Ala-Keiteleen Sydänyhdistys ry

Tietoturva ja verkon käytön riskit

Tietoturva ja salasanat

- Tietoturva ja verkon turvallinen käyttö
- Salasanojen turvallisuus
- Virusten torjunta
- Laitteen tietojen puhdistus
- Puhelimien ja tablettien turvalliseen käyttöön liittyviä asioita

Laitteiden turvallinen käyttö

- Suojaa laitteen avaaminen aina salasanalla, koodilla tai sormenjälkitunnistuksella, erityisesti puhelimet ja tabletit
- Määritä asetusten kautta laitteen näytön sammuminen ja lukkiutuminen automaattiseksi haluamasi ajan kuluttua
- Muista ottaa laitteesta varmuuskopiot ellei se toimi automaattisesti
- Huolehdi päivityksistä
- Huolehdi virusturvasta
- Älä lainaa laitetta tuntemattomille
- Jos käytät yleisissä tiloissa olevaa tietokonetta, muista tyhjentää selaushistoria äläkä merkitse salasanoja tallennettavaksi

Tarpeellisia toimenpiteitä puhelimessa ja tabletissa

- Sulje ja poista muistia ja tallennustilaa kuormittavat turhat ohjelmat.
- Siirrä kuvat ja videot puhelimesta
- Siivoa tarpeettomat tiedostot pois
- Karsi turhat luvat sovelluksilta
- Katkaise virrat kerran päivässä

Yleistä netin riskeistä

- Yleisohje – minkä kerran laitat nettiin, on se siellä ja pysyy!
- Vastuu nettiin laitetuista tiedoista on tietojen laittajalla, ainakin toistaiseksi.
- Eri palveluyhteisöjen tietovuodot hakkeroinnin kautta yhä yleisimpiä.
- Palveluyhteisöjen käyttöehdoissa suurta kirjavuutta.
- Monet palveluntarjoajat haluavat kerätä yllättävän tarkkoja tietoja.
- Vain viranomaiset, vakuutusyhtiöt ja pankit tarvitsevat henkilötunnuksia, mieti tarkkaan mihin henkilötunnuksen annat – riskinä identiteettivarkaus
- Verkossa esiintyy paljon erilaisia kilpailuja, joihin osallistumalla sitoutuu ottamaan vastaan lukuisien yhteistyökumppanien viestejä/mainoksia.
- Roskaposteja liikkuu valtaisa määrä
- Keskustelupalstoilla on helppo esiintyä väärällä nimellä ja tiedoilla
- Mikään ei ole netissä ilmaista !!

Palveluyhteisöjen tietovuodot

- Näitä esiintyy enenevässä määrin, koska vuotaneet tiedot ovat rahanarvoista tavaraa. Tällaisia tietoja ovat esimerkiksi:
  - Käyttäjätunnukset ja salasanat
  - Sähköpostiosoitteet (toimivat usein käyttäjätunnuksena)
  - Salasanat
  - Luottokorttitiedot
- Miten näihin voi suojautua:
  - Tietovuotoihin ei käyttäjä itse voi vaikuttaa, ne ovat palveluyhteisöjen vastuulla
  - Pidä huolta salasanoistasi (näistä materiaalissa myöhemmin lisää)
  - Ole tarkkana, mihin annat luottokorttisi tiedot
  - Pankkikortin tietoja ja käyttäjätunnuksia sekä tunnuslukuja ei tarvitse antaa muualle kuin pankkiin tai pankkitunnuksilla tunnistautumiseen.

Palveluntarjoajien keräämät tiedot

- Anna palveluntarjoajille vain välttämättömät tiedot.
- Pankeille, vakuutusyhtiöille ja viranomaisille henkilökohtaiset tiedot menevät vahvan tunnistautumisen kautta. Osoite ja puhelinnumero sekä mahdollisesti sähköposti ovat asioita, jotka yleensä on tarpeellista näille antaa
- Henkilötunnus vain terveys- ja muille viranomaisille
- Osoite ja puhelinnumero sekä sähköposti vain jos nämä ovat pakollisia tietoja. Verkkokaupoissa kylläkin tarpeellisia.
- Pankkikortin tietoja vain pankin sivulle ja vahvan tunnistautumisen yhteydessä
- Luottokortin tietoja vain kertakäyttöisesti, ei missään tapauksessa tallennetuksi seuraavaa kertaa varten
- Tutustu palvelun tarjoajan käyttöehtoihin.

Verkossa esiintyvät kilpailut ja arvonnat

- Verkossa ja sosiaalisessa mediassa esiintyy lukuisia kilpailuja ja arvontoja.
- Hyvin monessa näissä on käyttö- tai osallistumisehdoissa, että järjestäjällä on oikeus jakaa osallistujan tiedot yhteistyökumppaneille. Tämä aiheuttaa sähköpostien ja myyntipuheluiden tulvan.
- Jotkut arvonnat ovat pelkkää huijausta eli vain tietojen kalastelua
- Kilpailun/arvonnan "onnelliset voittajat" ovat melko usein taruolentoja
- Palkinnot eivät aina vastaa sitä, mitä luvataan, tai ne ovat esimerkiksi vanhentuvaa mallia tms

Keskustelupalstat ja kommentoinnit

- Keskustelupalstoilla ja esimerkiksi uutisten kommentoijana voi usein toimia anonyyminä tai ainakin se on helppoa väärällä nimellä.
- Mieti tarkkaan, mitä nettiin kirjoitat. Kun sen olet sinne lähettänyt, et saa sitä koskaan pois.
- Näihin kirjoitetut tekstit on helppo kopioida eteenpäin mihin tahansa ympäristöön.
- Nettikirjoittelussa on helppo esiintyä kasvottomana ja sen huomaa usein kommenteista. Teksti voi olla hyvinkin rajua.

Riskit verkkokauppojen käytössä

- Monet verkkokaupat tallentavat korttitiedot, jolloin ne on vaarassa joutua vääriin käsiin tietovuotojen yhteydessä
- Turvallisimpia verkkokauppoja ovat sellaiset, jotka käyttävät maksujen käsittelyssä kolmansia osapuolia, kuten Nets, Maksuturva, PayTrail tai PayPal.
- Varmista aina, että verkkokauppa on luotettava. Tee esimerkiksi haku ”xxx-verkkokauppa kokemuksia”
- Monet verkkokaupat edellyttävät rekisteröitymistä. Jos se ei ole pakollista, älä tee sitä ellet aio tilata samasta paikasta toistuvasti
- Jätä rekisteröityessä vain pakolliset tiedot.
- Nykyisen EU-tasoisen lainsäädännön mukaan sinulla on oikeus nähdä, mitä tietojasi on tallennettu ja voit pyytää niiden poistamista
- Varmista ennen tietojen syöttämistä, että selaimen nettiosoitteen rivillä on näkyvissä ”lukkosymboli”

Korttitiedot – verkkokaupassa maksaminen

- Turvallisin tapa verkkokaupassa maksamiseen on oman pankin palvelujen kautta maksaminen
- Luottokortilla maksamista puoltavat seuraavat seikat
  - Osalla pankeista on luottokortilla maksamiseen liitetty vakuutus
  - Jos ostaa matkoja luottokortilla ja matkatoimisto tai lentoyhtiö menee konkurssiin, saa rahat takaisin luottokorttiyhtiöltä
  - Ulkomaiset verkkokaupat hyväksyvät yleensä luottokortin ja useimmat myös pankkikortin, mahdollisesti PayPal-maksupalvelun
- Jos olet rekisteröitynyt verkkokauppaan, tarkista maksutapahtuman jälkeen, onko kortin tiedot tallennettu ”Omat tiedot” kohtaan. Jos ne on siellä, kannatta ne poistaa

Sovellusten lataaminen puhelimeen ja tabletille

- Sovellusten lataaminen on nopeaa ja monet niistä ovat ilmaisia ja maksullisetkin ovat hyvin edullisia
- Applen laitteelle sovelluksia voi ladata vain Applen omasta kaupasta eli AppStoresta
  - Apple pitää tiukassa kontrollissa, mitä AppStoren kautta jaetaan
- Anroid-pohjaisille laitteille sovelluksia saa ladattua Googlen oman GooglePlayn lisäksi muiltakin netissä löytyviltä sivuilta
  - Google kontrolloi omaa GooglePlay kauppaa ja sieltä jaettavia sovelluksia
  - Laitevalmistajien omilla sivuilla on heidän omat kontrollinsa
  - Muilla sivustoilla ei ole yleensä mitään tarkistuksia

Ohjelmien asentaminen tietokoneelle

- Tietokoneille tarkoitettujen ohjelmien tarjonta ei ole käytännössä millään tavalla kontrolloitua. Virustarkistus tietokoneella on ehdoton edellytys.
- Ohjelmia kannattaa ladata ja asentaa vain tunnetulta, ohjelmiston valmistajan omilta sivulta.
- Keskustelupalstoilta on hyvä ennakkoon tarkistaa muiden käyttäjien kokemuksia.
- Tietokoneelta on hyvä ottaa varmuuskopio ennen uuden ohjelman asentamista.

Riskit sosiaalisessa mediassa

- Sosiaalisessa mediassa tiedot saattavat levitä täysin hallitsemattomasti.
- Facebookissa on olemassa yksityisyyden rajoitukset, mutta nekään eivät takaa täyttä yksityisyyttä
- Kaikki keskustelupalstoihin kirjoitettu on vapaata riistaa!
- Kaikki minkä nettiin kirjoitat on siellä yleensä pysyvästi. Niitä on lähes mahdotonta saada pois.

Salasanat

- Miksi salasanoja tarvitaan
  - Suojaamaan henkilökohtaisia tietoja
  - Suojaamaan laitteistoa
  - Käyttäjän tai käyttöoikeuden tunnistus yhdessä käyttäjätunnuksen kanssa
- Hyvä salasana
  - Ulkopuolisille vaikeasti selvitettävä
    - Pitkä, erikoismerkkejä, ei arvattava
  - Käyttäjälle helposti käytettävä
    - Helppo muistaa jonkun muistisäännön avulla
- Huono salasana
  - Helposti arvattava.
    - Esim. syntymäaika (oma, lapsen, puolison), lemmikki, auton rekisterinumero, lapsenlapsen nimi, yms.
    - Oletussalasana, kuten 0000 tai 12345 tai qwerty
  - Helposti koneella murrettava
    - Sanakirjan sana, lyhyt, ei erikoismerkkejä, yleisesti käytettyjen listalla
    - Tunnettujen salasanojen listalla

Salasanojen luokittelu

- Erilaiset salasanoja vaativat palvelut ja sivustot voi luokitella toisarvoisiin, tärkeisiin ja kriittisiin.
- Salasana kannattaa määrittää ja säilyttää palveluluokittelun perusteella

Toisarvoisten palveluiden salasanat

- Toisarvoiset palvelut ovat sellaisia, joihin ei tallennu mitään merkittäviä tietoja itsestäsi. Esim. keskusteluryhmät nimimerkillä, yms.
- Näissä voit käyttää vaikka kaikissa samaa, helppoa salasanaa.
  - Esim. Ville55 tai palvelun nimi ja vakio-osa Veturi&Ville55
- Sähköpostiosoitteeksi osoite, jossa ei haittaa, vaikka tulee roskapostia
- Salasanat voi tallettaa omalle koneelle, jolloin niitä ei tarvitse muistaa kirjautuessa

Tärkeiden palveluiden salasanat

- Palveluun talletetaan tarkempia henkilötietoja tai muuta tietoa, jonka joutuminen vääriin käsiin olisi kiusallista tai tunnuksesi kaappaamalla voi aiheuttaa jotain muuta vahinkoa sinulle.
  - Verkkolehtitilaukset, verkkokaupat, yms.
- Salasana on pitkä, sisältää erikoismerkkejä, isoja ja pieniä kirjaimia ja numeroita. Murresanat ovat hyviä osana salasanaa.
  - Salasanassa voi olla esim. Vaihtuva osa + monimutkainen vakio-osa, esim.
    - So2ra&Viiksekäs59vNuapur
    - Il6mat&Viiksekäs59vNuapur
- Sähköpostiosoitteeksi kakkososoite, jota et käytä henkilökohtaiseen viestintään
- Salasanat voi ehkä tallettaa omalle koneelle, mikäli koneesi on suojattu lukituskoodilla

Kriittisten palveluiden salasanat

- Kriittisiä palveluita ovat sellaiset, joiden avulla sinulle on mahdollista aiheuttaa rahallista tai muuta tuntuvaa vahinkoa.
  - Viranomaispalvelut (Omakanta, Vero), sähköpostisi, tietokonetilit (Google, Microsoft, Apple, Facebook), maksupalvelut (verkkopankit, PayPal), jne.
- Salasanan tulee olla palvelukohtainen, vähintään 15 merkkiä pitkä, sisältää erikoismerkkejä isoja ja pieniä kirjaimia ja numeroita.
- Sitä ei voi johtaa muista salasanoistasi.
- Esim 1. Salalause, jossa sanat väärinkirjoitettuja, murteellisia ja sijamuotoja
  - Muistiohje (voi olla vaikka puhelimen muistiossa): Missä on mökkini!
  - Salasana: MullapaOnTup4nenRisuSaaresa!
- Esim 2. Muodostamissääntö ja Muistilause
  - Sääntö: yksittäisistä sanoista poimitaan alkukirjain (myös yhdyssanoista). Sanan alkukirjain isolla, muut pienellä.
  - Muistilause: Kuukkelin posti ja mummon osoite
  - Gmailin salasana: Kuukkelinposti & Rovaniemi Nivavaara Matkavaarantie 23 A 7 !
  - Salasana: Kp&RnNvMvt23A7!
- Älä talleta näitä salasanoja koskaan koneelle ja tai pilvipalveluun
- Käytä kaksivaiheista tunnistusta, jos mahdollista.
- Sähköpostiosoitteena henkilökohtaisessa viestinnässä käytetty

Salasanojen muistaminen

- Paperilapulle
  - Talletettuna lukittuun paikkaan
  - Ehkä jotenkin koodattuna (oma sääntö)
- Tallennus koneelle
  - Salasanaohjelmaan voit tallettaa kaikki salasanat. Jos et käytä sitä, niin:
  - Vain toisarvoiset ja ehkä tärkeitä
  - Ei koskaan kriittisiä salasanoja
  - Tallennetut salasanat on helppo selvittää koneelta, ellet käytä pääsalasanaa
  - Laita selaimen asetukset sellaiseksi, että se ei automaattisesti tallenna kirjautumistietoja (käyttäjätunnus ja salasana). Kiellä tallennus kokonaan tai aseta niin, että tallentamiselle kysytään aina sinun hyväksyntäsi. Ole huolellinen antaessasi hyväksynnän.
- Koneelle tallennettujen salasanojen varmuuskopiointi pilvipalveluihin
  - Riski, että joku taho hyödyntää tietoa
  - Ei kannata tallettaa kriittisiä salasanoja

Pääsalasana

- Jotkut selaimet (Esim. Firefox) tarjoavat mahdollisuuden suojata tallennetut salasanat ns. pääsalasanalla.
  - Kun asetat pääsalasanan, tallenna se johonkin turvalliseen paikkaan.
- Toiset (esim. Edge, Chrome ja Opera) suojaavat salasanat tilin tai koneen lukituskoodin avulla. Jos ne tietää niin pääsee katsomaan tallennetut salasanat

Salasanageneraattorit

- Ohjelmia, jotka generoivat puolestasi halutun mittaisia salasanoja.
  - Eivät usein kovin käytännöllisiä, ellet käytä tallennusta ja automaattitäyttöä, tai tallennussäilöä ja kopioi/liitä komentoparia.
- Viestintävirastolla on tarjolla oma salasanageneraattori, jolla voi kokeilla, miten hyödyntää sattumanvaraisuutta salalauseen valitsemisessa. Se löytyy osoitteesta www.pidempiparempi.fi

Salasanaohjelmat

- Salasanaohjelmat hallinnoivat salasanojasi ja/tai suojaavat ne yhden salasanan (pääsalasanan) taakse.
  - Tarvitsee muistaa vain yksi salasana. Sen rinnalla on mahdollista käyttää myös sormenjäljen tai kasvojen tunnistusta, mikäli laite tukee niitä.
  - Selvitä, miten pääsalasana palautetaan (QR-kuvalinkki tai joku muu tapa)
- Ohjelmia on mahdollista käyttää pelkästään suojattuna salasanasäilönä.
- Uusien salasanojen generoinnin ja hallinnan voi antaa ohjelman tehtäväksi.
  - Aina kun rekisteröidyt palveluun, ohjelma luo ja tallettaa halutessasi palvelun salasanan, jota ohjelma myöhemmin käyttää, kun kirjaudut palveluun..
  - On mahdollista (usein maksullisissa versioissa) synkronoida salasanat kaikille laitteillesi, jotka käyttävät kyseistä salasanaohjelmaa
  - Voit sallia myös automaattisen kirjautumisen sivuille, joiden salasanat ohjelma tietää
  - Sinä itse päätät mitä salasanoja ohjelma tallettaa ja hallinnoi
- Luotettavia ja helppokäyttöisiä (tutustu huolella käyttöohjeisiin)
- Voit tallettaa salasanasäilöön myös muita tietoja (esim. luottokortin numerot)
- Last Pass, True Key, Dashlane, Kaspersky, 1Password ,F-secure Key.

Jos unohdat salasanasi

- Palvelun tarjoajan ”Unohditko salasanasi” –palvelu
  - Kirjataan rekisteröityessä palautuksen sähköposti tai puhelinnumero, johon varmennus (vahvistuslinkki, koodi, yms.) lähetetään
- Määrätään tunnistus tehtäväksi kaksivaiheinen tunnistuskoodin avulla.
- Kirjataan varmennuskysymys ja sen vastaus
  - Esim. Mummosi tyttösukunimi (ehkäpä vielä väärä tai väärin kirjoitettu)
- Toiminta unohtaessa
  - Valitse ”Unohdin salasanani” toiminto ja seuraa ohjeita.
  - Vastaa varmennuskysymykseen, tai kirjoita tekstiviestillä puhelimeen, tai sähköpostiin lähetetty koodi, tai klikkaa sähköpostiin lähetettyä linkkiä
  - Määritä uusi salasana ja vahvista se.
  - Tallenna uusi salasanasi itsellesi talteen
  - Jos palvelun salasana on tallennettuna usealle käyttämällesi laitteelle, määritä uusi salasana myös niihin, ellei se synkronoidu automaattisesti.
  - Joissakin palveluissa tunnistaudutaan uudelleen pankkitunnuksilla tai mobiilivarmenteella. Tunnistautumisen jälkeen määritä uusi salasana ja muista se.

Kaksivaiheinen tunnistautuminen

- Yleensä verkkopalveluun kirjaudutaan kahdella tiedolla:
  - Ensin käyttäjätunnus
  - Sitten salasana.
- Kaksivaiheisessa tunnistautumisessa tietoja annetaan yksi lisää.
- Usein tähän tarkoitukseen käytetään PIN-koodia tai vastaavaa tunnusta, joka on kertakäyttöinen
- Lisätunnistuskoodi annetaan joko
  - Puhelimeen tekstiviestinä tai ilmoituksena
  - Sähköpostiin
  - Toiseen käyttäjän ennalta ilmoittamaan laitteeseen
- Eri palvelut käyttävät hiukan eri termejä, Kaksivaiheinen *tunnistautuminen*, *vahvistus* ja *todennus* ovat kuitenkin sama asia
- Palvelun tarjoajista osa antaa ensin eri vaihtoehdot valittavaksi ja lähettää sen jälkeen kertakäyttöisen koodin tai viestin käyttäjän haluamalla tavalla

Virusten torjuntaohjelmat

- Virustorjunta on tarpeellista Windows –järjestelmissä sekä Anroid-pohjaisissa älylaitteissa (puhelin, tabletti)
- Applen järjestelmiin kohdistuvat virukset eivät ole niin yleisiä kuin Windows-järjestelmiin. Virustorjunta on silti suositeltavaa
- Virustorjuntaohjelmia on sekä ilmaisia että maksullisia
- Ilmaiset virusturvaohjelmat selviytyvät perustason suojauksesta, mutta ne ovat itseasiassa maksullisten versioiden mainosversioita, joilla houkutellaan asiakasta ostamaan maksullinen versio.
- Maksulliset versiot ovat monipuolisempia kuin ilmaiset perusversiot ja niihin on saatavissa 1-3 tai jopa useampia lisenssejä yhtenä pakettina

Tunnetuimpia virustorjuntaohjelmia

Windows ympäristö (ilmaisia)

- F-Secure Safe
- Avast Free Antivirus
- Norton Antivirus
- McAfee Internet Security
- Microsoft Windows Defender
- Kaspersky Internet Security
- Avira Antivirus Pro
- ym

Anroid-laitteet

- Bitdefender mobile security
- Norton mobile security
- Avast mobile security
- ESET mobile security
- F-Secure Safe
- Norton

Applen Mac-laitteet

- F-Secure Safe
- Norton
- Bitdefender mobile security
- McAfee

Apple iPhone ja iPad -laitteet

- F-Secure Safe
- Norton
- Bitdefender mobile security
- McAfee

Tietokoneen ja älylaitteiden tietojen puhdistaminen ja ylläpito

Tietokone

- CCleaner
- Bleachbit
- Avast Cleanup
- Avast Driver Update
- EasyCleaner
- Fcleaner
- HDCleaner

https://neptunet.net/tag/puhdistusohjelmat/

Puhelin ja tabletti

- CCleaner
- Avast Cleanup
- Clean Master
- DU Speed Booster & Cleaner
- Go speed
- Power Clean
- Ace cleaner

https://fossbytes.com/best-android-cleaner-apps/

Virustorjunta ja siivousohjelmat

- Useimmista ohjelmista on saatavissa sekä ilmainen että maksullinen versio.
- Monet ilmaiset versiot tuovat näytölle ilmoituksia ”löytämistään uhkista”, jotka saa poistettua vain maksullisella versiolla. Nämä eivät ole kaikki todellisia uhkia vaan myyntikikkoja
- Myös maksulliset ohjelmat saattavat tuoda näytölle vastaavia ilmoituksia ja usein ne liittyvät maksullisen version laajentamiseen
- Tietokoneelle ja älylaitteelle voisi olla suositeltavaa ainakin Ccleaner, joka ei paljoa turhia ilmoituksia näytölle tuo
- Kaikki tällaiset ohjelmat päivittyvät melko usein ja niistä tulee näytölle päivitysilmoituksia, jotka ovat aiheellisia

Mitä teen kun koneeseeni tulee virus?

- Jos virusohjelma varoittaa viruksesta tai epäilet itse sitä, niin:
  - Tutki tarkemmin virusohjelman ilmoitusta ja seuraa ohjeita.
  - Päivitä viruskuvaukset, skannaa virukset ja seuraa poisto-ohjeita.
  - Jos ongelma ei poistu, kokeile jotain puhdistusohjelmaa (CCleaner. tms)
  - Hae netistä ohjeita ja kokeile niillä
  - Jos em. keinot eivät, hanki apua
- Jos kone jumiintuu ja tulee jokin virusilmoitus ja/tai kiristysviesti, niin:
  - Katkaise verkkoyhteys ja sammuta laite.
  - Jos osaat, niin hae netistä ohjeita (toisella koneella) ja yritä poistoa
  - Jos et osaa, niin hanki apua.
- Ennakoi virusuhka
  - Varmista, että koneessa on käynnissä oleva virusohjelma (ilmoitukset)
  - Asenna etenkin järjestelmäpäivitykset, mutta myös sovelluspäivitykset, sitä mukaa kuin niitä tulee. Näin varsinkin silloin kun ne korjaavat tunnetun haavoittuvuuden.
  - Pidä varmuuskopiot ajan tasalla. On viruksia, joista eroon pääsy vaatii koneen täydellisen uudelleen asennuksen (tietokoneet) tai tehdasasetusten aktivoinnin (Android ja muut älylaitteet, esim. tv). Näissä tilanteissa menetät kaikki omat tietosi, ellei niitä ole tavalla tai toisella varmuuskopioitu.

Roskapostin poistaminen

- Roskapostit ovat yleinen ja aina kasvava ongelma
- Suurin osa eri sähköpostiohjelmista suodattaa roskapostit automaattisesti, mutta toiminta ei ole 100 prosenttista. Gmail ja Outlook ovat ehkä tehokkaimpia tässä tehtävässä.
- Tietokoneella sähköpostia käytetään yleisimmin jollain selaimella (Chrome, Firefox, Explorer, Opera…)
- Älypuhelimessa ja tabletissa on yleensä valmiina joku sähköpostisovellus ja sellaisia voi ladata lisää. Esimerkiksi Android –laitteissa Gmail-sovellus
- Sähköpostijärjestelmiä on lukemattomia. Yleisimpiä ovat:
  - Googlen Gmail
  - Yahoo
  - Microsoftin Outlook
  - @pp.inet.fi
  - @kolumbus
  - @welho

Roskapostin suodatus Gmail:ssa tietokoneella

- Saapunut sähköposti merkitään Roskapostiksi tulleen postin listan yläpuolella olevalla kuvakkeella.
- Valitse ensin roskapostiksi haluamasi viestit ruksaamalla viestin alussa oleva valintaruutu
- Klikkaa seuraavaksi listan yläpuolella olevaa ”huutomerkkikuvaketta” ja klikkaa vielä kohta *(Ilmoita roskapostista)*
- Gmail ohjaa vastaavat viestit jatkossa suoraan Roskapostikansioon
- Saman voit tehdä siirtämällä tulleen viestin hiirellä vetämällä roskapostikansioon

Roskapostin suodatus Gmail:ssa puhelimella ja tabletilla

- Anroid-pohjaiset laitteet
  - Valitse listalta ne viestit, jotka katsot roskaposteiksi ja kosketa sen jälkeen oikealla ylhäällä näkyvää kolmen pisteen kuvaketta. Valitse valikosta "Merkitse roskapostiksi"
  - Näkyvän viestin otsikon perässä on myös kolmen pisteen kuvake. Sitä koskettamalla saat esille valikon, josta voit valita "Estä xxx.xxxxx"
- Applen laitteet
  - Valitse tulleitten viestin listan yläpuolelta *Muokkaa* –komento ja merkitse viestien eteen ilmestyneet ympyrämerkit niiden viestien kohdalla, jotka haluat siirtää Roskapostiksi.
  - Valitse vasemman reunan viestien alla olevasta kohdasta *Siirrä* ja sen jälkeen avautuvasta kansiolistasta Roskakori
- Älä avaa viestiä, joka vaikuttaa hyvin epäilyttävältä (virusvaara!) Tuhoa tällaiset viestit tai siirrä ne suoraan *Roskaposti* –kansioon
- Huom! Roskakori ja Roskaposti ovat eri asia

Tarpeettomien viestien vähentäminen

- Jos joltakin lähettäjältä saapuvat viestit eivät enää ole tarpeellisia tai ne eivät kiinnosta, voit tehdä seuraavaa:
  - Jos viestin lähettäjän kohdalla näkyy teksti ”Peru” tai vastaavaa, kosketa tai klikkaa kyseistä kohtaa niin tieto menee lähettäjälle, joka voi poistaa sinut listalta.
  - Viestin lopussa saattaa olla pienellä kirjoitettuna ”Jos et halua…. Peruuta…” tai vastaavaa (englanniksi Ubsubscribe). Sitä kautta saat myös viestien lähetyksen peruttua (ehkä ..)
  - Näitä keinoja ei kannata suin päin käyttää muiden kuin kotimaisten palvelujen kohdalla ellet ole varma, että viesti ei ole roskapostia.
  - Jos roskapostia yrittää peruuttaa vastaamalla viestiin, yltyy roskapostien tulo kyseiseltä lähettäjältä entisestään!

Roskaposti / Mainosposti / Käyttövinkit / Ilmoitukset

- Mainosposti ja käyttövinkit ovat usein sellaista postia, jonka olet itse tietoisesti tai tietämättäsi tilannut. Ne tulevat ”tutulta” taholta, jonka kanssa olet asioinut.
  - Saat ne useimmiten estettyä käymällä lähettäjän sivuilla asettamassa mainonnan ja viestinnän asetukset sellaiseksi, että viestejä ei enää lähetetä.
  - Usein viestin lopussa on linkki, jonka kautta voit estää vastaavat viestit
- Roskaposti tulee sinulle tuntemattomilta lähettäjiltä
  - Estäminen lähes mahdotonta sen jälkeen kun sitä alkaa tulemaan
  - Älä ikinä vastaa näihin viesteihin ja avaa niiden linkkejä. Tuhoa ne avaamatta. Viestiin reagoiminen on merkki siitä, että joku lukee posteja > lähettäminen kiihtyy.
  - Voit saada roskapostia ilman omaa syytä. Lähettäjä on saanut osoitteesi jostain.
- Roskaposteilta välttyminen
  - Älä rekisteröidy epämääräisille sivuille, joissa kysytään sähköpostia. Jos kuitenkin rekisteröidyt, niin käytä mahdollista roskaposteja varten erillistä sähköpostiosoitetta.
  - Älä lankea ilmoituksiin, että olet voittanut jotain.
  - Älä vastaa kyselyihin, joissa luvataan vastaamisesta palkkio.
- Puhelimeen tulevat ilmoitukset voit säätää asetuksista sovelluskohtaisesti.
- Hanki uusi sähköpostiosoite, jos henk.koht. viestinnän osoitteesi ”saastuu”.

Sovellusten asentaminen Anroid-pohjaiselle laitteelle

- **Androidin** käyttöjärjestelmä ei ole suljettu, kuten **Applella**. Android-puhelimeen saa asennettua sovelluksia monenlaisista lähteistä.
- Joillakin laitevalmistajilla, kuten Samsungilla, on jopa oma sovelluskauppa. Se on esiasennettuna monissa malleissa.
- Sovelluksia voi asentaa monista muistakin paikoista, kunhan laitteelle antaa siihen luvan.
- Netistä löytyy monia niin sanottuja **kolmannen osapuolen sovelluskauppoja**. Suurin niistä on Amazon Store.
- Sovelluksia saa myös täysin **epävirallisista lähteistä**. Esimerkiksi suositun Pokemon Go -pelin laiton versio sisälsi haittaongelmia.
- Sovellusten *tuntemattomat lähteet* eivät automaattisesti ole haittaohjelmien pesäkkeitä. Peruskäyttäjälle ohje on silti selkeä:
- **Älä asenna sovellusta mistä vain, vaan käyttöjärjestelmän virallisesta sovelluskaupasta.** Android-laitteen käyttäjälle se on **Google Play**.

Android-laitteissa pyörii automaattisesti suojaustoiminto Google Play Protect. Se tarkistaa Play-kaupasta ladattuja sovelluksia ja varoittaa mahdollisista haitoista.

Sovellusten ja ohjelmien käyttöoikeudet

- Puhelinten ja tablettien sovelluksille ja tietokoneiden ohjelmistoille voidaan asettaa rajoituksia eri toimintojen käyttöoikeuksiin. Rajoitukset löytyvät Asetuksista, mutta eri laitteissa eri paikoista.
- Mieti, mitkä sovellukset saavat käyttää esimerkiksi kameraa ja mikrofonia, entä sijaintitietoja.
- Esimerkiksi Googlen Chrome käyttää oletusarvoisesti kameraa, mikrofonia, sijaintitietoa ja tallennusta. Ehkä tallennus on näistä latausten tekemiseen tarpeellista.
- Kamera -sovellus toimii oletusarvoisesti samoin. Onko tarpeellista vain kamera ja tallennustila? Sijaintitiedon käyttäminen kuvissa tuo kenties lisäarvoa maisemakuvauksessa, mutta ei välttämättä sisätilojen kuvaamisessa.

Sijaintitietojen salliminen/kieltäminen

Älypuhelimissa ja tableteissa voidaan Sijaintitiedot asetusten kautta

- sallia aina
- Sallia vain sovellusta käytettäessä (suositeltavaa sovelluskohtaisesti)
- Estää kokonaan

Hyödyt

- Tarpeellinen esimerkiksi navigaattorin yhteydessä ja karttapalveluissa yleensä
- 112-palvelu onnistuu paikannuksessa
- Sovellukset voivat lähettää ajantasaista tietoa paikallisista palveluista ja esimerkiksi liikenteen sujumisesta (V-Trafi), säätiedoista ja ennusteista (Foreca, Ilmatieteenlaitos)
- Voit tarvittaessa jakaa sijaintitietosi muille käyttäjille (Google Maps)

Haitat

- Sovellukset ja laitevalmistajat saavat tietoonsa sijaintipaikkasi ja sen avulla esimerkiksi mainontaa pystytään kohdentamaan tarkemmin ja tehokkaammin.
- Sijaintipaikan paljastuminen joissakin valokuvissa ei ole ehkä tarpeellista. Esimerkiksi kuva matkalta otettuna ja tallennettuna Someen antaa muille tiedon, ettet ole kotona.

Jos sijaintitiedot eivät ole sovelluksen toiminnan kannalta oleellisia, kannattaa ne laittaa pois päältä.

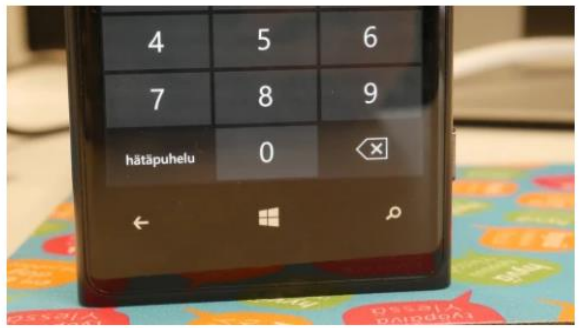
Sijaintitietojen hallinta

- Anroid-pohjaiset laitteet
  - Android 6.0. ja sitä uudemmat versiot (puhelimia esimerkiksi Samsung, Huawei jne. polku voi hieman vaihdella laitteesta toiseen):
  - Asetukset > Sovellusten hallinta / Sovellukset > valikko (kolme pistettä) > Sovelluksen oikeudet > Sijainti > valitse, mille sovelluksille haluat antaa oikeudet.

- Jos puhelimessasi on **Google Maps**, se tallentaa sijaintitietoja aikajanalleen, jollet ole sitä erikseen kieltänyt.
- Katso, missä olet liikkunut. Sinun pitää kirjautua sivulle samoilla tunnuksilla, joilla käytät Googlen palveluita puhelimellasi. Voit poistaa sijaintihistorian puhelimen Google Maps-sovelluksesta:
- *Google Maps > Valikko > Asetukset > Henkilökohtainen sisältö > Poista koko sijaintihistoria.*
- Voit kieltää Google Mapsia tallentamasta sijaintihistoriaasi valitsemalla *Henkilökohtainen sisältö* -kohdasta **Sijaintihistoria ei ole käytössä.**

Muutamia hyödyllisiä tietoja puhelimen käyttöön

Samsung-puhelimen lukitusnäyttö: Punaisesta luurista pääsee hätäpuheluun. Kuva: YLE



Windows-puhelimen lukitusnäyttö. Kuva: YLE

- Kenttä hukassa tai näyttö lukossa
  - Voit aina soittaa 112-hätänumeroon, vaikka oman operaattorisi verkko olisi kateissa tai puhelin lukittuna
  - Lukitusnäytöltä numeronäppäinten alta löytyy teksti tai kuvake, josta pääsee hätänumeroon.

Ehdoton sovellus: 112 Suomi

- Lataa tilalle ilmainen 112 Suomi -sovellus. Sen avulla hätäkeskus näkee sijaintisi, vaikka et tietäisi tarkkaa osoitetta.
- 112 Suomi perustuu satelliittipaikannukseen. Se yltää parhaimmillaan alle kymmenen metrin tarkkuuteen
- Tallenna sovellukseen oma puhelinnumerosi. Ja mikä tärkeintä: Muista myös soittaa hätäpuhelu 112 Suomi -sovelluksen kautta.
- Sovellus osaa hakea paikkatiedon ilman nettiyhteyttä. Hätäkeskus ei kuitenkaan näe koordinaattejasi, ellet soita sovelluksesta - nettiyhteys auki.
- Älä hermostu, jos sovellus ohjaa sinut vielä puhelimen omaan soittonäkymään - näin käy joissakin Android- puhelimissa. Sieltä vain 112:lla eteenpäin.
- Lisää yhteystietoihin ns. ”ICE nimi” –numeroita, joissa läheisesi nimen yhteydessä on ICE nimen edessä (ICE = In Case of Emergency)
  - Hätätilanteessa pelastusviranomaiset osaavat hakea ICE –numeroita, jos on tarvetta ottaa yhteyttä läheisiin