Turvallinen netinkäyttö

Ilkka Veuro ja Tuulikki Paturi

5.3.2020 Leppävaara

Tietoiskun tavoite

- Esitellä turvalliset ja järkevät nettikäytön tavat
  - Tekemisen kohteissa
  - Salaisissa ja henkilökohtaisissa tiedoissasi
  - Näytön tarkkailussa ja havainnoinnissa
- Perustella miten tunnistat turvallisen ja järkevän

Turvaohjelmistot (ns. Virustorjuntaohj.)

- Enter ry:n opastajien näkemys tietoturvaohjelmistoista
- Tabletti: ei välttämätöntä tarvetta tai ilmainen Avast / AVG tai maksullinen kuten F-Secure Safe
- Älypuhelin: ei välttämätöntä tarvetta tai ilmainen Avast / AVG tai maksullinen kuten F-Secure Safe
- Läppäri ja tietokone: Microsoftin oma turvaohjelmisto riittää tai maksullinen kuten F-Secure Safe
- Apple-tuotteet: ei välttämätöntä tarvetta turvaohjelmistoille
- Avoimissa wifi/wlan yhteyksissä maksullinen VPN takaa turvallisuuden, vaikka käyttäisi pelkän http://osoitteen liikennettä

Kodin kyberopas:

Tärkein tietosuoja olet sinä itse

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

Panu Moilanen
lehtori
Kyberturvallisuus, Jyväskylän yliopisto

Opettele nämä asiat:

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

Testaa salasanoja

Kokeile, miten turvallisia salasanoja keksit tai käyttämiesi salasanojen rakennemuodot ovat:

https://yle.fi/aihe/artikkeli/2017/02/01/digitreenit-17-salasanakone-testaa-kuinka-nopeasti-salasana-murretaan

https://howsecureismypassword.net/

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

Kodin kyberopas:

Hyvä salasana

- Pitkä, ei monimukainen merkki&kirjain&nro -sekoite
  - 20 merkkiä tai pidempikin
  - Sanaerottimina erikoismerkkejä (!#%&) ja numeroita
- Palvelun vakavuuden perusteella joko vaikea tai hyvin vaikea salasana
- esimerkkejä
- JWW!Albatrossi1938jokaLepattamattaLiitaaTaivaansinessa
- Jtmjjmmmuvj25vy = muistisääntönä: Joulupukki tulee meille jo jouluaaton iltana mutta muualla maailmassa usein vasta joulukuun 25. päivän vastaisena yönä
- OmaKeemeilini2016aloitettuna

Vahva salasana

- Käytä pitkiä salasanoja:
  - pitkät salasanat ovat vahvempia
  - voit käyttää helposti muistettavia ilmauksia tai suosikkikappaleen, -runon tai -lainauksen sanoja.
  - välilyöntien käyttö on sallittu vain harvoin
  - ääöå ÄÖÅ ei sallittuja eli ei skandimerkkejä
- Esimerkkejä:
  - TR1915ItseTuoppiniJaljetMaTunnen [taivutus –ni, -t, -nen; slangi ma]
  - Rehe11isyys mAAn P3R11
  - 5isko tahtoisin j44d4, mutta moottoritie on kuuma
  - V@k@ vanha V@in@m0inen, tiet@j@ i@n-ikuinen

Kolme turvatasoa
1. Toisarvoiset

Salasanan rakenne: Palvelukohtainen osa + helppo vakiosana

- Esimerkiksi viihteelliset (peli)sivut, joilla vain katsellaan tai pelataan ja henkilöllisyydellä ei ole väliä.
- Sähköpostiosoitteeksi kakkos- tai kolmoisosoite, jota käyttää vain viihdepalveluihin rekisteröitymiseen.
- toisarvoisissa palveluissa voi käyttää **samaa salasanaa pienellä variaatiolla,** esimerkiksi:
  - Kissasivut.com-palvelussa salasana **Kiszingzang**
  - Lentopallo.fi:ssä salasana **Lenzingzang**

lähde MikroPC http://www.mpc.fi/neuvot/hyva+salasana++tassa+kaikki+mita+sinun+tarvitsee+tietaa/a766662

Kolme turvatasoa
2. Tärkeät

Salasanan rakenne: Palvelukohtainen osa + salalause

Pituus ennen kaikkea

- Salasanan pituus tuo enemmän turvaa kuin erikoismerkit.
- Esim. **xxxxOtaPullaaJaKahvia!** palvelukohtainen osa on xxxx ja loppu salalausetta. Esim. mallista "palvelun nimen neljä viimeistä kirjainta takaperin + salalause" on varsin vaikeasti pääteltävissä muiden palveluiden salasanat
- Tällä periaatteella Twitterin salasana voisi olla **retto**Tabullaaochc**A**hvia!

Kolme turvatasoa
3. Kriittiset

Erilliset salalauseet

- Ei mitenkään pääteltävissä muista salasanoistasi

Kriittisiä palveluita

- **sähköposti** (palveluiden salasanan palautus), **Facebook ja PayPal ja pankkien salanumerot** (käytä postinumeroiden yhdistelmää ei syntymäaikaa)
- rahallista tai muuta vahinkoa (maine, oikeus/tuomio) tuottavat palvelut

Suunnittele salasanasi

Oman salasanapolitiikan muodostamiseksi kannattaa toviksi paneutua.

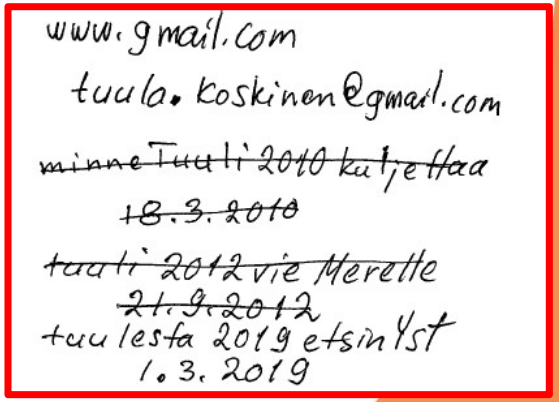
Muistat ne paremmin!

Vältä ”ääkkösiä”,

- niitä ei löydy ulkomailla hotellin koneelta
- ääå äÖÅ voivat mennä läpi salasanan vaihdossa mutta eivät toimikaan !+!

Näin säilytät salasanat

- opettele ulkoa tärkeimmät salasanasi
  - Esim. sähköpostin ja tietokoneen salasana, älypuhelimen näytön lukitus = SIM-kortin lukitus
- Taltioi salasana & tunnus & palvelun nettiosoite
  - paperille tai
  - salasanapalveluun pilveen tai
  - omalle tietokoneelle ja matkapuhelimeen salasanaohjelman avulla
    - Esim. Password Safe, KeyPass free ja F-Secure Key

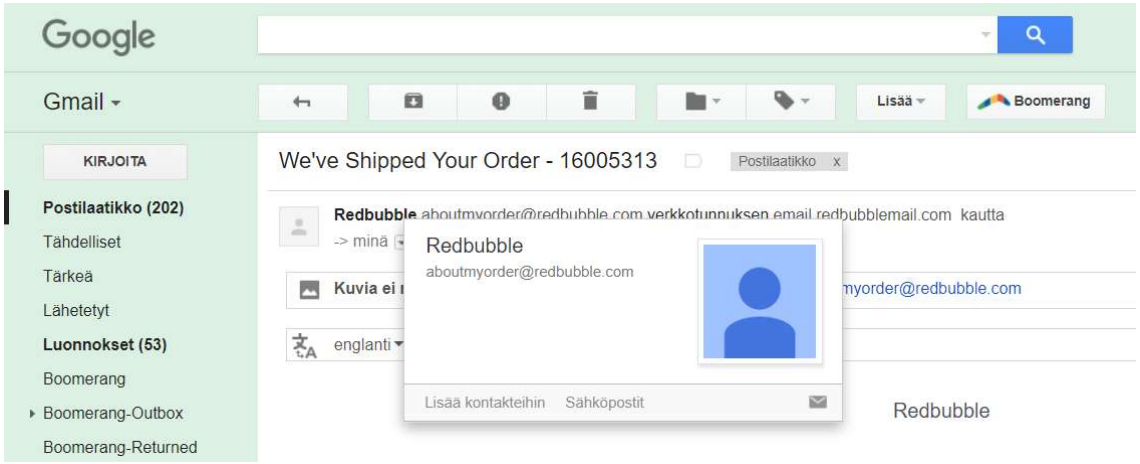


Opettele sähköpostin turvallinen käyttö

- Tarkasta sähköpostin lähettäjä
  - Todellinen lähettäjätunnus pitää olla aina näkyvissä, asetukset
- Älä avaa tai lataa tuntemattoman todellisen lähettäjän liitteitä
- Älä klikkaa sähköpostissa olevaa linkkiä
- Älä lähetä tärkeitä henkilökohtaisia tietoja sähköpostissa
  - Eräissä tapauksissa silti välttämätöntä kuten työpaikan haku jne

-------- Alkuperäinen viesti --------
Aihe: GRANT AWARD PROMOTION BY GOOGLE!!!
Päiväys: 10.8.2019 19:53
Lähettäjä: "Sundar Pichai" <pponden1@nippondenso.co.jp>
Vastaanottaja: Recipients <pponden1@nippondenso.co.jp>
Vastaus osoitteeseen: Alegre.dan.Googl@googlemail.com

Tarkasta epäilyttävän viestin lähettäjä



- Vie hiiren nuoli lähettäjän sähköpostiosoitteen päälle.
- Älä klikkaa.
- Ruudulle avautuu ikkuna tai rivi, joka kertoo, mistä sähköpostiosoitteesta viesti on oikeasti lähetetty

ESIMERKKEJÄ HUIJAUSLÄHETTÄJISTÄ

Lähettäjä Google <mail@catweb.jp>
Lähettäjä: Facebook Inc <radiouniversitaria@ufg.br>
Lähettäjä: Päivittää asiakaspalvelu@0p.fi

Aihe: Official Letter From FBI
Lähettäjä: Christopher Wray <rlavor@argo.com.br>

Lähettäjä: asiakaspalvelu@opi.fi
Lähettäjä: "Elisa" <metzgerei.geiger@gmx.de>
Lähettäjä: "Google Inc™"vendas@oceanohotel.com.br

Perusta useampi sähköpostitili

- Ensisijainen osoite asiointiin ja yhteydenpitoon, esim.
  - **etunimi.sukunimi@palvelu.xx**
- Toissijainen osoite mainosrahoitteisiin palveluihin
  - **nimimerkki@palvelu.xx**
- Käytä **tori.fi ja huuto.com** tms. palveluissa osoitetta, joka ei paljasta oikeata nimeäsi

Älä avaa tai lataa tuntemattoman lähettäjän liitetiedostoja

Älä avaa liitteitä, joiden tiedostopäätteet ovat .COM, .EXE, SHS, .PIF ja .VBS jopa .PDF

Mene palvelun internet-sivulle kirjoittamalla itse osoite,
ei käyttämällä sähköpostiviestissä olevaa linkkiä kuin varmoissa tapauksissa

- Odottamaltasi lähettäjältä (abs.läh.osoite) odottamasi viesti
- Viranomaisen turvapostin viesti

Pankki ja poliisi eivät koskaan kysy mitään henkilökohtaista tavallisella sähköpostilla

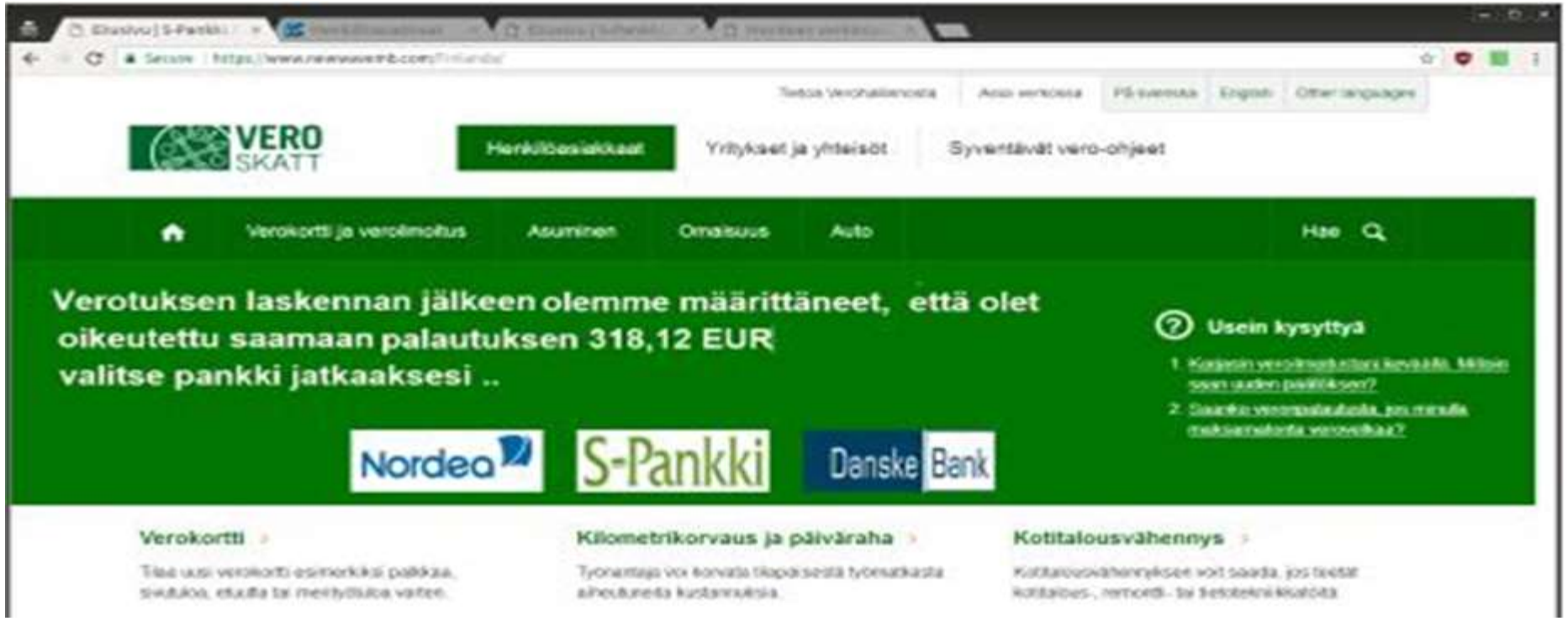
Kodin kyberopas

Älä klikkaa sähköpostin linkkiä

- Sait tuntemattomalta lähettäjältä sähköpostiviestin, jossa sinulle annetaan linkki.
- Kyse voi olla **tietojen kalastelusta** (Phishing), joka vie pankin oikeita nettisivuja **muistuttavalle** valesivulle
- Kun syötät valesivulle tietosi, ne päätyvät ulkopuolisten tietoon
- 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 linkin nimessä kerrottu osoite.

Verohallinnon nimissä lähetetty tietojenkalasteluviesti

Viestintävirasto 7.9.2017



Roskaposti

- Roskaposti on ei-toivottua, suurina massoina lähetettyä, ei kenellekään erityisesti kohdistettua sähköpostiviestintää.
- Roskaposti ruuhkauttaa sähköpostijärjestelmiä ja tukkii ihmisten sähköpostilaatikoita.
- Roskapostiviestit ovat usein mainontaa, mutta ne voivat sisältää myös tietojen kalastelua (Phishing) tai aktivoida kiristyshaittaohjelmia (Ransomware).

Roskapostin tunnistaminen

- **<u>Tarkista lähettäjä</u>** **!++!**
- Tarkastele viestin kieliasua
- Tarkista linkin osoite
- Hae tietoja viestistä ja osoitteista netistä
- Kuulostaako liian hyvältä ollakseen totta
- Sähköpostilla eikä tekstiviesteillä ei kysellä henkilötietoja, salasanoja, luottokorttitietoja jne

Suojautuminen roskapostilta

- Älä avaa tuntemattomia liitetiedostoja tai linkkejä
- Älä koskaan anna luottokortti- ja tilitietojasi sähköpostitse
- Älä vastaa roskapostiin
- Älä peruuta (Unsubscribe) viestijakelua tuntemattomilta
  - Asialliset mainostajat voi peruuttua, asiattomien peruuttamistoimi johtaa lisääntyvään asiattomaan roskaan
- Merkkaa ei-toivotut postit roskapostiksi
- Estä tarvittaessa lähettäjältä tulevat sähköpostit
- Käytä useita sähköpostiosoitteita
- Lopeta roskapostin valtaama sähköpostiosoite: **ota tilalle gmail**
  - Sähköpostin vaihto: käännä uuteen, lopeta vanha kun ei enää tarvetta

Pidä tietosi turvassa

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
- Älä laita vierasta USB-tikkua koneeseesi

F-Securen tutkimusjohtaja **Mikko Hyppönen** muistuttaa, että ainoa keino välttää vaikkapa Googlea tai Facebookia keräämästä tietojasi on olla käyttämättä niitä.

Nettiselainten yksityinen selaus -tila

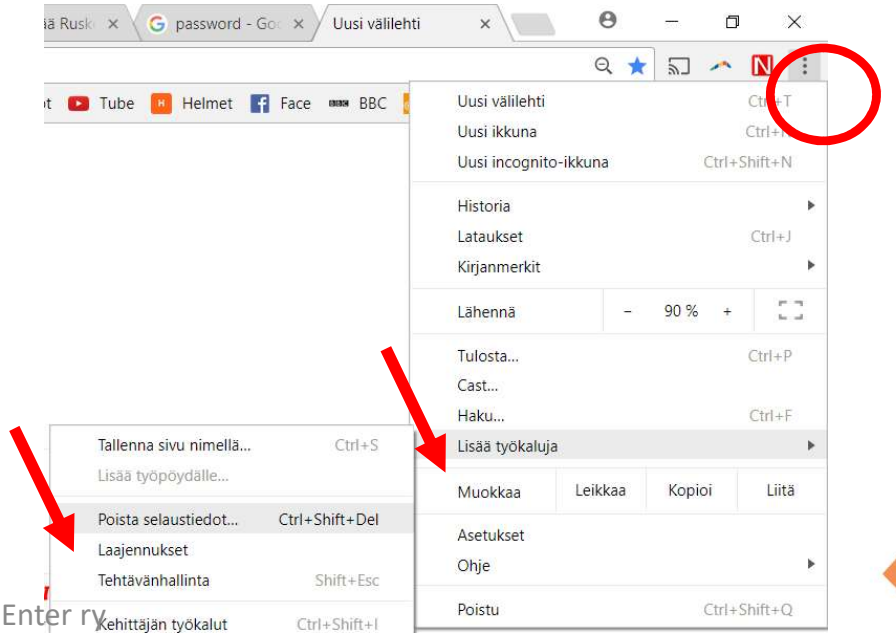
- estää selainta tallentamasta käyttäjän sivuhistoriaa, hakuhistoriaa tai evästetietoja pysyvästi käytettävään laitteeseen (puhelin, tabletti, läppäri, pöytäkone).
- tarjoaa automaattisesti tapahtuvaa tiedon poistamista, minkä vuoksi tilan käyttäminen on järkevää.
- Käyttö ei kuitenkaan estä Internet-palveluntarjoajien tai verkkosivujen suorittamaa tarkkailua, mainosten kohdentamista, haittaohjelmien toimintaa eikä monia muita yksityisyyden suojalle haitallisia toimia.

Nettiselainten yksityinen selaustila asetukset

- Google Chrome (Incognito-tila)
  - Oik.yläkulm.kolme pistettä-> Uusi incognito-välilehti (tai Ctrl+Shift+N)
- Mozilla Firefox (Yksityinen selaus)
  - Oik.yläkulm.kolme viivaa -> Uusi yksityinen ikkuna
- Microsoft Edge (InPrivate-selaus)
  - Oik.yläkulm.kolme pistettä-> Uusi InPivate-ikkuna (tai Ctrl+Shift+P)
- Microsoft Internet Explorer (InPrivate-selaus)
  - Suojaus -> InPrivate-selaus (tai Ctrl+Shift+P)
- Opera (Yksityinen selaus)
  - Opera -> Ominaisuudet -> Kohde perään välilyönti ja –newprivatetab -> OK

Älä jätä palvelua auki

- Kirjaudu aina ulos palvelusta, kun käytät yhteiskäyttöistä laitetta
- Jos et ollut yksityistilassa, poista myös selaushistoria
  - esim. Chrome



Älä usko

- Nettisivulla näkyy yllättävä varoitus tai ilmoitus
- Huomaa yläreunan Ilmoitus ”Annons”, kyseessä on mainos
- Anna vain Microsoftin itse korjata virheensä

Varmuuskopioi ahkerasti

- Henkilökohtaiseksi kohdistettu haittaohjelmahyökkäys onnistuu erittäin usein (ATP=advanced persistent threat)
- Ota varmuuskopiot säännöllisesti, viikko vai muutama päivä !
- Muistitikku tai ulkoinen kovalevy:
  - Kotona tikulla tai ulkoisella kovalevyllä tiedot säilyvät tallessa irroitettuna koneesta. Hakkerit ja tietoverkkojen murtautujat eivät pääse niihin käsiksi.
- Pilvipalvelu: Pilvestä saat tietosi käyttöön missä tahansa.
  - Haittaohjelma salaa ketterästi myös pilven tiedostot

Haittaohjelmat

Haittaohjelmat, esimerkiksi:

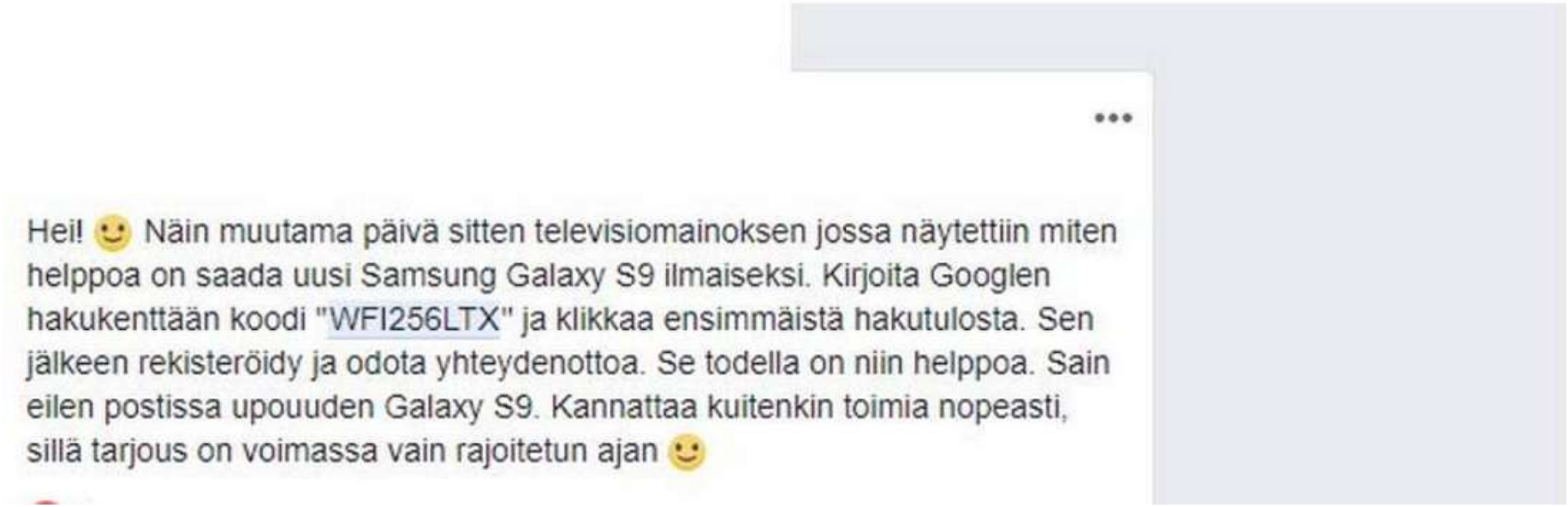
- Kiristysohjelmat – **älä maksa**
- Vakoiluohjelmat – **älä lataa netistä mitä tahansa ilmaisia ohjelmia**
- Tietojenkalastelu – **älä usko liian hyvää tarjousta**
- Tietokoneen kaappaus, palvelunestohyökkäykset – **pidä virustorjuntaohjelmisto ajan tasalla**

Huijaukset, esimerkiksi:

- Tilausansat - **älä usko liian hyvää tarjousta**
- Huijarit - **älä usko liian hyvää tarjousta**
- Romanssihuijaus – **älä usko, amerikkalainen upseeri on joukko nigerialaisia**

HUIJAUKSET | TIVI 28.10. klo 12:06

Älä missään tapauksessa klikkaa: WFI256LTX on kallis tilausansa



Pankin tekemä kortin kuoletus voi olla ainoa ratkaisu

Lisätietoja

https://www.poliisi.fi/rikokset/huijaukset/

Huijauksen monet muodot

Valepoliisi-ilmiö
Ajankohtaista tietoa uusista huijaustavoista
Nigerialaiskirjeet ja niihin verrattavat lottovoitot
Internet-kaupat
Nettirakas voi olla petollinen
Internet-rahapelit
Tilitietojen huijaaminen ja muu ns. phishing
Sijoituspetokset
Lomaosakehuijaukset
Laskun muotoon laaditut tarjouskirjeet

Pankit

- Kirjaudu itse valiten pankin internetsivujen kautta
- TÄRKEÄÄ: Älä koskaan mene verkkopankkiin painamalla linkkiä, jota sinulle lähetetään esimerkiksi sähköpostissa tai tekstiviestissä.
- Tarkasta, että yhteys pankkiin on suojattu: Selaimen osoiterivillä osoitteen alussa pitää lukea **https://, ei http://**

Verkkopankin turvallinen käyttö

- Varmista, että tietokoneen tietoturva on kunnossa (Windows 10 Defender riittää).
- Pankki ei koskaan kysele pankkitunnuksia tai turvalukuja sähköpostilla.
- Pankkihuijauksissa saatetaan kysyä useampaa peräkkäistä turvalukua.
- Lopeta istunto Kirjaudu ulos-linkistä.
- Yhteiskäyttöiseltä koneelta tyhjennä lopuksi selaimen selaushistoria.
- Tarkista säännöllisen usein tiliotteesi väärien rahasiirtojen havaitsemiseksi ajoissa.

Viesti johtaa pankin valesivulle

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

Mobiilipankki

- Älykännykässä tai tabletissa oleva pankin sovellus on turvallisempi kuin selaimen kautta kulkeva liikenne, koska sen liikennettä ei voi kaapata
- Älykännykässä tai tabletissa pitää olla näytön lukitus päällä koko ajan
- Koodissa kukin numero vain 1 kerran, 0...9 väli parempi kuin syntymäajat pp.kk, pp.kk parempi kuin 123456, postinumerot ovat välillä 0...9

Esimerkki pankin turvallisuusohjeista

https://www.nordea.fi/henkiloasiakkaat/turvallisuus/

Turvallisuus

Ajankohtaista

Älä luovuta pankkitunnusten tietoja kenellekään

Verkkopalvelujen turvallinen käyttö (pdf, 226KB)

Neuvoja

Jos pankkitunnuksesi katoavat

Jos korttisi katoaa

F-Secure Online Scanner

Tietoturva

Tietoturva | Suojaa laitteesi | Verkkouhat | Raportoi huijausyrityksestä | Korttien käyttö

Pankkiasiointi verkossa

Pankin tietoturvaratkaisut

Kolmannen osapuolen ratkaisut

Kysymyksiä ja vastaukset

Turvallinen pankkiasiointi verkossa

Nordea suojaa aina tiedot pankkisalaisuutta ja tietosuojaa koskevien lakien, määräysten ja vaatimusten mukaisesti.

Asiakkaana sinun vastuullasi on kuitenkin varmistaa, että käyttämäsi laite on suojattu ja että olet valppaana antaessasi tietoja. Asiointi verkossa on turvallista, kun huolehdit tietokoneesi tietoturvasta ja toimit vastuullisesti:

- Pidä tietokoneesi palomuuri aina toiminnassa
- Päivitä tietokoneesi virustorjuntaohjelma säännöllisesti
- Ole valppaana asioidessasi verkossa
- Säilytä ja käytä pankkitunnuksiasi huolellisesti

Vastuusi ja velvollisuutesi pankkitunnusten käyttäjänä

Lue lisää Kodin kyberoppaasta

- Mistä tiedän, että pankkitietojani urkitaan
- Mitä teen, jos epäilen, että tietokoneessani on verkkopankkiin hyökkäävä haittaohjelma
- Mitä teen, jos pankkitietojani kalastellaan

- Maksukortin lukijan salalukijan tunnistus: katso Poliisin esitys www.youtube.com Hae ”skimmauslaite”

Maksukortit

Aseta maksukortille turvarajat

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.

Käytä maksunvälittäjää

- Checkout ja PayPal ovat tunnettuja maksujen välittäjiä. Kun käytät niitä, korttisi tiedot jäävät vain maksunvälittäjän haltuun.
- Laskutuspalvelu Klarna, jos nettikauppa sitä vaihtoehtoa tarjoaa.
  - Jos maksaa heti laskun saavuttua, ei mene mitään lisämaksuja; toimii verkkokaupan ja asiakkaan välissä
  - hoitaa laskutuksen ja välittää maksusi verkkokaupalle
  - et joudu antamaan luottokorttisi tietoja
  - pääset näkemään tilaamasi tuotteet ennen kuin sinun pitää maksaa niistä. Se vähentää huijatuksi tulemisen riskiä.

Käytä turvallisen maksamisen palvelua

- Jos verkkokaupan nettisivuilla on Verified by Visa ja MasterCard SecureCoden tunnus, verkko-kauppias on liittynyt palveluun oman pankkinsa kautta.
- Ensin teet ostokset ja siirryt maksamaan verkkopankkiisi ja sen jälkeen palaat verkkokauppiaan sivuille

Voinko luottaa lähimaksuun?

- Lähimaksu lisää turvallisuutta, sillä kukaan ei pääse näkemään tunnuslukuasi

- Jos haluat lähimaksun pois, leikkaa saksilla antenni poikki

Verkkokaupat

Viestintävirasto
https://www.youtube.com/watch?v=ut9RgdGweQs

Lue Kodin kyberoppaasta:

- Näin arvioit verkkokauppoja
- EU:ssa on samat säännöt verkkokaupalla
- Tee näin, kun ostat yksityiseltä myyjältä
- Mitä teen, jos menin tilausansaan?

Kodin kyberopas

Tilausansat

Näin tunnistat tilausansat

- 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!

Kodin kyberopas

Ota some haltuun

Toimi fiksusti somessa

- Suojaa yksityisyyttäsi
- Harkitse mitä sanot tai jaat

Näin suojaat omaa, perheesi ja ystäviesi yksityisyyttä: 1/2

- 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.
- 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.

Näin suojaat omaa, perheesi ja ystäviesi yksityisyyttä: 2/2

- 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.

Tietoturva Facebookissa

- Facebook on ilmainen, mutta hintana on yksityisyyden menetys.
- Kaikki Facebookissa julkaistu tieto, kuva tai muu päivitys voi tulla julkiseksi jollakin tavalla.
- Kerran julkaistua tietoa ei saa milloinkaan kokonaan pois.
- Älä hyväksy kaveriksesi tuntemattomia henkilöitä.
- Piilota kaverilistasi, jotta et jaa kavereittesi tietoja roskapostittajille.
- Tarkista omat yksityisyysasetuksesi, mm. mitkä tiedot haluat näkyvän Vain minulle, Kavereille vai Julkisesti.
- Tarkista Näytä henkilönä -toiminnolla miten Kaverit tai Kaikki näkevät FB-profiilisi.
- Älä kirjaudu Facebook-tunnuksillasi muihin palveluihin, tietosi päätyvät mainostajille sekä FB-profiilin kaappaaja pääsee sovelluksiin.
- Laita Turvallisuus -asetuksissa Ilmoitus, jos FB-tilillesi kirjaudutaan uudesta koneesta.
- Huijarit käyttävät valemainoksia, -tarjouksia ja –kilpailuja.
- Ilmianna epäilyttävä julkaisu FB ylläpidolle julkaisun oikeasta ylänurkasta aukeavan valikon kautta.
- Poista turhat FB-sovellukset tai estä sovellukset kokonaan.

Kodin kyberopas

Suojaudu identiteettivarkaudelta

- 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. 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.

KERTAUS
10 keinoa toimia turvallisesti netissä

Massachusetts Institute of Technology (MIT) Cambridge Yhdysvallat

- Käytä vahvoja salasanoja
- Pidä ohjelmistot ajan tasalla
- Käytä tietoturvaohjelmistoa läppärissä/pöytäkoneessa
- Varmuuskopioi säännöllisesti
- Lukitse tietokone / kännykkä / tabletti
- Ole varovainen avatessasi sähköpostiviestejä ja selatessasi verkkoa
- Käytä luotettavia verkkoja
- Poista luottamukselliset tiedot
- Käytä palomuuria
- Pysy ajan tasalla tietoturva-asioissa

Järkevästi toimimalla netinkäyttö on turvallista, hauskaa ja hyödyllistä

- Tietoturva on toimintatapoja ja asenteita arkipäivän netinkäytössä.
- Tietoturva ei ole pelkästään palomuurin ja tietoturvaohjelman ajantasalla pitoa.
- On hyödyllistä ymmärtää tietoturvan merkitys ja oppia tunnistamaan erilaisia tietoturvauhkia.
- Uhkia monesti liioitellaan!

- kysymysosuus

- Jos haluat esityksen näytetyt sivut, lähetä vapaamuotoinen pyyntö sähköpostilla ilkka.veuro@kolumbus.fi

Kiitos!

Tietoiskun taustaineistoa:

www.entersenior.fi/opiskele-itse/_Tietoturva

https://turvallisuuskomitea.fi/kodin-kyberopas-ohjeita-digitaaliseen-arkeen/