraston satoihin tietokoneisiin levisi haittaohjelma vuonna 2016. Se ilmeisesti yritti liittää viraston tietokoneet rikolliseen bottiverkkoon. Verkko ei ehtinyt aktivoitua ennen kuin haittaohjelma huomattiin. Potilas- ja asiakastietoihin haittaohjelma ei päässyt käsiksi.
Haittaohjelman lähettäjää ei tiedetä. Kaupunki pitää mahdollisena, että ohjelma pääsi työkoneisiin jonkun työntekijän saastuneen USB-muistitikun kautta. Haittaohjelman poisto maksoi kaupungille 95 000 euroa.

Lähde: Helsingin Sanomat

Postiluukusta tipahti saastuneita USB-tikkuja Australiassa

Melbournen kaupungin asukkaat saivat syyskuussa 2016 kotiinsa saastuneita USB-tikkuja. Niitä tipautettiin sisään postiluukusta. Asukkaat, jotka laittoivat tikun tietokoneeseen, saivat siitä vakavia ongelmia, poliisi kuvaa. Poliisi julkaisi nopeasti tikuista varoituksen.
Saastuneet muistitikut ovat vanha kikka. Ehkä kuuluisin tikulla levitetty haittaohjelma on Stuxnet. Se on tietokonemato, joka vakoilee ja uudelleen ohjelmoi teollisuuden tietojärjestelmiä.
Stuxnet päätyi iranilaiseen ydinlaitokseen saastutetun USB-tikun avulla. Laitoksen tietokone, johon Stuxnet päätyi, ei ollut yhteydessä internetiin. Mato rikkoi ydinkeskuksen erottelulaitteet sentrifugit. Ohjelma sai sentrifugit pyörimään liian nopeasti, jolloin ne menivät rikki. On arveltu, että madon tarkoitus oli hidastaa Iranin ydinohjelmaa. Stuxnet löytyi vuonna 2010.

Sanasto haltuun

Hakkeri tarkoittaa innokasta tietokonealan harrastajaa. Hakkereiksi kutsutaan usein myös tietojärjestelmiin murtautujia.

Linkki on kuva, teksti tai sana, joka vie käyttäjän toiselle nettisivulle.

Pilvi, pilvipalvelu on tietojen tallennuspalvelu, jota monet it-alan yritykset tarjoavat. Tiedot tallentuvat yrityksen verkossa olevalle palvelimelle.

Salasana on kirjaimista, numeroista ja erikoismerkeistä koostuva avain, jonka avulla pääset käyttämään käyttäjätunnustasi.

Salasanapalvelulla voit tallentaa kaikki salasanasi turvaan pilvipalveluun.

Tiedostopääte on tiedoston nimeen liittyvä tunnusosa, jonka avulla erityyppiset tiedostot erottuvat toisistaan. Päätteessä on yleensä kolme kirjainta. Se erotetaan tiedoston nimestä pisteellä.

Turvakysymysten avulla eri palvelut voivat varmistua, että oikea henkilö pyytä lupaa tilin käyttöön. Niitä voi tarvita, jos olet unohtanut esimerkiksi salasanan tai käyttäjätunnuksen.

USB-tikku on ulkoinen muistitikku, jolle voi tallentaa tietoja.

Valesivu on jonkin yrityksen tai muun palvelun oikeita internetsivuja muistuttava valesivu. Valesivulla käyttäjiä harhautetaan antamaan esimerkiksi verkkopankin tai luottokortin tunnukset.

3 HAITTAOHJELMISTA EROON

Vaikka olet huolehtinut tietokoneesi tietoturvasta, on mahdollista, että koneellesi kuitenkin pääsee haittaohjelmia. Ne voivat olla niin uusia, että kaikki virustorjuntaohjelmat eivät tunnista niitä vielä.

Internet on helppo ja edullinen väline, jolla haittaohjelmia voi levittää. Siksi se houkuttelee myös epärehellisiä käyttäjiä.

Haittaohjelmat leviävät muun muassa sähköpostien ja saastuneiden nettisivujen kautta. Kun internetin käyttäjä menee sivuille, jonne on saatu laitettua haittaohjelma, se siirtyykin sieltä käyttäjän koneelle.

Tyypillisesti voit saada haittaohjelman, kun lataat videoita, kuvia tai ohjelmia arveluttavilta nettisivuilta. Nykyään haittaohjelma voi siirtyä koneellesi myös luotettavina pidetyiltä nettisivuilta.

Viime vuosina myös huijaukset ovat lisääntyneet nopeasti. Internetin käyttäjä houkutellaan antamaan huijareille henkilökohtaisia tietoja, lähettämään rahaa tai ostamaan olemattomia tuotteita.

Alla on kerrottu yleisimmät haittaohjelmatyypit, joihin voi internetissä törmätä. Ohjeet neuvovat, miten pääse haittaohjelmista eroon.

Tavallinen internetin käyttäjä kohtaa netissä useimmiten näitä riskejä:

Haittaohjelmat, esimerkiksi:

- Kiristysohjelmat
- Vakoiluohjelmat
- Tietojenkalastelu
- Tietokoneen kaappaus, palvelunestohyökkäykset

Huijaukset, esimerkiksi:

- Tilausansat
- Huijarit

VINKKI

Poliisi, Kyberturvallisuuskeskus ja tietoturvayhtiö F-Secure pitävät yllä netissä sivustoa, joka antaa ajankohtaista tietoa kiristysohjelmista. Se myös neuvoo kiristyksen kohteeksi joutuneita.

Sivuston osoite on http://www.ransomware.fi/

Kiristysohjelmat

Voit joutua kiristyksen kohteeksi tietoverkoissa monella tavalla. Yksi keino ovat kiristyshaittaohjelmat (ransomware). Voit saada haittaohjelman tietokoneellesi esimerkiksi, kun lataat ilmaisen ohjelman tai avaat sähköpostissa liitetiedoston, johon haittaohjelma on piilotettu.

Kiristysohjelma lukitsee kaikki tiedostot ja valokuvat koneeltasi. Kiristysohjelma pyytää sinua maksamaan lunnaat. Kun maksat, saat ns. salausavaimen. Se on pieni ohjelmisto, joka poistaa lukituksen.

Salausavaimesta saatetaan pyytää muutama sata euroa. Vaikka maksat, ei ole varmaa, että salaus poistuu. Menetät silloin sekä rahat että tiedostosi. Kiristysohjelmien kohteena ovat usein tavalliset tietokoneen käyttäjät.

Suomessa löydettyjä kiristysohjelmia ovat esimerkiksi Cryptowall ja TorrentLocker. CryptoWallin lukitsemat tiedot voi purkaa vain salausavaimella. TorrentLockerin lukitsemat tiedostot voidaan joskus palauttaa ilman salausavaintakin.

Kiristäjä voi esiintyä jopa poliisina

Kiristäjä saattaa joskus esiintyä poliisina. Viestiin on voitu liittää poliisin virkamerkin kuva, jotta se on uskottavampi. Viestin saajaa pyydetään maksamaan sakko, jotta hän saa koneensa taas käyttöönsä.

Kyse on huijauksesta. Viranomaiset eivät lukitse tietokoneita eivätkä vaadi maksua lukituksen avaamisesta

Riisuitko nettikameralle? Voit saada kiristyskirjeen.

Tapasitko netissä kiinnostavan henkilön, jonka kanssa jutustelu kääntyi seksiin? Saatoit kohdata kiristäjän.

Nettituttu viekoittelee sinut puhumaan tuhmia tai riisuutumaan. Keskustelukumppanisi nauhoittaa keskustelun ja riisuutumisen. Sen jälkeen hän alkaa kiristää sinulta rahaa. Pyydetyt summat saattavat olla tuhansia euroja. Jos et maksa, kuvat ja ääninauhat uhataan lähettää esimerkiksi puolisolle tai ne päätyvät nettiin.

Myös nettiromanssit valeprofiilien kanssa voivat muuttua kiristykseksi. Lue lisää luvusta 9. Älä maksa kiristäjälle. Ota yhteyttä poliisiin.

Vakoiluohjelmat

Vakoiluohjelmat ovat haittaohjelmia, jotka keräävät tietoa laitteen käyttäjästä ja lähettävät sitä hyökkääjälle.
Voit saada vakoiluohjelman tietokoneelle, jos esimerkiksi lataat netistä ilmaisia ohjelmia. Niiden kylkiäisenä koneelle tulee haittaohjelmia.
Sniffer-niminen vakoiluohjelma tallentaa koneen ja internetin liikennettä. Se yrittää saada haltuunsa salasanoja ja tunnuksia.
Keylogger-haittaohjelma seuraa näppäinten painalluksia ja nauhoittaa ne. Nauhuri saa selville kaiken, mitä teet koneella salasanoja myöten.

Tietojenkalastelu (phishing)

Tietojenkalastelu tarkoittaa sitä, että ulkopuolinen urkkii henkilökohtaisia tietojasi.
Voit saada esimerkiksi sähköpostissa houkuttelevan mainoksen, tarjouksen, kyselyn tai mahdollisuuden osallistua kilpailun. Jotta saat voiton tai edullisen tarjouksen, joudut antamaan esimerkiksi henkilötunnuksen, verkkopankkitunnukset tai maksukortin tiedot. Ne päätyvätkin rikollisten haltuun. Tunnista tietojenkalasteluviestit, ja poista ne sähköpostista avaamatta.

Tunnistat tietojenkalasteluviestin näistä piirteistä:

- Saat sähköpostiviestin, jota et ole odottanut.
- Et tunnista viestin lähettäjää tai lähettäjän sähköpostiosoitetta. Lähettäjä saattaa vaikuttaa luotettavalta. Lähettäjäksi kerrotaan esimerkiksi pankki tai luottokorttiyhtiö.
- Viestiä ei välttämättä ole osoitettu sinulle henkilökohtaisesti.
- Viesti on kirjoitettu huonolla suomella tai englanniksi.
- Viestissä esimerkiksi varoitetaan turvallisuusuhasta tai kerrotaan teknisestä viasta, joka edellyttää kiireellisiä toimia.
- Viestissä voidaan luvata rahaa tai uhata sulkea tilisi.
- Viestissä oleva linkki tai verkko-osoite ohjaa sivulle, jossa sinulta kysytään luottamuksellisia tietoja.

Lue lisää erityisesti pankki- ja maksukorttitietojen urkkimisesta luvusta 4.

Tietokoneen kaappaus ja palvelunestohyökkäykset

Joku ulkopuolinen voi ottaa haltuunsa tietokoneesi tai sen osan. Haltuunotto onnistuu esimerkiksi haittaohjelman avulla. Voit saada kaappaushaittaohjelman esimerkiksi, kun avaat epämääräisen sähköpostin liitetiedoston. Ohjelma voi tulla myös internetistä ladattavan ilmaisohjelman kylkiäisenä.
Kaappaaja voi käyttää tietokonettasi esimerkiksi peittelemään omia tekemisiään. Koneesi voidaan laittaa levittämään roskapostia. Kaappaaja on voinut myös levittää koneesi avulla laittomia ohjelmia tai vaikka ladata lapsipornoa. Kaappaaja voi myös kaapata esimerkiksi webkameran ja laittaa sen vakoilemaan sinua.
Usein kaappaaja käyttää tietokonetta palvelunestohyökkäykseen jotakin yritystä tai julkishallinnon palvelua kohtaan. Palvelunestohyökkäys tarkoittaa sitä, että suuri joukko tietokoneita laitetaan lähettämään liikennettä yhtä aikaa hyökkäyksen kohteeksi joutuneille nettisivuille. Nettisivut menevät tukkoon. Sivuja ei voi käyttää tilapäisesti tai pysyvästi.
Palvelunestohyökkäyksen tekijä haluaa kiusata tai hakee huomiota. Hän voi yrittää kiristää rahaa hyökkäyksen lopettamisesta.
Uusi ilmiö on, että palveluestohyökkäyksiin valjastetaan mukaan kotona olevia laitteita, joissa on nettiyhteys. Lue lisää esineiden internetistä (IoT, Internet of Things) ja oman lähiverkon suojaamisesta sivulta 7.

Hyökkäys Kelan palveluihin jatkui monta päivää.

Kela joutui palvelunestohyökkäyksen kohteeksi lokakuussa 2016. Hyökkäyksiä oli useina päivinä.
Hyökkäys kohdistui Kelan käyttämiin tunnistuspalveluihin sekä Kanta-palveluun. Kanta-palvelut sisältävät muun muassa sähköiset potilastiedot ja sähköiset reseptit. Tiedossa ei ole, mistä hyökkäys tuli ja kuka sen teki.

Lähde: Helsingin Sanomat 15.10.2016

Mistä tiedän, että koneellani on haittaohjelma?

- Aina et mistään. Haittaohjelman tekijä haluaa, ettet huomaa sitä, jotta ohjelma ehtii tehdä, mitä se on ohjelmoitu tekemään.
- Virustorjuntaohjelma kertoo, että se on havainnut jonkin haittaohjelman.
- Tietokone käyttäytyy omituisesti, esimerkiksi nytkähtää tai siirtyy yllättäen toiselle sivulle.
- Kuvaruutuun ilmestyy teksti, joka kertoo, että kone on lukittu. Sinua pyydetään maksamaan vaadittu summa rikollisten tilille. Koneellesi on päässyt kiristysohjelma.
- Kone tökkii ja hidastelee. Se voi merkitä, että sitä käytetään parhaillaan palvelunestohyökkäyksessä.

Mitä teen, jos epäilen, että koneellani on haittaohjelma?

- Anna virustorjuntaohjelman poistaa tai eristää haittaohjelma.
- Jos epäilet, että tietokone on kaapattu, irrota verkkokaapeli tietokoneesta tai sulje modeemi. Laita sen jälkeen virustorjuntaohjelma tarkastamaan kone.
- Yritä poistaa koneen lukinnut kiristysohjelma vain, jos olet taitava tietokoneen käyttäjä. Älä maksa kiristäjälle. Ilmoita poliisille.
- Jos haittaohjelma tai sen aiheuttamat ongelmat eivät poistu, vie kone ammattilaisen puhdistettavaksi.

VINKKI

Voit tarkastaa internetissä olevilla ns. online scannereilla, onko koneellasi haittaohjelmia. Ne saattavat löytää haittaohjelman, jota tietoturvaohjelma ei löydä.
Käytä vain tunnettujen, luottavien tietoturvayritysten online scannereita. Niitä ovat esimerkiksi F-Securella, Nortonilla ja Symtechillä.

VINKKI

Voit katsoa yleisimmät netissä liikkuvat haittaohjelmat, niiden nimet ja lyhyt esittely täältä:
Kyberturvallisuuden verkkokurssi, Jyväskylän yliopisto,
https://peda.net/jyu/it/kyberturvallisuus/kkv

Kyberturvallisuuskeskus valvoo internetin turvallisuutta

Viestintäviraston Kyberturvallisuuskeskus valvoo Suomessa tietoverkkojen turvallisuutta. Se seuraa verkkoliikennettä ja jakaa tietoa haittaohjelmista teleyrityksille ja verkkopalvelun tarjoaville yrityksille. Keskus myös kerää tietoa netissä liikkuvista haittaohjelmista.

Seuraa keskuksen varoituksia

Kyberturvallisuuskeskus julkaisee varoituksia, jos liikkeellä on erityisen haitallisia tai nopeasti leviäviä haittaohjelmia. Varoituksia tule myös, jos tietokoneohjelmissa on havaittu haavoittuvuuksia.

Varoitukset löytyvät keskuksen internetsivuilta
https://www.viestintavirasto.fi/kyberturvallisuus
Varoitus on voimassa, kunnes kyberturvallisuuskeskus ilmoittaa, että tilanne on hallinnassa ja tietoturvapuutteet on saatu kuntoon.

Värikoodi kertoo, miten vakava varoitus on:

	Punainen kolmio kertoo, että tilanne on kriittinen. Netin käyttäjien pitää tehdä suositellut korjaukset tai puhdistukset välittömästi.
	Keltainen kolmio kertoo, että tilanne on vakava. Netin käyttäjän pitää noudattaa yleistä varovaisuutta. On mahdollista, että koneelle pitää tehdä korjauksia tai puhdistuksia.
	Varoituksen voimassaolo on päättynyt.

Kyberuhkia on viisi eri tyyppiä:

TAUSTAA

1. Kyberaktivismi (eli kybervandalismi tai haktivismi)
   Kyberaktivismia on yksittäisten hakkerien tai hakkeriryhmien toiminta. Se voi olla osin vaaratonta kokeilunhalua tai halua näyttää taitojaan.
   Haktivismi on tietoverkoissa tapahtuvaa aktivismia. Haktivisti tai -ryhmä halua saada huomiota tai muutosta johonkin asiaan. Haktivismia on esimerkiksi internetsivuille murtautuminen ja niiden sotkeminen.
2. Kyberrikollisuus
   Kyberrikokset tarkoittavat rikoksia, joita tehdään tietoverkkojen kautta. Niitä ovat esimerkiksi petokset, häirintä, uhkailu, laittoman materiaalin levittäminen tai palvelunestohyökkäys. Kyberrikollisuus on tärkein tavalliseen tietokoneen käyttäjään kohdistuva kyberuhka.
3. Kybervakoilu
   Kybervakoilulla hankitaan salaisia tietoja yksityisiltä ihmisiltä, yrityksiltä ja valtion hallinnolta. Tavoitteena on saada taloudellista, poliittista tai sotilaallista etua. Tietoverkkojen kautta vakoillaan erityisesti yrityksiä. Myös valtioita vakoillaan. Kybervakoilu on valtioille suurin kyberuhka. Sen avulla urkitaan tietoja kohdemaasta.
   Tietojen avulla yritetään esimerkiksi vaikuttaa maan sisäisiin asioihin.
4. Kyberterrorismi
   Kyberterrorismi tarkoittaa hyökkäyksiä yhteiskunnan toimintakyvylle tärkeitä tietoverkkoja kohtaan. Tarkoitus on aiheuttaa vahinkoa ja pelkoa ja saada maan johto taipumaan terroristien vaatimuksiin.
5. Kyberoperaatiot
   Kyberoperaatiot ovat osa nykyaikaista sodankäyntiä tai pienempää valtioiden välistä kriisiä. Operaatiot sisältävät toisen maan asioihin vaikuttamista ja maan johdon painostamista. Kohteena ei ole vain kohdemaan sotavoimat vaan myös esimerkiksi talouselämä ja päättäjät.
   Kyberoperaatioita tekevät valtiot sekä niiden rahoittamat tai niiden suojeluksessa toimivat ryhmät.
   On arvioitu, että maailmassa on kymmenen valtiota, jotka pystyvät lamauttamaan kyberoperaatioilla toisen maan laaja-alaisesti.

Kyberrikollisuus on suurin kyberuhka tavalliselle tietokoneen käyttäjälle

Sana kyber viittaa sähköiseen tietojen käsittelyyn eli tietotekniikkaan, sähköiseen tiedonsiirtoon, tietoverkkoihin ja tietokoneisiin. Kun käytät internetiä, maksat maksukortilla tai lähetät viestin matkapuhelimella, liikut kybermaailmassa. Kyber kuuluu meidän kaikkien arkeen.

Kyberuhkat ovat uhkia, jotka voivat vaarantaa tietoverkkojen oikean toiminnan. Se tarkoittaa, että joku voi vahingoittaa tietoverkkoja tai käyttää tietoverkkoja vahingolliseen tarkoitukseen. Niitä ovat esimerkiksi rikokset, kiusanteko tai rikollisen materiaalin levittäminen.

Tietoverkkojen väärinkäyttäjiä voivat olla yksittäiset ihmiset, ryhmät, yritykset ja valtiot.

Sanasto haltuun

Esineiden internet (Internet of Things, IoT) tarkoittaa sitä, että useilla kodinkoneilla ja muilla vastaavilla laitteilla (esimerkiksi valvontakameroilla, autoilla jne.) on internetyhteys. Se mahdollistaa muun muassa laitteiden etäkäytön.

Lähiverkko on esimerkiksi kodin tai yrityksen oma sisäinen verkko. Se yhdistää modeemin ja kaikki sitä käyttävät laitteet, esimerkiksi tietokoneet ja älykodinkoneet. Lähiverkko on yleensä langaton. Modeemi erottaa lähiverkon ja internetin tietoverkot toisistaan.

Palvelunestohyökkäys tarkoittaa tapahtumaa, jossa jollekin verkkosivulle ohjataan niin paljon liikennettä, että se menee tukkoon eikä pysty palvelemaan asiakkaitaan.

4 PANKIT JA MAKSUKORTIT

Internet on tehnyt mahdolliseksi sen, että voit kotona hoitaa pankkiasioita, maksaa laskuja, varata ja maksaa matkoja ja lippuja, ostaa verkkokaupoista ja käydä kauppaa muiden kanssa. Et joudu enää menemään laskupinon kanssa pankin konttoriin tai pankkiautomaatille. Pääset ostoksille kauppoihin, jotka ovat satojen kilometrien päässä. Se helpottaa arkea ja tuo valinnan varaa, vaikka asut kaukana liikekeskuksista.
Siellä missä raha liikkuu, siellä liikkuu myös rikollisia. Opettele turvalliset tavat käyttää rahaa internetissä. Niin et päästä rosvoja kukkarollesi netissäkään.

Kuva: Freepik.com

PANKIT

Pankeilla on omat, internetissä toimivat verkkopankkinsa. Saat verkkopankin käyttöön, kun teet siitä sopimuksen pankkisi kanssa. Saat verkkopankkitunnukset, joilla pääset verkkopankkiin hoitamaan pankkiasioitasi.
Verkkopankkien käyttö on turvallista, jos olet huolehtinut tietokoneesi tietoturvasta. Se tarkoittaa, että tietokoneellasi on hyvä virustorjuntaohjelma ja selaimessasi ja ohjelmissasi on aina uusimmat, päivitetyt versiot (ks. ohjeet luvusta 1).
Yhtä tärkeää on, ettet päästä tietokoneellesi haittaohjelmia: et esimerkiksi klikkaa huolettomasti linkkejä, availe outoja sähköposteja ja anna tietoja kalasteleville rikollisille luottokortin numeroa, henkilötunnusta tai tilitietojasi (ks. ohjeet luvusta 2).

Tunnista pankkitietojen urkinta

- Haittaohjelmat
- Pankkien valesivut
- Tietojenkalastelu
- Pankkitietoja kysytään puhelimessa

Käytät verkkopankkia turvallisesti näin:

- Kirjaudu pankin internetsivujen kautta
  Kun haluat käyttää verkkopankkia, mene pankkisi internetsivuille ja valitse sieltä linkki, josta pääset verkkopankkiin.
  TÄRKEÄÄ: Älä koskaan mene verkkopankkiin painamalla linkkiä, jota sinulle lähetetään esimerkiksi sähköpostissa tai tekstiviestissä.
- Tarkasta, että yhteys pankkiin on suojattu
  Kun saavut verkkopankkiin, katso ruudun vasenta yläreunaa selaimen osoiterivin vieressä. Siellä pitää olla lukon kuva. Selaimen osoiterivillä osoitteen alussa pitää lukea https://, ei http://.
  Lukko ja s-kirjain tarkoittavat, että tietokoneen ja pankin välinen yhteys on salattu. Ulkopuolinen ei pääse tilillesi eikä näe, mitä teet verkkopankissa. Lukko ja s-kirjain kertovat myös, että olet pankin aidoilla sivuilla. Huijarit tekevät nykyään uskottavan näköisiä verkkopankkisivuja, joilla urkitaan tunnuslukujasi. Niissä lukkoa ja s-kirjainta ei yleensä kuitenkaan ole.

Tästä tunnistat salatun yhteyden

https:// salattu yhteys.
http:// salaamaton yhteys.
Tarkasta osoiteriviltä, että olet pankin oikeilla sivuilla:
Katso, mitä verkkopankin osoiterivillä lukee (ks. s. x).
Jos se on sama kuin pankin verkko-osoite, olet oikeassa paikassa.

Haittaohjelmat

Tietokoneellesi voi tulla haittaohjelmia. Niitä voit saada esimerkiksi sähköpostin liitetiedostoista ja videoista, kuvista ja ohjelmista, joita lataat netistä.
Haittaohjelma voi esimerkiksi avata pop up -ikkunan sillä aikaa, kun asioit verkkopankissa. Ikkuna voi pyytää sinua esimerkiksi vastaamaan kyselyyn. Ikkunan tarkoitus on harhauttaa sinua hetkeksi. Kun vastaat kyselyyn tai teet jotakin muuta mitä ikkuna sinulta pyytää, rikolliset saavat aikaa siirtää rahaa tililtäsi.

Vakoiluohjelma puolestaan tallentaa kaikki näppäinten painallukset koneellasi (keylogger, ks s. x). Niin verkkopankkisi salasana päätyy huijareille. Voit saada sen jälkeen puhelun tai sähköpostin, jossa kysytään pankkitunnuksia (ks. s. x). Jos erehdyt antamaan ne, ulkopuoliset kirjautuvat verkkopankkiin tilillesi.

Tietokoneeseen päässyt haittaohjelma teki pop up -ikkunan, kun käyttäjä hoiti pankkiasioita verkkopankissa. Sen tarkoitus on harhauttaa pankin asiakasta hetkeksi. Hyökkääjä voi sillä aikaa siirtää rahaa tililtä.

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 pitää painaa.
Jos painat, päädyt pankin valesivuille. Ne voivat näyttää uskottavilta ja muistuttaa pankin oikeita nettisivuja. Niitä on usein vaikea erottaa oikeista sivuista. Joskus vain selaimen osoiterivillä oleva osoite kertoo, että oletkin huijareiden tekemillä valesivuilla. Siellä ei lue pankin oikea osoite vaan jotakin muuta. Ole tarkkana, ero voi olla pieni.
Aiemmin huijausviestit ja -sivut tunnisti yleensä siitä, että niiden suomen kieli oli tökeröä. Nykyään huijausviestit voivat olla myös hyvää kieltä. Niiden tekstien suomentamisessa voidaan käyttää kielenkääntäjiä.

Lähettäjä: 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

Danske Verkkopankki lähestyi asiakasta sähköpostilla. Sen mukaan pankin turvallisuusosasto tekee kriittisiä päivityksiä. Asiakasta pyydetään klikkaamaan linkkiä ja antamaan tietoja. Kyse on pankkitietojen urkinnasta. Tunnistat huijaksen huonosta kielestä ja lähettäjän tiedoista.

Tietojenkalastelu

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

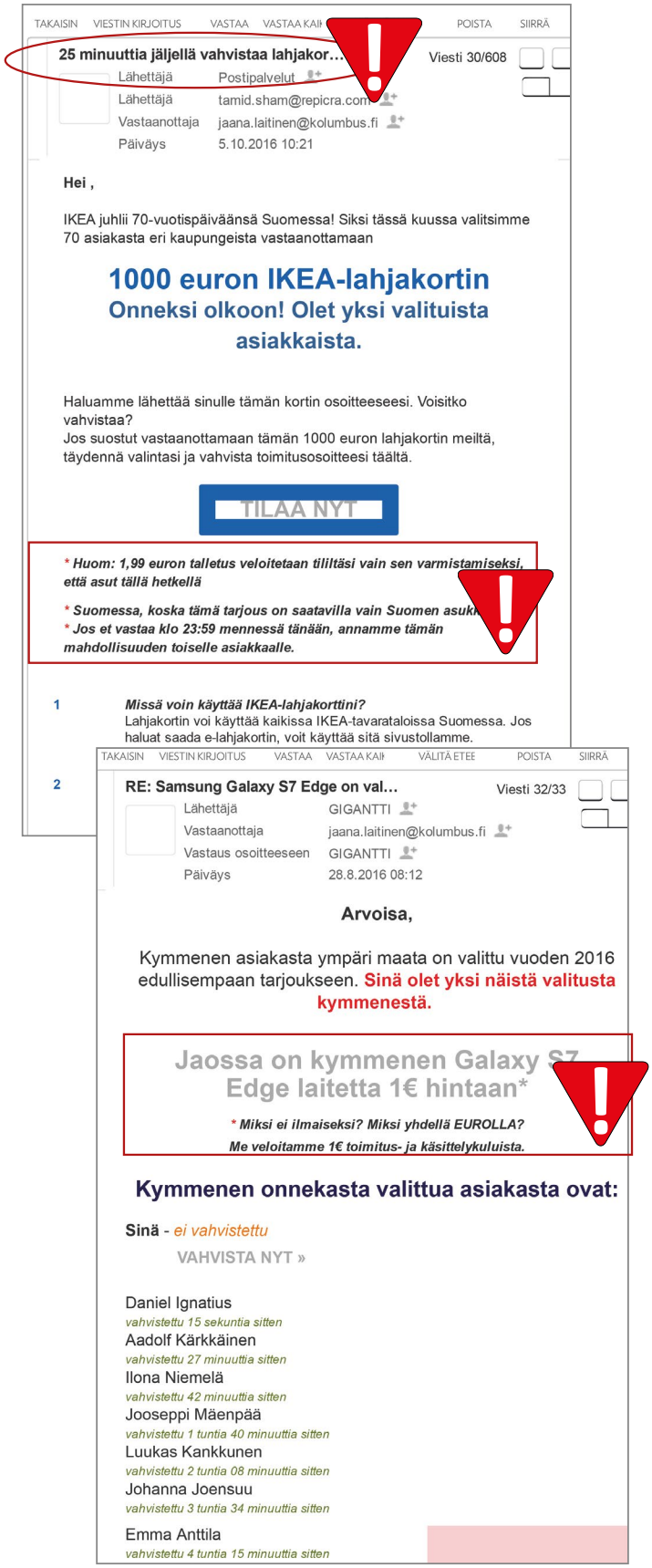
Tietoja kalastellaan monin kekseliäin keinoin. Saatat saada sähköpostin, jossa sinua houkutellaan osallistumaan kilpailuun tai vastaamaan kyselyyn. Kiitokseksi luvataan vaikka kallis matkapuhelin ilmaiseksi tai eurolla. Joskus sinua pyydetään testaamaan kallista laitetta. Palkaksi siitä luvataan ilmainen tuote.

Tarina jatkuu niin, että jotta tuote tai palkinto voidaan lähettää sinulle, joudut antamaan viestin lähettäjälle henkilötietojasi. Sinulta kysytään esimerkiksi osoite, henkilötunnus, pankkitunnukset ja/tai luottokortin tiedot.

Luottokortin tietojen kysymistä voidaan perustella esimerkiksi sillä, että niin halutaan varmistaa, että tuotteen testaaja tai kisan voittaja on suomalainen.

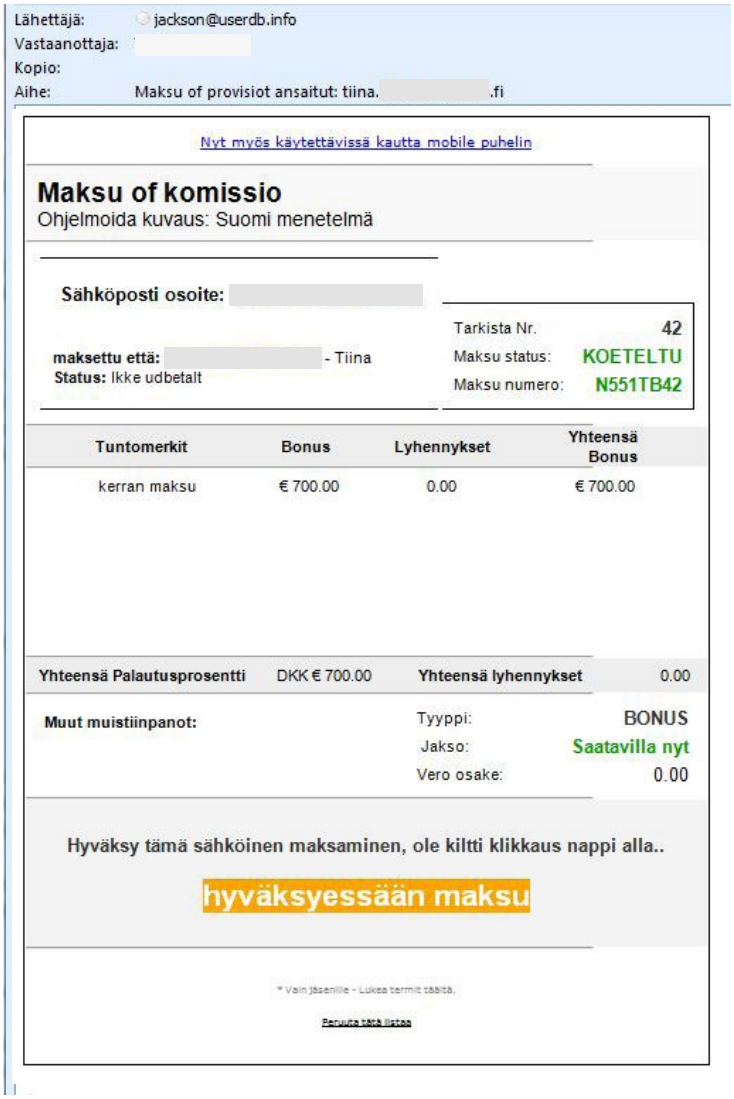
Kalasteluviestit ovat usein taitavasti tehtyjä ja houkuttelevia. Joskus niissä on aikaraja, jonka kuluessa sinua pyydetään reagoimaan. Esimerkiksi viesti sanoo, että tarjous on voimassa vain tunnin. Viestissä tikittää kello, jossa aika hupenee. Sen tarkoitus on, että klikkaat tarjousta ja annat tietosi nopeasti. Et ehdi miettiä, kannattaako niin tehdä. Et saa aikaa googlata internetistä, voiko tarjous olla totta.

Niin kannattaa tehdä. Netissä yleensä selviää nopeasti, että kyse on tietojen kalastelusta tai muusta huijauksesta.



Voit ilmoittaa tietojenkalastelusta Viestintäviraston Kyberturvallisuuskeskukselle. Sen sähköpostiosoite on cert@ficora.fi

Kerro sähköpostissa tietojenkalastelusivun internetsivun osoite tai huijaussähköpostin lähettäjän sähköpostiosoite. Näet sen, kun laitat hiiren lähettäjän nimen päälle.



Ole kiltti klikkaus nappi alla...

Sähköpostin lähettäjä haluaa lähettää sinulle provisioita 700 €. Viesti on yritetty saada näyttämään uskottavalta maksutositteelta. Se ei ole oikein onnistunut: viestissä on monia kielivirheitä, jotka paljastavat sen huijaukseksi.

Pankkitietoja kysytään puhelimessa

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

Jos pankkikorttisi tai luottokorttisi on kadonnut tai varastettu, varas saattaa soittaa ja kysyä tunnuslukua. Niin hän pääsee käyttämään korttiasi.

Vaikka soittaja kuulostaa uskottavalta, älä kerro henkilötietoja tai pankkitietojasi puhelimessa. Kerro ne vain, jos olet itse soittanut pankkiin ja pankki kysyy niitä, kun se haluaa varmistaa henkilöllisyytesi.

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

Jos haluat varmistua siitä, että soittaja todella on esimerkiksi viranomainen, pyydä soittajan nimi, puhelinnumero ja toimipaikka. Rehellinen virkamies kertoo ne mielellään.

Älä soita annettuun numeroon, sillä vastaaja saattaa olla huijari itse tai hänen rikostoverinsa. Puhelu saattaa joskus mennä maksulliseen numeroon.

Sen sijaan katso numerohausta tai kysy numerotiedustelusta soittajan työpaikan numero ja soita sinne. Kysy, onko teidän palveluksessa tämä ja tämä henkilö ja miksi hän kysyy henkilökohtaisia tietojani puhelimessa.

Verkkopankin käyttäjätunnus ja avainlukulista pitää säilyttää salassa ja erillään

Korkein oikeus (KKO) linjasi ennakkopäätöksessään, mitä henkilökohtaisen verkkopankkitunnuksen huolellinen säilyttäminen edellyttää.
KKO katsoi, että käyttäjätunnus ja avainlukulista on säilytettävä kotonakin erillään. Ne eivät saa olla toisten tiedossa tai helposti löydettävissä.
Tapauksessa vaimo säilytti tunnusta ja avainlukulistaa kotonaan niin, että myös mies tiesi niiden säilytyspaikan. Mies otti salaa vaimon nimissä tämän pankkitunnuksilla sadan euron kuluttajaluoton. Mies tuomittiin petoksesta.
Kun luotto jäi maksamatta, sen myöntänyt yhtiö vaati, että vaimo on velvoitettava suorittamaan luotto yhtiölle. KKO katsoi, että vaimo menetteli huolimattomasti ja velvoitti vaimon maksamaan yhtiölle luoton.

Lähde: http://korkeinoikeus.fi/fi/index/ennakkopaatokset/precedent/1477564782152.html

"Älä ikinä anna tietojasi kalasteluviesteihin. Poista kalasteluviestit sähköpostista tai tekstiviestien joukosta avaamatta."

Älä kerro pankkitunnuksia tai luottokortin tietoja puhelimessa, jos joku soittaa ja kysyy niitä.

Poliisi varoittaa valepoliiseista

Poliisihallitus varoittaa valepoliiseista, jotka huijaavat ikäihmisiä. Poliisina esiintyvät henkilöt yrittävät huijata vanhukselta pankkikortin, tunnusluvut sekä rahaa ja arvoesineitä. Valepoliisit voivat soittaa ja tulla kotiin.
Poliisi sai vuoden 2016 ensimmäisen puoliskon aikana lähes sata ilmoitusta poliisina esiintyvistä henkilöistä. Tapauksia on ollut erityisesti pääkaupunkiseudulla, mutta myös esimerkiksi Sisä-Suomen, Itä-Suomen, Hämeen ja Oulun poliisilaitosten alueilla.
Poliisihallitus muistuttaa, että poliisi ei koskaan kysele pankkikortin tunnuslukuja tai PIN-koodeja puhelimessa tai henkilökohtaisesti. Poliisi ei lukitse matkapuhelimia, tietokoneita tai tabletteja ja vaadi maksua laitteen avaamisesta.
Poliisi ei kuoleta tai sulje pankki- tai luottokortteja. Poliisi ei myös tule kotiin kysymään, miten paljon rahaa tai arvo-omaisuutta asunnossa on.
Jos poliisi soittaa etkä ole varma, että kyseessä on oikea poliisi, soita siihen poliisilaitokseen, jossa hän sanoo työskentelevänsä. Kysy, työskenteleekö poliisi siellä. Poliisilaitosten vaihteiden yhteystiedot löytyvät poliisin verkkosivulta www.poliisi.fi.
Jos ovelle ilmaantuu henkilö, joka sanoo olevansa poliisi, pyydä häntä näyttämään virkamerkkiä.
Jos poliisipartio on ovella etkä usko heidän olevan poliiseja, soita hätäkeskukseen. Numero on 112.

Lähde: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/varo_valepoliiseja_-_poliisi_ei_kysele_pankkikortin_tunnuslukuja_puhelimitse_tai_henkilokohtaisesti_49585

Mistä tiedän, että pankkitietojani urkitaan

- Jos verkkopankissa tapahtuu jotakin outoa.
- Kun olet menossa verkkopankkiin, voi käydä niin, että sinut siirretään saman tien toiselle sivulle. Huomaat sen pienenä nykäyksenä sivulla.
- Joskus sivun päälle ilmestyy sininen rengasikoni kesken pankissa asioinnin. Ikoni kertoo, että tietokone lataa tietoa.
- Kesken asioinnin verkkopankin sivulle saattaa ilmestyä myös ns. pop up -ikkuna eli pieni ikkunaruutu. Se voi olla mainos, mutta se voi myös harhauttaa sinua siksi aikaa, kun rahaa siirretään tililtäsi. Tietokoneellesi on silloin päässyt aiemmin haittaohjelma, joka alkaa toimia, kun menet verkkopankkiin.
- Joskus haittaohjelma ei anna itsestään merkkiä. Et huomaa sitä mistään. Vasta kun katsot tilitietojasi näet että tililtä on lähtenyt rahaa laittomasti.

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.

Mitä teen, jos pankkitietojani kalastellaan:

- Älä kirjoita huijaussivuille tai -viestiin verkkopankin tunnuslukua tai salasanaa. Älä anna sinne luottokorttisi tietoja tai omaa henkilötunnustasi.
- Sulje pankin valesivu tai sähköpostissa tullut huijausviesti.
- Jos jo annoit tietoja kalastelusivuille, ota heti yhteyttä pankkiisi. Älä epäröi. Jo pelkkä epäily siitä, että tilitietojasi on päässyt ulkopuolisten käsiin, riittää yhteydenoton syyksi.

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

MAKSUKORTIT

Kun ostat palveluita tai tavaroita verkkokaupoissa, maksat niistä yleensä luottokortilla. Verkkokauppa kysyy luottokorttisi numeron, voimassaoloajan ja turvaluvun kortin kääntöpuolelta.
Maksaminen on turvallista, jos olet yhtä huolellinen kuin käyttäessäsi verkkopankkia. Varmista, että maksuyhteys on salattu ja tietokoneesi päivitykset ovat ajan tasalla (ks. luku 1). Asioi vain luotettavissa verkkokaupoissa (ks. luku 5).

Näin lisäät verkkomaksamisen turvallisuutta

- Aseta maksukortille turvarajoitukset
- Käytä maksunvälittäjiä
- Käytä turvallisen maksamisen palvelua

Aseta maksukortille turvarajat

Voit lisätä maksukorttisi turvallisuutta laittamalla kortille maksu- ja nostorajoituksia. Mene verkkopankkiisi, ja etsi sieltä kortteja koskeva valikko. Löydät sieltä kohdan, josta voit tehdä rajoitukset. Kysy omasta pankistasi millaiset turvarajoitukset sen maksukorteille voi tehdä. Joissakin pankeissa on mahdollista laittaa rajoituksia vain debit-kortille, ei luottokortille. Turvarajoitukset minimoivat vahinkoa, joka voi syntyä, jos kortti katoaa tai päätyy epärehellisen ihmisen käsiin. Rajoitukset määrittävät, miten paljon hän pystyy nostamaan ja maksamaan kortilla esimerkiksi päivän aikana tai yhdellä kertaa.
Rajoitusten tekeminen verkkopankissa on ilmaista ja nopeaa. Rajoitukset tulevat voimaan heti.
Kun ostat tai maksat jotakin isompaa, voit hetkeksi poistaa rajoitukset. Palauta ne taas matalalle tasolle maksamisen jälkeen. Voit vaihdella turvarajoituksia tarpeidesi mukaan myös esimerkiksi ulkomaanmatkan ajaksi.

Voit laittaa esimerkiksi nämä rajoitukset maksukortillesi:

Nostorajoitus	Valitse summa, jonka kortilla voi korkeintaan nostaa pankkiautomaatista: ■ yhdellä nostokerralla ■ vuorokauden aikana
Maksurajoitus:	Valitse summa, jonka kortilla voi korkeintaan maksaa ■ yhdellä maksukerralla ■ vuorokauden aikana yhteensä
Maarajoitus (geoblocking):	Määritä maa, jossa korttiasi voi käyttää, esimerkiksi vain: ■ Suomi ■ Pohjoismaat ■ Eurooppa
Internet-käytön rajoitus:	Määritä, saako luottokortillasi tehdä ostoksia internetissä vai ei.

Nordea

Turvarajat

Voit muuttaa vuorokausikohtaisia käteisnosto- ja maksurajoja omien tarpeidesi mukaan. Valitse haluamasi euromäärät vähimmäis- ja enimmäismäärien väliltä. Hyväksy muutos OK-painikkeella. Lue lisää turvarajoista ja niiden vaikutuksista korttien käyttöön ?-painikkeen alta.

Voit tehdä turvarajojen muutoksen veloituksetta.

Muuta turvarajoja

Kortti		Kortin numero	
Nordea Credit -yhdistelmäkortti		1234 5678 9123 46567	
Debit-numero		1234 5678 1234 5678	
	*	Pakollinen	
Käteisnostojen turvaraja/vrk	*	100	EUR (0
Maksujen turvaraja/vrk	*	800	EUR (0

Kortin käyttö kaupan maksupäätteillä ja automaateilla

Kortti	Käyttöalue	Tilapäinen käyttöalue
Tuohi MasterCard	Suomi ▼	Lisää poikkeus
Nordea Credit -yhdistelmäkortti	Suomi ▼	Lisää poikkeus

Kortin käyttö internetissä

Kortti	Sallittu käyttöalue	
Tuohi MasterCard	○ Internet-käyttö sallittu	◉ Internet-käyttö ei ole sallittu
Nordea Credit -yhdistelmäkortti	○ Internet-käyttö sallittu	◉ Internet-käyttö ei ole sallittu

Tältä näyttävät esimerkiksi Nordean verkkopankin sivut, joilla voit tehdä rajoitukset maksukortteihisi.

Käytä maksunvälittäjiä

Jotkut verkkokaupat tarjoavat mahdollisuutta maksaa esimerkiksi Checkoutin tai PayPalin kautta. Ne ovat maksuja välittäviä palveluja. Ne tunnistavat sekä maksajan että maksun saajan, esimerkiksi verkkokaupan. Ne varmistavat verkkokaupalle, että maksu on maksettu, mutta ne eivät anna sille luottokorttisi tietoja.

Checkout ja PayPal ovat tunnettuja maksujen välittäjiä. Kun käytät niitä, korttisi tiedot jäävät vain maksunvälittäjän haltuun. Et joudu antamaan niitä monelle eri verkkokaupalle. Se vähentää riskiä, että korttisi tiedot päätyvät rikollisille, jos käyttämääsi verkkokauppaan tehdään tietomurto.

Voit käyttää maksamiseen myös laskutuspalvelu Klarnaa, jos nettikauppa sitä vaihtoehtoa tarjoaa.

Kun käytät Klarnaa, et joudu antamaan luottokorttisi tietoja. Pääset myös näkemään tilaamasi tuotteet ennen kuin sinun pitää maksaa niistä. Se vähentää huijatuksi tulemisen riskiä.

Klarna toimii verkkokaupan ja asiakkaan välissä. Klarna hoitaa laskutuksen ja välittää maksusi verkkokaupalle.

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 oma sulkunumeronsa. Löydät ne täältä: https://www.korttiturvallisuus.fi/Apua/

Käytä turvallisen maksamisen palvelua

Turvallisen maksamisen palveluja ovat Verified by Visa ja MasterCard SecureCode. Ne ovat verkkomaksamisen turvallisuutta parantavia palveluja, jotka korttiyhtiöt Visa ja MasterCard ovat kehittäneet.

Jos verkkokaupan nettisivuilla on Verified by Visa ja MasterCard SecureCoden tunnus, verkkokauppias on liittynyt palveluun oman pankkinsa kautta.

Jos haluat käyttää palvelua, pyydä pankkiasi liittämään sinut siihen. Jotkin luottokortit käyttävät palvelua automaattisesti. Varmista pankistasi, onko oma maksukorttisi sellainen.

Osa pankeista edellyttää, että niiden asiakas käyttää turvallisen maksamisen palvelua aina, kun hän maksaa verkkokaupoissa.

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. Kuittaat ostokset verkkopankkitunnuksilla tai pankin antamalla tunnusluvulla.

Palvelu vahvistaa, että maksu onnistui. Sen jälkeen palaat verkkokauppiaan sivuille. Saat sieltä vahvistuksen tilauksesta.

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

- Soita heti pankin sulkupalveluun. Vastuusi maksukortin käytöstä päättyy siihen. Jos joku käyttää maksukorttia väärin sen jälkeen, vastuu siirtyy kortin myöntäneelle korttiyhtiölle.
- Tallenna pankkisi sulkunumero matkapuhelimeesi. Niin voit soittaa heti, kun huomaat kortin kadonneen tai kirjoitit kortin tietoja huijaussivuille.
- Jos tililtäsi katoaa rahaa, etkä ole tehnyt siirtoja itse, ilmoita siitä pankille. Pankki neuvoo, miten teet pankille oikaisupyynnön tilisi tapahtumista.
- Tee rikosilmoitus poliisille.

Voinko luottaa lähimaksuun?

Uusissa maksukorteissa on mukana mahdollisuus käyttää lähimaksua. Lähimaksuominaisuuden tunnistaa radioaaltoja kuvaavasta logosta.

Kortin lähimaksulla voit maksaa alle 25 euroa maksavan ostoksen, kun käytät korttia lukulaitteen lähellä. Korttia ei tarvitse laittaa maksupäätteeseen, etkä joudu näppäilemään tunnuslukua. Säästät aikaa ja vaivaa.

Lähimaksu lisää turvallisuutta, sillä kukaan ei pääse näkemään tunnuslukuasi.

Joudut välillä laittamaan kortin maksupäätteeseen ja antamaan tunnusluvun, vaikka käytätkin lähimaksua. Niin varmistetaan, että kortti on oikean käyttäjän hallussa.

Käytön turvallisuutta lisää myös se, että pieniä lähimaksuja ei voi tehdä rajattomasti peräkkäin. Ilman tunnusta maksettavien maksujen määrä on rajoitettu. Samoin maksujen yhteissumma tunnuslukukyselyjen välillä on rajallinen.

VINKKI

Sirukortti on turvallisempi

Sirullinen maksukortti on turvallisempi kuin pelkkä magneettijuovakortti. Sirukortin tietojen kopiointi on vaikeaa. Sen sijaan magneettijuovan tiedon voi lukea nopeasti ns. skimmauslaitteella. Rikolliset laittavat skimmauslaitteita esimerkiksi pankkiautomaatteihin.

Skimmauslaite lukee magneettikortilta tiedot ja lähettää ne tietoverkkoja pitkin rikolliselle. Rikollinen siirtää ne tyhjälle kortille ja käy nostamassa rahat jossakin päin maapalloa.

Myös sirukortin katoamisesta pitää ilmoittaa pankkiin tai sulkupalveluun. Rikollinen voi tehdä kortilla ostoksia verkkokaupoissa.

Jos rikollinen sai haltuunsa myös kortin tunnusluvun, hän voi maksaa ja nostaa sillä rahaa kuin omalla kortillaan.

Muista hyvät korttitavat

- ☑ Kun näppäilet kortin tunnusluvun, suojaa toisella kädellä.
- ☑ Säilytä kortti ja tunnusluku erillään. Opettele tunnusluku mieluiten ulkoa.
- ☑ Älä anna korttia muiden haltuun esimerkiksi ravintolassa tai liikkeessä.
- ☑ Älä jätä korttia vartioimatta esimerkiksi autoon, työhuoneeseen tai hotellihuoneeseen.
- ☑ Tarkista aina maksun summa ennen kuin hyväksyt sen.
- ☑ Seuraa tilisi tapahtumia säännöllisesti verkkopankissasi.

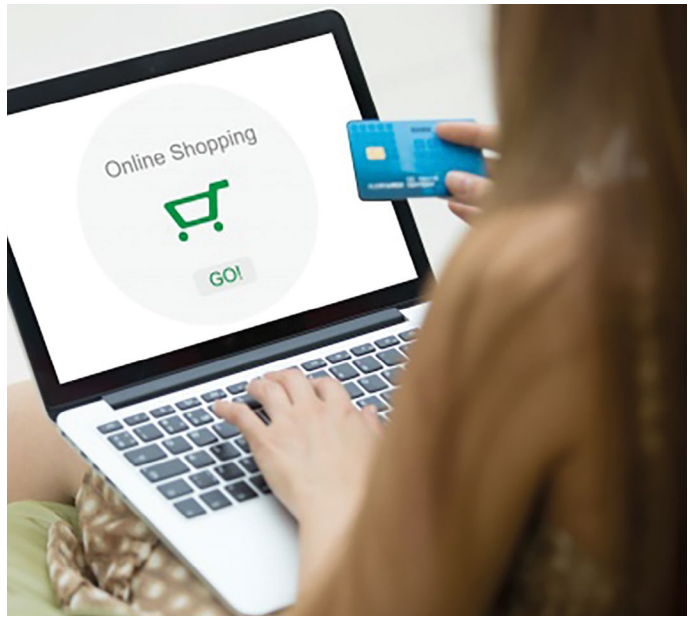
Lähde ja lisätietoja: www.korttiturvallisuus.fi

Kuva: Rodeo

5 VERKKOKAUPAT

Internetin ansiosta voit ostaa tavaraa verkkokaupoista ympäri maailmaa.

Ulottuvillasi on runsaasti kauppoja, joihin et helposti pääse fyysisessä maailmassa. Valikoima on runsaampi, voit etsiä tuotteista tietoja, vertailla niitä ja löytää parhaan hinnan. Netissä voit myös kysyä muiden kokemuksia tavarasta, jonka haluat ostaa.
Suurin osa verkkokaupoista toimii yhtä luotettavasti kuin fyysiset kaupat. Huijareita ja käärmeöljykauppiaita oli ennen internetin kauttakin. 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.



Kuva: Freepik.com

Näin arvioit verkkokauppoja:

- Tunnetut ja vakiintuneet kaupat toimivat luotettavasti myös verkkokauppoina. Poliisin mukaan etenkin pienten piirin erikoiskauppojen kanssa voi tulla ongelmia.
- Sivujen ulkonäkö ei kerro, voitko luottaa verkkokauppaan. Myös huijareiden verkkokaupat voivat olla hienot, isolla rahalla tehdyt ja luotettavan näköiset. Niiden kielikin on usein jo hyvää. Aiemmin epärehellisten verkkokauppojen tekstit olivat usein huonoa suomea, ja ne oli tehty käännöskoneilla.
- Verkkokaupan nettiosoite ei kerro, missä maassa kauppa toimii. Esimerkiksi .fi-tunnus ei enää takaa, että verkkokauppa on suomalainen. Tunnuksen omistaja voi toimia missä päin maailmaan tahansa.
- Kuluttajaviranomaisten hyväksymää logoa tai sertifikaattia, joka takaa verkkokaupan rehellisyysen, ei ole. Suomessa Verkkoteollisuudella on Luotettavaa toimintaa -laatumerkki. Se kertoo, että liiton jäsenet sitoutuvat toimimaan luotettavasti. Liittoon kuuluu verkkokauppoja omistavia yrityksiä.
- Verkkokauppoja edustavalla Ecommerce Europella on oma eurooppalaisen verkkokaupan laatumerkki. Se haluaa lisätä rajat ylittävän verkkokaupan luotettavuutta ja luottamusta sitä kohtaan.

Ennen kuin ostat, tee nämä:

- Lue muiden antama palaute. Kirjoita selaimen hakuriville verkkokaupan nimi ja sana kokemuksia. Esimerkiksi: Huivikauppa kokemuksia. Jos verkkokauppa toimii ulkomailla, kirjoita englanniksi verkkokaupan nimi ja problems, esimerkiksi Yours problems.
  Katso, millaisia kommentteja verkkokaupasta on annettu. Ovatko ne pääosin myönteisiä vai kielteisiä? Mistä muut ostajat valittavat? Jos kielteisiä kommentteja on paljon, harkitse, kannattako kaupasta tilata.
- Tutki, miten avoimesti verkkokauppa toimii. Tarkasta, kertooko verkkokauppa yhteystiedot ja tiedot peruutusoikeudesta. Tarkasta, mitä tietoja verkkokauppa antaa itsestään. Kertooko se avoimesti yhteystietonsa eli osoitteen, sähköpostiosoitteen ja asiakaspalvelun tiedot. Jos verkkokaupalla on puhelinnumero, se pitää kertoa.
  Katso, kertooko verkkokauppaa oikeudestasi peruuttaa tilaus ja neuvoo, miten se tehdään.
  Jos tietoja ei ole tai ne on piilotettu ja niitä on vaikea löytää, tuotteen palauttaminen tai tilauksen peruminen voi olla vaikeaa.
- Maksutavat. Varmista, että voit ostaa luottokortilla. Jos tavara ei tulekaan tai siinä on vikaa, voit vaatia hyvitystä luottokorttiyhtiöltä.
- Jos epäröit ostaa verkkokaupasta, älä osta.

EU:ssa on samat säännöt verkkokaupalla

Ei ole samantekevää, missä päin maailmaa toimivasta verkkokaupasta tilaat tavaraa. EU:ssa kaikilla jäsenmailla on samat säännöt ja asetukset, jotka koskevat verkkokauppaa.

Verkkokauppa on etämyyntiä, jossa ostajalla on 14 päivää aikaa peruuttaa ostos. Sinulla on se oikeus, kun ostat EU-maassa toimivasta verkkokaupasta. Jos tuotteella ei ole palautusoikeutta, se pitää kertoa.

Jos joudut ongelmiin suomalaisen verkkokaupan kanssa, saat apua kuluttajaneuvonnasta. EU:ssa kuluttajien ja verkkokauppojen riitoja sovittelee Euroopan kuluttajakeskus EKK. Siihen kuuluvat myös EU:n ulkopuoliset Islanti ja Norja. EKK auttaa, jos joudut pulaan EU:ssa, Islannissa tai Norjassa toimivan verkkokaupan kanssa.

Jos ostat verkkokaupasta EU:n ulkopuolelta ja kohtaat ongelmia, voit pyytää apua kuluttajaneuvonnasta. On hyvä kuitenkin tietää, että EU:n ulkopuolisia verkkokauppoja ja -yrityksiä voi olla vaikea saada vastuuseen tai aina edes vastaamaan yhteydenottoihin. Laki suojaa kuluttajan oikeuksia esimerkiksi Aasiassa eri lailla kuin EU:ssa.

Lisäksi kaikki EU:n ulkopuolelta tilatut tavarat eivät välttämättä ole yhtä turvallisia kuin EU:ssa valmistetut.

Lisätietoja verkkokaupoista ja kuluttajan oikeuksista saat Kilpailu- ja kuluttajaviraston nettisivulta:

www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/verkkokauppa-posti-ja-puhelinmyynti-etamyynti/

www.kkv.fi/ratkaisut-ja-julkaisut/julkaisut/kuluttaja-asiamiehen-linjaukset/aihekohtaiset/verkkokauppa-ja-muu-etamyynti/

Kun tilaat verkkokaupasta, et aina voi olla varma, että paketissa on oikea tuote. Tuotteen vaihto tai palautus voi joskus olla vaikeaa. Tutustu palautusehtoihin ennen tilaamista.

Kun Ville myy ja Kalle ostaa

Internetin kautta voit ostaa tavaroita myös muilta ihmisiltä, et vain yrityksiltä. Suuria myyntikanavia ovat esimerkiksi Huuto.net ja Tori.fi.

Tavaroita liikkuu yksityisten ostajien ja myyjien välillä myös Facebookin kierrätysryhmien ja kirpputorien kautta. Myös muun muassa käytettyjen autojen ja veneiden kauppiaat ja ostajat kohtaavat netissä omilla sivuillaan.

Netissä toimivat kierrätysryhmät ja käytettyjen tavaroiden kaupat edistävät kierrätystä ja pidentävät tavaroiden käyttöikää. Sitä kautta ne vähentävät jätekuormaa ja säästävät energiaa ja ympäristöä.

On hyvä kuitenkin muistaa, että kuluttajansuoja ei koske yksityisten henkilöiden välistä kauppaa. Se tuo turvaa vain, kun ostat yrityksestä.

Kun ostat yksityiseltä myyjältä, et voi pyytää apua kuluttajaviranomaisilta, jos kaupassa tulee ongelmia. Niiden toimivalta ei ulotu yksityishenkilöiden väliseen kauppaan.

Netin kautta tavoitat ostajia ja myyjiä, läheltä ja kaukaa. Se parantaa valinnan varaa. Nettikaupan haittapuoli on, ettet aina pysty tutkimaan tuotetta, jonka haluat ostaa. Olet kuvien ja myyjän kuvauksen varassa.

Yleensä myyjä haluaa tuotteesta maksun ennen kuin hän lähettää tuotteen ostajalle. Ostaja ottaa riskin, ettei tuote ehkä tulekaan tai kun menet hakemaan sitä, sitä ei ole olemassa.

10 000 euron vene olikin huijaus

Kajaanilainen mies löysi internetistä nettivene.com-sivulta kiinnostavan ilmoituksen moottoriveneestä. Hän teki kaupat ja maksoi veneestä 10 500 euroa myyjän pankkitilille.

Kun mies ajoi hakemaan venettä Leppävirralta, kävi ilmi, ettei venettä olekaan. Veneen myynti-ilmoitus oli huijaus. Poliisitutkinnassa kävi ilmi, että kajaanilaismies oli maksanut veneen hinnan 57-vuotiaan joensuulaismiehen tilille. Myös huijauksessa käytetty puhelinnumero kuului hänelle.

Mies väitti, että tuntematon mieskolmikko maksoi hänelle 500 euroa ja 12 tölkkiä olutta vastineeksi siitä, että hän antoi huijareiden käyttöön nimensä, tilinsä ja puhelinnumeronsa. Huijarit katosivat veneestä maksetut rahat taskuissaan. Heitä avustanut mies sai neljän kuukauden ehdollisen vankeustuomion.

Lähde: Karjalainen 14.9.2016

Tee näin, kun ostat yksityiseltä myyjältä

- **Tutki myyjän saama palaute**
  Tutki, mitä muut ostajat ovat sanoneet myyjästä. Kauppapaikoilla (esimerkiksi Huuto.net, Tori.fi) voit lukea palautteita, joita kauppakumppanit ovat antaneet toisilleen. Kauppapaikkojen ylläpitäjät poistavat epärehellisiksi osoittautuneita myyjiä ja ostajia palveluistaan. Samoin Facebookin kirpputoreilla ja kierrätysryhmissä on valvojat, joilta voi kysyä, onko jostakusta myyjästä tai ostajasta valitettu. Epärehelliset jäsenet poistetaan niistä nopeasti.

- **Maksa luottokortilla**
  Maksa käteisellä tai tilisiirrolla vain pienet summat. Karta myyjiä, jotka vaativat vain käteistä, varsinkin, jos tavara on kallis. Maksa luottokortilla aina kuin voit. Jos myyjä onkin epärehellinen, voit saada rahat takaisin, jos hyvin käy.
  Poliisin on vaikea ja työläs selvittää nettikauppaan liittyviä petoksia etenkin, jos epärehellinen myyjä on ulkomailla. Luultavaa on, että menetät rahat, jos maksoit ostoksesta huijarille ulkomaille.

- **Käytä postiennakkoa**
  Kun käytät postiennakkoa, saat nähdä tavaran postissa ennen kuin maksat siitä. Voit avata paketin ja tarkistaa päällisin puolin, että paketissa on ostamasi tavara ja se on luvatussa kunnossa.

- **Pyydä uusi kuva**
  Pyydä, että myyjä kirjoittaa lapulle haluamasi sanan ja ottaa tuotteesta kuvan lapun kanssa. Näin varmistut, että myyjällä on todella tavara, jonka aiot ostaa. Myynti-ilmoituksen kuva voi olla napattu internetistä.

- **Tutki ensin, maksa sitten**
  Älä maksa kallista tavaraa näkemättä sitä. Maksa vasta, kun menet hakemaan ostajalta tavaran, esimerkiksi auton. Voit maksaa paikan päällä esimerkiksi pankin konttorissa tai verkkopankissa, jolloin myös myyjä varmistuu, että olet maksanut.
  Älä tartu liian houkuttelevaan myynti-ilmoitukseen. Mieti hetki, miksi myyjä myy kaupoissa 900 euroa maksavan uuden matkapuhelimen 300 eurolla. Myyjä saattaa myydä varastettua tai olematonta puhelinta.

Ostaja ei saanut PlayStation-pelejään.

Osasto: **Pelikonsolit ja pelaaminen** Pelikonsoli: **Playstation 4** Laske hinta kuljetuk
Sijainti: **Uusimaa - Hanko, Hanko Pohjoinen**
Hinta: **25 €**

Myydään 3kpl Hyvässä Kunnossa Olevia ps4 Pelejä
Pelit: Fallout 4, Call Of Duty Black Ops 3, Final Fantasy
Myyn Kaikki Pelit Pakettina Yhteydenotot Sähköpostitse: [redacted]@gmail.com
Pelit Voi Noutaa Hangosta Tai Voin Postittaa Pelit

Sponsoroitu:
Bonusta elektroniikasta ja muista verkko-ostoksistasi. Lunasta 10 € lisäetusi. Bonusway

Näin huijaus eteni:

15. syyskuuta 2016 klo 16.28 Salla
<tori@tori.fi> kirjoitti:
Moi! Haluaisin ostaa noi pelit :) Saisiko ne postitettuna Vantaalle?
T. Salla

Viestin lähettäjän puhelinnumero: +35850•••••••
Viestin lähettäjän sähköpostiosoite: •••••••@hotmail.com
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
Yllä oleva viesti lähetettiin Tori.fi:n verkkosivujen kautta, ilmoituskaavaketta käyttäen.

Ilmoitus: ”Playstation 4 Pelejä”.
Näet ilmoituksen täältä: http://www.tori.fi/vi/30284288.htm
Henkilö joka on ottanut sinuun yhteyttä ei tiedä sähköpostiosoitettasi kunnes vastaat tähän sähköpostiin. Palvelumme ei voi vastata, että lähettäjän sähköpostiosoite (•••••••@hotmail.com) on oikea.

Ystävällisin terveisin

Tori.fi

Lähettäjä: Jari [redacted] <[redacted]@gmail.com>
Lähetetty: 15. syyskuuta 2016 16:29
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
Moikka Salla Postitus Vantaalle Onnistuu

Lähettäjä: Jari [redacted] <[redacted]@gmail.com
Lähetetty: 15. syyskuuta 2016 16:59
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
25e On Hinta Ja Laitan Pelit Heti Postiin Kun Maksusuoritus Näkyy Tililläni

15. syyskuuta 2016 klo 16.33 Salla <•••••••@hotmail.com> kirjoitti:
Hienoa! Ja hinta oli sen 25 €? Milloin ehdit laittaa postiin?
Postitus osoitteeseen:
Salla
•••••••••••••• 1 E 40
••••• Vantaa

15. syyskuuta 2016 klo 19.46 Salla <•••••••@hotmail.com> kirjoitti:
Saisinko tilinumeron, niin voin maksaa?

Lähettäjä: Jari <[redacted]@gmail.com>
Lähetetty: 15. syyskuuta 2016 20:01
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
Moi FI •••••••••••••••• Osuuspankki Bic: OKOYFIHH
Laita Mulle Osoitteesi Minne Postitan Pelit Heti Kun Maksu Näkyy Tililläni Laitan Pelit Postiin

---

16.9.2016 14.54 Salla <•••••••@hotmail.com> kirjoitti:
Hei! Maksoin pelit nyt. Minulla on Nordea pankkina, joten voi mennä pari pv maksun näkymiseen.

22.9.2016 15.49 Salla <•••••••@hotmail.com> kirjoitti:
Moi. Laitoitko jo postiin pelit?

Lähettäjä: Salla <•••••••@hotmail.com>
Lähetetty: 8. lokakuuta 2016 15:39
Vastaanottaja: Jari ••••
Aihe: Re: VS: Aihe: Playstation 4 Pelejä
Terve
Pelit alkaa olla jo sen verran myöhässä että pikkuhiljaa voisit vastata. Mikäli et vastaa tähän viestiin ensi viikon tiistaihin mennessä, teen poliisille rikosilmoituksen.
Salla

Mies myi netissä pelejä ja halusi maksun pankkitililleen. Ostaja ei ikinä saanut pelejä. Hänen olisi kannattanut pyytää, että myyjä lähettää pelit postiennakolla. Ennen maksamista paketin voi avata ja varmistaa, että siellä on sovitut tuotteet.
Jos myyjä ei halua käyttää postiennakkoa, kannattaa miettiä, aikooko hän alun perinkään lähettää myymiään tavaroita.

”Maalaisjärki ja epäilevä mieli auttavat pitkälle verkossa.”

Tero Muurman
Rikoskomisario
Keskusrikospoliisi
Kyberkeskus

”Jos tarjous on liian hyvä ollakseen totta, se ei ole totta.”

Tiesitkö, että voit joutua lain edessä vastuuseen, jos ostat varastettua tavaraa.

TILAUSANSAT

Tilasitko netistä omegaöljykapseleiden näytepakkauksen ilmaiseksi tai pikkurahalla? Pakkaus tulee, mutta sen jälkeen alkaa tulla lisää kapseleita ja laskuja. Menit tilausansaan.

Tilausansa tarkoittaa sitä, että tilasit mainoksen tai viestin pohjalta jotakin, mitä et tiennyt tai ymmärtänyt tilaavasi. Sitouduit kalliimpaan tai pidempään tilaukseen kuin tarkoituksesi oli. Tilausehtoihin ns. pikkuprintissä olikin kohta, jota et huomannut lukea. Siinä sanotaan, että tarjouksen tilaaminen johtaa kestotilaukseen tai määräaikaiseen tilaukseen, jos et peru tilausta määrätyssä ajassa.

Tyypillisesti tilausansoissa tarjotaan ilmaiseksi tai kokeilujaksoina laihdutuspillereitä, vitamiineja, öljykapseleita, unen saamista edistäviä tuotteita, alusvaatteita, kosmetiikkaa ja deittipalveluja.

Samat ja samanlaiset tilausansat kiertävät usein verkossa eri maissa ympäri Eurooppaa, vain kieli ja tuotenimi vaihtuvat. Saatat joutua ansaan myös osallistumalla harmittomaan tai hyödyllisen tuntuiseen kilpailuun, kyselyyn tai kuluttajatutkimukseen.

Tilausansoihin törmäät usein Facebookissa tai muualla netissä olevasta mainoksesta. Tilausansoja ropsahtaa myös sähköpostiisi. Voit myös saada esimerkiksi Facebookissa ystäväsi nimissä lähetetyn suosituksen jostakin tuotteesta. Luotat siihen, koska lähettäjä on tuttavasi. Tosiasiassa suosituksen lähettäjä on huijari, joka käyttää hyväksi tuttavuuttanne.

Näin tunnistat tilausansat:

Tilausansoihin voivat viitata esimerkiksi alla olevat mainoslauseet. Ne on poimittu todellisista tilausansaviesteistä:

- Vastaa nyt ja saat älypuhelimen pelkillä toimituskuluilla!
- Kokeile veloituksetta!
- Näytepakkaus vain postikulujen hinnalla!
- iPhone 4 nyt vain 3 €!
- Saat HD-videokameran, vain 10 euroa!
- Saat jäsenyyden ja lahjan vain yhdellä eurolla!
- Kerro mitä mieltä olet ja saat tennarit!
- Onnea, olet voittanut!

Lähde: Kilpailu- ja kuluttajavirasto

Tilausansoissa tarjotaan ilmaiseksi tai kokeilujaksoina tyypillisesti laihdutuspillereitä, D-vitamiinipillereitä ja Omega3-öljykapseleita.

Mitä teen, jos menin tilausansaan?

- Palauta tuote. Pelkkä tuotteen palauttaminen ei kuitenkaan merkitse sitä, että peruutat tilauksen tai että et mielestäsi ole tehnyt tilausta lainkaan.
- Tee tilauksesta ja laskusta reklamaatio eli valitus yritykselle. Perustele, miksi lasku on aiheeton.
- Tarkista, onko sinulla velvollisuus maksaa lasku (http://www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/huijaukset/lasku-ilman-tilausta-ilmaiset-naytepakkaukset/tarkista-velvollisuutesi-maksaa-lasku/). Aiheeton maksaminen innostaa huijaria jatkamaan tilausansojen tekemistä, sillä ne tuottavat sille rahaa.
- Jos saat laskun perintätoimistolta, tee valitus myös sinne. Kerro, miksi lasku on perusteeton. Älä maksa laskua, vaikka perintätoimisto uhkaa oikeudella ja luottotietojen menettämisellä. Huijari toivoo, että pelottelu saa epävarman tilaajan maksamaan laskun.
- Jos asia ei selviä, pyydä apua kuluttajaneuvonnasta.

Kun asiakaspalvelu ei toimi, tilaus ei aina sido ostajaa

Tilausansat ovat yleistyneet viime vuosina. Ne kuormittavat kuluttajaneuvontaa ja ahdistavat ansaan joutuneita.
Kuluttaja-asiamies onkin hakenut hovioikeudelta linjauksia tyypillisiin ongelmiin, joita verkkokaupassa tulee eteen.
Yksi ennakkopäätös koski tilannetta, jossa ostaja ei saanut yhteyttä myyjäyrityksen asiakaspalveluun. Myyjäyritys ilmoitti vain asiakaspalvelun puhelinnumeron. Asiakas soitti siihen useasti, mutta numero ei vastannut. Ostaja ei siksi voinut perua tilausta. Koska asiakaspalvelu ei toiminut, hovioikeus linjasi, että tilaussopimus ei sitonut ostajaa.
Toinen päätös koski sitä, tilasiko asiakas pelkän näytepakkauksen vai enemmän. Oikeuden mukaan ostaja joutuu maksamaan vain näytepakkauksesta.

Kilpailu- ja kuluttajaviraston ohjeet tilausansaan joutuneelle:

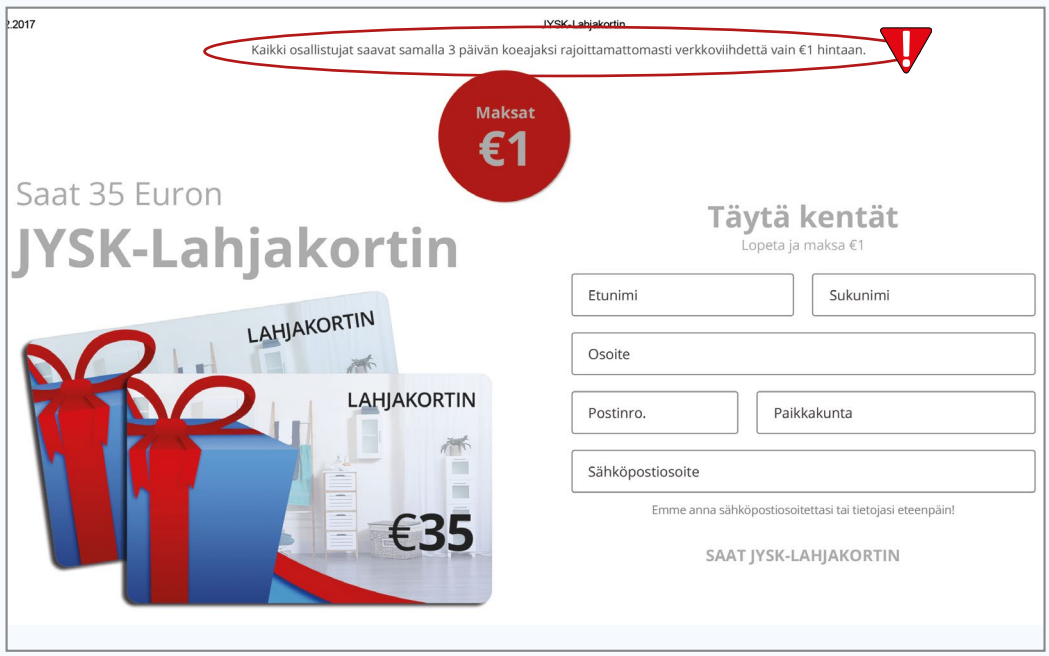
www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/huijaukset/lasku-ilman-tilausta-ilmaiset-naytepakkaukset/

"Voit joutua ansaan myös, kun osallistut harmittomaan tai hyödyllisen tuntuiseen kilpailuun, kyselyyn tai kuluttajatutkimukseen."

Jyskin lahjakortti paljastui tilausansaksi

Vuoden 2017 alussa somessa levisi tieto, että huonekaluliike Jysk myy 35 euron lahjakortteja 1 eurolla. Ja mikä parasta, lahjakortteja saattoi ostaa miten paljon vain. Kampanjan tueksi oli tehty Iltasanomien nettisivua muistuttava valesivu.

Se kertoi, että Jysk yrittää välttää konkurssin jakamalla lahjakortteja. Valesivulta linkki johti varsinaisille lahjakorttien kampanjasivuille. Siellä kävi ilmi, ettei lahjakortteja saakaan noin vain. Kävijän pitää osallistua arvontaan, jossa voi voittaa lahjakortin. Pieni, vaalea teksti ilmoitti, että lahjakortin arvontaan osallistuva osallistuu automaattisesti ”verkkoviihteen kokeilujaksoon”.



Sen jälkeen osallistujan luottokortilta veloitetaan automaattisesti 90 euron (joissakin versioissa 88 tai 69 euroa) kuukausimaksuja. Lahjakortti osoittautuikin luottokorttitietojen kalastaluksi ja tilausansaksi. Asiakkaalle ei edes kerrottu, mitä verkkoviihdettä hän alkaa saada.

6 ÄLYPUHELIMET JA TABLETIT

Internetyhteydellä varustettu älypuhelin ei ole enää vain puhelin. Se on mukana kulkeva pieni tietokone, jossa on paljon henkilökohtaisia tietoja.
Sillä pidetään yhteyttä monella tavalla, siihen tallennetaan tietoa ja sen kautta tehdään ostoksia ja maksetaan laskuja.
Älypuhelimeen liitttyy myös tietoturvariskejä. Puhelin on yhteydessä moniin verkkoihin myös tietämättäsi. Se tekee päivityksiä ja muun muassa seuraa, missä liikut.
Älypuhelimiin tulee nykyään entistä enemmän myös haittaohjelmia ja huijausviestejä.
Suojaudut riskeiltä, kun pidät huolta puhelimen tietoturvasta, suojaat itse laitteen sekä käytät puhelinta fiksusti.

Suojaa älypuhelimesi näin:

- Vaihda liittymän SIM-kortin tunnusluku
- Ota käyttöön puhelimen automaattinen lukitus
- Suojaa puhelin suojakoodin, salasanan tai kuviolukon avulla
- Ota varmuuskopiot
- Käytä varkaudenhallintajärjestelmää
- Suojaa puhelimesi haittaohjelmilta

Vaihda liittymän SIM-kortin tunnusluku

Kun hankit puhelinliittymän, vaihda puhelimessa saman tien sen SIM-kortin tunnusluku. Älä käytä oletustunnuslukua, esimerkiksi 0000 tai 1234. Luvaton käyttäjä kokeilee niitä ensiksi.
PIN-koodin ei tarvitse olla neljä numeroa. Se voi olla selvästi pidempi numerosarja, joka on myös vaikeampi arvata.

Kuva: Rodeo

Ota käyttöön näytön automaattinen lukitus

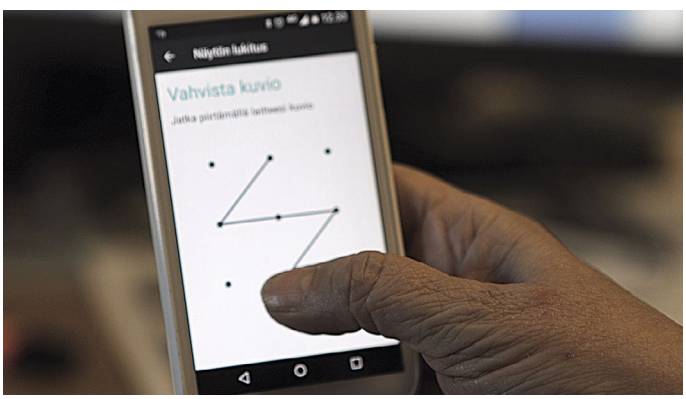
Lukitus estää puhelinta soittamasta vahingossa taskun tai laukun pohjalta. Se estää ulkopuolisia käyttämästä puhelinta, jos se varastetaan tai se katoaa. Laita lukitukselle järkevä viiveraja oman puhelimen käytön mukaan.

Suojaa puhelin suojakoodin, salasanan tai kuviolukon avulla

Niiden avulla suojaat puhelintasi luvattomalta käytöltä (SIM-kortin PIN-koodi suojaa liittymää, ei laitetta). Kuviolukkoa, numerojonosta koostuvaa koodia ja kirjoitettavaa salasanaa tarvitset myös, kun käytät puhelimen etähallintaa.

Kuviolukolla, suojakoodilla tai salasanalla voi lukita laitteesi. Saat laitteen käyttöösi, kun annat sille koodin tai salasanan. Älä käytä yleisiä suojakoodeja, esimerkiksi 00000 tai 12345. Katso sivulta 12, miten teet vahvan salasanan.

Älä unohda salasanaa, koodia tai kuviolukkoa. Jos tunnus unohtuu, kysy apua laitteen valmistajalta tai myyjältä.



Ota varmuuskopio

Ota varmuuskopiot osoitekirjastasi, muistiinpanostasi ja valokuvistasi. Näin ne ovat tallessa, vaikka puhelin katoaa tai rikkoontuu.

Voit tehdä varmuuskopion puhelimen muistikortille, tietokoneelle tai pilvipalveluun. Älä tee varmuuskopiota puhelimen muistikortille, jos sitä ei ole salattu tai suojattu. Muistikortti on helppo irrottaa puhelimesta. Sen tiedot voidaan lukea toisella puhelimella tai tietokoneella.

Helpointa on laittaa puhelin tekemään varmuuskopiot automaattisesti. Se on mahdollista useimmissa puhelimissa. Ota palvelu käyttöön puhelimen asetukset-osiosta.

Puhelimessa voi olla jo valmiina sovellus, joka ottaa automaattisesti varmuuskopiot. Kopiot tallentuvat laitteen tai käyttöjärjestelmän valmistajan palvelimelle.

Voit myös ladata puhelimeen sovelluksen, joka ottaa varmuuskopiot. Sovelluksen voit ladata laitteen tai käyttöjärjestelmän valmistajan sovelluskaupasta (store). Pilvipalvelusovelluksia ovat esimerkiksi Microsoftin OneDrive, Applen iTunes ja Googlen Android-puhelimien Google+. Dropbox-sovellusta voit käyttää useimmilla puhelimilla.

Lue lisää varmuuskopioinnista sivulta 17.

Käytä varkaudenhallinta-järjestelmää

Varkaudenhallintajärjestelmän avulla voit hallita puhelinta etänä, jos se on kadonnut tai varastettu. Voit lukita kadonneen puhelimen, jäljittää sen sijainnin ja tyhjentää sen kaikki tiedot. Varkaudenhallinnan avulla estät ulkopuolista käyttämästä puhelimen ohjelmia, esimerkiksi kalenteria.

Voit käyttää puhelimen ja käyttöjärjestelmän omaa varkaudenhallintajärjestelmää tai ostaa sen jonkun ison, luotettavan yrityksen sovelluskaupasta. Voit katsoa tietoturvayritysten sivuilta, mihin sovelluskauppaan ne ohjaavat.

Applen iPhonen etähallintasovellus on Find my iPhone. Android-puhelimilla on Android Device Maganer ja Windows Phone -puhelimilla My Window Phone.

Voit käyttää myös ilmaisia sovelluksia. Maksulliset sovellukset ovat edullisia, ja niissä on enemmän toimintoja. Ne voivat esimerkiksi ottaa valokuvan puhelinvarkaasta.

Lataa varkaudenhallintasovellus puhelimeen. Rekisteröidy sen käyttäjäksi. Jos puhelin katoaa, mene internetissä sovelluksen sivuille. Kirjaudu sisään tekemilläsi tunnuksilla, ja ota puhelimesi hallintaasi etänä.

Harjoittele varkaudenhallintaohjelman käyttöä muutaman kerran. Niin osaa toimia, kun puhelin katoaa.

Suojaa puhelin haittaohjelmilta

Älypuhelimissa liikkuu entistä enemmän samanlaisia haittaohjelmia kuin tietokoneissa (ks. luku 3). Suojaa oma puhelin samalla lailla kuin tietokone.
Pidä puhelimen käyttöjärjestelmä ja muut ohjelmat päivitettyinä. Lataa puhelimeen sovelluksia vain puhelimen omasta sovelluskaupasta.
Harkitse myös virusturvan ja palomuurin hankkimista puhelimeesi. Voit ostaa niitä tietoturvayhtiöiltä. Puhelimiin on saatavana myös ilmaisia tietoturvaohjelmia.
Etenkin Android-puhelimiin kannattaa hankkia virusturva.

Käytä älypuhelinta fiksusti

Lainaa puhelintasi vain henkilölle, johon luotat. Epärehellinen käyttäjä voi nopeasti jakaa eteenpäin puhelimeen tallennettuja tietoja tai esimerkiksi soittaa kalliiseen, maksulliseen numeroon.
Epärehellinen käyttäjä voi myös aloittaa ryhmäpuhelun. Hän soittaa kaverille, joka liittää puheluun useita muita puhelimia. Vaikka puhelimen lainaaja lopettaa puhelunsa, muut voivat jatkaa puhumista kauan. Lasku tulee sille, jonka puhelin aloitti ryhmäpuhelun, eli sinulle.
Jos haluat auttaa puhelinta tarvitsevaa, kysy mihin numeroon hän haluaa soittaa. Näpyttele numero puhelimeen itse ja ojenna puhelin lainaajalle sen jälkeen.
Älä soita takaisin tuntemattomiin numeroihin. Puhelu voi ohjautua kalliiseen, maksulliseen palvelunumeroon. Varo etenkin tuntemattomia, ulkomaalaisia numeroita.
Tunnista huijaukset. Saat niitä tekstiviestillä tai viestipalveluiden (WhatsApp, Viber) kautta. Sinua voidaan esimerkiksi houkutella valesivuille. Siellä pyydetään antamaan henkilökohtaisia tietoja. Sinua voidaan myös pyytää soittamaan maksulliseen puhelinnumeroon tai liittymään kalliiseen palveluun. Poista viestit.
Älä piilota salasanoja ja tunnuksia matkapuhelimen muistioon, kalenteriin tai osoitetietojen sekaan. Jos joku löytää puhelimesi, hän osaa etsiä tunnuksia niistä. Käytä salasanaohjelmaa, ks. s. 13. Lataa älypuhelimelle sopiva salasanaohjelma ison yrityksen sovelluskaupasta.

Haittaohjelma saa puhelimen temppuilemaan

Epäile haittaohjelmaa, jos puhelimesi alkaa käyttäytyä oudosti:

- Puhelimen käyttö hidastuu, eikä uudelleen käynnistäminen auta.
- Puhelimen käyttöjärjestelmä kaatuu tai pysähtelee.
- Akku alkaa yhtäkkiä kulua entistä nopeammin.
- Puhelimelta lähtee runsaasti verkkoliikennettä ilman että olet itse muuttanut verkkokäyttäytymistäsi. Voit tarkistaa verkkoliikenteen määrän hallinta-asetuksista.
- Saat ylimääräisiä mainoksia tai ohjaudut väärille sivuille netissä.
- Saat paljon roskapostia.
- Tuttavasi kertovat, että he saavat sinulta tekstiviestejä, joita et ole lähettänyt.

Miten pääsen eroon haittaohjelmasta:

- Laita virusturvaohjelma tarkastamaan puhelin.
- Palauta tehdasasetukset.
- Asenna käyttöjärjestelmä uudelleen.
- Vie puhelin ammattilaisen puhdistettavaksi.

Mitä teen, kun luovun älypuhelimesta

- Tyhjennä puhelimen muisti.
- Jos puhelimessa on muistikortti, poista se ennen kuin kierrätät tai myyt puhelimen.
- Palauta matkapuhelimen tehdasasetukset.
- Poista pilvipalvelussa käytetty puhelin pilvipalvelun laitelistalta.

Mitä teen, kun ostan vanhan puhelimen

- Palauta tehdasasetukset.
- Tarkasta puhelimen asetuksista, onko puhelin liitetty pilvipalveluun, jota entinen omistaja käytti. Poista puhelin sieltä. Muuten tietosi saattavat päätyä puhelimen entiselle omistajalle.

Tutustu oman puhelimen asetuksiin

- Kun ostat uuden puhelimen, lue käyttöopas ja tutustu, mitä asetuksia voit tehdä puhelimeesi.
- Asetukset-osion kautta voit tehdä tärkeimmät puhelimen ja internetin turvalliseen käyttöön liittyvät asiat, jotka tässä oppaassa on neuvottu.

Näin käytät älypuhelinta ulkomailla

Kun matkustat älypuhelin mukana, kiinnitä huomiota siihen, miten paljon dataa puhelin siirtää.

Ulkomailla käytät paikallisen operaattorin verkkoa. Hinnat voivat olla paljon kalliimmat kuin Suomessa. Nyrkkisääntö on, että mitä eksoottisempi maa, sitä kalliimpaa verkon käyttö on.

Vaikka et käyttäisi matkalla verkkoa mihinkään, laskua voi kertyä satoja tai jopa tuhansia euroja. Älypuhelin päivittää käyttöjärjestelmää ja muita ohjelmia huomaamattasi paikallisessa verkossa. Varsinkin karttapalvelujen toiminta vaatii paljon verkkoliikennettä.

Lisäksi maksat siitä, mihin käytät puhelimen älytoimintoja. Etenkin videoiden katsominen ja verkossa pelaaminen voivat tulla kalliiksi ulkomaan matkan aikana.

On hyvä muistaa, että rajaton datan käyttöoikeus pätee usein vain Suomessa. EU-maissa voit käyttää älypuhelimen nettiä kohtuullisesti ilman lisämaksua kesästä 2017 lähtien. Muualla maksat yleensä erikseen kaikesta netin käytöstä.

Tee näin ennen matkaa ja matkalla:

- Tarkasta puhelinoperaattoriltasi, paljonko maksat puheluista kohdemaassa. Käytä puhelinta sen mukaan.
- Laita älypuhelimesta mobiilidata pois päältä, kun lähdet matkalle. Voit tehdä sen puhelimen asetukset-osiosta. Datasiirto on yleensä helppo laittaa päälle ja ottaa pois päältä.
- Kirjaudu hotellin, kahvilan, lentokentän ja muiden vastaavien paikkojen ilmaiseen langattomaan WLAN-verkkoon. Anna puhelimen tehdä tärkeät päivitykset ja muut datansiirrot siellä. Kun käytät ilmaista verkkoa, puhelinliittymääsi ei kerry laskua.
- Sovi lasten kanssa, milloin ja missä he voivat älypuhelimellaan pelata tai katsoa videoita.

VINKKI

Älypuhelin ei ole ikuinen. Jossakin vaiheessa puhelimen käyttöjärjestelmä tulee elinkaarensa päähän. Silloin puhelimeen ei enää tehdä päivityksiä eikä tietoturvan aukkoja korjata. Puhelimesta tulee turvaton käyttää. Viimeistään silloin kannattaa hankkia uusia puhelin.

Jos älypuhelin katoaa, tee näin:

- Soita kadonneeseen puhelimeen toisella puhelimella. Puhelimeen voi vastata rehellinen henkilö, jolta voit noutaa laitteesi. Useisiin puhelimiin voi vastata, vaikka laite olisi lukittu suojakoodilla tai salasanalla.
- Tee soitonsiirto. Pyydä operaattoriasi ohjaamaan liittymääsi tulevat puhelut varapuhelimeen, jota voit käyttää. Näin voit vastata sinulle tuleviin puheluihin.
  Voit siirtää puhelut varaliittymään itsekin. Kirjaudu operaattorisi sivuille, joilla asiakkaat voivat itse hallita liittymiään. Etsi kohta, jossa voit tehdä siirrot.
  Voit yleensä siirtää varapuhelimeen myös tekstiviestit.
- Jos olet ladannut puhelimeen varkaudenhallintaohjelman, käytä sitä.
- Pyydä operaattoriasi sulkemaan puhelin väliaikaisesti. Tee niin, jos epäilet, että joku voi soittaa sillä tai ulkopuolinen voi nähdä puhelimesta luottamuksellista tietoa. Niin voi käydä, jos puhelin katoaa esimerkiksi työmatkalla, lomamatkalla tai kauppareissulla. Jos puhelin katoaa kotona tai muualla, jossa ei ole ulkopuolisia, voit yrittää etsiä puhelimen.
  Kun operaattori sulkee liittymäsi, kukaan ulkopuolinen ei voi sitä käyttää. Saat liittymän taas käyttöösi asiakaspalvelun kautta. Olet vastuussa liittymän väärinkäytöstä siihen asti, kun ilmoitat katoamisesta operaattorille.
  Huomaa, että jos puhelinliittymä suljetaan, et pysty käyttämään varkaudenhallintajärjestelmää etänä.
- Ilmoita poliisille puhelimesi IMEI-koodi. Se on sarjanumero, jonka avulla puhelimesi voidaan tunnistaa matkapuhelinverkossa. Löydät koodin laitteen myyntipakkauksesta. Saat sen selville myös, kun näppäilet puhelimeesi koodin *#06* samalla lailla kuin numeron, johon haluat soittaa. Laita koodi muistiin.
  Poliisi välittää koodin operaattorillesi. Se taas jakaa tiedon muille suomalaisille puhelinoperaattoreille. Puhelintasi ei voi sen jälkeen käyttää suomalaisten operaattorien matkapuhelinverkoissa.
  Koodi välittyy myös monille länsimaisille operaattoreille.

Tabletit

Kalliit tabletit ovat pienikokoisia tietokoneita. Niissä on yleensä sama käyttöjärjestelmä kuin isommissa tietokoneissa. Tableteissa voi käyttää selainta ja tehdä samat asiat kuin varsinaisilla tietokoneilla.
Näitä tabletteja koskevat samat tietoturvaohjeet kuin muitakin tietokoneita. (ks. luku 1).
Edulliset tabletit muistuttavat älypuhelimia. Niissä käytetään samoja käyttöjärjestelmiä ja sovellukia kuin älypuhelimissa.
Näitä tabletteja koskevat samat tietoturvaohjeet kuin älypuhelimia.

VINKKI

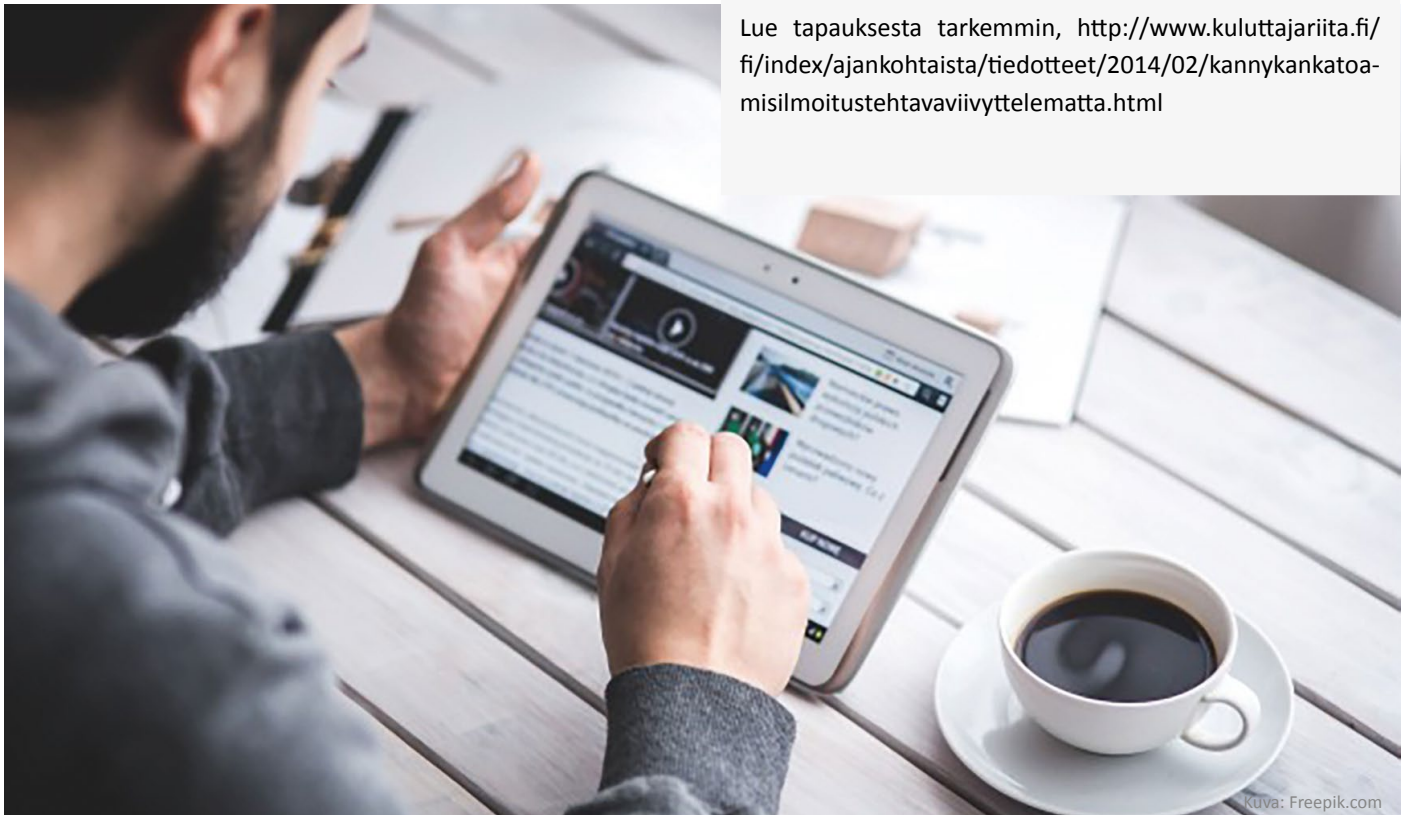
Tiesitkö, että vastaat puhelimen laskusta siihen asti, kunnes pyydät operaattoria sulkemaan liittymän?

VINKKI

Lataa tabletteihin ohjelmia vain isojen, tunnettujen yritysten kaupoista (storet).

Varas teki 27 000 euron laskun matkapuhelimella

Suomalaisen matkapuhelin varastettiin Espanjassa kadulla kesäyönä vuonna 2002. Puhelimen omistaja ilmoitti varkaudesta operaattorille seuraavana päivänä iltapäivällä viideltä. Siihen mennessä varas oli tehnyt liittymällä laskua 27000 euroa.
Operaattori oli jo ehtinyt sulkea puhelimen aamulla yhdeksän jälkeen, kun se huomasi, että liittymään kertyy laskua nopeasti.
Jos puhelimen omistaja on huolimaton, hän vastaa pääsääntöisesti vahingosta itse. Hän ei kuitenkaan vastaa ennalta arvaamattomista vahingoista. Vastuuta varkaan tekemästä laskusta voi myös yrittää sovitella.
Operaattori alensi oma-aloitteisesti puhelinlaskun määrän kolmasosaan. Se velkoi puhelimen omistajalta 7600:aa euroa. Puhelin omistaja vei asian Kuluttajariitalautakuntaan.
Lautakunta alensi korvattavan summan 2000 euroon.
Lautakunnan mukaan puhelimen omistaja toimi huolimattomasti, koska hän ei ilmoittanut puhelimen katoamisesta operaattorille heti aamulla.
Sen sijaan lautakunta piti ennalta arvaamattomana vahinkona sitä, että puhelin päätyi ammattirikollisille ja sillä ehdittiin tehdä 27000 euron lasku.
Lue tapauksesta tarkemmin, http://www.kuluttajariita.fi/fi/index/ajankohtaista/tiedotteet/2014/02/kannykankatoamisilmoitustehtavaviivyttelematta.html



Kuva: Freepik.com

7 OTA SOME HALTUUN

Ota verkko haltuun fiksusti. Tiedä, mitä siellä voi kertoa itsestä, perheestä, ystävistä ja omista tekemisistä. Jotkut asiat kannattaa jättää jakamatta.
Voit liikkua somessa turvallisesti, kun tunnistat huijarit ja valeprofiilit. Keskustele, perustele ja kyseenalaista asioita keskustelupalstoilla. Niin rakennat sinne hyvää keskustelukulttuuria.
Älä kuitenkaan räyhää tai kimmastu muiden asiattomista viesteistä.

Toimi fiksusti somessa

- Suojaa yksityisyyttäsi
- Harkitse mitä sanot tai jaat

Suojaa yksityisyyttäsi

Somen palveluiden kautta voit pitää yhteyttä sukulaisiin ja ystäviin. Voit jakaa kuvia, kertoa mielipiteesi ja peukuttaa asioita, joista tykkää. Voit tuottaa sinne videoita ja katsella muiden tuotoksia.
Somesta löydät aina seuraa ja esimerkiksi harrastukseen liittyviä yhteisöjä, joihin haluat kuulua.
On hyvä ymmärtää, että verkossa ja etenkin somessa pitää suojella yksityisyyttä. Ihan kaikkia omia ja muiden asioita ei siellä pidä kertoa.
Verkossa liikkuu tavallisten käyttäjien lisäksi esimerkiksi identiteettivarkaita, jotka keräävät sinusta tietoa. Sinusta saatetaan kerätä tietoa, jota myöhemmin käytetään hyväksi petoksissa.
Varsinainen tietojen keruun kohde voi joskus olla esimerkiksi työnantajasi. Sinusta ja läheisistä kerätään tietoja, joiden avulla saavutetaan luottamussuhde kanssasi. Voi käydä, että huomaamattasi annat urkkijoille tietoja työantajastasi.
Internetissä myös eri yritykset seuraavat sinua. Verkkohakusi, klikkauksesi, tykkäyksesi ja internetsivuilla käyntisi rekisteröityvät palvelun tarjoajan tietokantoihin.
Eri palveluista kerätyistä tiedoista voidaan koota sinusta hyvin tarkka profiili. Tietoja muun muassa myydään mainostajille, jotka voivat kohdistaa sinulle mainoksia. Huomaat sen helposti itsekin. Jos selaat esimerkiksi nettikauppojen kenkiä, katsomasi kenkämerkin mainos ilmestyy nopeasti sivullesi.

Näin suojaat omaa, perheesi ja ystäviesi yksityisyyttä:

- Älä kerro henkilökohtaisia tietoja. Niitä ovat esimerkiksi syntymäaika, henkilötunnus, osoite, puhelinnumero tai sähköpostiosoite.
- Älä julkaise kuvia, joissa näkyy lapsesi, autosi tai kotisi sisältä tai ulkoa.
- Julkaise muiden ihmisten kuvia vain, jos he antavat luvan. Niin suojelet myös muiden yksityisyyttä netissä.
- Älä julkaise kuvia lentolipuista tai lomareissulta tai kerro, milloin olet lomalla. Tieto saattaa kiinnostaa murtovarkaita. Lentolipuista voi kaapata tiedot ja vaihtaa niillä lentoaikaa sekä matkustajan nimen.
- Älä julkaise kännäyskuvia. Kuvat voivat tulla vastaan vuosien kuluttua. Kun kuvan laittaa verkkoon, sitä ei saa enää pois.
- Älä levitä intiimejä kuvia verkossa tai viestintäpalveluissa. Siellä perhe, naapurit tai vaikka työkaveritkin voivat ne nähdä.
- Mieti, kannattaako lähettää intiimejä kuvia ja videoita itsestä edes seurustelukumppanille. Jos rakkaus loppuu, seurustelukumppani saattaa julkaista ne netissä tai kiristää sinua niillä. Kumppanisi saattaa myös näyttää kuvasi muille.
- Jos annat sähköpostiosoitteen julkiselle foorumille, esimerkiksi nettikirpputorille, käytä osoitetta, josta ei käy ilmi nimesi. Osoitteen ei tarvitse olla mallia etunimi.sukunimi@palvelin.fi.
- Pidä huolta someprofiilistasi. Profiilisi kertoo sinusta paljon. Se, mitä kirjoitat, miten kirjoitat, mitä jaat ja ketkä ovat kavereitasi, saattaa kiinnostaa esimerkiksi työnantajia. Äkkiväärät kommenttisi saattavat päätyä myös läheisten silmiin tahtomattasi.
- Vältä työantajan arvostelua, sillä työnantaja saattaa seurata postauksiasi. Älä kerro liikaa työhösi liittyviä asioita muutenkaan.

VINKKI

Opeta myös lapsesi suojaamaan itseään somessa. Kerro, mitä hän voi turvallisesti jakaa ja mitä eri palveluihin ei kannata laittaa.

Suojaa tietosi verkossa

- Lue käyttämiesi ohjelmien ja somepalvelujen käyttäöehdot. Tarkasta palvelun yksityisyysasetukset. Oletusarvona on yleensä se, että annat sovellukselle mahdollisimman suuret oikeudet kerätä sinusta tietoa. Muuta asetukset niin tiukoiksi kuin sovellus sallii.
- Tutki käyttäjäehdoista, kenelle julkaisemiesi kuvien, tekstien ja videoiden oikeudet kuuluvat. Jotkut sovellukset vaativat, että luovutat niille julkaisemasi materiaalin oikeudet.
- Satsaa yksityisyyteen varsinkin Facebookissa. Voit esimerkiksi kieltää kohdennetun mainonnan, piilottaa kaverilistasi ja päättää, ketkä näkevät julkaisemasi materiaalin.
- Tutki, pysyvätkö viestisi ja tietosi salassa palvelussa, jota käytät. Jotkut palvelut salaavat viestit sinun ja sen henkilön tai ryhmän välillä, joille viestit lähetit. Kaikki eivät niin tee.
- Poista säännöllisesti tietokoneeltasi evästeet ja selaushistoria. Evästeet ovat pieniä ohjelmia, jotka seuraavat liikkumistasi netissä. Selaushistoria kertoo, millä sivuilla olet käynyt.

  Kirjoita selaimesi hakuun hakusanaksi poista evästeet tai poista selaushistoria. Niin pääset kohtaan, josta voi ne poistaa.

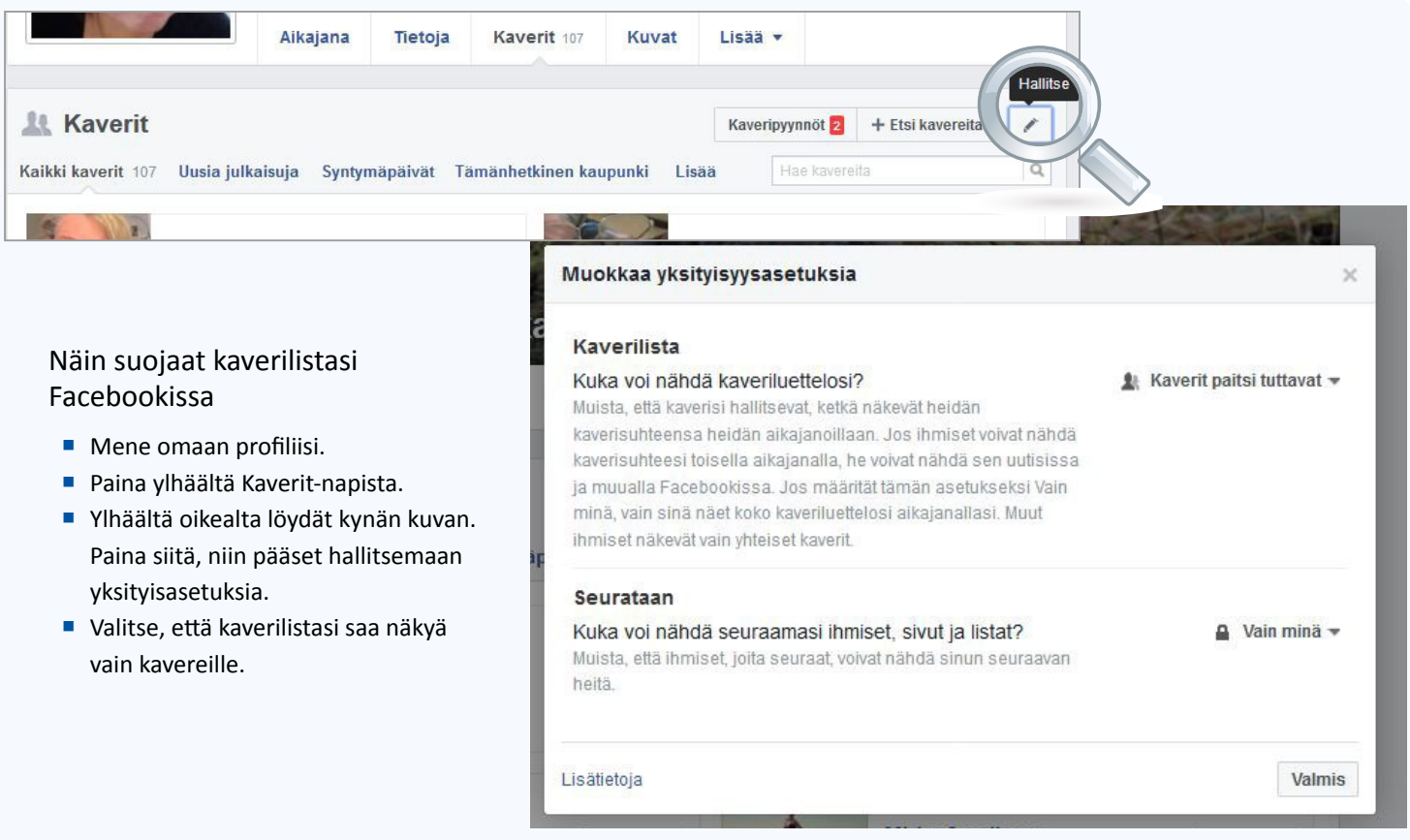
Harkitse mitä sanot ja jaat somessa

Netin keskustelupalstat, chatit ja monet somen palvelut tarjoavat nopean keskustelukanavan. Voit ottaa kantaa twiiteillä, osallistua yhteiskunnalliseen keskusteluun, vaihtaa mielipiteitä ja ottaa kantaa. Löydät sieltä samanmielisiä ja vastakkaisia näkökulmia edustavia keskustelijoita.

Verkko tarjoaa ihmisille uudenlaisen tavan antaa palautetta ja osallistua keskusteluihin, kertoa oma mielipide, kuulla mitä muut sanovat. Sanomasi leviää saman tien kaikkien halukkaiden nähtäville.

Tavoitat netin ja sähköpostin kautta myös yhteiskunnan päättäjät, virkamiehet ja median. Voit jopa saada aikaan uusia lakeja, kun teet kansalaisaloitteen ja löydät sille tarpeeksi kannattajia.

Siten verkko lisää sananvapautta, vahvistaa demokratiaa ja edistää kansalaisyhteiskuntaa. Vapaudella sanoa on myös kääntöpuoli. Netin keskustelupalstoilla ja somessa liikkuu paljon asiattomia kommentteja ja vihapuhetta. Myös kiusaamista on siirtynyt nettiin. Saatat joutua siellä kiusaaamisen kohteeksi tai itse syyllistyä rikokseen, kun et harkitse, mitä sanot.



Näin suojaat kaverilistasi Facebookissa

- Mene omaan profiiliisi.
- Paina ylhäältä Kaverit-napista.
- Ylhäältä oikealta löydät kynän kuvan. Paina siitä, niin pääset hallitsemaan yksityisasetuksia.
- Valitse, että kaverilistasi saa näkyä vain kavereille.

Muista nämä asiat, kun osallistut keskusteluun

- Harkitse mitä kirjoitat. Saatat kohdata mielipiteen, väitteen, uutisen tai vaikka kuvan, joka kiihdyttää ja vetoaa voimakkaasti tunteisiin. Suutut, ärsyynnyt tai pahoitat mielesi. Tekisi mieli antaa takaisin kaksin verroin tai tölväistä oikein kunnolla.
  Pysähdy hetkeksi. Keitä kahvit tai nuku yön yli. Oletko vielä silloin samaa mieltä?
  Tunnepuuskassa ei koskaan kannata laittaa nettiin mitään.
- Jos kommenttisi koskee toista ihmistä, muista, että sanasi voivat satuttaa häntä pahasti. Sanoisitko saman asian hänelle kasvotusten?
  Tietokone on vain väline, mutta viestisi lukee ihminen. Vaikka naputat viestisi yksin kotona, muista että some on viestintää ihmiseltä ihmiselle.
- Internet on julkinen kanava. Vaikka kirjoittaisit Facebookin suljetussa tai salaisessa ryhmässä, viestisi on silti julkinen. Jos vihjaat tai kerrot valheita jostakin ihmisestä tai jakelet tappouhkauksia, teet sen julkisesti. Siitä jää todiste, sillä somessa kerran sanomaasi et enää saa pois.
- Sananvapaus Suomessa tarkoittaa sitä, että kukaan ei estä sinua sanomasta mitä haluat. Olet kuitenkin aina vastuussa siitä, mitä sanot. Kun sanot oikein kipakasti, saatat huomaamattasi syyllistyä esimerkiksi kunnianloukkaukseen tai laittomaan uhkaukseen.
- Vaikka kirjoitat nimettömänä tai tykität nimimerkin takaa, oikea nimesi on mahdollista selvittää. Jokaisella tietokoneella on IP-osoite, josta jää jälki verkkoon.
- Älä provosoidu. Verkon palstoilla liikkuu tavallisten keskustelijoiden lisäksi ihmisiä, jotka tahallaan ärsyttävät ja hämmentävät. Siellä on myös trolleja ja mielenterveyden ongelmista kärsiviä ihmisiä. Älä mene halpaan. Jätä provosoivat kommentit huomiotta, äläkä jaa niitä eteenpäin.

Ilkeät kommentit ja viestit voivat olla rikos

Kunnianloukkaus

Lähetät jollekin viestin tai viestejä, joissa pilkkaat tai ivaat häntä, kerrot hänestä valheita, teet rasistisia huomauksia tai kommentoit roisisti hänen ulkonäköään. Saatat jakaa samanlaisia viestejä keskustelupalstoilla tai Facebookissa. Voit myös muokata jostakusta kuvia kiusaksi tai vitsiksi. Laitat ne sitten nettiin.
Viestit voivat aiheuttaa niiden kohteelle vahinkoa ja kärsimystä. Hän voi myös kohdata halveksuntaa niiden vuoksi. Jos niin käy, niin on mahdollista että olet syyllistynyt kunnianloukkaukseen. Voit saada sakkoa ja joutua maksamaan korvauksia uhrille.

Törkeä kunnianloukkaus

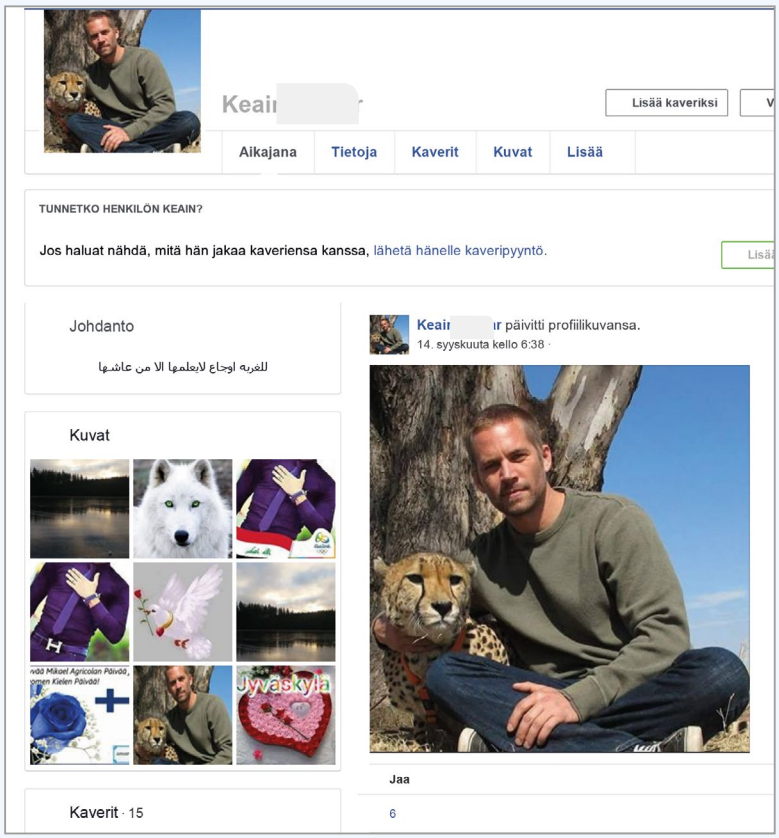
Jos yllä kuvatut viestit aiheuttavat kohteelle suurta tai pitkäaikaista kärsimystä tai erityisen suurta tai tuntuvaa vahinkoa, voit syyllistyä törkeään kunnianloukkaukseen. Riittää, että jompikumpi seuraus on suurta. Lisäksi rikoksen pitää olla kokonaisuutena arvosteltuna törkeä. Törkeästä kunnianloukkauksesta voi saada sakkoja tai enintään kaksi vuotta vankeutta.

Yksityiselämää loukkaavan tiedon levittäminen

Laitoitko nettiin arkaluontoisen vihjauksen, tiedon tai kuvan, joka koskee jonkun yksityiselämää? Tai latasitko nettiin kaverisi tai exäsi alastonkuvia?
Viesti voi olla totta. Sen kertominen julkisesti saattaa silti aiheuttaa vahinkoa ja kärsimystä ihmiselle, jota se koskee. Rangaistus yksityiselämää loukkaavan tiedon levittämisestä on sakot tai korkeintaan kaksi vuotta vankeutta. Voit myös joutua maksamaan korvauksia.

Mitä teen, jos minua kiusataan netissä?

- Älä lähde mukaan suunsoittoon tai väittelyyn. Silloin kiusaaja ei voi väittää, että sinä aloitit. Estät myös sen, että itsekin kiivastuksissa solvaat ja uhkaat kiusaajaa.
- Laita kiusaaja estolistalle somen palveluissa.
- Ilmoita kiusaamisesta palvelun ylläpitoon. Ylläpito voi poistaa kiusaajan viestit ja jopa koko profiilin.
- Jos olet alaikäinen, kerro kiusaamisesta vanhemmille. Jos kiusaaminen liittyy kouluun, kerro itse tai vanhempien kanssa asiasta myös koululle.
- Jos olet aikuinen, yritä ensin sovitella asiaa kiusaajan kanssa. Jos puhe ei auta, voit ottaa yhteyttä nettipoliiseihin. Nettipoliisi käy huomauttamassa kiusaajaa. Usein kiusaaminen loppuu siihen.
- Jos kiusaaminen silti jatkuu, voit tehdä rikosilmoituksen. Pidä tallessa kiusaajan viestit ja esitä ne poliisille. Jos asia etenee esitutkintaan, asiaa tutkitaan yleensä nimikkeillä kunnianloukkaus tai laiton uhkaus.



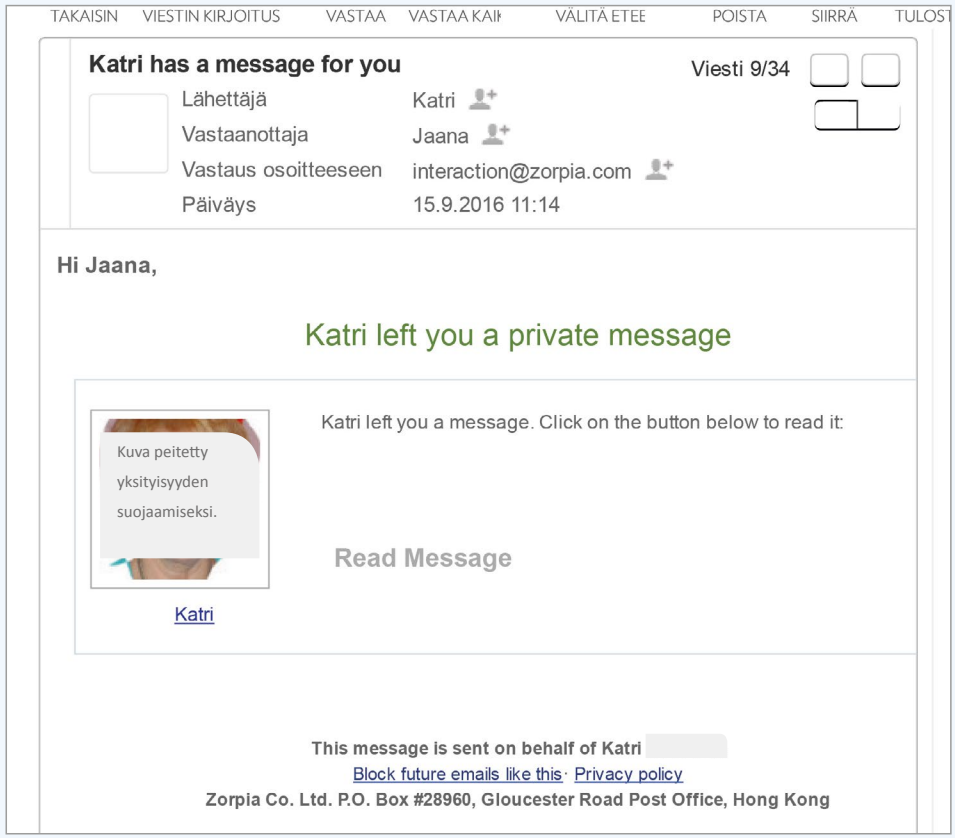
Saitko kaveripyynnön tuntemattomalta?

Kaikki eivät esiinny sosiaalisessa mediassa omilla nimillään ja kuvillaan. Esimerkiksi tämä Facebook-profiili käyttää yhdysvaltalaisen näyttelijän Paul Walkerin kuvaa. Walker kuoli autokolarissa vuonna 2013. Kuva on otettu eläinpuistossa Etelä-Afrikassa.

Valeprofiilit tunnistat usein myös siitä, että niillä ei juuri ole julkaisuhistoriaa ja kaverilista voi olla lyhyt.

Kuvasi voidaan varastaa somesta

Someen jakamasi kuvat voidaan kaapata. Suomalaisen naisen kuva oli otettu hänen deittisivulle tekemästään profiilista. Nyt huijari käyttää hänen kuvaansa ja etunimeään sähköpostissa, joka on lähetetty naisen kanssa työsähköposteja vaihtaneelle henkilölle. Huijari pyytää painamaan linkkiä, jonka takana muka on Katrin lähettämä viesti. Linkkiä ei pidä painaa.



Kunnianloukkaus Facebookissa toi vankeutta

Pohjois-Karjalan käräjäoikeus tuomitsi torstaina törkeästä kunnianloukkauksesta miehen, joka oli haukkunut toista miestä namusedäksi.
Tuomittu oli luonut julkisen Facebook-sivuston, jonka otsikkona oli “Namusetä (asianomistajan nimi) vankilaan”. Sivulla tuomittu väitti valheellisesti rikoksen uhrin olevan pedofiili. Sivulla oli myös kolme kuvaa, jotka oli kopioitu rikoksen uhrin omalta sivustolta.
Oikeus langetti 27-vuotiaalle miehelle neljän kuukauden ehdollisen vankeustuomion.

Lähde: STT 22.9.2016

"Älä räyhää, valehtele, solvaa tai juorua somessa. Voit joutua sanoistasi vastuuseen."

"Vaikka kirjoitat someen nimettömänä tai nimimerkin takaa, oikea nimesi on mahdollista selvittää."

Näin viestipalvelut suojelevat yksityisyyttäsi

Ihmisoikeusjärjestö Amnesty International selvitti vuonna 2016 netin viestipalveluiden turvallisuutta.
Järjestö vertaili yhtätoista maailmalla suosittua viestipalvelua. Niistä selvitettiin muun muassa, miten hyvin palvelu salaa viestit lähettäjän ja vastaanottajan välillä. Viestipalvelut saivat pisteitä myös sen mukaan, miten hyvin ne tunnistavat uhkat, joita verkossa kohdistuu palvelun käyttäjiin.
Vertailu tutki myös, kertovatko yritykset avoimesti valtion tietopyynnöistä ja sen, miten pyyntöihin on vastattu.

Näin eri viestipalvelut sijoittuivat tutkimuksessa. Korkein pistemäärä oli sata.
WhatsApp 73
Facebook Messenger 73
Applen iMessage 67
Applen FaceTime 67
Telegram Messenger 67
Google Hangouts 53
Line 47
Viber 47
Kakao Talk 40
Skype 40
Snapchat 26
Blackberry Messenger 20
Tencet QQ WEChat 0

Lähde: Amnesty Internationat: For your eyes only?
http://www.amnestyusa.org/research/reports/for-your-eyes-only

”Kadun hetkeä, kun painoin Julkaise-nappia”

Yhdysvaltalainen Carnegie Mellon -yliopisto kysyi Facebookin käyttäjiltä, minkä tietojen julkaisemista he katuvat. Tutkimus on vuodelta 2011.
Tutkimuksen otsikko on kuvaavasti Kadun hetkeä kun painoin Julkaise-nappia.
Eniten ihmiset katuivat näihin aiheisiin liittyviä julkaisujaan:
Ryypiskely ja huumeiden käyttö
Seksi
Sairaudet
Perheongelmat

Kuva: Freepik.com

Netti kulkee mukana

TAUSTAA

Internet on nykyään mukana ja käytettävissä jatkuvasti. Liikkeellä ollessa sitä käytetään ennen kaikkea matkapuhelimella. Kaksi kolmesta käytti internetiä matkapuhelimella kodin ja työpaikan ulkopuolella. Tabletilla nettiä oli vastaavasti käyttänyt joka neljäs.

Suomalaisista liki yhdeksän kymmenestä käyttää internetiä. Alle 55-vuotiaista internetiä käyttivät lähes kaikki. Kolme neljästä käyttää nettiä monta kertaa päivässä.

Aktiivinen netin käyttö on yleistä myös vanhemmille netin käyttäjille. Yli puolet 75–89-vuotiaista, jotka olivat ottaneet internetin käyttöönsä, käyttivät sitä monesti päivässä.

Internetiä käytetään asioiden hoitamiseen, tiedonhakuun, viestintään ja medioiden seuraamiseen. Verkkopankkia käyttää jo neljä viidestä suomalaisesta.

Tiedot ovat vuodelta 2016.

Väestön tieto- ja viestintätekniikan käyttö 2016, Tilastokeskus

Somea ovat esimerkiksi nämä palvelut

Facebookissa voit jakaa kokemuksia, tunteita ja kuulumisia. Siellä voit myös jakaa linkkejä ja muiden postauksia.
Facebookiin pitää ensin tehdä oma profiili. Voit sen jälkeen kutsua ystäviäsi kavereiksesi. Saat myös kaveripyyntöjä. Voit itse päättää, otatko kaveripyynnön esittäjän kaveriksi vai et.
Näet myös kavereidesi lähettämät kuvat ja viestit. Voit kommentoida kavereiden viestejä, jos haluat.
Messenger on viestipalvelu, jonka avulla voit keskustella muiden Facebookin käyttäjien kanssa.
YouTube on Internetissä toimiva videopalvelu. Voi lisätä sinne omia videoita tai voit katsoa ja kommentoida muiden lähettämiä videoita.
Twitter on keskustelu- ja uutiskanava, jossa käyttäjät julkaisevat enintään 140 merkkiä sisältäviä viestejä eli twiittejä. Twitterissä voit seurata ketä tai mitä tahansa henkilöä, organisaatiota ja uutislähdettä.
Skype on internetissä toimiva videopuhelupalvelu, jossa keskustelijat näkevät toisensa. Voit myös lähettää Skypessä pikaviestejä ja tiedostoja.
WhatsApp-viestisovelluksella voit lähettää pikaviestejä, kuvia, videoita, ääniviestejä, tiedostoja ja sijaintitietoja. Sen kautta voit lähettää viestiä yhdelle henkilölle tai ryhmälle. Palvelu toimii älypuhelimissa.
Snapchat on pikaviestipalvelu, jossa avulla voit lähettää kuvia ja videota. Voit lisätä niihin tekstiä ja erilaisia kuvakkeita. Voit lähettää viestejä palvelun muille käyttäjille tai omaan julkiseen osioon My storyyn. Muut voivat nähdä sinne lähetetyt viestit 24 tunnin ajan. Pikaviestit säilyvät vastaanottajan laitteessa 1–10 senkuntia.
Instagramissa voit jakaa omia kuvia tai katsella kavereiden tai muiden käyttäjien sinne laittamia kuvia. Kuvia voit myös kommentoida ja tykätä.
Pinterest on linkkien ja kuvien jakopalvelu. Sen avulla voit luoda ja ylläpitää kokoelmia, jotka perustuvat johonkin teemaan, esimerkiksi tapahtumaan tai harrastukseen.
Tumblr on blogipalvelu. Voit lähettää sinne kirjoituksia, videoita, linkkejä, kuvia ja musiikkia. Tumblrissa voit seurata muiden käyttäjien blogeja ja jakaa muiden käyttäjien postauksia. Sivustolla voit myös lähettää viestejä tai fanipostia muille käyttäjille.

Sanasto haltuun

Chatin (chat) kautta voi keskustella muiden internetinkäyttäjien kanssa.

Eväste tarkoittaa pientä tekstitiedostoa, jonka avulla palvelun tarjoaja yksilöi palvelun käyttäjät. Useimmiten evästeet ovat harmittomia ja myös hyödyllisiä. Jotkut evästeet voivat kuitenkin seurata koneen käyttöä.

IP-osoite (Internetin protokollaosoite) on numerosarja, josta voi tunnistaa jokaisen internetiin kytketyn tietokoneen.

Käyttöehdot tarkoittavat eri palveluntarjoajan asettamia ehtoja, jotka koskevat palvelun käyttöä.

Nettipoliisi on sosiaalisessa mediassa toimiva poliisi.

Selaushistoriaan tietokone tallentaa, millä internetsivuilla olet viimeksi käynyt.

Some tarkoittaa sosiaalista mediaa.

Someprofiili on someen tehty käyttäjäprofiili.

Sovellus on älylaitteella käytettävä ohjelma. Usein tietokoneohjelmia kutsutaan sovelluksiksi.

Trolli on henkilö, joka tahallaan ärsyttää ja häiriköi keskustelua internetissä ja ohjaa sitä haluamaansa suuntaan.

Twiitti, twiittaus on Twitter-viestipalveluun lähetetty lyhyt viesti.

Yksityisyysasetus tarkoittaa asetuksia, joilla voit esimerkiksi somen palveluissa määrätä, mitkä tietosi muut käyttäjät näkevät.

Ylläpitäjä on jonkin palvelun toimivuudesta vastaava henkilö. Hän voi esimerkiksi valvoa, että somen palvelussa noudatetaan palvelun kertomia sääntöjä.

8 ÄLÄ USKO KAIKKEA

Kun avaat tietokoneen, pääset loputtoman tietomäärän lähteelle. Pääset lukemaan, kuuntelemaan ja katsomaan julkaisuja. Et voi aina tietää, ovatko tiedot totta, kuvat aitoja ja henkilöt niitä, joita he väittävät olevansa.

Verkossa on luotettavan tiedon lisäksi muun muassa satiiria, uutisiksi naamioituja mainoksia, huijauksia, disinformaatiota, mielipidekirjoituksia ja propagandaa. Tietoa tulee lisää koko ajan. Verkossa on myös paljon vanhentunutta sisältöä.

Netissä joudut itse arvioimaan, mihin voit luottaa ja mitä ei kannata suin päin uskoa. Tarvitset medianlukutaitoa ja kykyä arvioida kriittisesti lukemaasi ja näkemääsi.

Arvioi netissä kohtaamaasi tietoa näin:

- **Tutki tiedon lähde**
  Luit kiinnostavan asian netistä. Tutki, kuka tai mikä taho ylläpitää sivustoa, joka kertoo asiasta. Sen jälkeen mieti, voitko luottaa lähteen tuottamaan tai jakamaan tietoon.
  Nettiin tuottavat sisältöä muun muassa viranomaiset, puolueet, ammattiliitot, elinkeinoelämän järjestöt, yritykset, yhdistykset ja järjestöt, yliopistot ja tutkimuslaitokset, yksityiset henkilöt, rikolliset, bloggarit, perinteiset mediat eli tv-yhtiöt, sanomalehdet ja aikakauslehdet sekä valemediat.
- **Kenen tuottamaa ja jakamaa tietoa uskot?**
  Mieti, mikä on tiedon tuottajan motiivi.
  Jokaisella, joka tuottaa ja jakaa tietoa netissä, on syy tehdä niin. Se voi olla tiedon jakaminen, yrityksen myynnin edistäminen tai yhteiskunnan keskusteluun vaikuttaminen. Arvioi, onko kyseessä mainospuhe, mielipide, viranomaisten antama tieto tai ohje tai esimerkiksi tunnetun media julkaisema uutinen.
  Yhdistykset ja järjestöt edistävät asiaa, jonka vuoksi ne on perustettu. Yhdistykset ja järjestöt ovat erilaisia. Pidätkö esimerkiksi Pelastakaa Lapset -järjestön ja Suomen kannabisyhdistyksen tuottamaa tietoa yhtä luotettavana?
  Poliitikot ja puolueet kertovat asioista omasta näkökulmastaan.
  Blogeista ja keskusteluista voit seurata, mitä mieltä seuraamasi ihmiset ovat eri asioista. On hyvä muistaa, että osa bloginpitäjistä saa rahaa yrityksiltä. Se saattaa vaikuttaa siihen, mitä bloggaaja sanoo eri tuotteista ja miksi hän niistä kirjoittaa. Keskustelupalstoilla sanan säilä lentää välillä kuumana. Ota kommentit mielipiteinä, älä tosiasioina.
- **Tutki muitakin lähteitä**
  Luit kiinnostavan tiedon. Älä oikopäätä usko, että se on totta, varsinkin jos se on kuohuttava asia. Tutki, mitä muut tiedon lähteet kertovat aiheesta. Lue mitä aiheesta kerrotaan esimerkiksi muualla netissä, mediassa tai tietokirjoissa. Niin saat asiasta laajemman käsityksen.
- **Tunnista valemediat ja valeuutiset**
  Valemediat ja valeuutiset ovat uusi ilmiö. Valemedialla tarkoitetaan yleensä sanomalehtien verkkolehtiä muistuttavia sivustoja, jotka eivät kuitenkaan toimi niin kuin oikea media. Valemediat jakavat tahallaan myös harhaanjohtavaa tietoa. Valemedian nettisivut voivat muistuttaa sanomalehtien nettisivuja. Sivujen ulkonäöstä et aina voi päätellä, oletko valemedian sivuilla.

Näistä merkeistä tunnistat valemediat ja valeuutiset:

- Tarinat herättävät voimakkaita tunteita. Ne voivat demonisoida ihmisryhmiä, joita kohtaan on voimakkaita ennakkoluuloja. Ne voivat sisältää väitteitä ihmisten yksityisasioista. Uutiset vetoavat usein ihmisten pelkoihin ja ennakkoluuloihin.
- Tarinat sisältävät yleistyksiä ja tarjoavat yksinkertaisia vastauksia ongelmiin. Ne eivät tuo esiin useita mielipiteitä tai näkökulmia. Ne tarjoavat väitteitä mutta eivät aina kerro lähteitä.
- Tuoreista uutistapahtumista lähtee liikkeelle vääristettyä tietoa.
  Esimerkiksi onnettomuuksista ja kriiseistä ilmestyy pian väritettyjä tulkintoja ja suoria valheita. Netissä saattaa levitä valokuvia, jotka valemedian mukaan on otettu tapahtumasta. Tosiasiassa ne voivat olla vanhoja, aiemmista onnettomuuksista ja tapahtumista otettuja kuvia. Samat uutiskuvat voivat pulpahtaa esiin vuosien kuluessa monta kertaa.
- Valeuutiset ovat keksittyjä uutisia. Ne matkivat ulkoisesti oikeita uutisia, mutta ne eivät ole totta.
  Aiemmin valeuutiset olivat julkkisjuoruja ja uskomattomia tapahtumia maailmalta. Sittemmin huijausjuttujen tekijät alkoivat tehdä rasistisia ja Euroopan pakolaiskriisiin liittyviä tarinoita. Valeuutiset leviävät tyypillisesti laajemmalle kuin niistä myöhemmin tehdyt korjaukset.

VINKKI

Kun kohtaat nopeasti leviävän, dramaattisen uutiskuvan, tutki sen historia. Google Kuvahaku paljastaa, onko sitä käytetty muussa yhteydessä aiemmin, ks. ohje sivulta 56.

Tunnistatko trollit ja informaatiovaikuttamisen?

Talvisodan aloittaneita Mainilan laukauksia ei ammuttu lainkaan. Tai Suomi ampui ne kohti Neuvostoliittoa. Suomalaiset ovat luvanneet olla liittymättä Natoon. Venäläisten turistien lapsia otetaan huostaan Suomessa.
Jos näit netissä yllä olevat uutiset, törmäsit trolleihin ja informaativaikuttamiseen.
Trollit aiheuttavat hämmennystä ja sekoittavat keskustelua keskustelufoorumeilla.
Trollit liittyvät joskus informaatiovaikuttaiseen. Sen avulla halutaan lisätä epävarmuutta kohdemaassa, kärjistää väestöryhmien välejä, lietsoa epäluottamusta viranomaisiin ja tiedotusvälineisiin, luoda turvattomuuden tunnetta ja vaikuttaa maassa käytävään keskusteluun.
Jätä trollien viestit huomiotta. Älä jaa niitä eteenpäin.

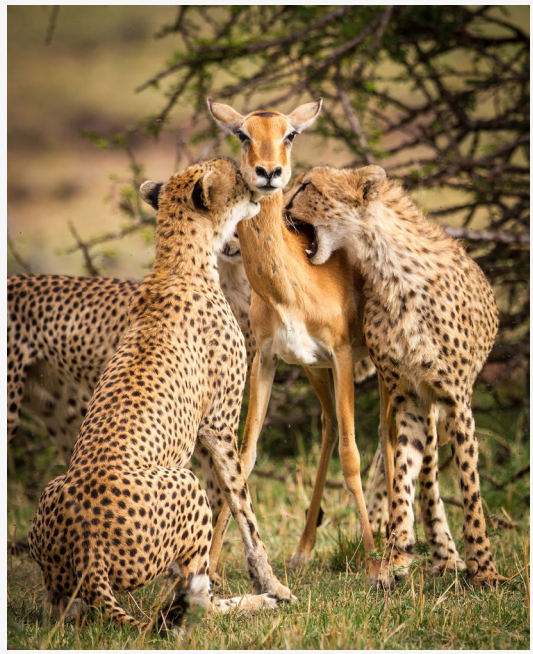
TAUSTAA

Media noudattaa Journalistin ohjeita

Suomalainen media noudattaa työssään Journalistin ohjeita. Ohjeet on laatinut Julkisen sanan neuvoston (JSN) kannatusyhdistys. Neuvosto valvoo niiden noudattamista.
JSN on tiedotusvälineiden kustantajien ja toimittajien perustama elin. Se tulkitsee hyvää journalistista tapaa ja puolustaa sanan- ja julkaisemisen vapautta.
Journalistin ohjeiden mukaan journalistilla on velvollisuus pyrkiä totuudenmukaiseen tiedonvälitykseen. Tiedot on tarkastettava mahdollisimman hyvin. Yleisön pitää voida erottaa tosiasiat mielipiteestä ja sepitteellisestä aineistosta. Kuvaa ja ääntä ei saa käyttää harhaanjohtavasti.
Journalistin ohjeiden mukaan etnistä alkuperää, kansallisuutta, sukupuolta, seksuaalista suuntautumista, vakaumusta tai näihin verrattavaa ominaisuutta ei pidä tuoda esiin asiaankuulumattomasti tai halventavasti.
Rikoksesta tuomitun nimen, kuvan tai muita tunnistetietoja voi julkaista, ellei se tuomitun asemaan tai tekoon nähden ole selvästi kohtuutonta. Nimen kertomisessa on syytä olla varovainen, kun kyse on vasta rikosepäilystä tai syytteestä.

Kuva ja valetarina leviävät maailmalla, kuvaajan vaikea estää kuvansa väärinkäyttö

Suomessa asuvan luontokuvaajan ottama valokuva ja siihen liittyvä valetarina leviävät nopeasti netissä. Kuvassa on impala-antilooppi, jonka kolme gebardia on ottanut kiinni. Kuvan on ottanut Suomessa asuva luontokuvaaja Alison Buttigieg. Hän tallensi ilmeisesti sairaan tai loukkaantuneen impalan luonnonsuojelualueella Keniassa. Impala oli yksin, eikä se yrittänyt karkuun. Kuvassa gebardiemo opetti kahta poikastaan saalistamaan.
Kuva lähti kiertämään somessa, mutta siihen tekaistiin valetarina. Sen mukaan kuva esittää suurta äidinrakkautta: emo uhraa henkensä, jotta sen poikaset saavat aikaa juosta karkuun saalistajilta. Valetarinan mukaan emo katsoo kuvassa turvaan juoksevia jälkeläisiään. Tarina vain ei ole totta.
Buttigieg on saanut vihapostia kuvan ja tarinan levitessä. Niiden mukaan kuvaajan olisi pitänyt estää impalan tappaminen. Joidenkin viestien mukana kuvaajan itsensä olisi pitänyt kuolla.
Alison Buttigieg on yrittänyt estää kuvan leviämisen.
– Valeuutisen elinvoima on ällistyttävä! Oli erittäin turhauttavaa, kun valheellinen tarina alkoi levitä. Ei ollut mitään keinoa hallita sitä, Alison kertoo.
Lähde: Iltasanomat 22.2.2017



© Alison Buttigieg

Trollitili yritti kääntää Imatran ampumisen venäläisvastaiseksi hyökkäykseksi

Kolme naista kuoli ammuskelijan uhrina Imatralla 3.12.2016. Naiset olivat poistumassa ravintolasta, kun paikkakuntalainen nuori mies ampui heidät metsästysaseella.
Tapauksen tultua julki juuri perustettu Twitter-tili alkoi aamupäivällä levittää vääriä tietoja tapahtuneesta. @ImatranUutiset-tilillä väitettiin, että ampuja on äärioikeistolainen ja uhrit venäläisiä.
Suomeksi ja englanniksi kirjoitetuissa viesteissä ampujan motiiveja väitetään rasistiksi ja uhreja Venäjän kansalaisiksi. Poliisin mukaan uhrit olivat suomalaisia paikallisia naisia.
Twitter-tilin ylläpitäjä väitti myös, että ampuja on suomalainen upseeri. Lisäksi hän yritti kytkeä tapauksen selvittelyyn mukaan muun muassa Venäjän suurlähetystöä ja turvallisuuspalvelu FSB:tä.
Twitter-tili suljettiin pian twiittien tultua julki.
Lähde: Etelä-Saimaa 4.12.2016

Valeprofiilin huijaus päätyi MV!-lehden jutuksi

MV!-lehti teki 20.9.2015 uutisen avustustyöntekijästä, joka toimi Torniossa pakolaiskriisin aikana samana syksynä.
Uutinen perustui Niina Salmisen kirjoituksiin Facebookissa. Salminen kertoi sivullaan, että ”turvapaikanhakijat käyttäytyvät sikamaisesti, ruoka ei kelpaa, majoitus ei kelpaa, vaatteet ei kelpaa ja kaksi meinasi käydä kimppun kun minulla ei ollut sopivaa laturia puhelimeen”. Toisessa viestissä Niina Salminen sanoi, että ”voin todeta että pääosa tänne tulleista n 90 % ovat nähneet sotaa vain televisiossa”.
Niina kertoi, että hän on Torniossa Kirkon ulkomaanavun avustustyössä.
Nopeasti kävi ilmi, että Niina Salminen oli valeprofiili. Profiilin kuva vei venäläiselle Facebookia vastaavalle sivulle. Kirkon ulkomaanapu ei toiminut Torniossa eli profiili ja sen viestit olivat keksittyjä.
MV!-lehti teki oikaisun seuraavana päivänä ja kertoi, että uutinen on väärä.

Valeuutiset mustamaalasivat Hillary Clintonia USA:n presidentinvaaleissa 2016

Laaja kampanja levitti tehokkaasti valeuutisia Hillary Clintonista ennen Yhdysvaltain vaaleja. Väitteen esitti arvostettu sanomalehti Washington Post. Se perustaa tietonsa kahteen riippumattomaan tutkimukseen.
Valeuutisia tekivät oikeistohenkiset uutissivustot ja lehdet. Niihin tarttuivat Venäjään liitetyt nettisivustot, maksetut trollit ja väärennetyt sosiaalisen median tilit. Ne alkoivat levittää valeuutisia massiivisesti.
Ne nousivatkin nopeasti esimerkiksi Facebookissa tavallisten amerikkalaisten nähtäville. Ihmiset jakoivat niitä eteenpäin. Lopulta valeuutisia jaettiin sosiaalisessa mediassa enemmän kuin oikeita uutisia.
Levinnein valeuutinen väitti, että paavi tukee Trumpia presidentiksi. Toinen paljon jaettu valeuutinen kertoi, että Hillary Clinton myi aseita Isisille. Clintonin kerrottiin myös kuuluvan pedofiilirinkiin, joka toimii erään pizzayrityksen kellarissa.
Valeuutiskampanjan tarkoitus oli vaikuttaa presidentinvaalien tulokseen. Uutiset mustamaalasivat Clintonia voimakkaasti ja maalasivat kuvaa jopa ydinsodasta, jos hänet valitaan.
On mahdotonta arvioida, millainen vaikutus propagandalla oli vaalitulokseen, lehti kertoo. Käsitys Clintonista epärehellisenä on kuitenkin Yhdysvalloissa levinnyt laajalle, vaikka häntä ei ole koskaan syytetty oikeudessa mistään.

Lähde: Iltasanomat 27.11.2016

Sanasto haltuun

Disinformaatio tarkoittaa tahallista harhaan johtavaa tietoa tai tiedotusta.

Informaatiovaikuttaminen on toisen valtion päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja siltä suojautumista.

Trolli on henkilö, joka tahallaan ärsyttää ja häiriköi keskustelua internetissä ja ohjaa sitä haluamaansa suuntaan.

Valemedialla tarkoitetaan itseään mediaksi kutsuvia julkaisuja, jotka yrittävät hämärtää tai vääristellä tosiasioita. Ne eivät noudata hyvää journalistista tapaa kuten mediat.

Valeuutinen on oikeita uutisia matkiva uutinen, joka kuitenkaan ei ole totta.

9 TUNNISTA HUIJARIT

Sähköpostiisi putoilee viestejä, joissa on vetävät otsikot. Sinulle luvataan isoa perintöä, voittoa tai mahdollisuutta tehdä bisnestä. Sinulta saatetaan pyytää apua vaikeuksiin joutuneelle ihmiselle. Saatat saada myös edullisen lainatarjouksen.

Älä mene lankaan. Jos et tunne lähettäjää, on suuri mahdollisuus, että viesti tulee huijareilta. Ne etsivät luottavaisia ja hyväuskoisia ihmisiä, joiden auttamishaluun tarinat vetoavat.

Yhteistä huijauksille on se, että sinulle luvataan paljon rahaa. Jotta saat rahat, joudut maksamaan erilaisia pieniä maksuja, esimerkiksi tullimaksuja, veroja, rahansiirtokuluja, välityspalkkioita.

Kun maksat kerran, tulee toinen rahanpyyntö. Rahan lypsäminen jatkuu niin kauan kuin jatkat maksamista. Luvattua voittoa, lainaa tai perintöä et ikinä saa, sillä kyse oli alun perinkin huijauksesta.

Internetin huijaukset ovat usein sähköpostien massapostituksia, joita ei ole kohdistettu varsinaisesti kellekään. Tavoite on saavuttaa suuri määrä ihmisiä. Vaikka vain pieni osa huijausviestien saajista jää haaviin, huijaukset tuottavat rahaa.

Huijaukset ovat ammattimaista ja kansainvälistä rikollisuutta.

Yksittäiset huijatut summat voivat olla kohtuullisen pieniä, kymmeniä tai satoja euroja. Silti Suomessakin on ollut tapauksia, joissa tavalliset ihmiset ovat menettäneet huijareille kymmeniätuhansia euroja. Uhrilta on saatettu lypsää pienissä erissä yhteensä jopa yli 100 000 euroa.

Mitä teen, jos saan viestin, joka kertoo esimerkiksi suuresta onnenpotkusta?

- Tutki, mistä osoitteesta viesti on lähetetty (ks s. 15). Jos viesti näyttää epäilyttävältä, poista se mieluiten avaamatta tai lukematta. Viestin avaaminen välittää tiedon viestejä lähettäville automaateille, että sähköpostiosoitetta käytetään aktiivisesti. Sinne alkaa virrata entistä enemmän roskapostia.
- Älä usko viestiä varsinkaan, jos et ole osallistunut arpajaisiin tai kilpailuihin. Ymmärrä, että joku yrittää huijata sinulta rahaa. Et saa luvattua voittoa vaan menetät rahaa.
- Jos jo maksoit huijareille, ota heti yhteys poliisiin. Hyvässä lykyssä maksu ehditään pysäyttää ennen kuin se lähtee Suomesta. Pankin tilisiirto siirtää rahat pois maasta saman tien, mutta luottokorttimaksut odottavat hetken ennen kuin raha siirtyy saajalle.

-------- Alkuperäinen viesti --------

Aihe: I am a lawyer in Republic of Togo and I will like you to stand as the appointed heir to my deceased client, who had a deposit of $7.2 Million with a bank here in Togo. He died in 2005 with his family members without any registered next of kin and the funds now has an open beneficiary mandate. Upon your reply I will give you the details. Rgds, Barrister Mark

Päiväys: 27.3.2017 10:53

Lähettäjä: Bar JeanPierre Mensah <ooolity3@gmail.com>

Vastaanottaja: undisclosed recipients: ;

Vastaus osoitteeseen: Bar JeanPierre Mensah <oolity3@gmail.com>

Togolainen lakimies tarjoaa entisen asiakkaansa jättämää perintöä. Mies kuoli 2005, eikä hänellä ole perillisiä. Mieheltä jäi 7,2 miljoonan dollarin talletukset pankkiin Togossa.

Rahat on nyt tarkoitus jakaa hyväntekeväisyyteen. Lakimies lupaa lähettää tarkempia tietoja, kunhan otat häneen yhteyttä sähköpostilla.

Tällaiset viestit tunnettiin ennen nigerialaiskirjeinä. Nyt niitä on helppo levittää sähköpostilla. Tarkoitus tässäkin on lypsää rahaa hyväuskoisilta erilaisina kuluina, joita rahan lähettämisestä Suomeen huijarin mukaan koituu.

Naura hetki, ja poista sitten viesti koneeltasi.

-------- Alkuperäinen viesti --------
Aihe: terveisiä sinulle
Päiväys: 20.9.2016 18:03
Lähettäjä: Easyloan Financial Services® <hromero@corrientes.gov.ar>
Vastaanottaja:
Vastaus osoitteeseen: Easyloan Financial Company® <loanengine@gmail.com>

Hyvää päivää,
OlentunnetturouvaMariaLeo, Executiveasiamiehenhyvin tunnustettulaillinenluotonantoyhtiönEasyLoans.
Unitedmelainatarahaayksityishenkilöille
jayrityksille, jotka tarvitsevattaloudellista tukea.Onko teillähuonoluottotaitarvitsetrahaalaskut onmaksettava?Korko3%.

Jos olet kiinnostunut, täytälainanhakemus japalauttaase mahdollisimmanpianhenkilökohtaisia tietoja.

Koko nimi:
sukupuoli:
Arvioitu määrä:
kesto:
Puh:
Ymmärrätkö englantia?

Ole hyvä jaodottaakokolainahakulomakkeen,jotta voimme tehdälaskunjaaloittaalainakäsittelyhyväksyttäväksi.
Voit ottaa yhteyttämeihin:loanengine@gmail.com

Parhain terveisin,

MariaLeo.

Ottaisitko lainan tältä rahoitusalan yritykseltä?

Easyloan Financial Services lähetti yllä olevan lainatarjouksen suomalaisen henkilön sähköpostiin syyskuussa 2016.
Sähköpostin saaja pyysi lisätietoja. Kävi ilmi, että lainan rekisteröinnistä pitää maksaa 300 euroa. Kun henkilö kysyi tarkemmin rekisteröintimaksusta, Easyloan Financial Services ei enää vastannut.
Kyse oli huijausyrityksestä, jonka tarkoitus oli vähintäänkin saada uhri maksamaan huijareille 300 euroa. Lisäksi on mahdollista, että lainan ottajan tietoja olisi käytetty myös muuten. Easyloan Financial Services halusi kopion asiakkaan ajokortista tai muuta henkilötodistuksesta.

-------- Alkuperäinen viesti --------
Aihe: BUSINESS PROPOSAL
Päiväys: 17.9.2016 23:29
Lähettäjä: "Wong Shiu Ki"<info@technicka-prestavka.cz>
Vastaanottaja:
Vastaus osoitteeseen: <wong_shiuki@yeah.net>

Dear Friend,
I am Mr. Wong Shiu Ki, an Account Officer with the International Bank of Taipei and I have a very sensitive and confidential brief for you from international bank of Taipei, Taiwan. I am requesting for your partnership in re-profiling funds I will give the details, but in summary, the funds are coming via Bank of Taipei Taiwan.

This is a legitimate transaction; you will be paid 35% for your Management Fees". If you are interested, please write back and provide me with your confidential telephone and fax numbers, Country and I will provide further details and instructions. Please keep this confidential, as we can't afford more political problems. Finally, please note that this must be concluded within two weeks. Please write back promptly to my private email: wong_shiuki@yeah.net

If you are not interested kindly delete from your mailbox.

I look forward to it.
Regards,
Mr Wong Shiu Ki.

Pankkivirkailija ehdottaa yhteisiä bisneksiä

Suomalainen sai sähköpostilla bisnesehdotuksen pankin virkailijalta Taiwanista. Sen lähettäjä oli Mr Wong. Sähköpostin osoitetiedot kuitenkin viittaavat Tšekkiin. Mr Wong pyytää, ettet kerro saamastasi sähköpostista kenellekään turvallisuussyistä.
Yhteydenotosta ei käy ilmi, millaista bisnestä Mr Wong haluaa tehdä hänelle tuntemattoman suomalaisen kanssa.
Tällaisia viestejä ei pidä uskoa, eikä niihin kannata vastata. ”Mr Wongin” bisnes on huijata rahaa tai käyttää ”liikekumppania” hyväksi rahanpesussa.

"Huijausviestit ovat usein massapostituksia. Niitä on halpa levittää sähköpostilla miljoonille vastaanottajille.

Voit epäillä sähköpostia massapostitukseksi, jos vastaanottajan tieto puuttuu."

Miljoonavoitto Malesiasta tuli maksamaan naiselle 100 000 euroa

Suomalaisnainen sai sähköpostiinsa viestin, jossa kerrottiin, että hän on voittanut arpajaisissa 1,2 miljoonaa euroa. Nainen uskoi viestiä, vaikka hän ei ollut osallistut arpajaisiin.
Arpajaisvoitosta kertonut viesti tuli Malesiasta. Viestin lähettäjä kertoi, että naisen pitää maksaa rahojen siirrosta aiheutuvat kulut. Vasta sitten rahat voidaan lähettää naiselle Suomeen.
Nainen lähetti pyydetyn summan rahaa. Sen jälkeen rahapyynnöt jatkuivat eri syistä. Nainen lähetti Kuala Lumpuriin yhteensä liki 100 000 euroa. Luvattua arpajaisvoittoa hän ei ikinä saanut.

Lähde: Iltalehti 12.9.2016

Mies tarttui lainatarjouksiin – menetti nettihuijareille 130 00 euroa

Iäkäs mies sai suomenkielisen sähköpostin, jossa tarjottiin edullista lainaa. Korko oli 1 prosentti ja takaisinmaksuaika 30 vuotta.
Mies tarttui tarjoukseen, sillä hän aikoi ostaa suvun metsiä perheensä haltuun. Kaikkiaan mies neuvotteli kolmesta lainasta eri tahojen kansssa. Yksi lainan tarjoaja oli olevinaan suomalainen mies, joka työskenteli Istanbulissa Turkissa. Toinen väitti olevansa ranskalainen pankki, jolla oli suomalainen asianhoitaja. Kolmas lainan tarjoaja kertoi olevansa nainen, jolla oli oma rahasto Nigerian Abujassa.
Kun mies kyseli lainojen kustannuksista, hänelle kerrottiin, että niitä selvitellään vielä. Sen jälkeen mies alkoi saada laskuja.
– Aina oli niin, että kun tämän maksat, muita maksuja ei tule. Pian ilmeni jokin uusi, odottamaton kulu. Sellaista lypsämistä se oli. Siinä oli se houkutin, että kun vielä sen maksun hoidat, niin homma hoituu, mies kertoo.
– Se oli hirveän ovelasti hoidettu. Mukana oli virallisen näköisiä dokumentteja, ihan kuin pankki olisi myöntänyt lainan. Ne olivat keksittyjä juttuja.
Mies tarttui kaikkiin kolmeen lainatarjoukseen. Hän maksoi niistä kuluja yhteensä 130 000 euroa. Suurin yksittäinen maksu oli 5000 euroa. Lainaa hän ei koskaan saanut tililleen.

Lähde: Ilta-Sanomat 1.2.2017

"Jos et ole osallistunut mihinkään arvontaan tai kilpailuun, on hyvin epätodennäköistä, että olet oikeasti voittanut."

"Jos et tiedä mitään sukulaisesta, jonka perintöä sinulle tarjotaan sähköpostissa, sukulaista ei luultavasti ole olemassakaan."

"Lainatarjoukset, joissa sinulle tarjotaan isoa lainaa mitättömällä korolla ilman vakuuksia, ovat huijauksia. Joudut maksamaan loputtomasti kuluja, mutta lainaa et ikinä saa."

Romanssihuijaukset

Tapaat Facebookissa, deittipalstoilla tai muualla internetissä muukalaisen, joka rakastuu sinuun nopeasti ja tulisesti. Nettirakas haluaa, että sinäkin rakastut häneen ja uskot yhteiseen tulevaisuuteen, vaikket ole ikinä tavannut häntä kasvokkain.
Muukalaista ei luultavasti ole olemassa. Nettirakas saattaa olla huijareiden tekemä valeprofiili. Verkkojen auervaarat haluavat houkutella sinut rakkausansaan ja viedä sinulta rahaa.
Profiilin kuva on kaapattu jostakin netistä. Valeprofiilille on keksitty nimi ja peitetarina.
Suhde etenee nopeasti. Pian hän on tulossa luoksesi, kunhan vain autat häntä muutamassa pikku asiassa. Ne liittyvät aina rahaan: maksat matkalipun, autat maksamaan tullimaksuja tai tavaralähetyksen Suomeen, lainaat rahat rakkaasi tai tämän pojan sairaalamaksuihin.
Rakkaus roihuaa niin kauan kuin lähetät hänelle rahaa. Kun lakkaat maksamasta, rakas häviää tai alkaa kiristää sinua.
Rakkaushuijareiden uhreiksi joutuvat miehet ja naiset. Useimmat valerakkaat ovat ulkomailla asuvia ulkomaalaisia. Tietoverkkojen auervaarat voivat käyttää joskus myös suomalaisia nimiä. Opettele tunnistamaan huijarit ja valeprofiilit. Niin suojelet itseäsi ja nettiystäviäsi hyväksikäytöltä.

”Insinööri” lypsi naiselta 130 000 euroa

Nettituttavuus tuli kalliiksi varsinaissuomalaiselle naiselle. Hän menetti huijarille rahaa yhteensä noin 130 000 euroa.
Nainen tutustui kesällä 2016 internetissä mieheen, joka esiintyi englantilaisena insinöörinä. Insinööri kertoi työskentelevänsä Dubaissa. Nainen piti mieheen yhteyttä puhelimessa ja netissä.
Sitten alkoivat rahapyynnöt. Mies kertoi, että hänellä on tulossa iso urakka Dubaissa. Hän oli tilannut Kiinasta tarvikkeita. Ne kuitenkin juuttuivat tulliin. Mies kertoi, että hän tarvitsee lainaksi rahaa, jotta hän saa tarvikkeet tullista. Nainen lainasi rahat.
Rahojen saajaksi piti merkitä eri henkilö. Mies kertoi syyksi, ettei hän voi avata pankkitiliä Dubaissa.
Rahanpyynnöt jatkuivat aina eri syistä. Nainen otti jopa pikavippejä, jotta hän voi lähettää miehelle rahaa. Suurimmat miehen saamat erät olivat 20 000 euroa.
Lainoja mies ei maksanut koskaan takaisin. Nainen tajusi, että häntä on huijattu, ja ilmoitti poliisille.

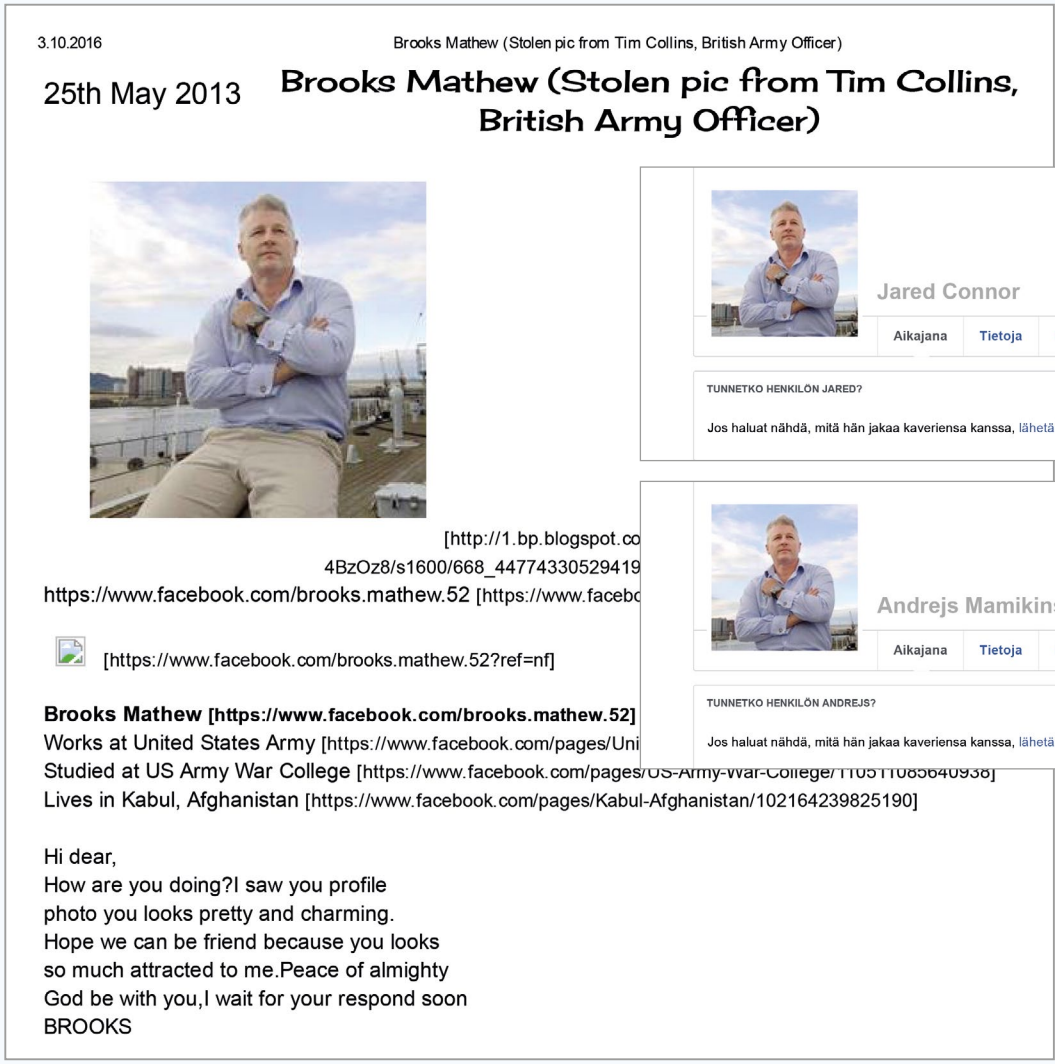
Lähde: Iltalehti 12.9.2016

Tee näin, jos saat epäilyttävän kaveripyynnön Facebookissa:

- Mieti, miksi sinulle täysin vieras ihminen haluaa olla kaverisi. Katso, onko teillä yhteisiä tuttavia, tapasitko hänet työn kautta tai yhdistääkö teitä harrastus. Löydätkö yhteyden teidän välille? Jos et, mieti, kannattaako kaveripyyntö hyväksyä. Kun torjut epäilyttävän kaveripyynnön, suojelet silloin myös kavereitasi. Huijari löytäisi kaverilistaltasi uusia, mahdollisia uhreja.
- Tutki, onko profiililla julkaisuhistoriaa ja kavereita. Jos niitä ei juuri ole, profiili on tehty äsken ja todennäköisesti huijausta varten.
- Lue, millaista kieltä profiili käyttää. Jos kieli on huonoa, se on voitu kääntää suomeksi käännösohjelman avulla. Profiilin tekijä voi olla ulkomailla, vaikka nimi olisi suomalainen.
- Tutki, käyttääkö profiili varastettua profiilikuvaa.
  Tee näin:
  - Klikkaa kuvaa hiiren oikealla painikkeella. Esiin tulee valikko, josta klikkaat Etsi kuvaa (Google). Saat tietää, millä muilla sivuilla kuvaa on käytetty.
  - Jos yllä oleva ei onnistu, käytä Googlen Kuvahakua. Klikkaa hiiren oikealla näppäimellä kuvaa. Esiin tulee valikko, josta klikkaat Kopioi kuvan osoite.
    Mene hakuohjelmalla (googlaa) sanat Google kuvahaku. Pääset sivulle, jossa on ikkuna ja siinä tyhjä rivi. Liitä siihen kopioimasi kuvan osoite. Paina vieressä olevaa kameran kuvaa. Paina Hae kuvan perusteella.

Jos kohtasit huijarin, toimi näin:

- Älä kerro hänelle yksityisasioita, esimerkiksi osoitetta ja tietoa perheestäsi.
- Älä siirry keskustelemaan hänen kanssaan kahden kesken esimerkiksi viestipalvelu Messengeriin.
- Katkaise yhteydenpito heti, jos hän alkaa pyytää rahaa. Poista valeprofiili kaverilistalta.
- Älä lähetä huijarille rahaa tai intiimejä kuvia.
- Jos lähetit jo rahaa, ota yhteys poliisiin. Älä häpeä tapahtunutta. Huijarit ovat taitavia.
- Jos sinua kiristetään seksikuvilla, kerro perheellesi, mitä voi olla tulossa. Kiristys voi jatkua, vaikka maksat.



Amerikkalainen upseeri Brooks Mathew etsii seuraa australialaisella treffisivulla. Sen mukaan Mathew työskentelee Kabulissa Afganistanissa. Brooks Mathews on valeprofiili, joka käyttää irlantilaisen everstin Tim Collinsin kuvaa.

Samaa kuvaa käyttävät myös muun muassa Jared Connor ja Andrejs Marnikins -nimiset valeprofiilit Facebookissa. Collinsin kuvalla on Facebookissa yli 100 valeprofiilia.

Katso, millaisia valeprofiilit ovat

Internetissä ja Facebookissa toimii sivustoja ja ryhmiä, jotka paljastavat valeprofiileja. Voit käydä katsomassa valeprofiileja esimerkiksi täältä:

https://www.scamwarners.com
https://scamhatersutd.blogspot.fi/
Facebookissa :
Military Love Lies and Scams
Military Photo's & More Are Being Stolen for Scammmers to Ca$h In
Romance Scammers of Ghana
ScamHaters United
Military Romance Scams
Military Imposters Awareness

Amerikkalainen eversti rakastaa sinua ikuisesti - tai ainakin niin kauan kuin rahasi riittävät

Saitko kaveripyynnön amerikkalaiselta everstiltä? Hän on komea ja luotettavan näköinen uniformussaan.
Amerikkalaisten everstien, kenraalien, lentokapteenien ja laivan kapteenien valeprofiilit ovat yksi huijausten muoto. Kaveripyyntöjä eversteiltä alkoi sataa myös suomalaisille naisille Facebookissa. Niitä eivät lähettäneet kuitenkaan sotilaat. ”Everstihuijauksien” jäljet johtavat läntiseen Afrikkaan. Siellä toimii liigoja, jotka etsivät verkossa naisia ja lypsävät heiltä rahaa. Naisten huijaaminen on suunnitelmallista ja ammattimaista.
Helsinkiläinen kansalaisaktivisti Tuula Visa on useita vuosia paljastanut Facebookin everstihuijauksia. Hän tekee yhteistyötä yhdysvaltalaisen huijareita paljastavan sivuston kanssa. Tuula Visa on kerännyt tietoa noin 300 valeprofiilista.

Visan mukaan rakkaushuijaus etenee näin:

Pehmittelyvaihe

Saat kaveripyynnön korkeassa asemassa olevalta amerikkalaiselta sotilaalta. Sotilaan kuva on varastettu netistä. Sotilaalle on keksitty nimi, sijoituspaikka ja elämäntarina.
”Eversti” kertoo elämästään. Hän on leski. Peitetarinaan kuuluu se, että nettirakkaallasi on runsaasti omaisuutta. Hän ei vain pääse siihen käsiksi juuri nyt työn vuoksi. Everstisi työskentelee siksi esimerkiksi Afganistanissa, Irakissa tai Syyriassa. Sieltä hänen on vaikea lähettää postia tai hoitaa pankkiasioita. Laivan kapteeni saattaa olla pitkällä valtamerireitillä pankin ulottumattomissa.
Eversti haluaa tietoja sinusta. Hän kysyy, oletko naimisissa, millaisessa asunnossa asut, onko sinulla uima-allas, montako autoa omistat, mikä on ammattisi ja asemasi työpaikalla. Niin hän tutkii, onko sinulla rahaa ja muuta omaisuutta.
Tutustumisvaihe kestää 4–5 viikkoa. Sinä aikana ”eversti” rakastuu sinuun tulisesti. Hän alkaa puhua yhteisestä tulevaisuudesta. Hän lupaa sinulle kartanot ja luksusautot ja ikuista rakkautta ja kaikkea kaunista. Tarkoitus on saada sinut rakastumaan ja uskomaan yhteiseen tulevaisuuteen.
Nettirakas saattaa pyytää sinua ottamaan intiimejä kuvia ja lähettämään hänelle.

Sitten tulee rahapyyntö

Pian nettirakkaasi haluaa tulla lomallaan Suomeen tapaamaan sinua. Hän vain tarvitsee rahaa lentolippuun, sillä hän ei pääse pankkiin kriisialueella, jossa hän on. Lähetät rahat lentolippuun. Hän ei pääsekään tulemaan, sillä jotakin yllättävää tapahtuu.
Hän saattaa lähettää sinulle omaisuutta postin kautta, sillä hänhän tulee myöhemmin asumaan luoksesi. Paketti juuttuukin lentokentälle. Hän pyytää sinulta rahaa vaaditun tullimaksun maksamiseen. Maksat, sillä tiedät, että laatikossa on rahaa ja kultaa.
Rakkaasi ei tule ikinä Suomeen. Rahanpyynnöt jatkuvat, aina tulee jotakin uutta, jossa vain sinä voit auttaa. Huijari lypsää rahaa niin kauan kuin maksat.

Kiristys alkaa

Jos epäröit lähettää rahaa, huijari muuttaa taktiikkaa. Hän vetoaa jumalaan ja äidintunteisiisi. Hän uhkaa itsemurhalla, jos et auta. Hän syyllistää, kun et halua auttaa, vaikka hän on pulassa. Rakkaus muuttuu kiristykseksi. Jos et maksa tai lakkaat maksamasta, alat saada uhkausviestejä.
Nettirakkaasi aikoo lähettää intiimit kuvasi lapsillesi tai työnantajallesi, jos et maksa. Hän uhkaa laittaa ne nettiin.
Jos annoit osoitteen paketin lähettämistä varten, huijari väittää, että olet osasyyllinen huijaukseen. Paketissa oli ehkä rahaa tai muuta arvokasta, jota yrititte saada Suomeen ohi viranomaisten. Säikähdät ja lopulta maksat.

Jos olet aloittanut tuttavuuden, johon liittyy Visan kuvaamia piirteitä, viisasta on lopettaa yhteydenpito ja poistaa profiili kavereistasi.

Alla olevat viestit ovat osia huijareita paljastavan Tuula Visan ja huijareiden Messengerissä käymistä keskusteluista. Viestit on käännetty käännösohjelmalla. Alun perin huijarit lähestyivät Visaa Facebookissa.

Burton Field: 8.8.2015 23:46

ello Elizabeth… Sain juuri vietin poikani opettaja Länsi-Afrikasta nyt, ja hän sanoi minun poikani oli auto-onnettomuudessa, kun hän oli hänen polkupyörällä, ja hän on ottaen sairaalaan tuolla Afrikassa ja lääkäri on antanut hänelle ensimmäinenen ensiapu hoito, jossa hän sanoi, että meidän on tallettava määrä 3258 puntaa häntä tekemään koko hoito hänen, koska hän menetti kolme pannulla verta ja hänen kaksi kylkiluuta murtuivat kuin puhun teille poikani on ja se oli vain kaksi päivää sitten kerroin hänelle, että olet hänen uusi äiti ja hän oli niin onnellinen, mutta en koskaan tiennyt jotain tapahtuisi hänelle Elizabeh rakastan häntä niin paljon hän

”Eversti” pyytää rahaa poikansa sairaalakuluihin

Burton Field -nimeä käyttävä huijari teki ensimmäisen rahapyynnön suomalaiselle naiselle, kun nettituttavuus oli kestänyt reilun kuukauden. Tarinan mukaan miehen poika loukkaantui liikenneonnettomuudessa. Pojan hoitoa varten mies tarvitsee rahaa yli 3258 puntaa eli noin 3700 euroa.

Huijari vakuuttaa rakkauttaan

Bielak Eufeniusz -niminen huijari vuodattaa rakkauttaan vuolain ilmaisuin ja sulosanoin.

Bielak Eufeniusz 21.7.2015

Tiedän nyt, että voimme tehdä jotain yhdessä, ja tiedän, että sinulla on siellä pelastamaan minut ja auttaa meitä lentämään. En ole koskaan kokenut sellaisa rakkautta, että me molemmat jakaa ja en ole koskaan ajatellut, että voisin löytää joku, joka voi sietää perheeni. Uskon todella, että Jumala itse toi sinut alas kunniaks taivaat yllä olevan ikuisesti minun enkelini. Mikään tässä maailmassa en tekisi puolestasi. Ja minä rakasta sinua ja vain sinua niin kauan kuin Jumala anna minun.

Joel Tim 5.9.2015

koska pyydän koska voin maksaa sen tänne niin he sanoivat että ei se on maksettava Lontoon heathrown lentokentälle veroksi. kiitos jos he kysyvät vain auttaa minulle maksaa heille rahaa ilman epäröintiä. Kiitos paljon huomaa myös kohteita sisällä 1,2 mijoonaa euroa rahaa ja minä luettelen ne alla Apple Laptop 1 kappale IApple 5S3 neljä kappale ja Apple table 2 , 4 samsung galaxy 351 , timanttisormus 6 kappale, 1 kultakorut laatikko ja missä sinua niin paljon kultaa. Toivottavasti sinulla on suuri päivä rakkaus.

Joel Tim -nimeä käyttävä huijari kertoo, että hän lähetti Facebook-rakkaalleen Suomeen paketin. Pakettikuitin mukaan paketissa on mm. kultaa ja 1,2 miljoonaa euroa rahaa.

Kuljetus kuitenkin juuttuu tulliin Heathrowin lentokentällä Englannissa, Joel Tim kertoo. Sinne pitää maksaa 5000 euroa, jotta paketti pääsee Suomeen. Joel Tim pyysi Facebook-rakastaan maksamaan rahat, koska hän ei pääse pankkiin Kabulissa Afganistanissa. Joel Tim työskentelee siellä Yhdysvaltain armeijassa logistiikasta vastaavana päällikkönä. Huijari käytti valeprofiilissa irlantilaisen everstin Tim Collinsin kuvaa.

10 SUOJAUDU IDENTITEETTIVARKAUDELTA

Sait puhelinlaskun, jossa on sinun nimesi ja osoitteesi mutta outo puhelinnumero. Sen perään posti tuo laskun luoton lyhennyksestä. Et kuitenkaan ole ottanut luottoa etkä tiedä mitään tietokoneesta, joka luotolla on hankittu.

Ostokset on tehnyt identiteettivaras. Identiteettivarkaus tarkoittaa sitä, että joku esiintyy sinuna tai käyttää nimeäsi ja henkilökohtaisia tietojasi.

Usein identiteettivarkauteen liittyy muita rikoksia. Tyypillisesti identiteettivaras avaa nimissäsi puhelinliittymän, ottaa pikavippejä tai tilaa tavaraa verkkokaupasta tai puhelinmyynnistä. Se onnistuu, kun identiteettivarkaalla on vain nimesi, osoitteesi ja henkilötunnuksesi.

Varas hakee postista paketit esimerkiksi väärennetyillä valtakirjalla. Laskut sen sijaan tulevat sinulle. Identiteettivaras voi myös käyttää luottokorttisi tietoja tai pankkitunnuksiasi, jos hän on saanut urkittua ne jostakin.

Somessa identiteettivaras saattaa tehdä nimelläsi valeprofiilin esimerkiksi Facebookiin, deittipalveluun tai keskusteluryhmään. Tarkoituksena voi olla kiusanteko tai mustamaalaaminen. Identiteettivaras voi esittää nimissäsi esimerkiksi mielipiteitä, jotka eivät vastaa omia käsityksiäsi.

Pidä huolta henkilökohtaisista tiedoistasi, niin riski joutua mukaan identiteettivarkauteen vähenee.

Mistä identiteettivaras saa henkilötietoni?

- roskalaatikkoon tai jätekatokseen laitetuista papereista, joissa yhteystietosi näkyvät. Esimerkiksi verotiedoissa tai potilastiedoissa näkyy henkilötunnus.
- lukitsemattomista postilaatikoista.
- varastetusta tai pudonneesta lompakosta ja sen korteista.
- pankkiautomaattiin asennetusta ns. skimmauslaitteesta.
- tietojenkalasteluviesteistä, joita saat sähköpostissa tai netin mainoksista (ks. s. x).
- soittamalla ja kysymällä tietoja. Soittaja voi esiintyä esimerkiksi poliisina tai verotoimiston virkailijana (ks. s. x).
- keräämällä sinusta tietoa esimerkiksi somesta.

Identiteettivarkaus

”Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava *identiteettivarkaudesta* sakkoon.”

Rikoslaki 38 luku 9a§

Identiteettivarkaudesta voi saada sakkoa

Identiteettivarkaudesta voidaan tuomita henkilö, joka käyttää ilman oikeutta toisen henkilötietoja tai tunnistamistietoja.

Teko on rangaistava, jos se on aiheuttanut taloudellista vahinkoa tai muuta, vähäistä suurempaa haittaa sille, jota tieto koskee. Taloudellista vahinkoa ovat esimerkiksi kulut, joita syntyy tilanteen korjaamisesta. Vähäistä suurempi haitta voi tarkoittaa sitä, että asian selvittäminen vaatii paljon vaivaa tai ei onnistu ollenkaan.

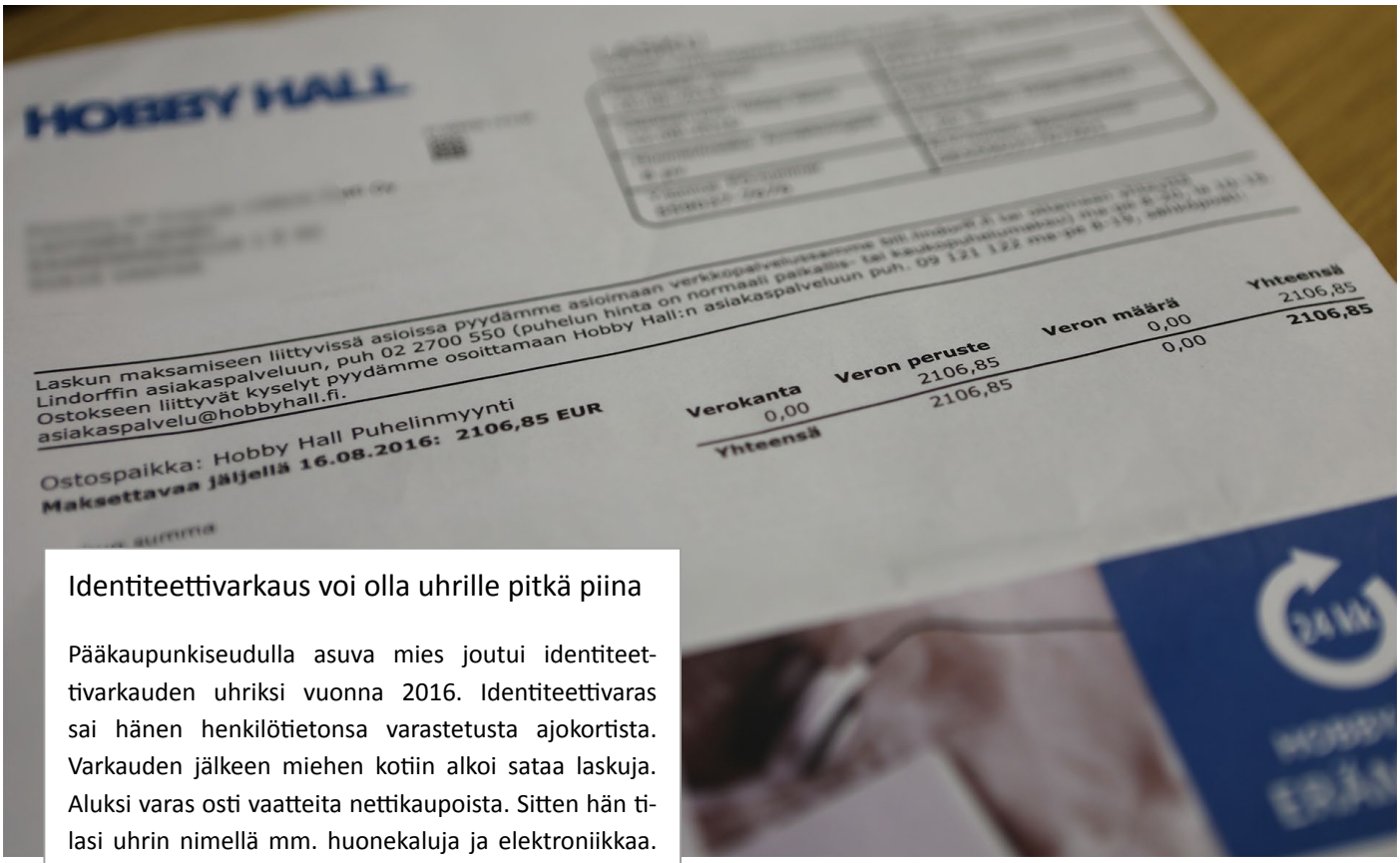
Identiteettivarkaudesta voi saada sakkoa. Identiteettivarkaus on asianomistajarikos. Poliisi alkaa tutkia asiaa vain, jos teet rikosilmoituksen.

Henkilötunnuksen voi muuttaa

Henkilötunnus on periaatteessa pysyvä tunnus. Se on tarkoitettu henkilön tunnistamiseen. Sen avulla esimerkiksi samannimiset ihmiset voidaan erottaa toisistaan.

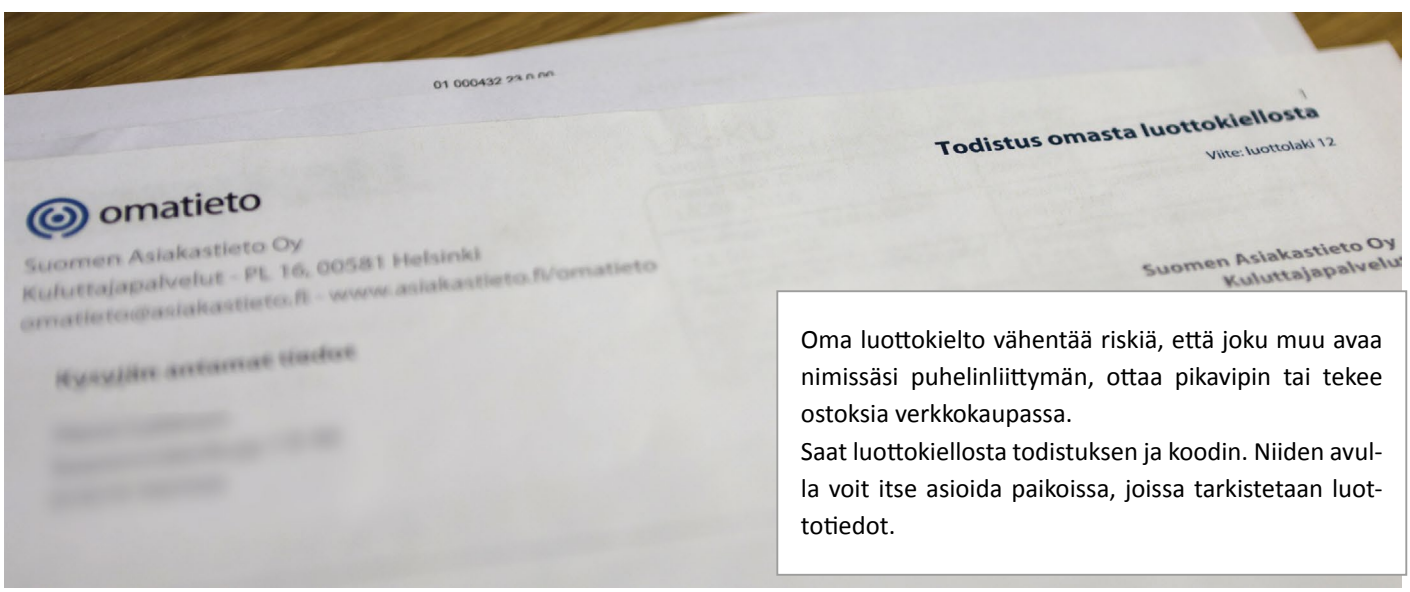
Henkilötunnuksen voi vaihtaa. Se on harvinaista, mutta mahdollista. Lain mukaan muuttaminen on sallittua esimerkiksi silloin, kun joku muu kuin henkilötunnuksen haltija toistuvasti käyttää väärin tunnusta. Näin on esimerkiksi, kun rikollinen tekee netissä petoksia nimissäsi.

Henkilötunnuksen vaihtamisesta päättää Väestörekisterikeskus. Se voi pyytää poliisilta arvion tunnuksen muuttamisen tarpeesta.



Identiteettivarkaus voi olla uhrille pitkä piina

Pääkaupunkiseudulla asuva mies joutui identiteettivarkauden uhriksi vuonna 2016. Identiteettivaras sai hänen henkilötietonsa varastetusta ajokortista. Varkauden jälkeen miehen kotiin alkoi sataa laskuja. Aluksi varas osti vaatteita nettikaupoista. Sitten hän tilasi uhrin nimellä mm. huonekaluja ja elektroniikkaa. Kaikkiaan vuoden aikana uhrin henkilötietoja käytettiin yli 70 kertaa. Tutkimuksissa kävi ilmi, että ainakin kaksi henkilöä oli käyttänyt hänen henkilötietojaan. Uhri teki jokaisesta ostosta rikosilmoituksen. Mies ei joutunut maksamaan varkaan tekemiä laskuja.



Oma luottokielto vähentää riskiä, että joku muu avaa nimissäsi puhelinliittymän, ottaa pikavipin tai tekee ostoksia verkkokaupassa.
Saat luottokiellosta todistuksen ja koodin. Niiden avulla voit itse asioida paikoissa, joissa tarkistetaan luottotiedot.

Miten estän henkilötietojeni joutumisen vääriin käsiin?

- Älä vie jätekatokseen papereita, joista henkilötietosi voi nähdä. Silppua tai polta paperit tai peitä henkilötietosi mustalla tussilla.
- Osta lukittava postilaatikko. Tyhjennä laatikko usein varsinkin silloin, kun odotat verottajalta postia.
- Pidä huoli lompakostasi. Älä pidä kaikkia tärkeitä asiakirjoja aina mukanasi lompakossa. Ota ravintolailtaan, festareille ja muihin vastaaviin tapahtumiin vain kortit, jotka välttämättä tarvitset.
- Älä levitä henkilötietojasi huolettomasti netissä (lue tietojenkalastelusta s. x). Älä kerro niitä puhelimessa kenellekään.
- Älä jaa sosiaalisessa mediassa kuvia, joissa henkilötunnuksesi näkyy.
- Tee maistraattiin tietojenluovutuskielto. Silloin identiteettivaras ei saa sieltä osoitettasi. Osa nettikaupoista hyväksyy tilausten tekemisen pelkällä osoitteella.
- Ota omaehtoinen luottokielto. Verkkokaupat, teleyritykset ja pikavippifirmat tarkastavat asiakkaiden luottotiedot. Luottotiedoissasi näkyy silloin luottokieltomerkintä. Ostosten tekeminen nimissäsi ei onnistu.

  Saat luottokiellosta kertovan todistuksen ja tunnuskoodin. Kun näytät todistuksen kaupassa tai annat koodin puhelimessa, voit itse asioida verkkokaupoissa tai tehdä luotollisia ostoksia kaupoissa.

  Luottotietorekistereitä ylläpitäviä yrityksiä on kaksi: Suomen Asiakastieto Oy ja Bisnode Finland Oy. Tee luottokielto kumpaankin yritykseen. Luotonantaja tarkastaa luottotiedot yleensä jommaltakummalta rekisterinpitäjältä.

  Bisnode Finlandin oma luottokielto on ilmainen. Sinne pyyntö luottokiellosta pitää tehdä kirjallisesti.

  Suomen Asiakastiedon omaehtoinen luottokielto maksaa parikymppiä kahdelta vuodelta. Voit ostaa sieltä myös palvelun, joka ilmoittaa joka kerta, kun luottotietojasi kysytään. Voit ostaa palvelut netin kautta.

Mitä teen, jos olen joutunut identiteettivarkauden uhriksi?

- Saat laskun ostoksista tai luotosta, joita et ole tehnyt tai ottanut. Ota heti yhteyttä liikkeeseen, josta tavara tai palvelu on ostettu. Kerro, että et ole ostanut tai tilannut tuotetta tai avannut puhelinliittymää.
- Tee rikosilmoitus poliisille. Et yleensä joudu silloin maksamaan identiteettivarkaan tekemiä ostoksia.
- Ota yhteyttä somen palvelun (Facebook, Twitter jne) ylläpitoon ja pyydä poistamaan valeprofiili. Poliisi ei saa poistaa materiaalia internetin eri palveluista.
- Voit tehdä rikosilmoituksen valeprofiilin toiminnasta. Valeprofiili on voinut tehdä nimissäsi rikoksia, esimerkiksi syyllistyä kunnianloukkaukseen.

LÄHTEET

Haastattelut:

Elenius Ville, Kyberkeskus, Vanhempi rikoskonstaapeli

Forss Marko, ylikonstaapeli, Helsingin nettipoliisi

Isabella Holm, kehityspäällikkö, Mediakasvatusseura

Juha Itkonen, ekonomisti, Suomen pankki

Risto Karhunen, johtaja, Finanssialan keskusliitto

Merja Lankinen, viestintäpäällikkö, Nets Oy

Mika Linna, johtava asiantuntija, Finanssialan Keskusliitto

Irina Lönnqvist, koulutussuunnittelija, Maanpuolustuskoulutusyhdistys

Jan Mickos, kyberturvallisuusjohtaja, CGI

Panu Moilanen, yliopistonlehtori, Kyberturvallisuus, Jyväskylän ylopisto

Tero Muurman, Kyberkeskus, rikoskomisario

Johanna Rautio, Viestintäviraston Kyberturvallisuuskeskus

Marcus Söderblom, toiminnanjohtaja, Suomen Mobiiliasiantuntijat

Teemu Tukiainen, erikoissuunnittelija, Väestörekisterikeskus

Kristiina Vainio, lakimies, Kilpailu- ja kuluttajavirasto

Tuula Visa, kansalaisaktivisti

Kirjalliset lähteet:

Forss, Marko: Fobban sosiaalisen median selviytymisopas, CrimeTime, 2014.

Haasio, Ari: Netin pimeä puoli. Suomalaisen Kirjallisuuden Seura 2013

Haasio, Ari: Koukussa nettiin: lapset, nuoret ja verkon vaarat.

Limne´ll, Jarno, Majewski, Klaus, Salminen Mirva: Kyberturvallisuus. Docendo 2014

Kyberturvallisuusohjeet ja parhaat käytännöt. Wärtsilä.

Langattomasti, mutta turvallisesti. Langattomien lähiverkkojen tietoturvallisuudesta. Kyberturvallisuuskeskus.

Mitä tulikaan sovittua? Yksityisyydensuoja internetpalveluiden sopimuksissa. Viestintävirasto. Kyberturvallisuuskeskus.

Rousku, Kimmo: Kyberturvallisuus. Tietoturvaa kotona ja työpaikalla. Talentun 2014.

Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013.

Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön 10/2014. Viestintävirasto. Kyberturvallisuuskeskus.

Tranberg, Pernille, Heuer, Steffan: Älä kerro kaikkea! Itsepuolustusopas verkkoon. Talentum 2013

Verkossa liikkujan työkalupakki. Toimi turvallisesti ja vastuullisesti. Viestintävirasto. Kyberturvallisuuskeskus.

Viestintäviraston Kyberturvallisuuskeskuksen vuosiraportti 2015

Internetlähteet:

https://peda.net/jyu/it/kyberturvallisuus/kkv

http://www.ransomware.fi/

https://www.poliisi.fi/tietoa_poliisista/poliisit_sosiaalisessa_mediassa/nettipoliisi/internetiin_liittyvia_rikoksia

www.facebook.com/kuluttajaneuvonta.fi

www.kkv.fi/kuluttajaneuvonta/

www.tietolisaaturvaa.fi

www.mustatulevaisuus.fi

www.verkkoteollisuus.fi

https://www.nets.eu/fi-fi/

http://www.asiakastieto.fi/web/fi

https://www.bisnode.com/suomi/juuri-nyt/yleista-tietoa/omaehtoinen-luottokielto/

https://www.viestintavirasto.fi/kyberturvallisuus.html

http://www.finanssiala.fi/pankkiturvallisuus/Sivut/default.aspx

http://vrk.fi/etusivu

http://www.maistraatti.fi/fi/Palvelut/kotikunta_ja_vaestotiedot/henkilotunnus/

https://www.f-secure.com/

https://www.viestintavirasto.fi/attachments/tietoturva/Salasanat_haltuun.pdf

http://www.kodindigiopas.fi/nettiyhteys/

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet.html

http://www.vaestoliitto.fi/nuoret/turvallisuus/media/

http://yle.fi/uutiset/osasto/uutisluokka/

http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html

ISBN: 978-951-25-2906-3 (pdf)
ISBN: 978-951-25-2907-0 (print)

www.turvallisuuskomitea.fi