Tietoturva päivittäisessä työssä

Tietoturva työpisteellä tietoiskut

Millaisia asioita tulee eteen työpaikan arjessa tietoturvan osalta

Nämä ovat tietoturva työpisteellä -tietoiskujen esityskuvat. Esityskuvan jälkeen on selittävää tekstiä tukemaan aineiston itsenäistä selaamista.

Esitys sisältää Helsingin kaupungin työtehtävissä tarvittavat tietoturvan osaamisen yleistiedot.

Tietoturva työpisteellä -tietoiskut on julkaistu videoina Helsinki-kanavan tietoturva työpisteellä -sarjassa.

Helsinki

Tietoturva päivittäisessä työssä

Muutama peruskäsite

Luottamuksellisuus ..... **tiedon salassa pito**
Tieto varjellaan asiattoman ulottuvilta

Eheys ..... **tiedon luotettavuus**
Tieto säilyy sellaisena kuin se on tarkoitettu, eikä vääristy

Saatavuus ..... **tiedon käytettävissä oleminen**
Tieto on saatavilla silloin kun sitä tarvitaan

Todennus ..... **käyttäjän tunnistaminen**
Tiedetään varmasti kuka tietojen käyttäjä on

Kiistämättömyys ..... **käytön todentaminen**
Voidaan varmistua siitä mitä tietojen kanssa kukin on tehnyt

Vaatimusten mukaisuus ..... **käyttöympäristön hyväksyminen**
Tietojenkäsittely tai järjestelmä vastaa niitä vaatimuksia mitkä sille on määrätty.
Esimerkiksi korttimaksamisen teknisten vaatimusten mukaisuus.

Helsinki

Lisätietoja esimerkiksi Sanastokeskus TSK ry:n TEPA-termipankista ja kyberturvallisuuden sanastosta
http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Tietoturva ja muut asiat

Tietoturva liittyy moneen asiaan, mutta kaikki tietojenkäsittely ei ole tietoturvaa. Tietosuojaan (henkilötietojen suojaamiseen) liittyy tietoturvajärjestelyt, mutta myös muut asiat kuten hyvä hallinto. Tietotekniikka on muutakin kuin tietoturvaa. Myös tietoturva sisältää itsessään monia ulottuvuuksia – jo pelkästään tekninen ja hallinnollinen tietoturva vaativat erilaisia osaamisia toteuttajiltaan.

Oman työsi sujuvuuteen liittyvään tietoturvaan saat perusasioita näistä tietoturva työpisteellä tietoiskuista.

Tietoturva liittyy niin digitaalisten tietojen turvaamiseen kuin tietojen turvaamiseen paperilla, kuvissa, keskusteluissa, kaikissa tilanteissa ja paikoissa.

Helsinki

Helsingin tietoturvassa onnistumisen perustana

Vastuullisuus

Osaaminen

Tekniikka

Lähtökohtana on henkilöstön vastuullinen asenne tietoja käsitellessään. Onnistumisen mahdollistaa hyvä tehtävien osaaminen, myös tietoturvassa. Onnistumista tukee turvallinen, luotettava, sujuvaan työntekemiseen sopiva tieto- ja viestintätekniikka.

Työaseman käyttö

Pöytätietokone
kannettava tietokone
tai muu vastaava

Helsinki

Mistä tiedät kuka käyttää tietoja?

Helsinki

Työasemaan
kirjaudutaan omalla henkilökohtaisella käyttäjätunnuksella,
toisten henkilöiden tunnuksia ei saa käyttää.

Helsingin kaupungin henkilöstön sähköisen identiteetin perustana on henkilökohtainen tietoverkon toimialueelle kirjautumisen tunnus (”AD-tunnus”).

Useissa tapauksissa Helsingin työaseman (verkon) käyttäjätunnuksella kirjautuminen riittää käyttäjän todentamiseen.

Käyttäjätunnukset, käyttöoikeudet

Työasemaan ja kaupungin verkkoon kirjaudutaan yhdellä tunnuksella (”AD-tunnus”, AD = Active Directory).
Töihin voidaan tarvita useita käyttäjätunnuksia.
Käyttäjätunnuksia tarvitaan, koska niiden perusteella määritellään oikeudet tietoihin ja tietojärjestelmiin (”ohjelmiin”).

Tunnuksia on useita, koska jotkut järjestelmät eivät käytä kaupungin AD-tunnusta käyttäjän tunnistamiseen. Joihinkin taas kirjaudutaan automaattisesti AD-tunnuksella kirjautumisen jälkeen (kertakirjautuminen; SSO = single sign-on”).

Kirjautumisissa on aina käytettävä omaa käyttäjätunnusta eikä salasanoja saa kertoa muille.

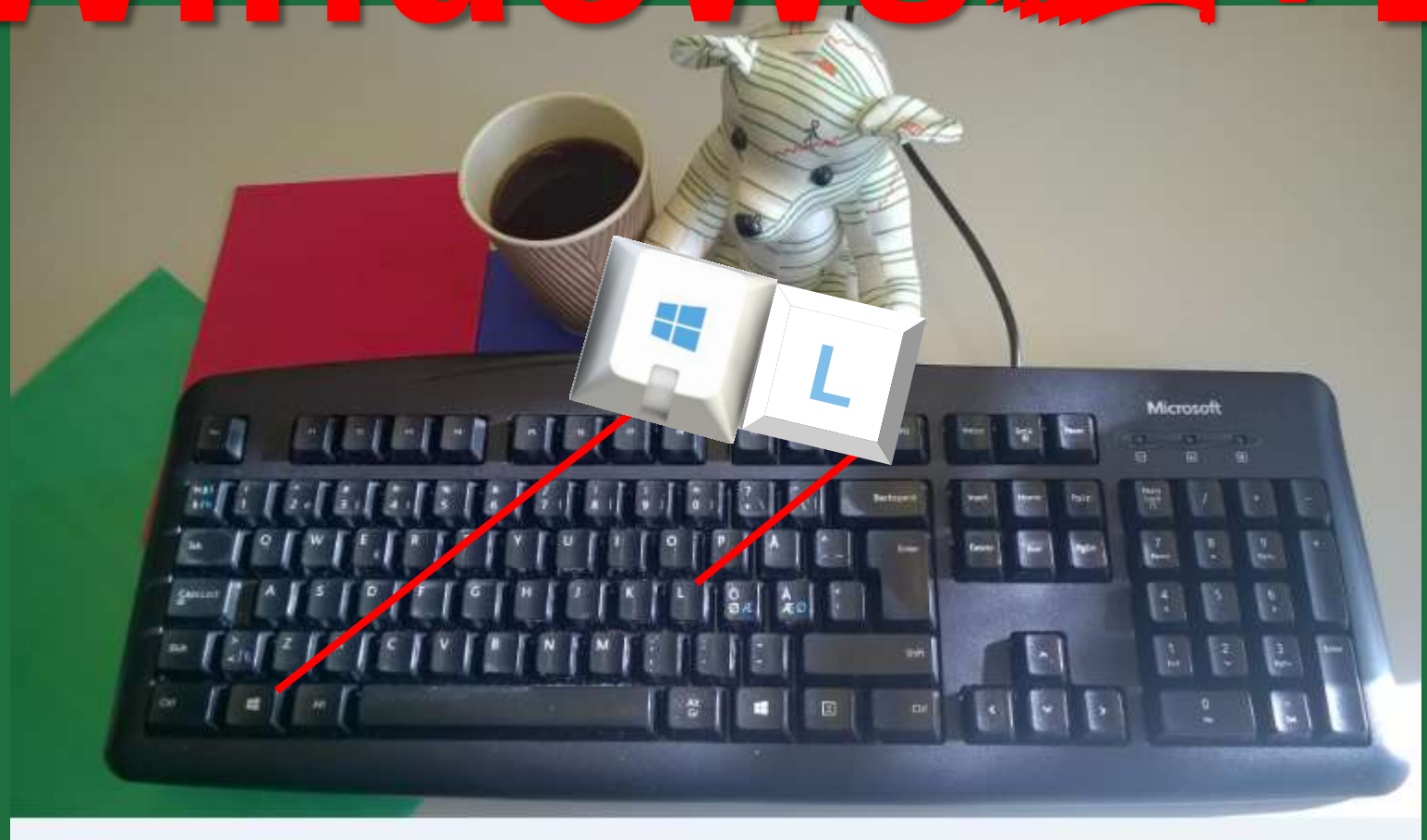
Käyttäjätunnusta ja/tai salasanaa ei myöskään saa sanoa puhelimessa eikä lähettää sähköpostitse, vaikka joku niitä tiedustelisi.

Ylläpitäjät eivät tarvitse eivätkä käytä käyttäjien salasanoja.

Tarvittaessa ylläpitotehtävät tehdään yhdessä käyttäjän kanssa.

Kun poistut työpisteeltä, lukitse työasema.

Windows ⊞ +L



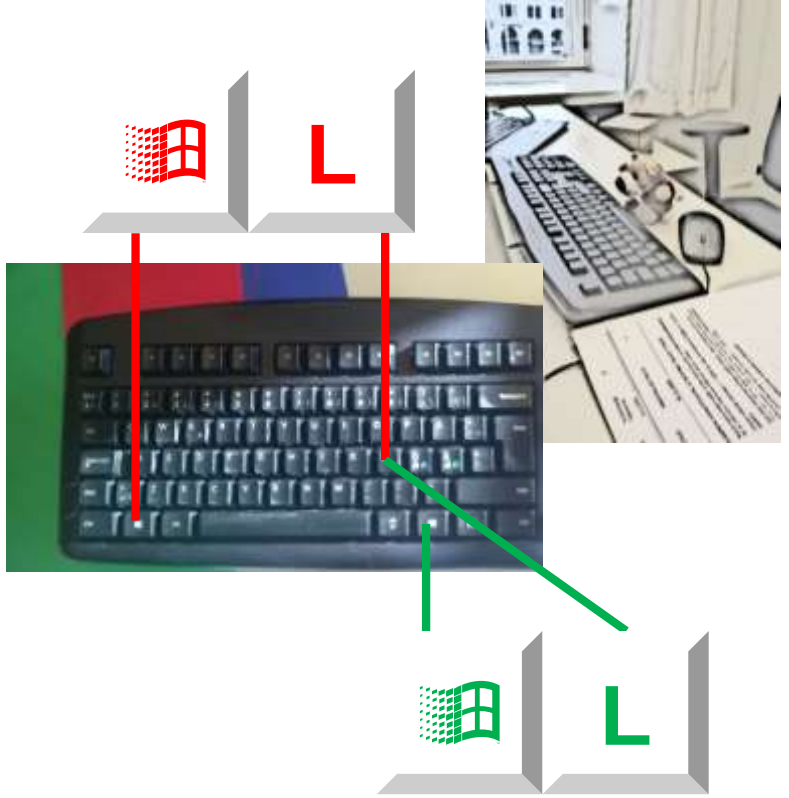
Helsinki

Kun poistut työpisteeltä, lukitse työasema.
Esimerkiksi Windows+L (lock/lukitse) -näppäilyllä.

Laita myös työpaperit pois näkyviltä.

Suojattava aineisto tulee laittaa
lukkojen taakse kun sitä ei tarvita -
lukolliseen pöytälaatikkoon, kaappiin ja/tai
huoneen ovi lukkoon.

Näin myös yön ajaksi, sillä
yölläkin työtiloissa voi olla kulkijoita.



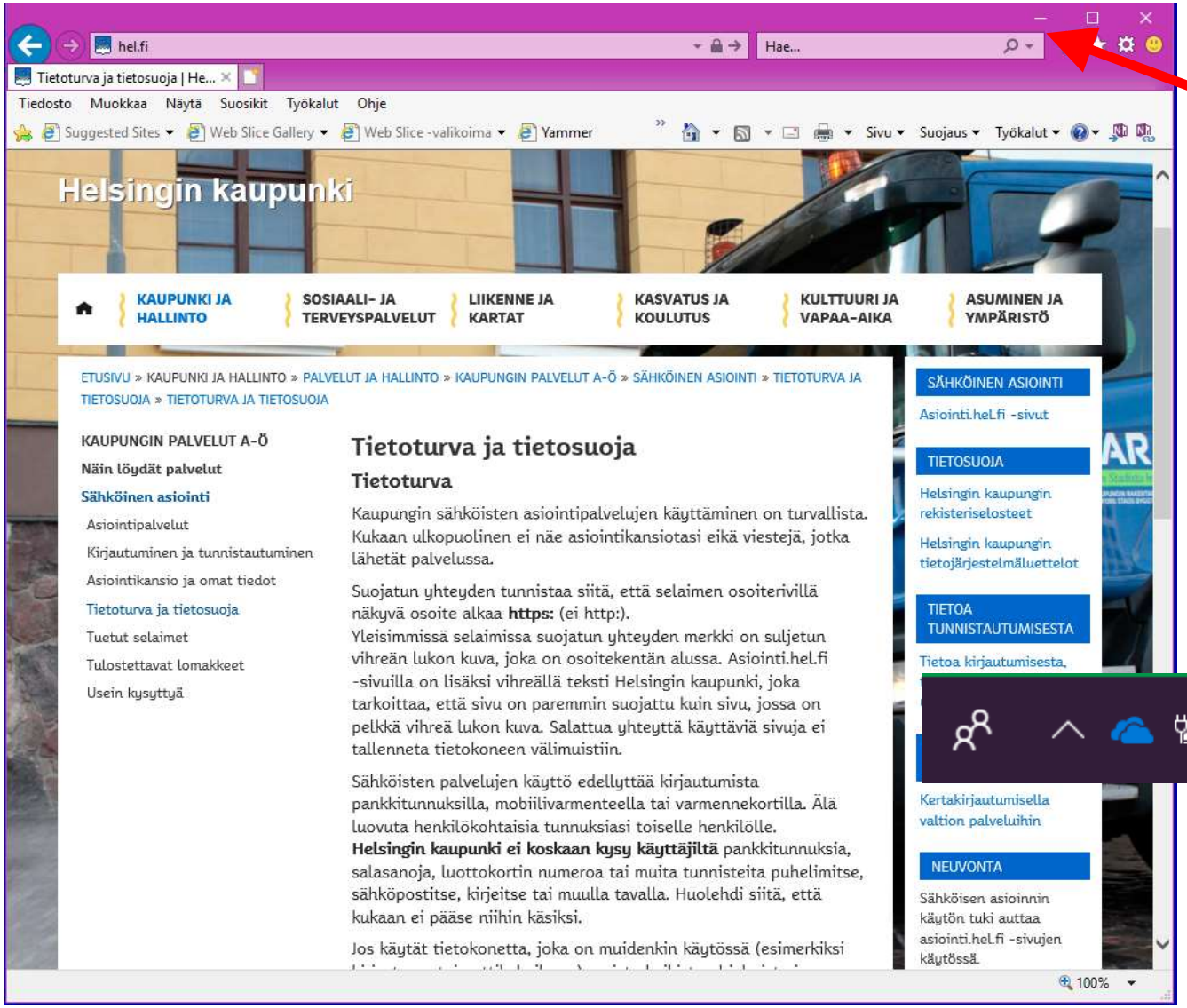
MIKSI:

Näkyvillä olevasta aineistosta voi nähdä asioita,
jotka eivät kävijälle kuulu.
Avoimesti saatavilla olevan aineiston mukaan ottaminen käy
sekunneissa.

Tietojen oikeasta käsittelystä vastaa hän, kenelle tiedot on annettu käyttöön.

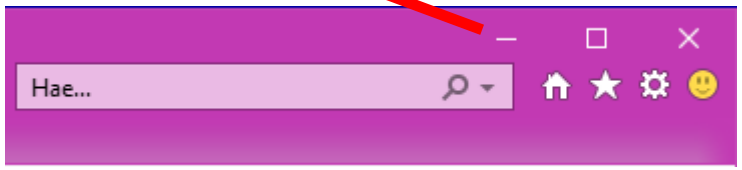
Ps. Windows-näppäintä käyttävät pikanäppäimet
https://support.microsoft.com/fi-fi/help/12445/windows-keyboard-shortcuts

Peitä näyttö olan yli katsojilta



Pienennä yksi ikkuna

- -valinnan napauksella



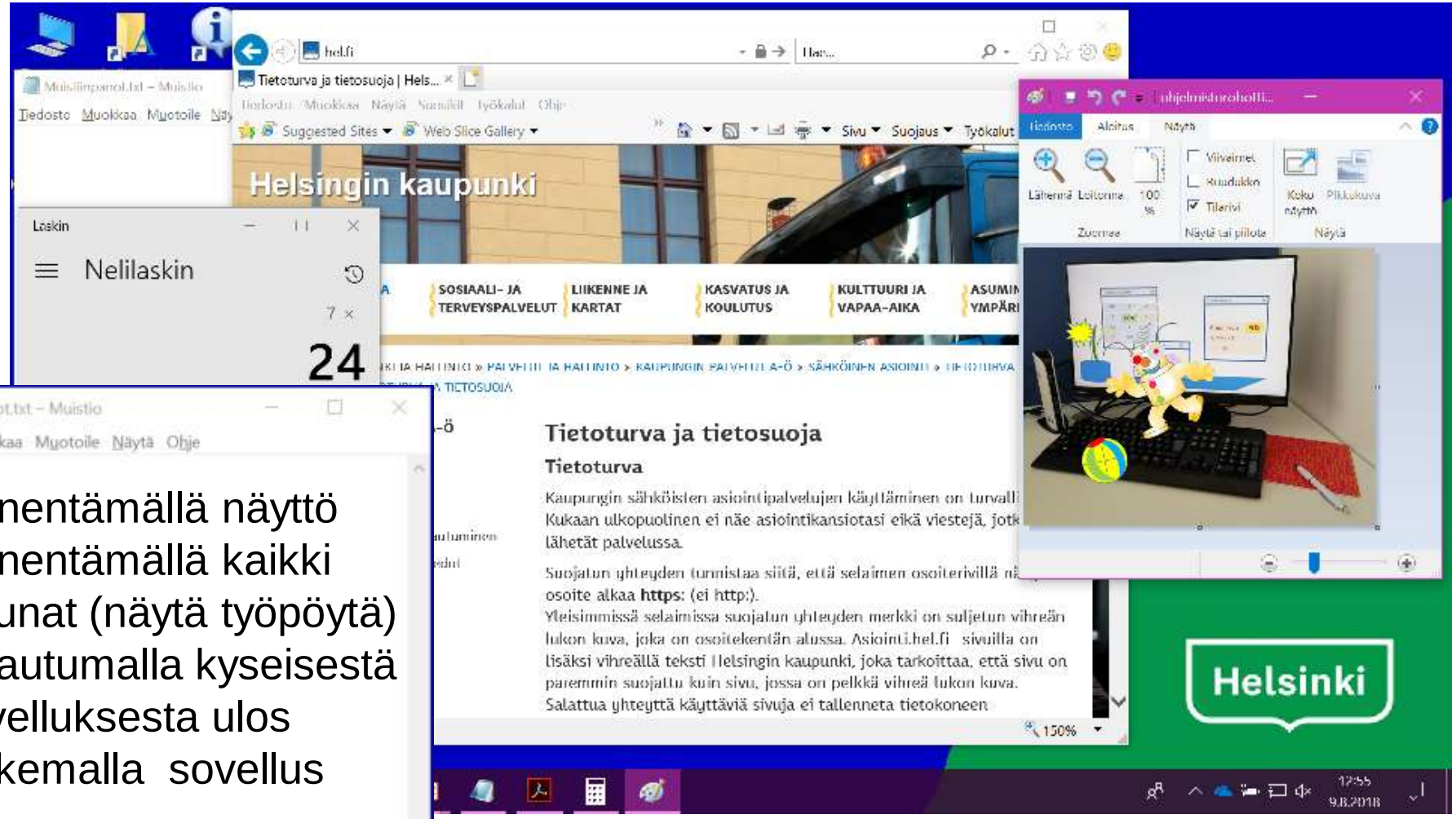
Näytä työpöytä

tai

Pienennä kaikki yhdellä napauksella alanurkkaan

Helsinki

Jos työasemaa ei juuri tällä hetkellä voi sulkea, niin näytöllä näkyvät tiedot voi laittaa nopeasti pois asiattomien näkyviltä



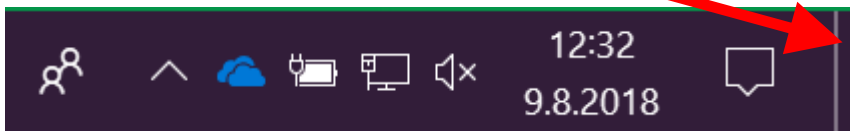
- pienentämällä näyttö
- pienentämällä kaikki ikkunat (näytä työpöytä)
- kirjautumalla kyseisestä sovelluksesta ulos
- sulkemalla sovellus

tai sähkö pois näytöstä ☺

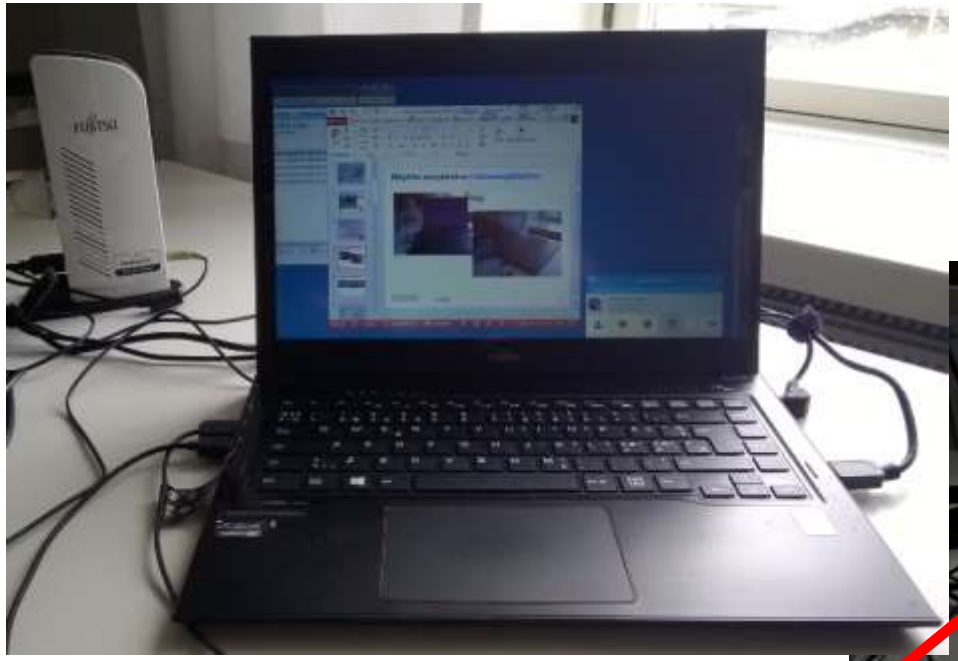
Näyttää tyhjän työpöydän (tai tuo takaisin ikkunat juuri edeltävän Windows+D ”desk” näppäilyn jälkeen)

Näytä työpöytä
Pienennä kaikki yhdellä napauksella alanurkkaan

tai läppärin kansi kiinni

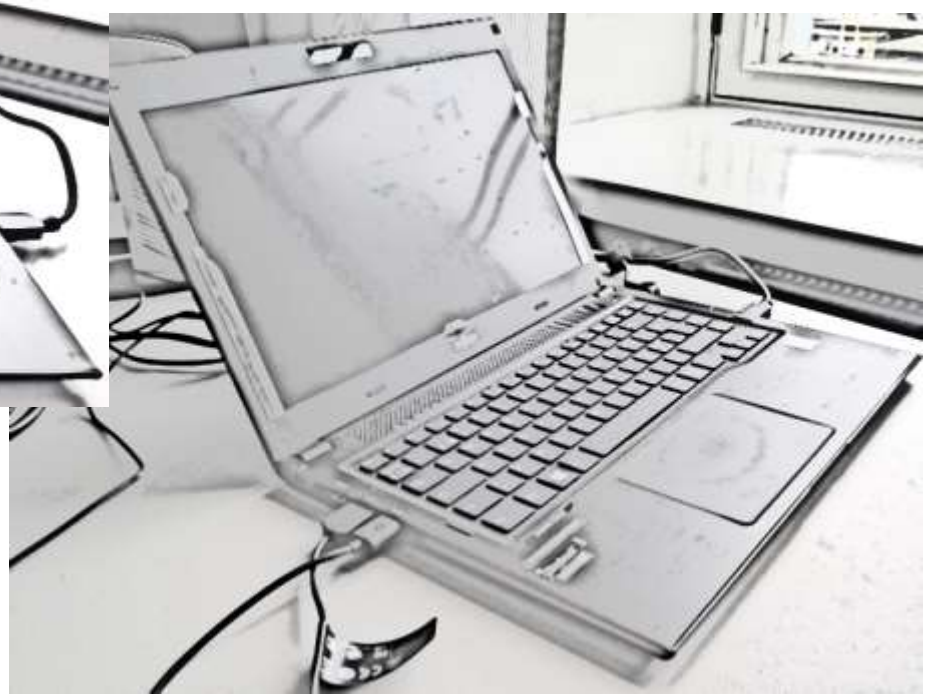


Näytön suojakalvo (tietosuojakalvo)



Estää näytön sisällön lukemisen sivusta

Työhuonejärjestelyt, sermit, ikkunakaihtimet toimivat tilaratkaisuina näytön lukemisen estämiseen. Samoin pöydän sijoittelu.

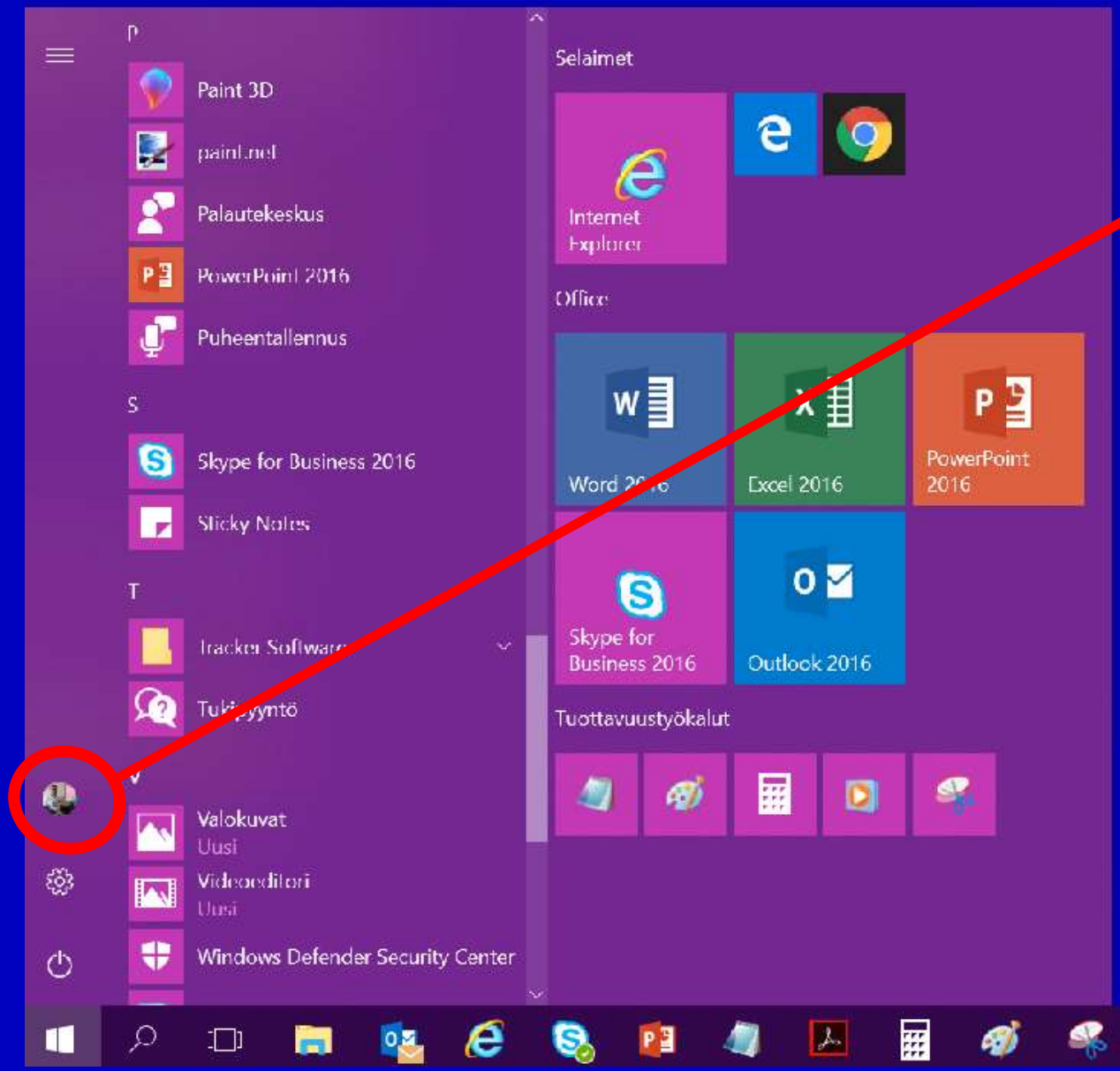


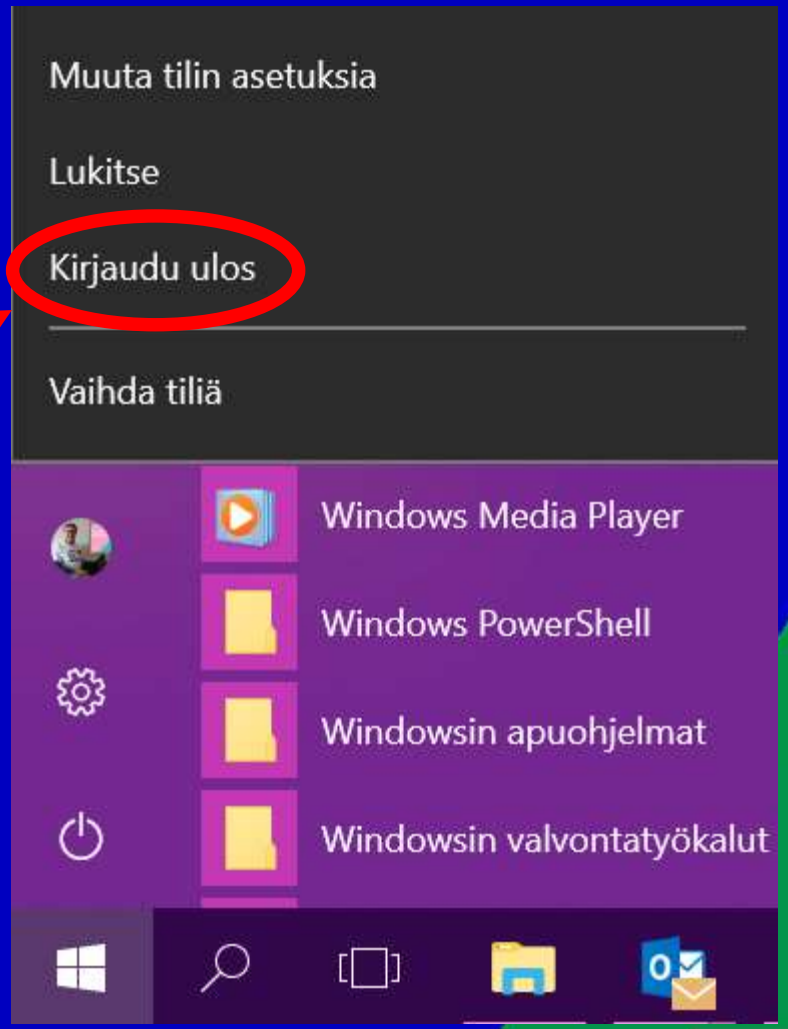
Myös etä- tai matkatöissä
(monipaikkaisessa työssä)
on katsottava että tietoja
ei pääse asiattomille

Tietosuojakalvoa voi kysyä lähituelta (ICT-tuki)

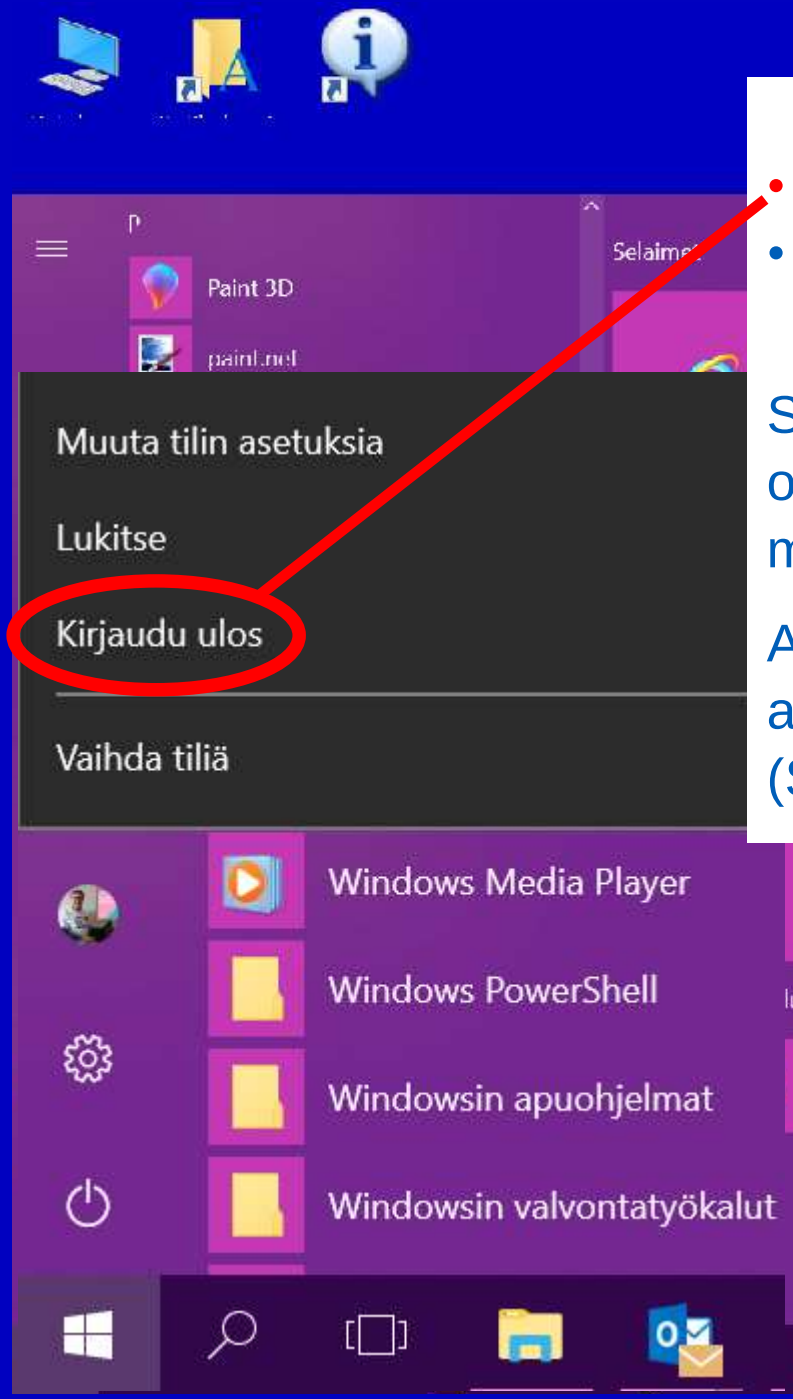
kahvilassa, kirjastossa,
ratikassa, kokoushuoneessa…

Poistuessa





Helsinki



- Lähtiessäsi kirjaudu ulos tietokoneelta ja
- jätä kone käyntiin verkkoon liitettynä, niin ohjelmien päivitykset voidaan ladata sillä aikaa.

Säännölliset tietoturva-, korjaus- ja muut ohjelmistopäivitykset pitävät tietokoneympäristön mahdollisimman hyvänä käyttää ja turvallisena.

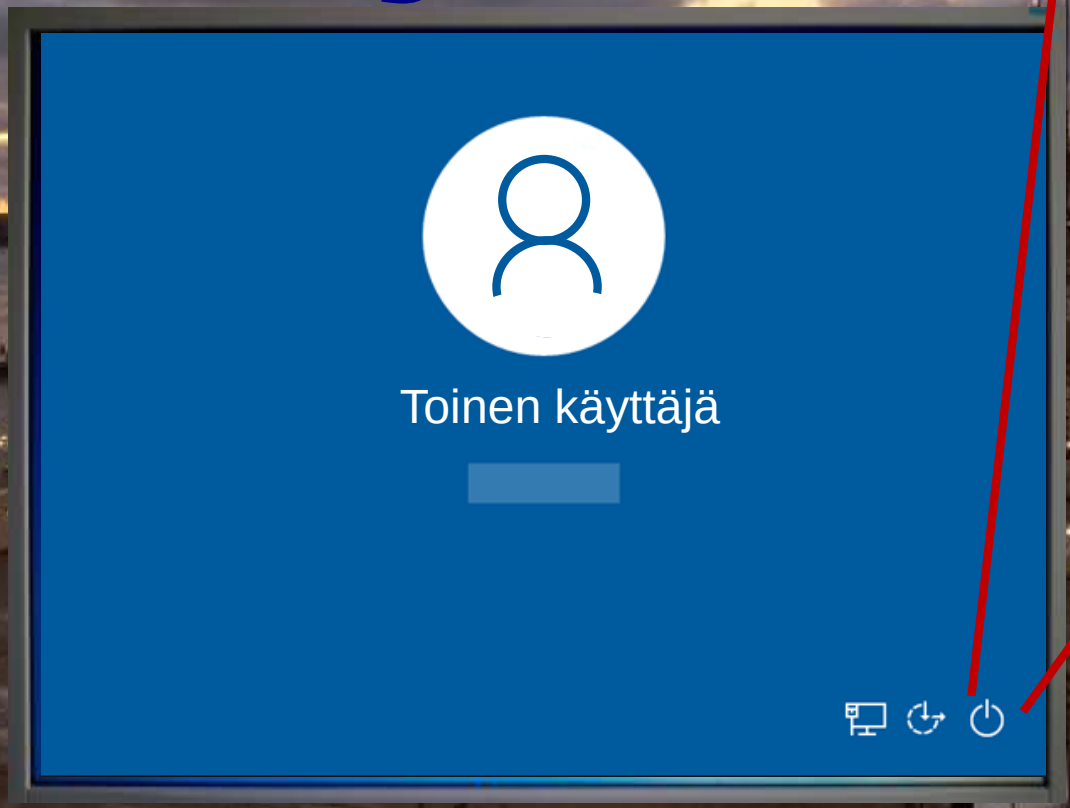
Aamulla koneen käynnistys viimeistelee mahdolliset yön aikana tulleet päivitykset.
(Sammuta-käynnistä tai Käynnistä uudelleen)

☺ Energian säästämiseksi sähköt voi kytkeä yöksi pois näytöstä

Työpaikan tapana voi olla myös tietokoneiden vieminen kaappiin vuoron lopussa

Helsinki

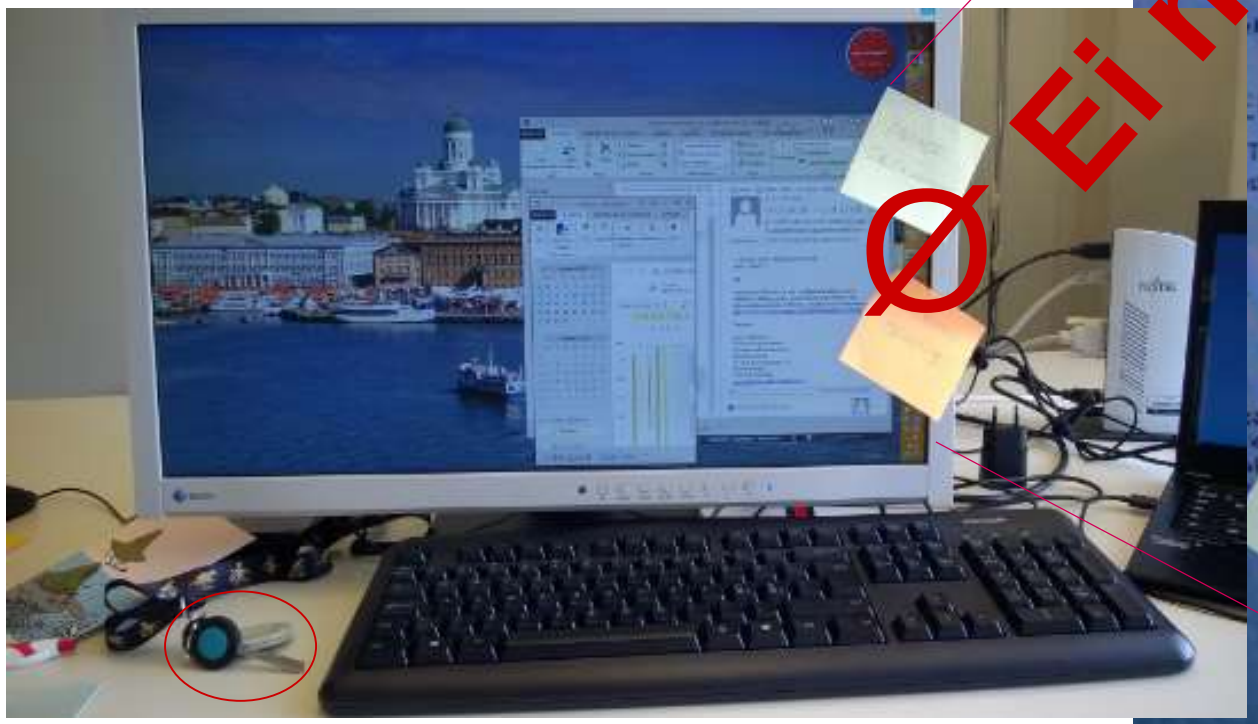
...ja saapuessa uudelleen käynnistys

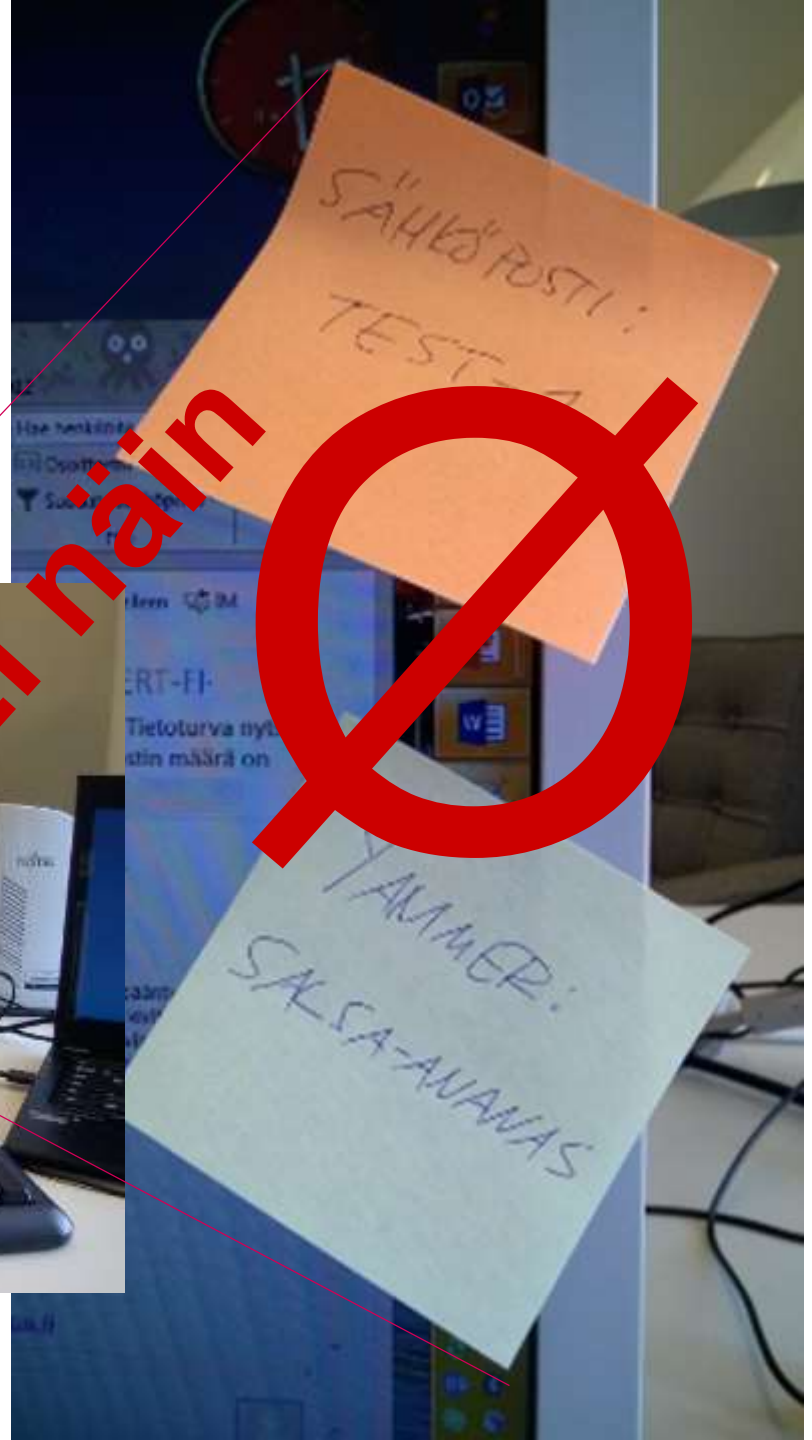


Lepotila
Sammuta
Käynnistä uudelleen

Helsinki

Salasanat
Tunnusluvut





Helsinki

Keksi salasanoille muistisäännöt

Salasanat ja tunnusluvut ovat arvokkaita kuin avaimet

Niitä ei kannata säilöä näkyvillä.
Hyvä salalause/tunnusluku on **p i t k ä** ,
sinun helppo muistaa ja
muiden vaikea arvata.

10… 15…	pituus ainakin 10 tai 15 merkkiä
Aa Bb Cc Dd Ee Ff …	isoja ja pieniä kirjaimia
0 1 2 3 4 5 6 …	numeroita
+ = - / ! : ; …	muita merkkejä

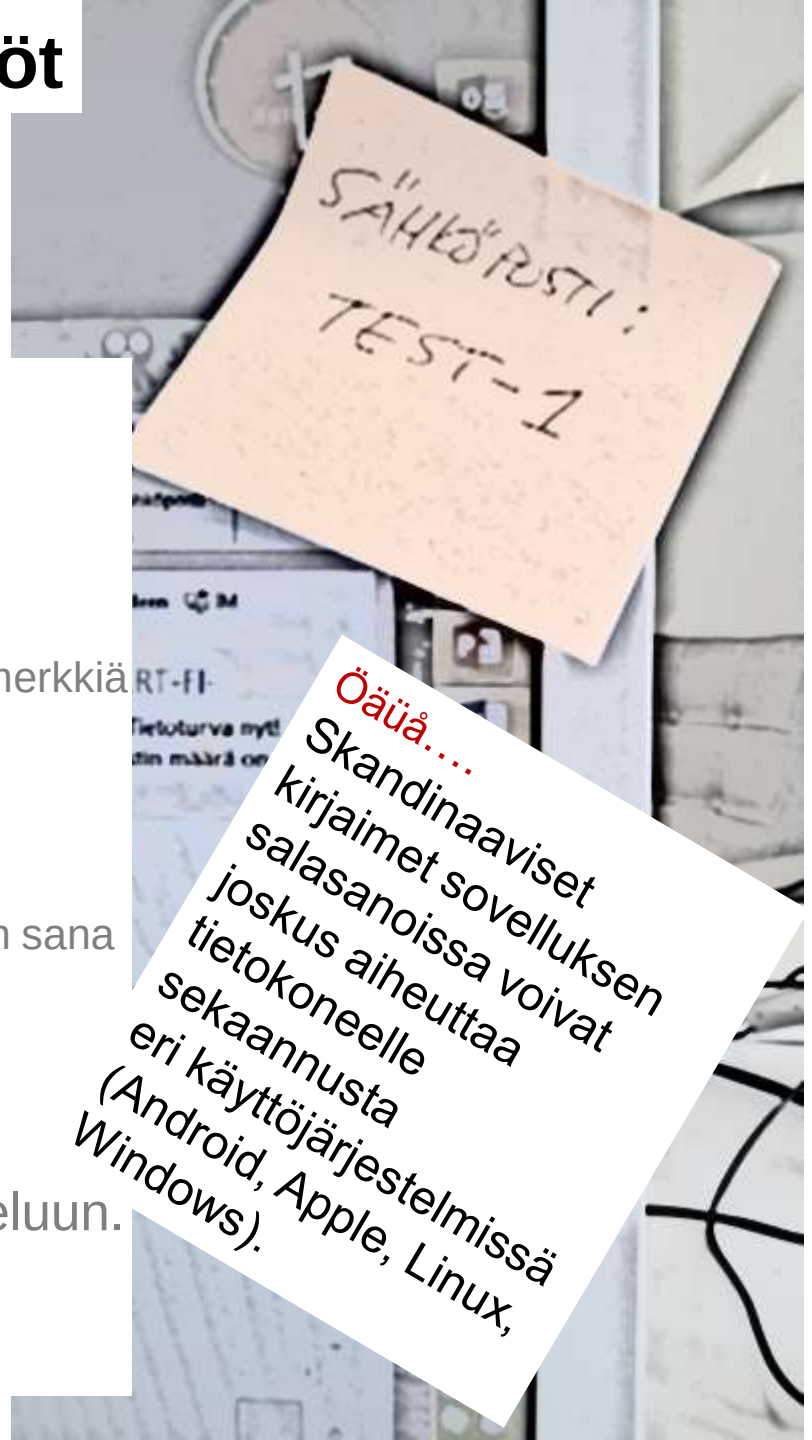
tai ainakin **pitkä**, joka ei ole perusmuotoinen sana

Eri tunnukset eri paikkoihin.

Eri tunnukset töihin ja omiin kotiasioihin.

Salasanoja/PINnejä tarvitaan vielä moneen palveluun.

Ps. Viestintäviraston salasanalinko:
pidempiparempi.fi



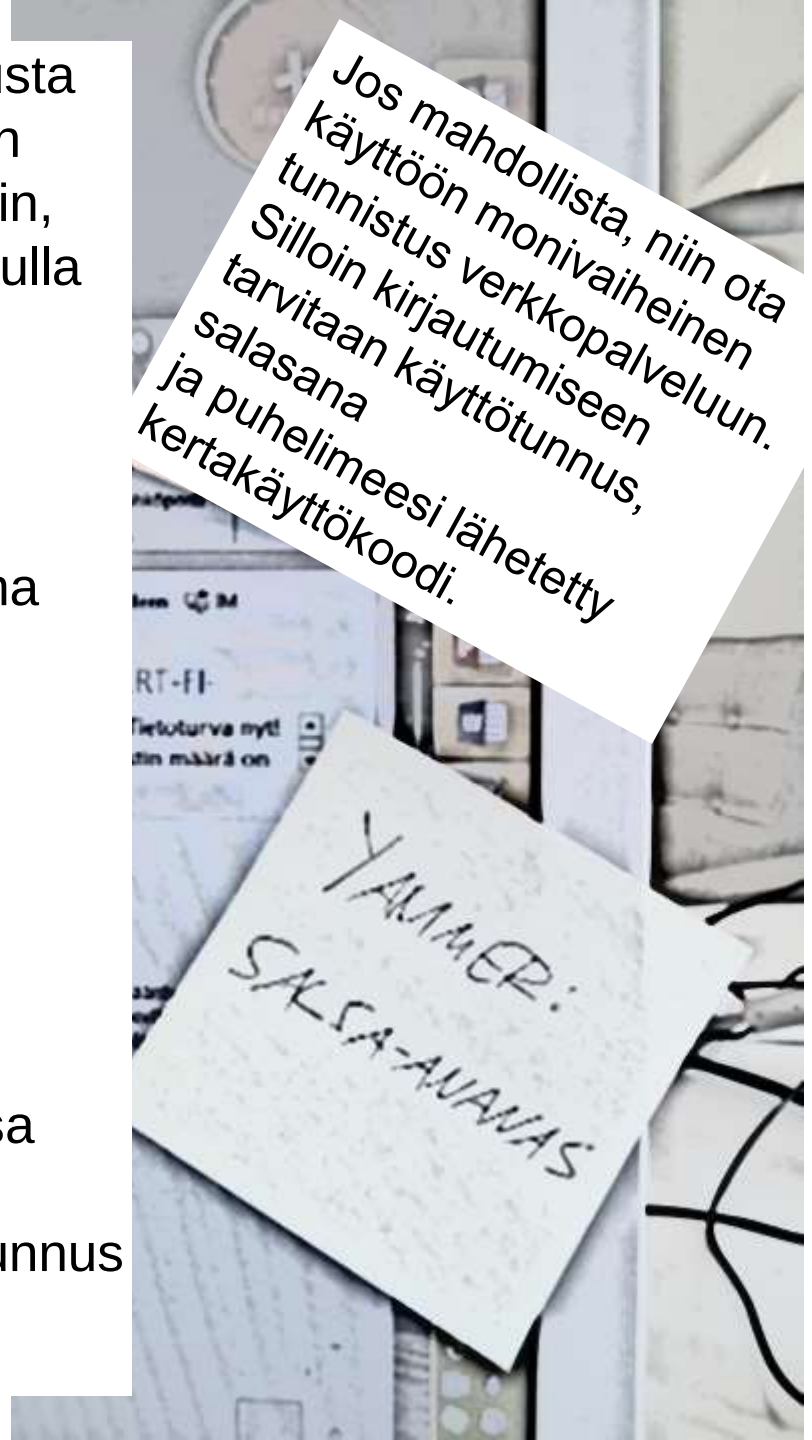
Helsinki

Jopa yli kymmenen vuotta sitten verkkopalvelusta varastettuja salasanoja kiertää verkkorikollisten hallussa. Jos vanha salasana vielä käy jonnekin, niin rikollinen saattaa päästä tekemään sen avulla petoksia.

Kun käyttää eri käyttötunnuksia (kirjautumisen sähköpostiosoitteita) ja eri salasanoja eri palveluihin, niin vaikka yhden palvelun salasana joutuisikin rikollisen haltuun, niin sillä ei pääse muihin palveluihin.

Jos salasana tulee annettua vahingossa huijaussivulle, niin vaihda se heti, ilmoita asia lähituelle (ICT-tuelle) ja omalle esimiehelle.

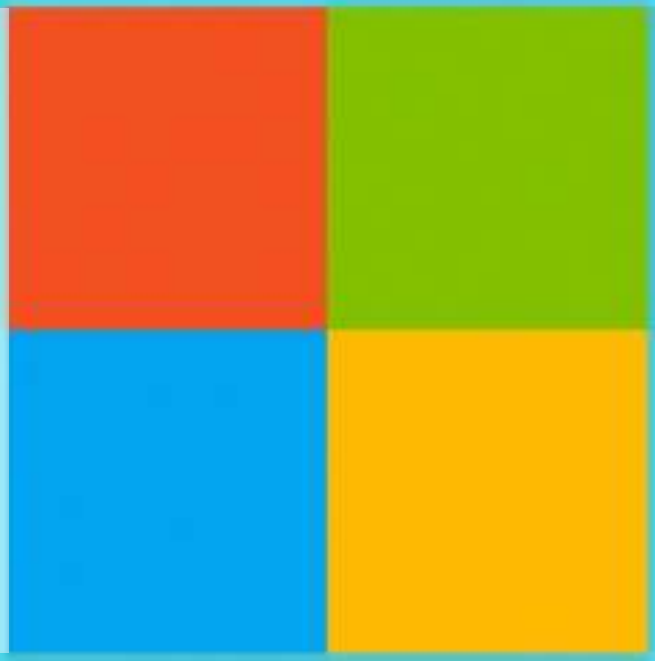
Edelleen tosi yleinen huijaus on sellainen, jossa koetetaan saada käyttäjä antamaan huijausverkkosivulla jonkun palvelun käyttäjätunnus ja salasana.



10 tai 15 merkkiä <
< 3 kuukautta

Vaihda **salasana** 3 kuukauden välein
tai vaikka useamminkin ja
AINA HETI JOS EPÄILET SEN
JOUTUNEEN ASIATTOMAN TIETOON
sekä jos järjestelmä pyytää

Käytä ainakin 10 merkkiä pitkiä salasanoja
ja vielä mieluummin yli 15 merkkisiä



Älä kierrätä samaa salasanaa uudestaan ja uudestaan ja uudestaan ja uu

Helsinki

Eri salasanat ja tunnukset töihin kuin omiin koti/harrastusasioihin

Vaihda aina oletussalasanat ja -numerokoodit

Monivaiheinen tunnistus on parempi

Helsinki

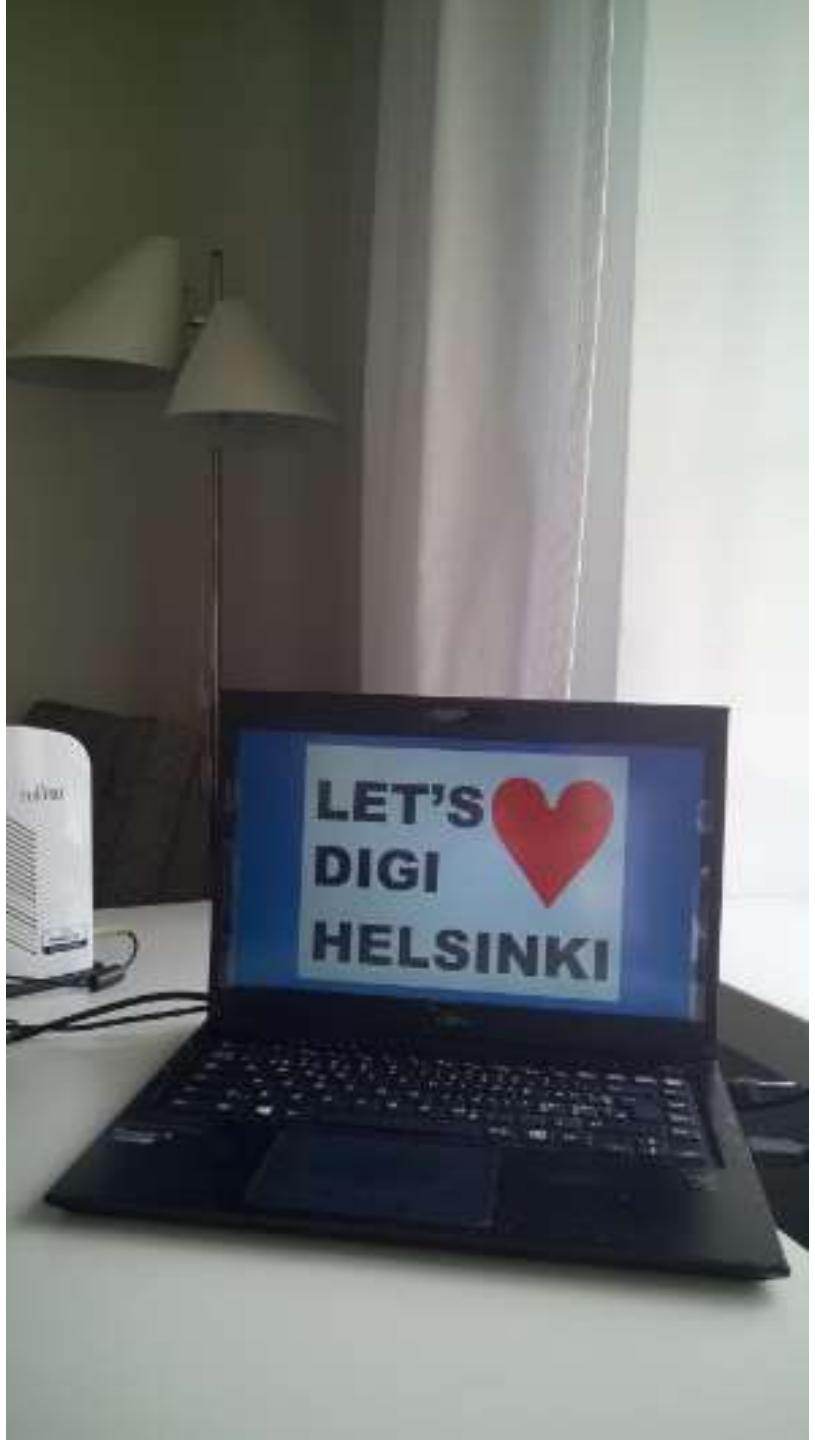
Työasemat

Digitaaliset työvälineet
Etäyhteys

Työasema

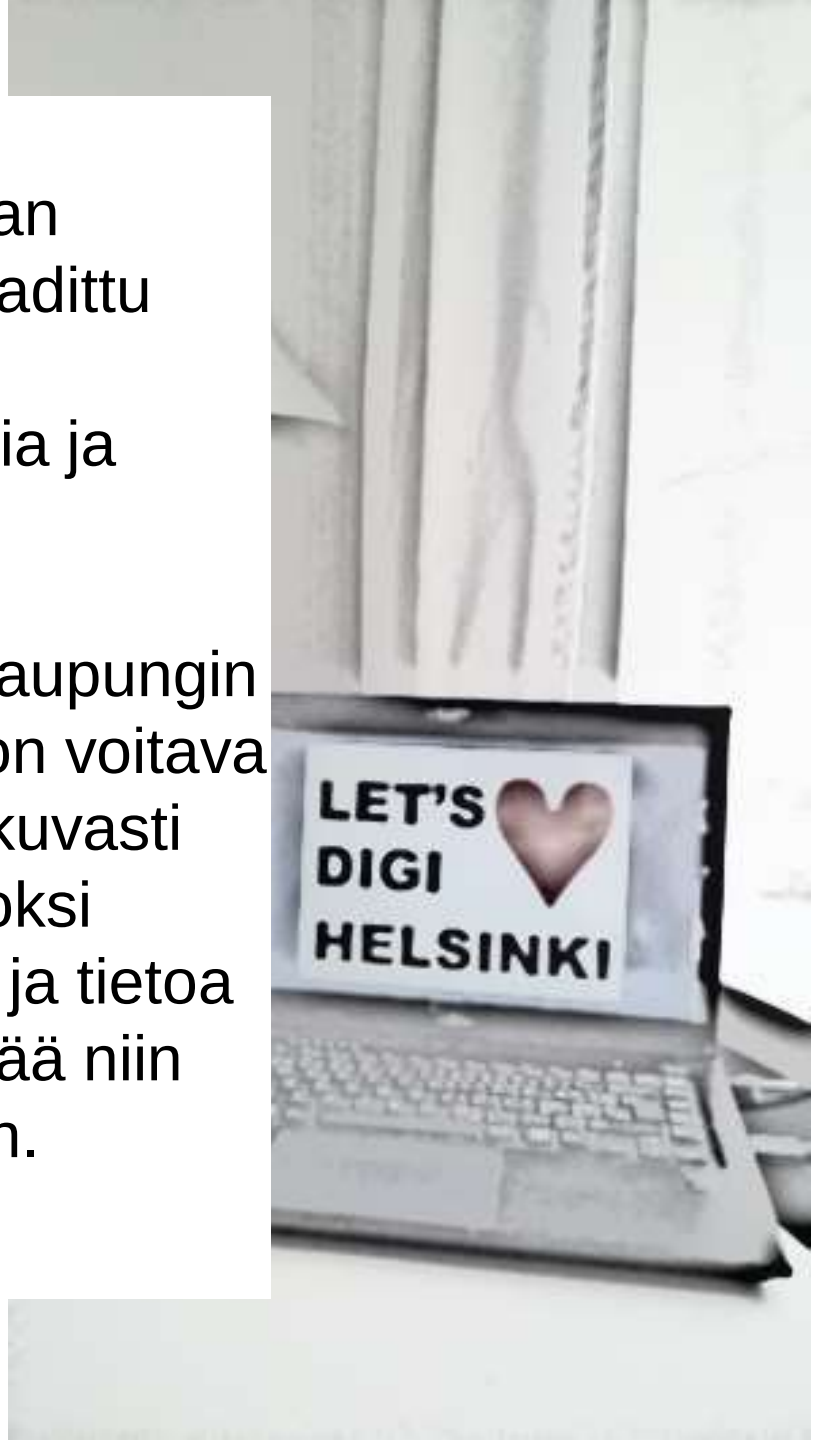
Työasemissa käytettävät ohjelmat on vakioitu, osa on kaupunkitasoisia vakio-ohjelmia, osa toimialan tai yksikön omia. Ohjelmat on valittu siten, että ne ovat kaupungin ympäristöön soveltuvia ja mahdollisimman yleiskäyttöisiä.

Työasemiin asennetaan vain työssä tarvittavia ohjelmia, koska ylimääräiset ohjelma-asennukset saattavat aiheuttaa häiriöitä muiden ohjelmien toiminnassa. Kaupungin työasemissa käytettäviä ohjelmia ei saa kopioida kotikäyttöön, se on laitonta.



Toimintavarmuuden takaamiseksi työasemaympäristöt on mahdollisimman vakioituja. Kaupungin työasemat on laadittu työtehtävien mukaisiksi. Käyttäjien mahdollisuuksia tehdä omia asennuksia ja laitteistoasetuksia on rajoitettu.

Kaupungin työasemat kuuluvat koko kaupungin kattavaan työasemaverkkoon. Tietoa on voitava tuottaa ja tuotetun tiedon on oltava jatkuvasti tarvitsijoiden käytettävissä. Tämän vuoksi työasemien on oltava toimintavarmoja ja tietoa on voitava sujuvasti ja turvallisesti siirtää niin kaupungin sisällä kuin kumppaneillekin.



Kaupungin omistamista kannettavista tietokoneista, tableteista, älypuhelimista ja muista laitteista on pidettävä hyvää huolta. Katoamistapaukset pitää ilmoittaa heti lähitukeen ja laitteen hankkineelle henkilölle sekä omalle esimiehelle.

Etäkäytössä työnantajan laitteita saa käyttää ainoastaan siihen valtuutettu työntekijä. Ylläpito vastaa viraston laitteista ja huolehtii, että käyttäjille annettuihin laitteisiin on asennettu asianmukaiset tietoliikenteen salauksen, virustorjunnan ja palomuuriohjelmat. Ylläpito asentaa myös sallitut etäkäyttöyhteydet.

Laitteiden käyttäjän on noudatettava annettuja ohjeita.

Käyttäjä ei saa tehdä laitteisiin omia asennuksia.

Lähituelta voi kysyä kuinka saadaan käyttöön sellaisia uusia ohjelmia, joita ei vielä ole tarjonnassa.

Omat työvälineet

Omaa tietokonetta, älypuhelinta tai muuta laitetta käyttäessään henkilö itse vastaa siitä, että tietoturva ei vaarannu.

Muilla kuin työnantajan tarjoamilla välineillä tehtävästä tietojenkäsittelystä on sovittava esimiehen kanssa.
Laitteen on oltava ajantasainen myös virustorjunnan sekä palomuurin osalta.
Omien työvälineiden käyttöön liittyvät etä/matkatyöohjeet saat omalta toimialaltanne tai yksiköltänne.

Kaupungin tietojenkäsittelyä ei saa vaarantaa omia työvälineitä käytettäessä.

Etäyhteyden käyttö - kirjautuminen

Etäyhteys Helsingin työympäristöön saadaan työtehtävien mukaan.
Se saattaa olla käytettävissä muiltakin kuin työnantajan hallinnoimilta koneilta.

Jotkin yleiset palvelut voivat olla käytettävissä perustunnistautumisella (etäkäytön käyttäjätunnus ja salasana), mutta työtehtäviin tarvittaviin palveluihin tunnistaudutaan tyypillisesti kaksivaiheisella tunnistautumisella:

1. Siirry palvelun sisäänkirjautumisen sivulle.
2. Anna ensi etäkäytön käyttäjätunnuksesi.
3. Anna siihen liittyvä salasana.
4. Järjestelmä tarkistaa ne, ja lähettää palveluun rekisteröityyn sinun puhelinnumeroosi kertakäyttökoodin (PIN-numero).
5. Anna koodi, jonka jälkeen pääset käyttämään palvelua.

Käyttäjän vahva tunnistaminen

Helsinki

Usea peräkkäinen väärä kirjautumisyritys lukitsee käyttötunnuksen.

Etäyhteyden käyttö - katkaisu

Kun etäyhteys on käynnistetty, niin se katkeaa automaattisesti, jos tietoliikennettä ei ole yhtään pitkähköön aikaan. Kun yhteys on katkennut, ja jatketaan taas sellaisia töitä, joissa verkkoyhteyttä tarvitaan, niin etäyhteyden avaaminen vaatii uudelleen kirjautumisen.

Kun kone kysyy käyttäjätunnusta ja salasanaa, anna ne.
Kun järjestelmä lähettää sinulle uuden PIN-numeron, syötä se PIN-kyselyyn.

Ja jos kone on ollut levossa/suljettuna, mutta käyttökatkon jälkeen (esimerkiksi takaisin toimistolle tultua) se jostain syystä muistaa hakea etäkäyttöyhteyttä, niin se saattaa pyrkiä tunnistamaan etäyhteyden. Normaalisti toimistolla ei käytetä etäyhteyttä.

Muista katkaista etäyhteys kun työskentely päättyy ja et enää käytä sitä.

Haloo! Puhelimessa?

Helsinki

Helsingin kaupunginmuseo helsinkikuvia.fi / kuvaaja Väinö Kannisto

Pidä puhelin mukana, älä jätä pöydille.

Lukituskoodin käyttö päällä
niin että näyttö lukkiutuu kun puhelinta ei käytetä.

Tämä koskee kaikenlaisia henkilökohtaisia älylaitteita (*”personal digital assistant”*).

Katso työpuhelimesi oma, tarkempi ohjeistuksenne ja toimi niiden mukaan.

Esimerkiksi kelle soitetaan ongelmista.

Henkilötietoja ovat kaikki tietyn ihmisen yksilöivät tiedot

Huomaa, että puhelimeen tallennetut kuvat, yhteystiedot, viestit tai muut tallenteet voivat sisältää samanlaisia tietoja kuin tietokone.

Tietojen salassapitoa ja suojaamista koskevat samat periaatteet niin tietokoneissa, tableteissa, älypuhelimissa, muistitikuilla kuin muissakin laitteissa (”tallennusalustoissa”).

ja paperilla ja puhuessa - puhelimeenkin

ja verkkokokouksessa (skype, Teams)

Jos et voi varmasti tunnistaa puhelun toista osapuolta tai et voi olla varma ketkä kaikki puhelua kuuntelevat toisessa päässä, niin puhu vain sellaisia asioita joita voi tunnistamattoman henkilön kanssa puhua.

Esimerkiksi henkilötietojen kanssa tulee aina olla huolellinen.

Korkeasaaren eläintarha korkeasaari.fi / kuvaaja Mari Lehmonen

Vaihda aina oma PIN
operaattorin oletusnumerosarjan tilalle

Pidä näppäimistön lukittuminen päällä

Helsinki

Laukku matkalla


LL-1.9.2018


LL-1.9.2018


JR-1.9.2018


JR-1.9.2018


MP-1.9.2018


MP-1.9.2018

Pidä laukku mukanasi kun sen sisällä on arvotavaraa
tai lukkojen takana kaapissa/huoneessa.

Arvotavaroita voi pitää mukanaan pienemmässä laukussa tai taskuissa.
Tietokonetta voi kantaa muun näköisessä kuin läppärilaukussa.
Jumppareppu ei näytä niin arvokkaalta kuin tietokonelaukku.
Luottokorttiyritysten mainosnimilappuja ei kannata laittaa laukkuihin.
Eikä läppärin kanteen tarroja, jotka herättävät mahdollisen varkaan huomion.
Ne voivat houkuttaa varkaita.

Jos hallussasi on aineistoa, joka on pidettävä koko ajan mukana, sille voi varata oman pienen, mahdollisimman huomaamattoman asiakirjataskun, jossa aineisto kulkee kokoustauolle/lounaalle/kahville silloin kun sitä ei voi jättää lukkojen taakse.

Matkalle otettavissa laitteissa vain matkalla tarvittavat tiedot.

Toimistolla

Yhteiset työvälineet
Kokoushuoneet
Materiaalien hävittäminen
Lukolliset kaapit

Helsinki

Tyhjän pöydän periaate


”Tyhjän pöydän periaate”
≈ tiedot ei jää pöydälle

Helsinki

Työpaperit pois näkyvistä

- Jos et juuri nyt voi heti laittaa aineistoja
  pöydältä
  kansioon,
  kaappiin,
  pöytälaatikkoon
  pois näkyviltä,

niin laita

- paperit tekstipuoli alaspäin

tai

- päällimmäiseksi jotain aivan muuta.

Tulosteet

Tulosteet ajoissa talteen

Nouda tulosteet heti saman tien.
Muista ottaa alkuperäiset mukaan skannatessa/kopioidessa.
Muista myös skannatun tiedoston poistaminen yhteisestä skannauskansiosta, jos skannatut tiedostot haetaan hakemiston kautta.

Kysy lähituelta ohjeita kuinka teidän kirjoittimilla otetaan ”turvatuloste”

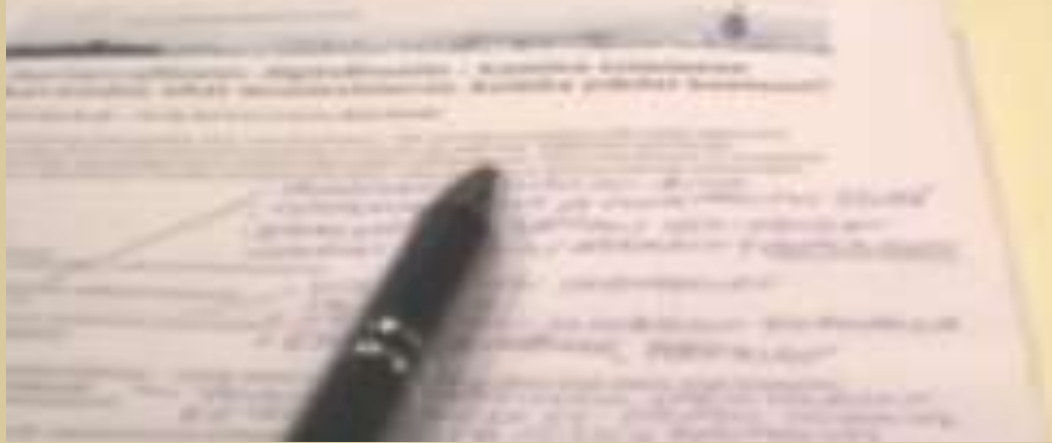
Esimerkiksi

Tulostettaessa valitaan turvatulostus ja joko annetaan itse PIN-numero, joka syötetään myös kirjoittimella tai käytetään henkilökorttia tulostuksen käynnistämiseen kirjoittimella.

Helsinki

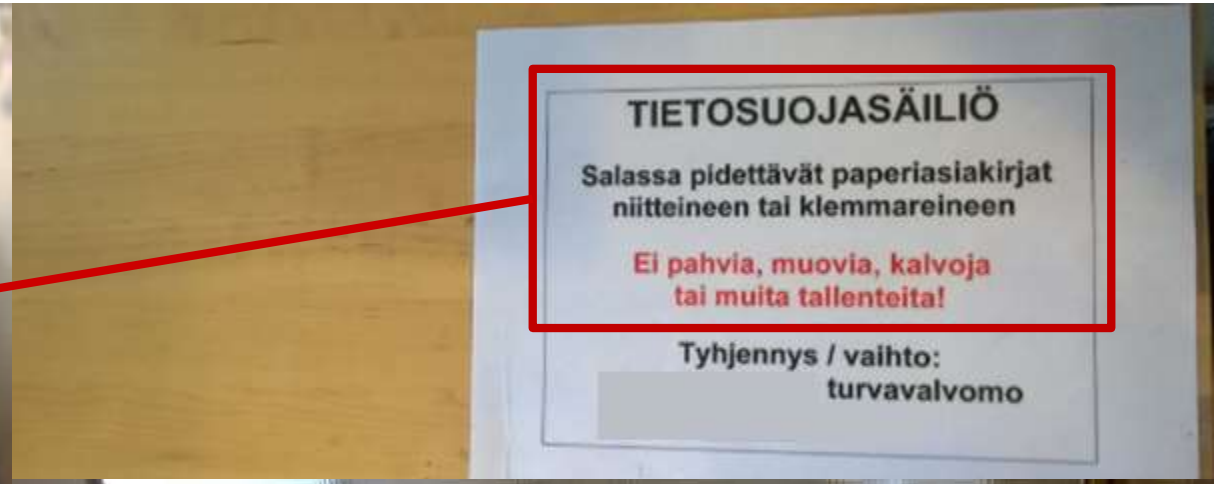
Fläppitaulu muistiinpanotaulu

Ota kokouksen muistiinpanot mukaan kokouksen jälkeen, pyyhi taulut
Älä jätä sivullisten näkyville työmuistiinpanoja – jo ihan siisteydenkin vuoksi



Helsinki

Lajittele tietojäte



Helsinki

- Tietosuoja-aineistot (kuten esimerkiksi henkilötietoja sisältävät paperit) silppuriin tai silputtavien laatikkoon lukkojen taakse.
- Kierrätyspapereihin vain julkista tietoa sisältävät paperit (lehdet, mainoskirjeet…).
- CDt/DVDt ja tuhottavat muistitikut (piirtoheitinkalvotkin yms.) paikalliseen keräyspisteeseen tietosisältönsä mukaisesti tuhottavaksi.
- Roskakoreihin vain niihin kuuluvia roskia. Tietosuoja-aineistot (kokouspaperit yms.) eivät kuulu roskakoriin.
- Kokoushuoneiden fläppitaulujen/ muistiinpanovihkojen paperit otetaan mukaan ja tuhotaan kokouksen jälkeen tietosisältönsä mukaisesti.
- Ja taulut pyyhitään ☺

Arvokas lukkojen taakse

Helsinki

Niin työtiloissa suojattava tieto
kuin muukin arvokas aineisto
pidetään lukkojen takana

ja se on siellä myös asiattomien
katseilta piilossa.

Tavalliset aineistot tavalliseen
lukittuun kaappiin / vetolaatikkoon,

korkeampaa turvaa tarvitsevat
arvonsa mukaiseen
paloturva / kassakaappiin.

Tilaturvallisuus tukee tietoturvaa

Pidetään huolta työtiloista, työtiloissa liikkuvista ihmisistä ja työvälineistä

Helsinki

Avaimet
Kulkutägit
Kulkutunnisteet

Helsinki

Pidä avaimet mukanasi
taskussa tai käsilaukussa.

Työavaimet kannattaa pitää erillään
kotiavaimista.

Pidä avaimet erillään henkilökortin ripustuslenkistä
tai muista tarkoista osoitetiedoista.

Yhteystietona avainlenkkiin voi laittaa harkinnan
mukaan kaupungin vaihteen puhelinnumeron
ellei toisin ole ohjeistettu.

MIKSI:

Avainten löytäjä ei heti voi arvata minne avaimilla
pääsee.
Pöydälle jääneet avaimet on helppo napata
sekunneissa ja itse et pääse lukkojen takana olevilla
avaimilla takaisin.

Pidä myös tägit/kulkutunnisteet mukanasi taskussa tai käsilaukussa kuten avaimet.

Erillään henkilökortin ripustuslenkistä
tai muista osoitetiedoista.

Tunnusnumero (PIN) pidettävä erillään tägistä.

MIKSI:

Löytäjä ei heti voi arvata minne niillä pääsee ja mikä on ovi-koodi.

Ps. Tavanomaista korkeampaa turvaa vaativien tilojen tägit (RFID-tunnisteet) kannatta säilyttää säteilyä läpäisemättömässä suojakotelossa, ettei niitä voi etälukea.

Huolehdithan, että lukitusta ovesta ei tule mukanasi henkilöä, jonka ei tulisi tilaan päästä.

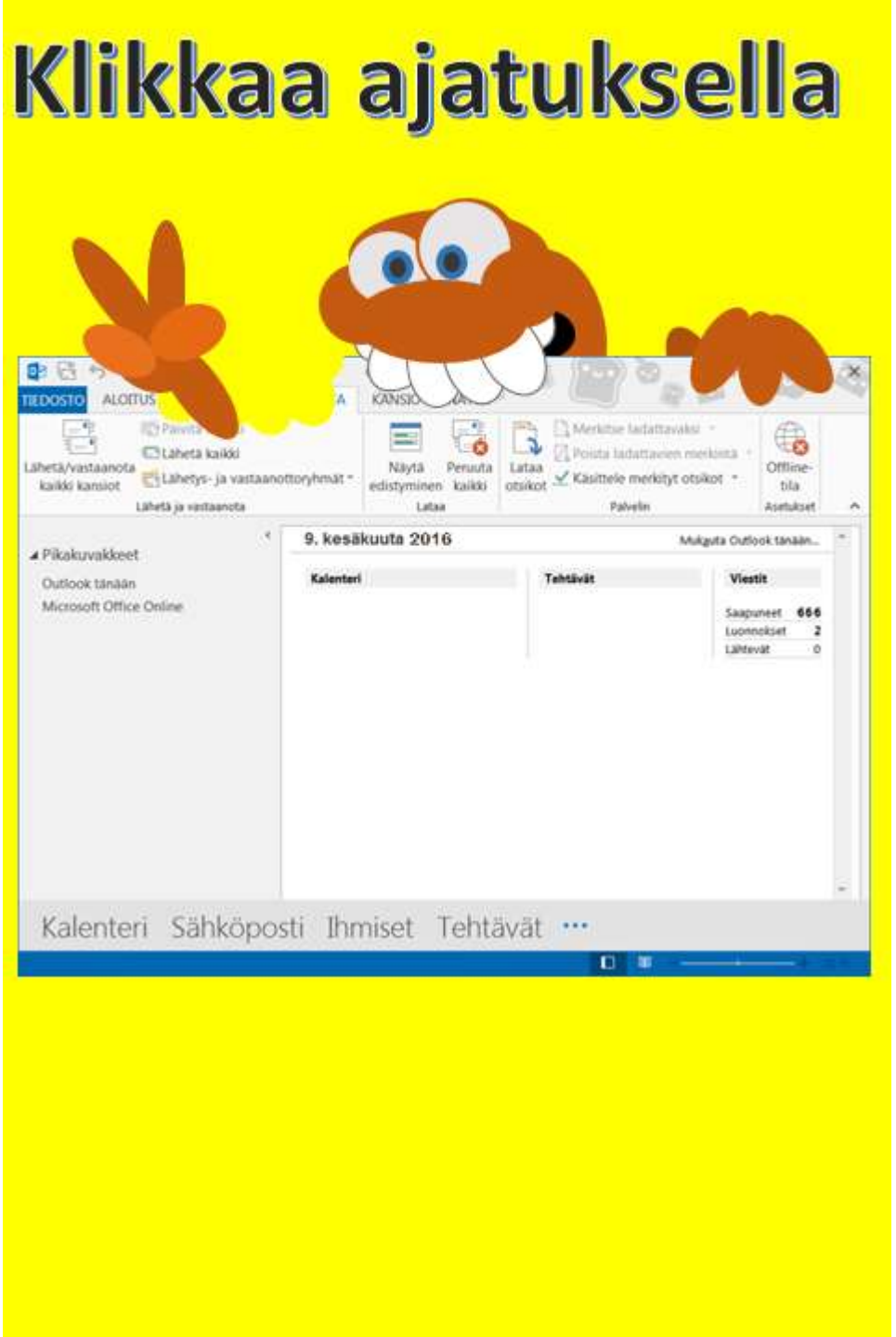

Teknisestä tietoturvasta
Haittaohjelmien suodatus
Salakirjoittaminen
Varmistukset
Helsinki

Ilmoitus
haittaohjelmasta

Jos työasemien ”virustutka” havaitsee haittaohjelmia, niin
ict-tuki saa siitä automaattisesti tiedon ja sinun kanssa sovitaan koneen siivoamisesta yhdessä.

Jos koneellasi on toimintahäiriö, niin
ota yhteyttä omaan ict-tukeesi!

Jos satuit antamaan tunnuksesi huijaussivulle, niin ilmoita siitä heti ict-tukeen, vaihda uusi salasana välittömästi, ja ilmoita sitten omalle esimiehellesi sekä tee tietosuojailmoitus tietosuojan yhteyshenkilöllenne!



Klikkaa ajatuksella

Selkeästi asiattomat viestit saa poistaa lukematta.

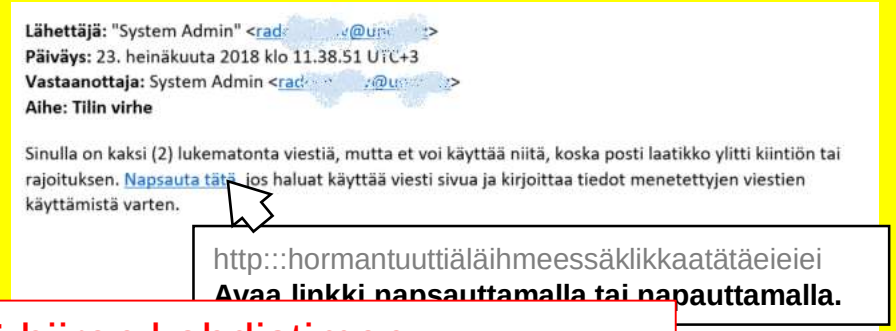
Shift+delete -näppäily

poistaa Outlookissa viestin viemättä sitä Poistetut viestit (Deleted items) -kansioon.

Ei kannata vastata, eikä klikkailla mukana olevia linkkejä.

Väärennetyt lähettäjätiedot voivat näyttää oikeilta, jopa työkaverin osoitteelta.

Roskaa voi tulla viestien sekaan, vaikka postia automaattisesti ja jatkuvasti siivotaan.
Läpi tulleista roskista ei ole välttämätöntä ilmoittaa ict-tuelle, toki saa ilmoittaa.
Jos ongelmana on muutakin kuin muutama, yksittäinen roskaposti,
ota reippaasti yhteyttä lähitukeesi.



Viemällä hiiren kohdistimen osoitteen päälle näkee minne se veisi, mutta **älä klikkaa**!

Helsinki

Virustorjunta

Työasemissa on keskitetty virustorjunta. Tietokoneen toimintaa häiritsevien haittaohjelmien leviämisnopeus ja määränkasvu ovat niin suuria, että virustorjuntaohjelmistojen tunnistus ei aina välttämättä pysy ajan tasalla. Tämän vuoksi on tärkeää käyttää harkintaa sähköpostin ja internetin käytössä.

Älä avaa oudoilta lähettäjiltä tulleita viestejä, eikä niiden liitetiedostoja.

Älä avaa tutuiltakaan tulleita viestejä, jos niiden aihekenttä (”otsikko”) herättää varovaisuutesi. Ota vaikka yhteyttä lähettäjään, ja kysy onko viesti todella häneltä sinulle tarkoitettu.

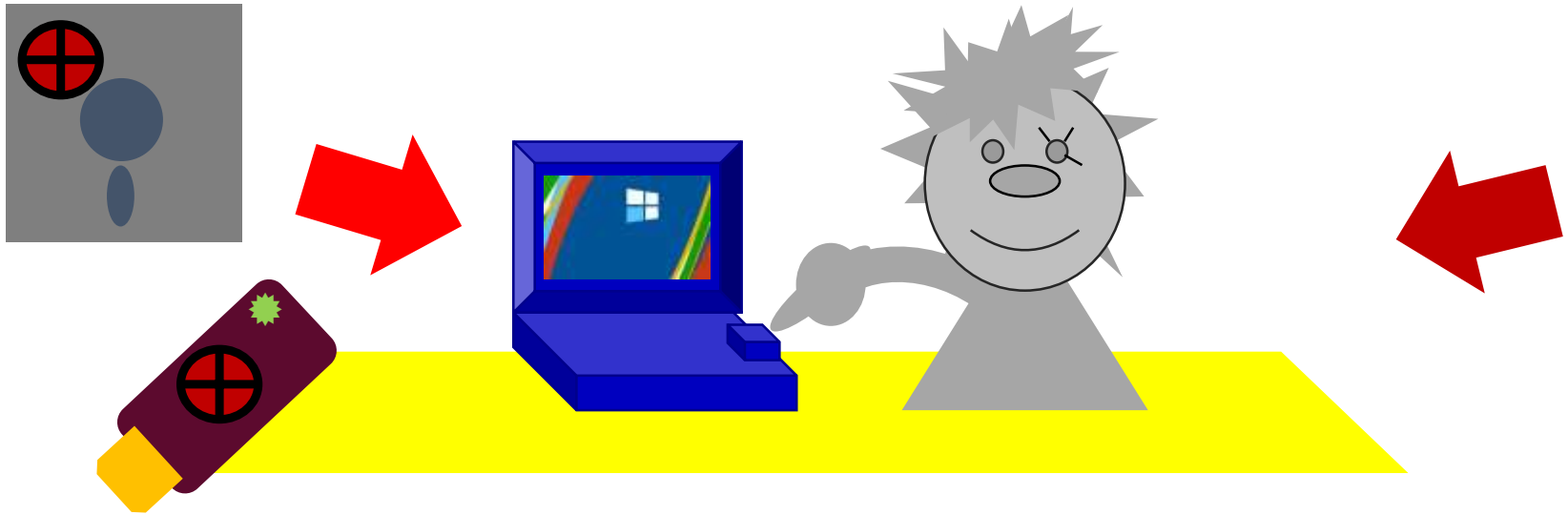
Älä välitä eteenpäin saamiasi virusvaroituksia. Kaupungin haittaohjelmatorjunta säätää jatkuvasti roskapostin suodatusta automaattisesti.

Jos työaseman käytössä on ongelmia, **ota reippaasti yhteyttä ict-tukeesi.**

Haittaohjelmia (viruksia) voi tulla tietokoneelle

Älä ota sisältöä käyttöön tuntemattomissa Office asiakirjoissa

siirrettäviltä tallennuslaitteilta,
vanhoista taltioista (”levyistä”),
varmistuksista
(”vanhoista tiedostoista”),
sähköpostiliitteinä,
viestien klikattavien linkkien päästä,
ja ihan asiallistenkin verkkosivujen liitteistä (”mainosliitteistä”).

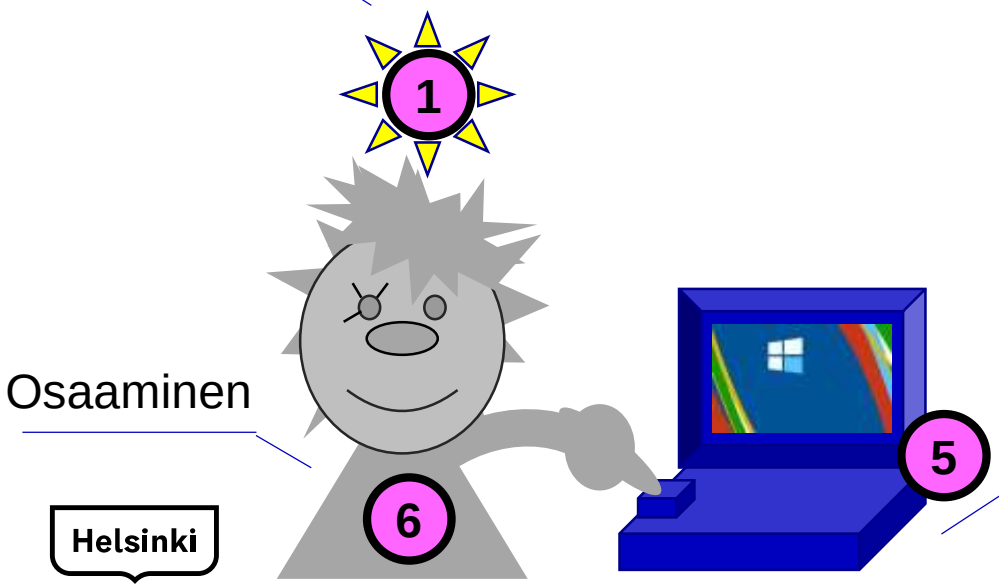


Haitallinen sisältö

Operaattorin
tietoliikenteen
suodatus

Haittaohjelmasuodatus
sisä- ja ulkoverkon
reunalla

Vastuullinen asenne,
oivaltaminen

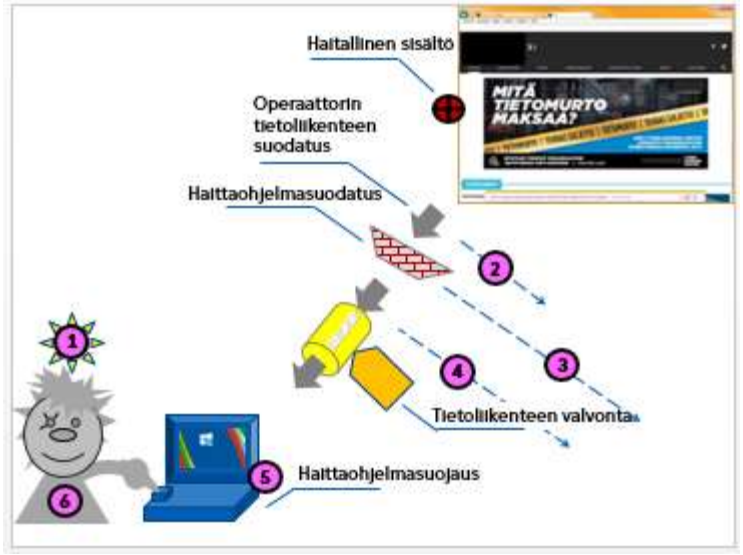


Tietoliikenteen teknisen laadun valvonta

Osaaminen

Haittaohjelmasuojaus ja työaseman palomuuri

Tietoturvallinen tekniikka



2 Haitallisesta verkko- ja viestitietoliikenteestä pyritään automaateilla siivoamaan teknisesti vaarallinen sisältö. 3 4 5

Haitallinen sisältö voi tulla sinänsä ihan asiallisen tietoliikenteen seassa.

- Tärkein osa tietoturvassa onnistumista on henkilön oma vastuullinen
1 asenne tietojenkäsittelyyn
- ja tehtävissään tarvittava ajantasainen
6 osaaminen

jota turvallinen tekninen ympäristö tukee.

Vastuullisuus

Osaaminen

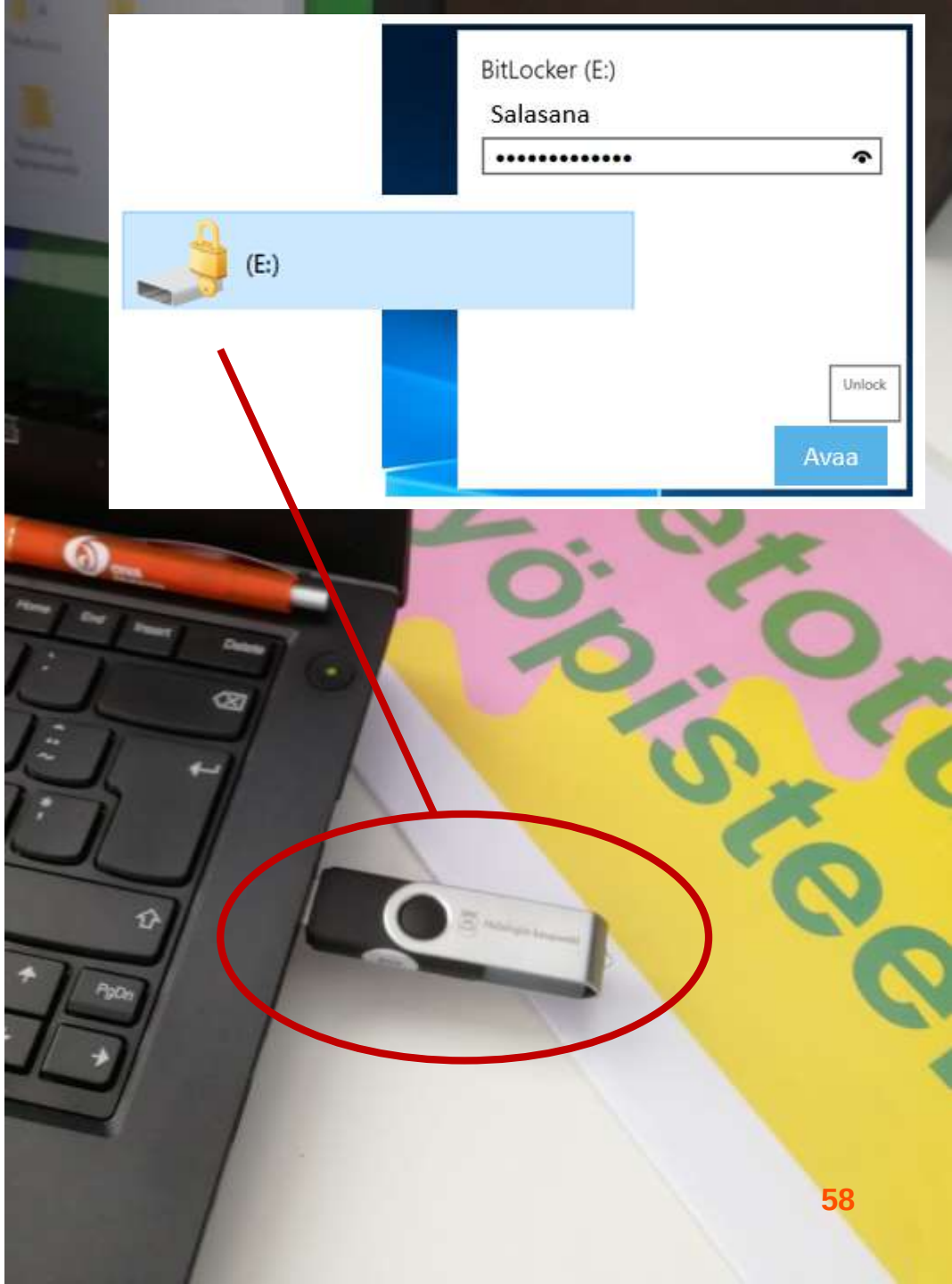
Salakirjoittaminen

Tiedostojen suojaamiseen käytettäviä salakirjoitusohjelmia voi kysyä ICT-tuesta.

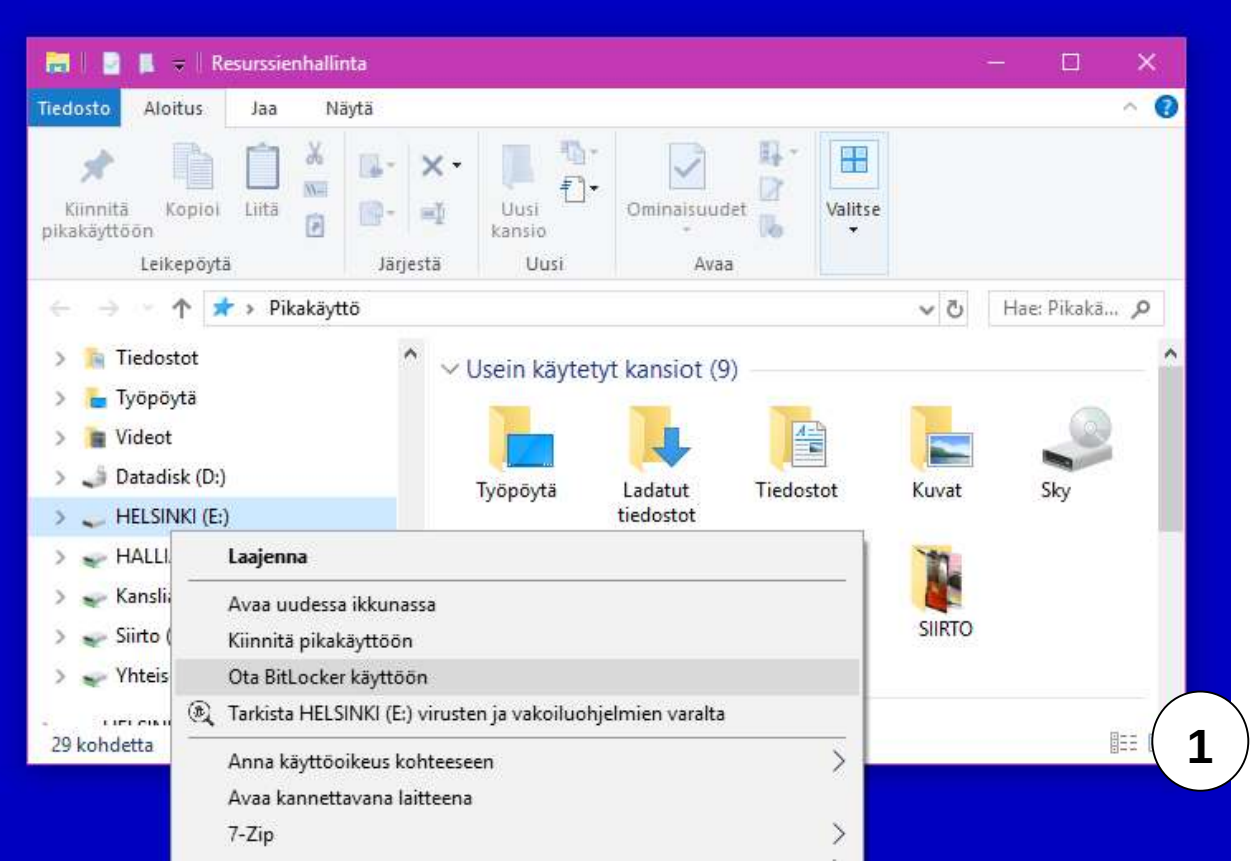
Työpaikan Windows 10 -ympäristössä erillisen muistitikun salaaminen onnistuu käyttöjärjestelmän BitLocker-toiminnolla:

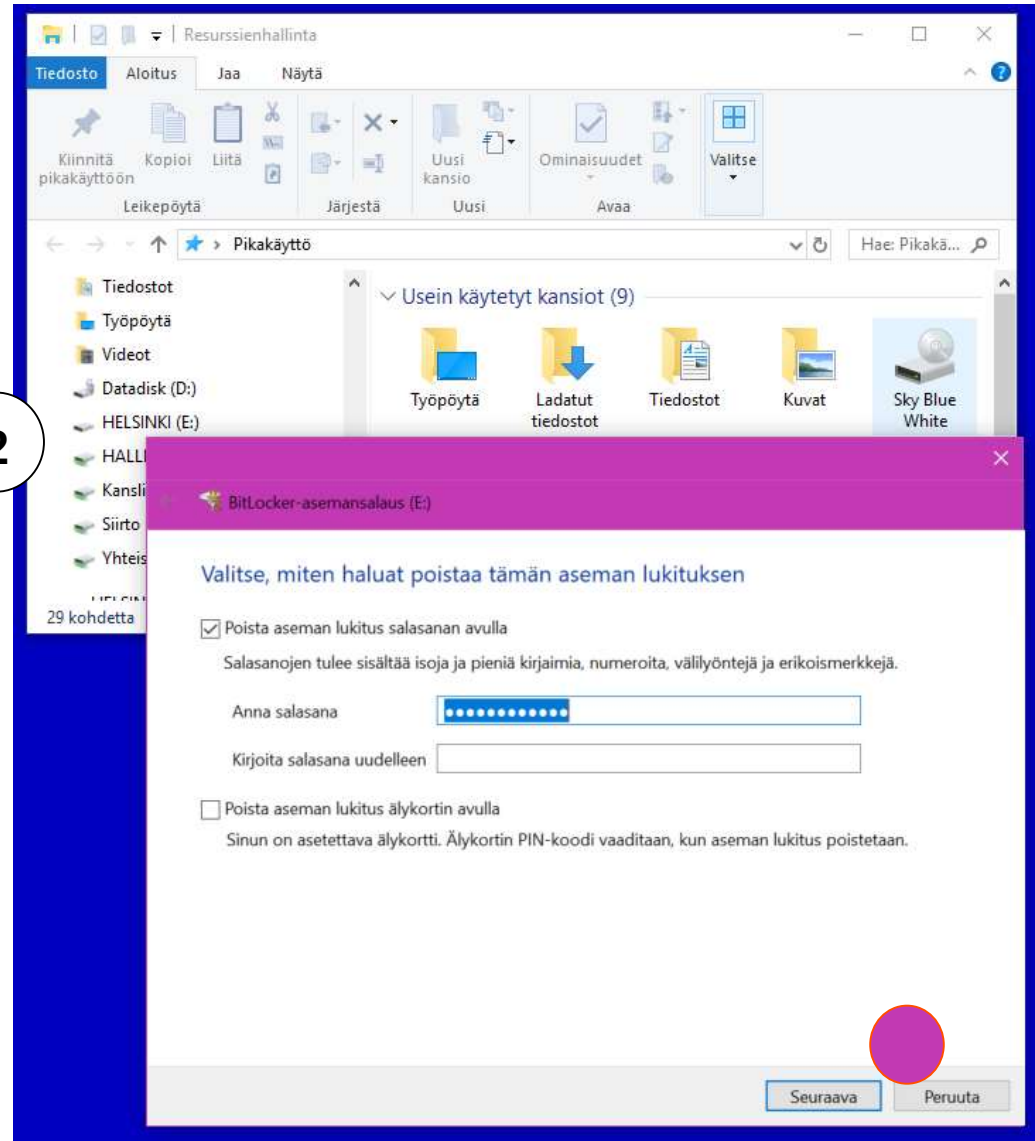
1. Liitä (tyhjä) muistitikku koneeseen.
2. Valitse resurssilistauksessa muistitikun kohdalta ”Ota BitLocker käyttöön” –valinta.
3. Anna pitkä salasana, joka vaaditaan muistitikun tietojen avaamiseksi. Salasana pyydetään kahdesti, jotta se tulee kirjoitettua oikein.
4. Salaaminen tyhjensi tikun ja sitä voidaan jatkossa käyttää antamalla salasana uudestaan, kun muistitikku liitetään koneeseen.

Jos salasanaa ei muista, niin muistitikkua ei saa auki, mutta sen voi ottaa käyttöön (tyhjänä) taas uudestaan uudella salasanalla. Hakemistolistauksessa salatun muistilaitteen tunnistaa lukon kuvasta.



Muistitikun salaaminen työpaikan Windows 10:ssä





Hiiren oikea klikkaus muistitikun kohdalla → Valitse ”Ota BitLocker käyttöön” → Anna pitkä salasana kahdesti

Helsinki

Muistitikut

kaikenlaiset muistilaitteet

Tiedostojen jakaminen

Helsinki

Käsittele siirrettäviä muistilaitteita huolella

4 gigatavun muistitikulle mahtuu yksi puolentunnin jakso HDTV-laadun tv-sarjaa, 4 tuntia tavallisen laadun tv-ohjelmaa tai valvontakameran kuvaa.

Puoli miljoonaa sivua muistiinpanoja eli useita kymmeniä hyllymetrejä mappeja.

128 gigatavun muistitikulle 32 kertaa enemmän

Työkoneeseen liitettäessä
USB-tikku/muistilaite
voi siirtää haittaohjelman mukanaan.

Virusskannaus mieluiten erillisellä tietokoneella.

Korkeampaa turvaa tarvitseva aineisto on salakirjoitettava muistilaitteelle laitettaessa

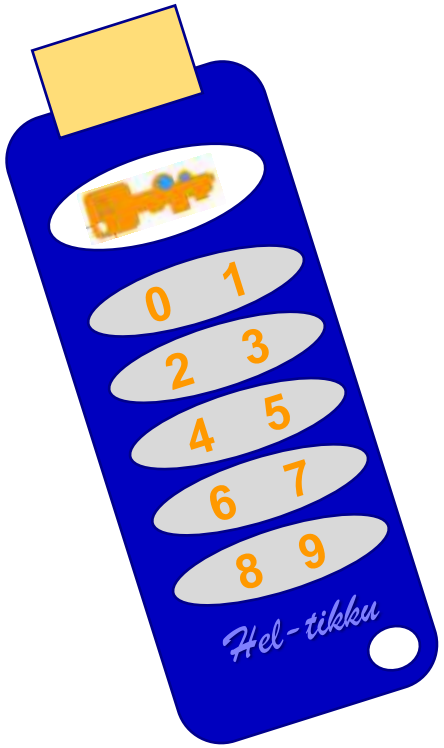
ja samalle tikulle vain saman laatuista aineistoa (ei sekaisin julkista ja salattavaa samalle muistitikulle).

Yksi muistitikku kullekin käyttötarpeelle – ei kannata laittaa kaikkea sekaisin yhdelle ja samalle muistitikulle.

Kun tikulle on kerran laitettu salassa pidettävää aineisto, niin sitä saa käyttää enää ainoastaan salatulle aineistolle (ei saa kierrättää julkisen aineiston käyttöön).

USB-muistin salaaminen

PIN-suojattu salattu muistitikku sisältää numeronäppäimistön



Myös salakirjoituksella suojattuja muistitikkuja on saatavilla. Niiden avaaminen vaatii käyttäjän itse keksimän PIN-numeron antamisen.

Jos PIN unohtuu, niin tikku pitää alustaa uudelleen ja tiedot tyhjentyvät.

Tällainen tikku sopii suojattuun tiedon siirtoon tietokoneiden välillä, muttei pitkäaikaiseen tallentamiseen.

Automaattinen lukitus suojaa muistitikun, kun se irrotetaan tietokoneesta. Käyttäjä antaa tikkuun oma PIN-numerokoodin. Sama muistitikku voi toimia Windows-, Mac- ja Linux-ympäristöissä.

Tarvittaessa kysy muistitikkujen käytöstä teidän omalta lähituelta (ICT-tuki).

Joissain ympäristöissä USB-tikkuja ei saa käyttää ilman erillistä lupaa.

USB-muistitikkujen kytkeminen

Muistitikku voi sisältää ohjelmia, joita ei näe sen sisällysluettelossa

Muistitikulle mahtuu kokonainen käynnistyvä käyttöjärjestelmä, jolla saattaa voida käynnistää tietokoneen

Joissain ympäristöissä USB-tikkuja ei saa käyttää ilman erillistä lupaa, sillä muistitikkujen mukana voi tulla haittaohjelmia, jotka käynnistyvät automaattisesti liitettäessä tikku koneeseen.

Mahdollisuuksien mukaan kannattaa käyttää verkosta ”irrallisia” laitteita esitelmiin tilaisuuksissa, joissa useita tikkuja kytketään koneeseen esitysten siirtämiseksi.

Olisi hyvä virusskannata muistitikku erillisellä laitteella ennen kytkemistä työpaikan verkkoon liittyvään laitteeseen.

”Löytötikuista” ei tule kokeilla mitä sieltä löytyisi, vaan

vie löytynyt muistitikku löytötavaroiden vastaanottajalle.

Tiedostojaon käyttö Windows OneDrive

Muistitikun sijaan voi olla mahdollista käyttää tiedostonjakoa tiedostojen siirtoon käyttäjältä toiselle tai tietokoneiden välillä.

Esimerkiksi Helsingin kaupungilla käytössä olevalla OneDrive-palvelulla tiedosto voidaan siirtää hallitusti. OneDrive löytyy esimerkiksi työpaikan Microsoft Office 365-palvelusta (office.fi, office.com).

Talletetaan tiedosto OneDriveen ja jaetaan se halutun käyttäjän kanssa lähettämällä hänelle sähköpostilla linkki tiedostoon.

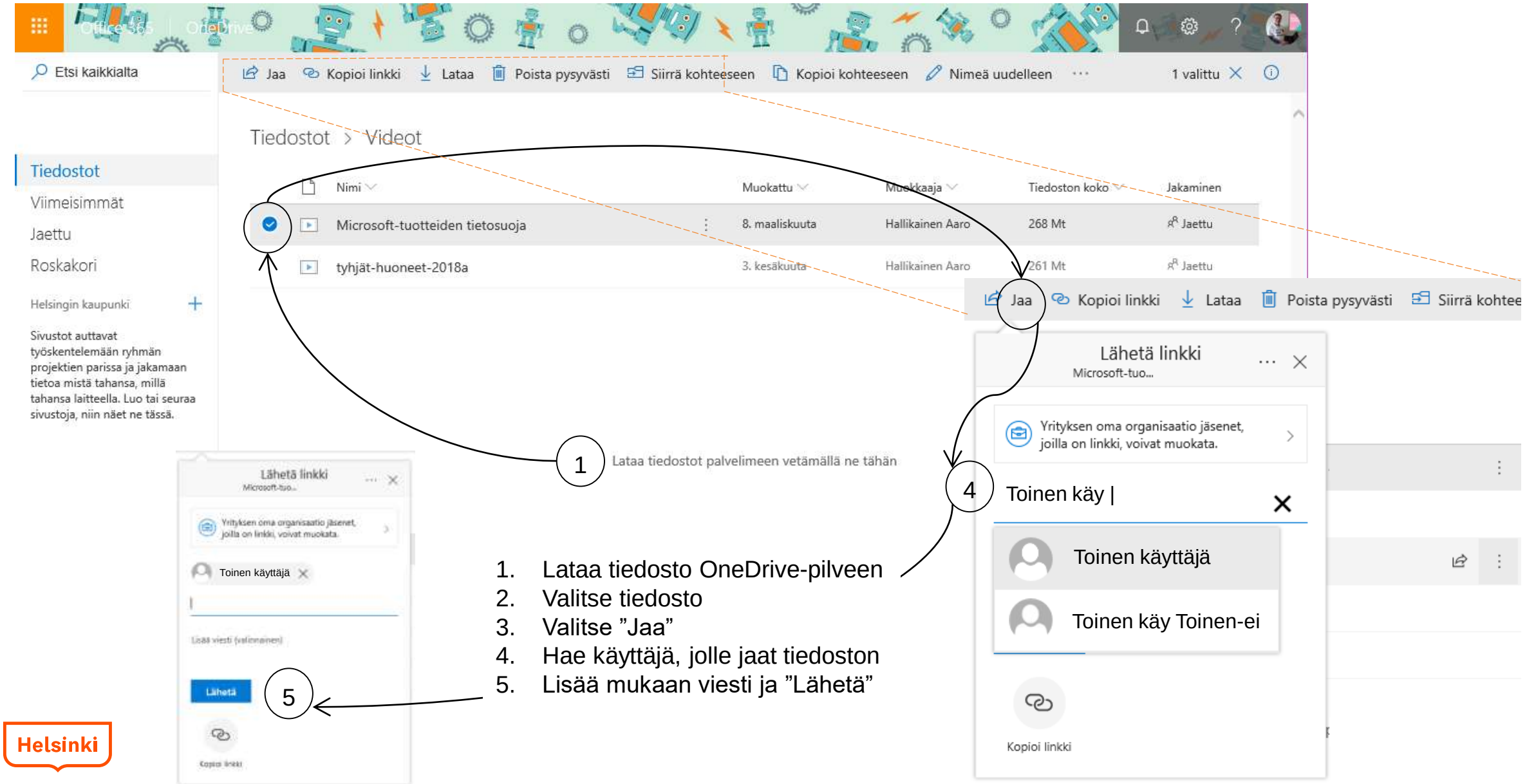
Kun henkilö on hakenut tiedoston, niin sen voi poistaa OneDrivesta.

Näin tiedosto ei unohdu jäämään muistitikulle.

Kysy tiedostojen siirtopalvelusta omalta lähitueltasi / tietohallinnosta.

Toimialalla tai yksiköllä voi olla omia tapoja / ratkaisuita jakaa tiedostoja.

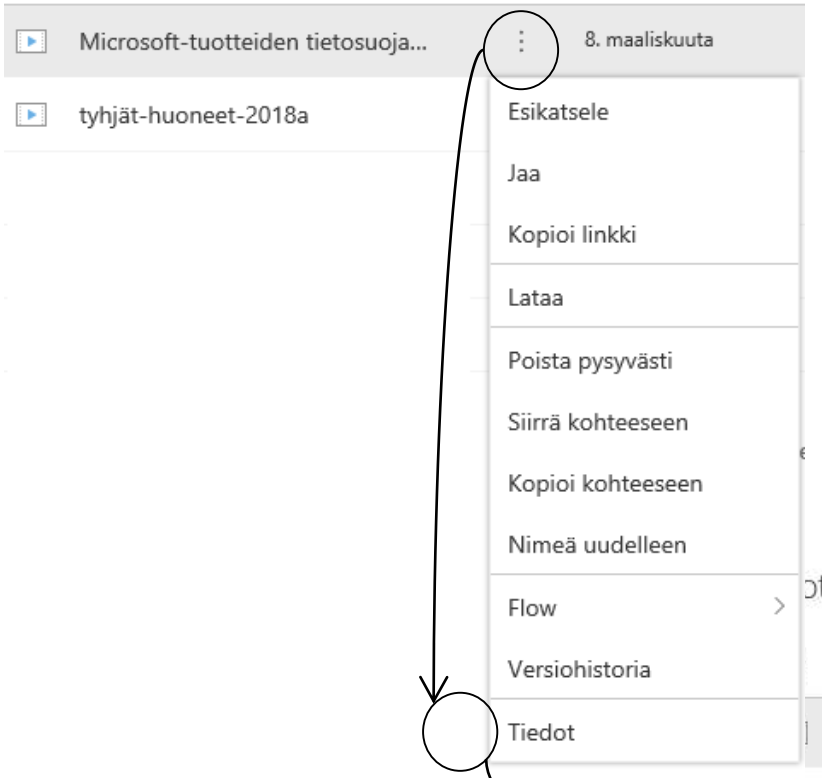
OneDrive – Ison tiedoston jakaminen



1. Lataa tiedosto OneDrive-pilveen
2. Valitse tiedosto
3. Valitse ”Jaa”
4. Hae käyttäjä, jolle jaat tiedoston
5. Lisää mukaan viesti ja ”Lähetä”

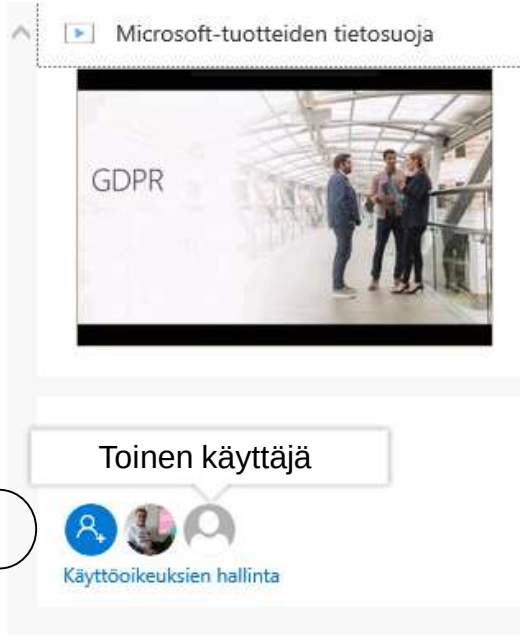
Helsinki

OneDrive – Tiedoston käyttöoikeudet



Tiedoston käyttöoikeudet näkee ja niitä voi muuttaa ”Tiedot”-valinnasta

1. Valitun tiedoston kohdalla
2. Klikkaa ⋮
3. Valitse ”Tiedot”
4. Näet käyttäjien tiedot
5. ja voit muuttaa niitä ”Käyttöoikeuksien hallinta”-valinnasta



Helsinki

Varmuuskopio

Helsinki

Korkeasaaren eläintarha korkeasaari.fi / kuvaaja Mari Lehmonen

Tärkeät tiedot varmuuskopioidaan

ja kokeillaan silloin tällöin että ne voidaan tarvittaessa palauttaa takaisin käyttöön.

Työpaikan verkkoaseman hakemistot varmuuskopioidaan automaattisesti.

Työaseman paikallinen levy sopii vain sellaiselle tiedolle, jota ei kaipaa jos se häviää.

Jos tiedot menevät käyttökelvottomiksi, niin varmuuskopioilta saadaan tiedot takaisin.

Varmuuskopiot ovat vakuutus kiristyshaittaohjelmien varalle

Erilaiset kiristyshaittaohjelmat ovat nousseet uutisiin ja merkittäväksi ongelmaksi. Tiedostot salakirjoittavan haittaohjelman ja myös laiterikosta johtuvan tietojen menettämisen viimeinen suojakeino on ajantasaiset tietojen ja ohjelmien varakopiot/varmuuskopiot.

Varmuuskopioita on erilaisia:

- Samalla laitteella/levyllä oleva lähikopio siltä varalta että tarvitsee pian ottaa vanha tieto käyttöön
- Eri tallennusvälineellä (muistitikku, toinen tietokone, usb-levy…) oleva samoissa huonetiloissa (samassa palotilassa) oleva melko tuore kopio siltä varalta että tiedot tarvitsee asennella uudestaan
- Toisessa tilassa (pilvipalvelussa tms.) oleva turvakopio ison ongelman varalta

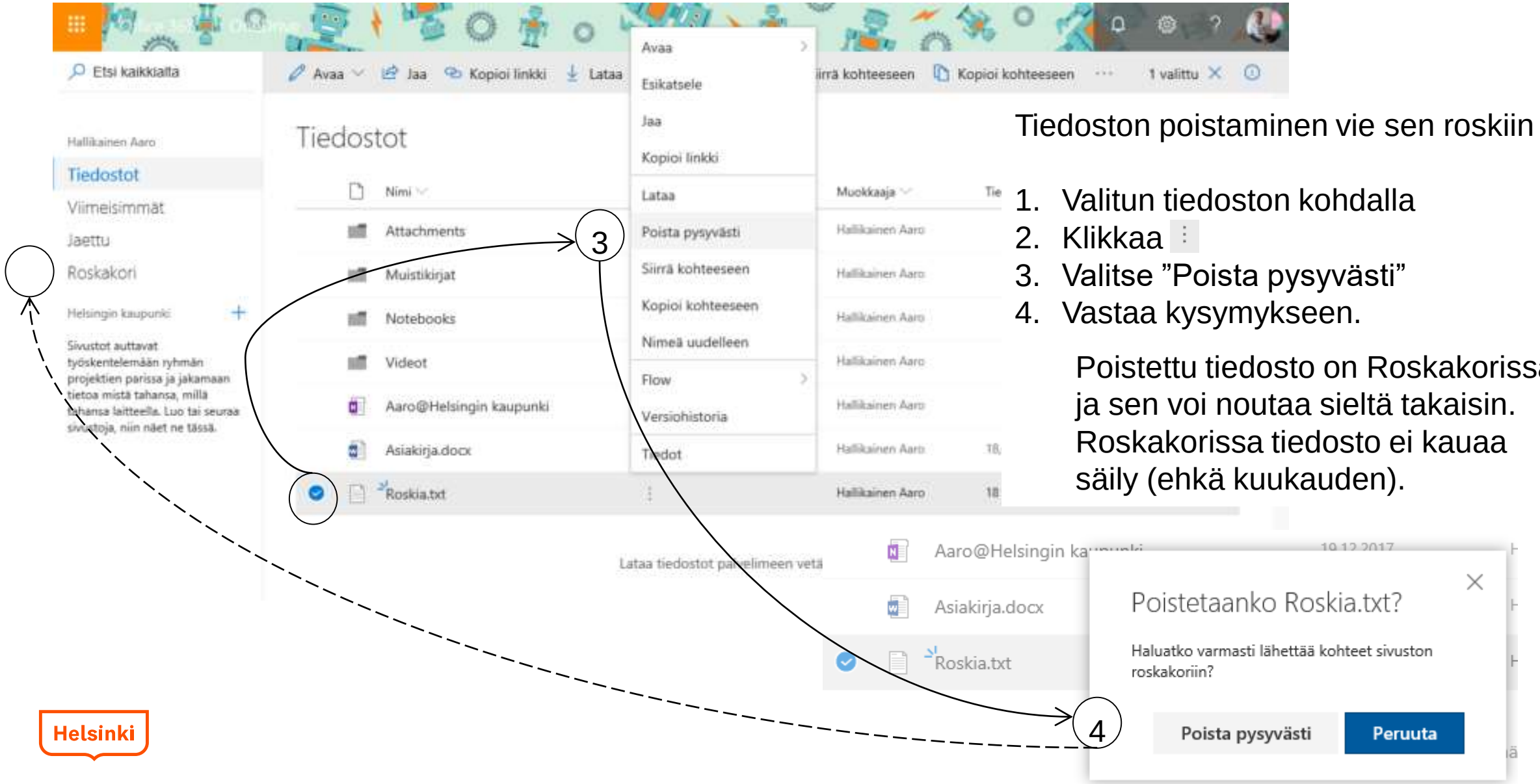
Tiedostojen säilyminen ja poisto

Varmuuskopiot otetaan tietyin säännöllisin ajoin. Tyypillistä on, että verkkolevyn tiedot on mahdollista saada takaisin jonkin rajatun ajan takaa (esimerkiksi vuoden tai muutaman kuukauden). Varsinaisten tietojärjestelmien tiedot taas varmuuskopioidaan yleensä useiden vuosien ajalta.

Työpaikan verkkoaseman kotihakemiston ja OneDriven tiedostot säilyvät siellä toistaiseksi. OneDrivessa käyttäjän itse poistama tiedosto siirretään ensin ”sivuston peruskäyttäjän roskakoriin” ja sieltä se poistuu ”toisen vaiheen roskakoriin” joista kummastakin käyttäjä voi sen itse vielä käydä hakemassa takaisin käyttöön.

Roskakoreissa tiedostot eivät kuitenkaan kauaa säily – ehkä kuukauden tai muutaman kuukauden. Verkkoaseman kotihakemistosta poistettu tiedosto ei ole käyttäjän itse palautettavissa. Työaseman paikallisesta hakemistosta poistettu tiedosto taas löytyy tietokoneen paikallisesta roskakorista.

OneDrive – Tiedostojen hallinta

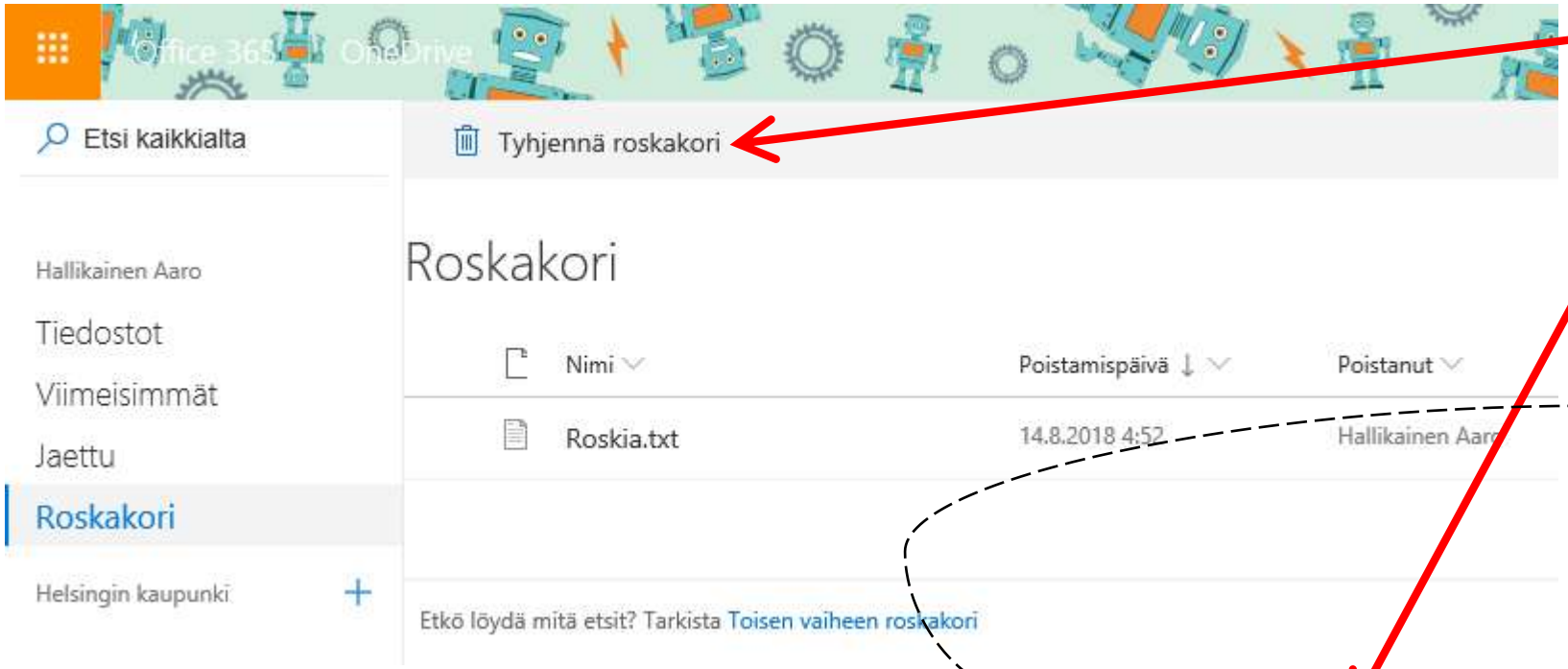


Tiedoston poistaminen vie sen roskiin

1. Valitun tiedoston kohdalla
2. Klikkaa ⋮
3. Valitse ”Poista pysyvästi”
4. Vastaa kysymykseen.

Poistettu tiedosto on Roskakorissa ja sen voi noutaa sieltä takaisin. Roskakorissa tiedosto ei kauaa säily (ehkä kuukauden).

Roskakori – Tyhjennä, palauta, poista



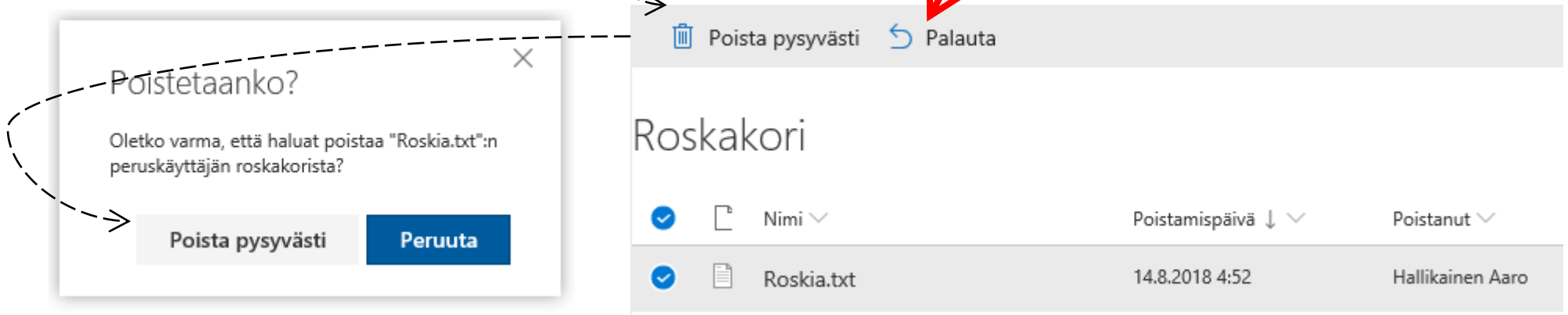
Roskakorin voi tyhjentää

tai valita tiedoston jonka

1 palauttaa takaisin sinne mistä se poistettiin tai

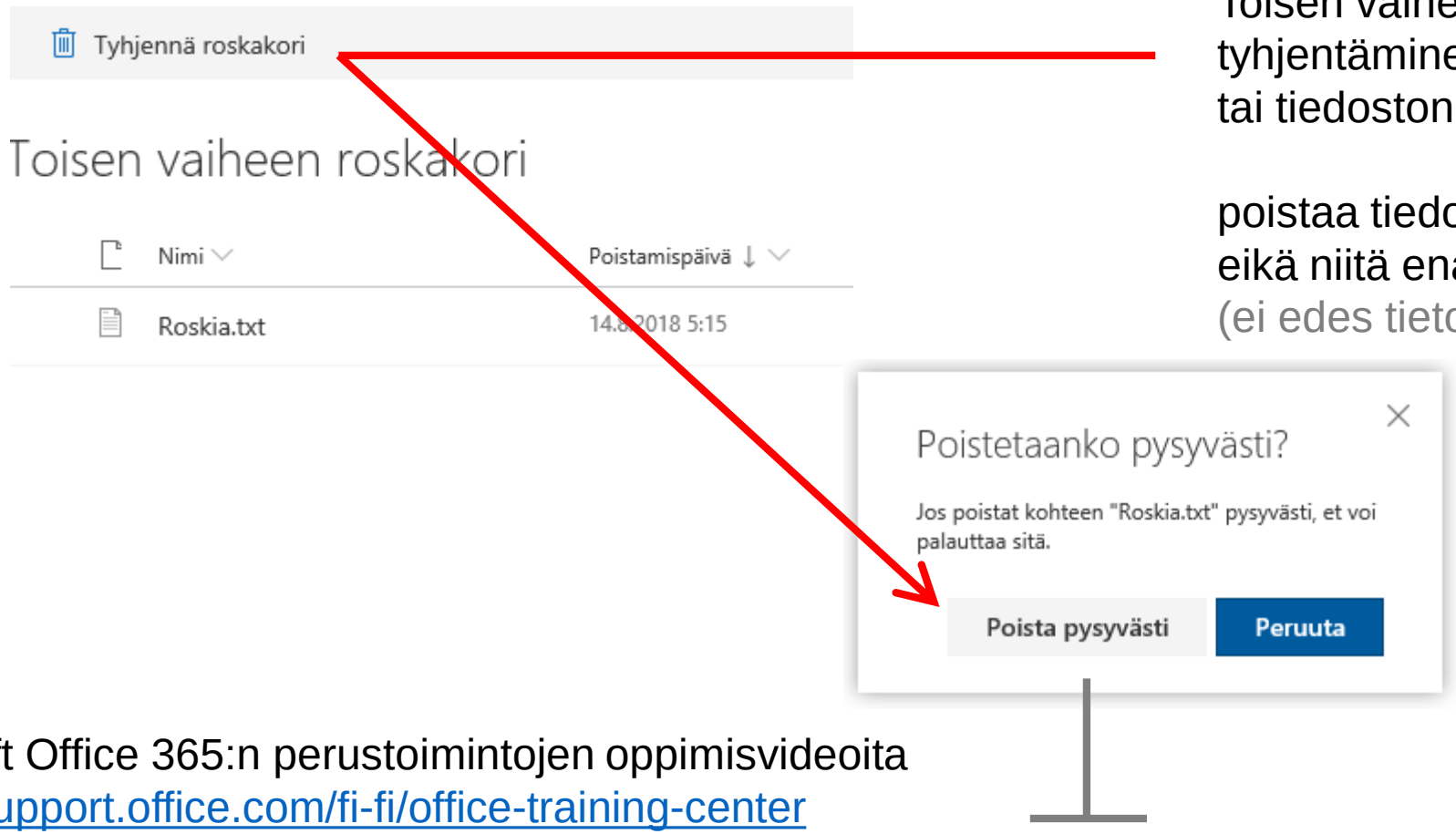
2 poistaa pysyvästi

jolloin roskat menevät ”toisen vaiheen roskakoriin”



Helsinki

OneDrive - Poista pysyvästi



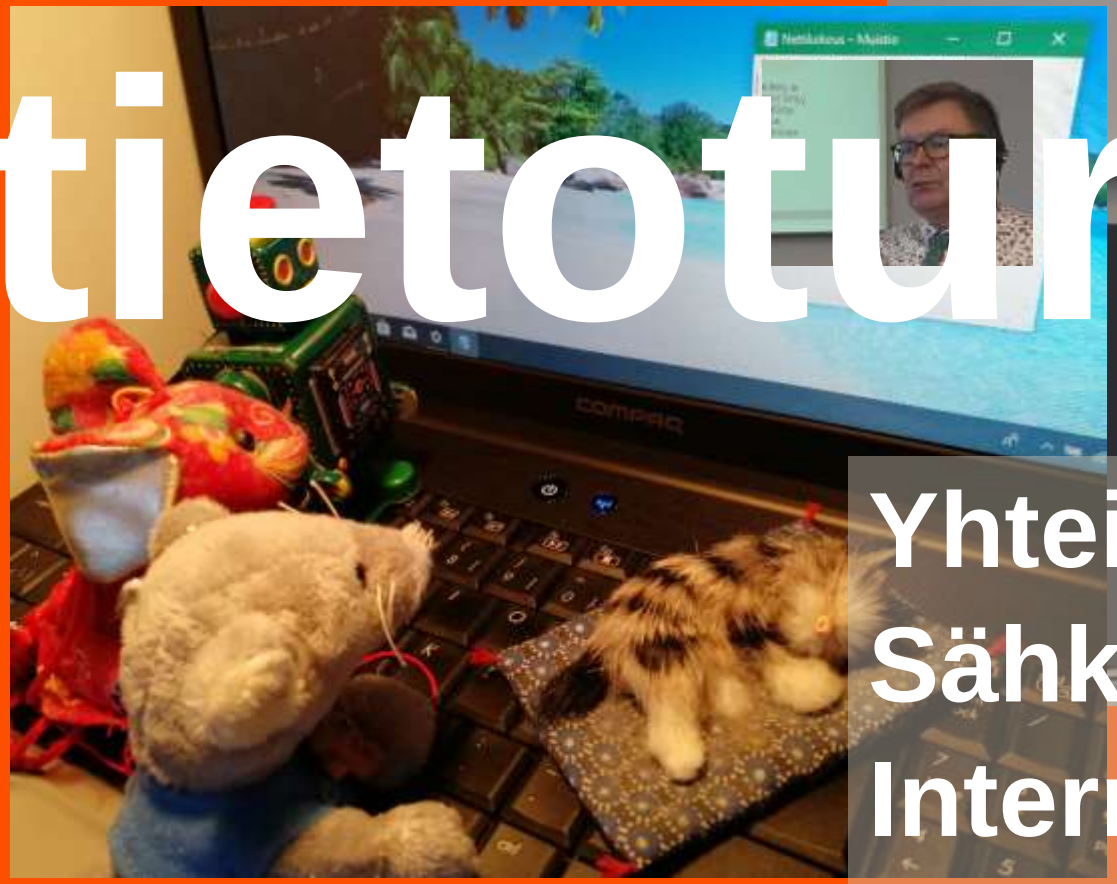
Toisen vaiheen roskakorin tyhjentäminen
tai tiedoston poisto sieltä

poistaa tiedostot pysyvästi
eikä niitä enää saa takaisin
(ei edes tietohallinto).

Microsoft Office 365:n perustoimintojen oppimisvideoita
https://support.office.com/fi-fi/office-training-center

Officen vihjeitä ja vinkkejä
https://support.office.com/office-training-center/featured-tips

Viestinnän tietoturva



Yhteistyö ja tiedon jakaminen
Sähköposti
Internet
Sosiaaliset mediat

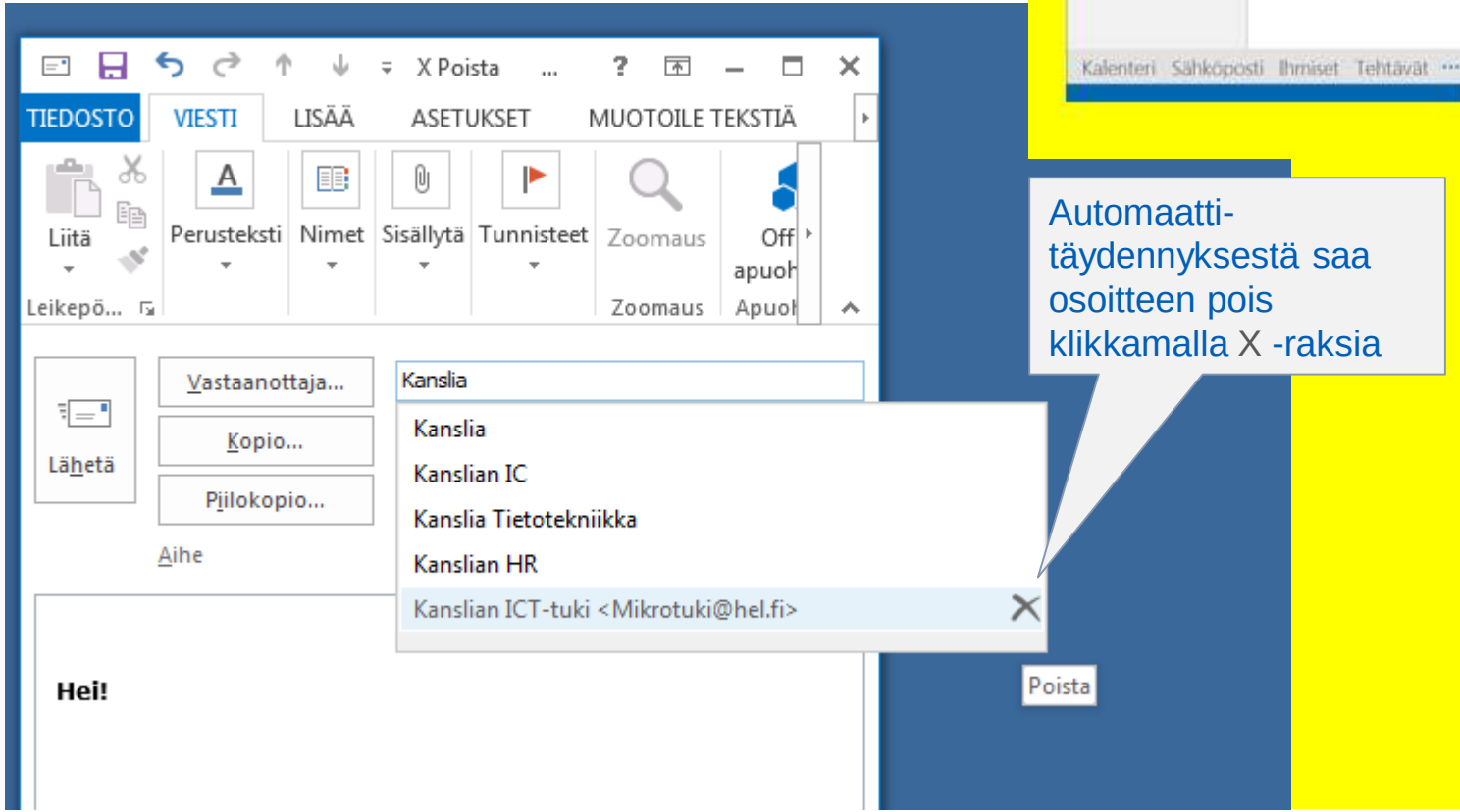
Helsinki

Sähköposti

tavanomaiseen viestintään

Älä uudelleen ohjaa työpaikan sähköposteja yksityisiin postilaatikoihin.

Tarkista vastaanottaja huolellisesti.



Helsinki

Sähköposti

Klikkaa ajatuksella

Hoidettaessa työasioita sähköpostin avulla lähettäjän tulee varmistua viestin perillemenosta.

Huomioi, että henkilökohtaiselle sähköpostiosoitteelle lähetetty viesti ei välttämättä mene perille esimerkiksi vastaanottajan pitkän poissaolon tai verkkoliikenteen ruuhkaisuuden takia.

Virusvaaran vähentämiseksi
liitteiden käsittelyssä on noudatettava huolellisuutta.

Tarpeettomia liitteitä ei kannata lähettää. Usein tekstin voi kirjoittaa suoraan sanomakenttään.

Liitettä ei pidä avata, jos lähettäjä on tuntematon tai sanomakentässä ei ole viestiä.

Suurikokoisia tiedostoja ei kannata lähettää sähköpostin liitteenä vaan käyttää siirtoon soveltuvaa ryhmätyötilaa tai esimerkiksi Helsingin työkäyttöön tarjolla olevaa OneDrivea.

Sähköpostin käytössä kiellettyjä asioita ovat massapostitukset summittaiselle joukolle sekä ketjukirjeiden luominen ja välittäminen.

Suojattu sähköposti

Jos tarvitset salassa pidettäville tiedoille soveltuvaa sähköpostia, niin kysy paikalliselta tueltanne kuinka saat sellaisen käyttöösi.

Helsingin kaupungilla on tarjolla viranomaiselle hyväksyttävää laatua oleva suojatun sähköpostin järjestelmä sitä työssään tarvitseville.

Helsingin kaupunki / Kuvaaja Aaro Hallikainen

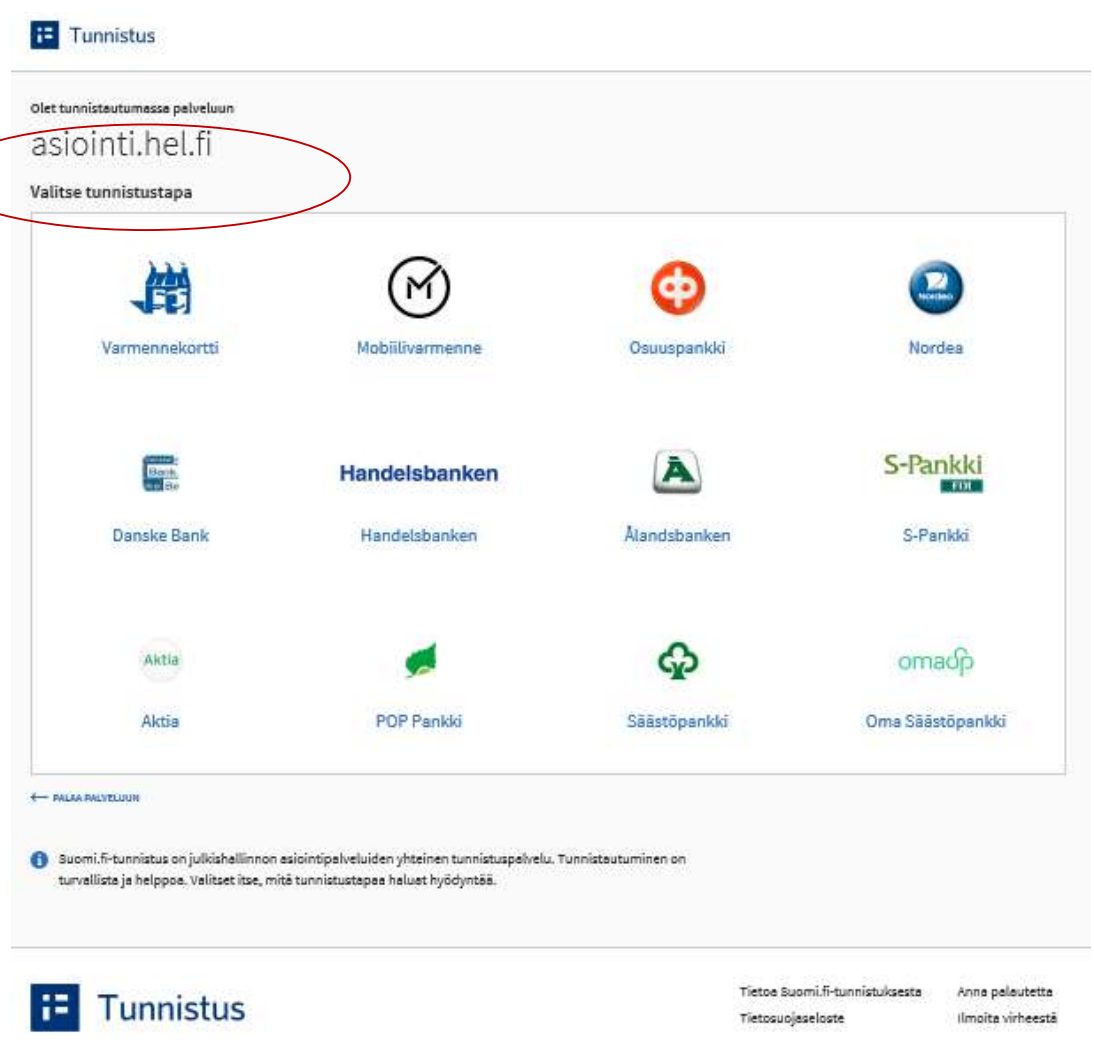
Turvallinen asiointi

Turvallinen tietojen vaihto onnistuu asiointijärjestelmillä.

Niissä vastaanottaja tunnistetaan luotettavasti pankkitunnuksilla tai puhelimen mobiilivarmenteella.

Käyttötunnus-salasana-pari ei ole yleisesti luotettava tunnistus. Sosiaalisten medioiden käyttötunnukset eivät ole luotettava tunnistus (Facebook, Google tms. tunnuksella yksilöity asiointi ei ole vahva tunnistus).

Ääni puhelimessa ei ole luotettava tunnistus.

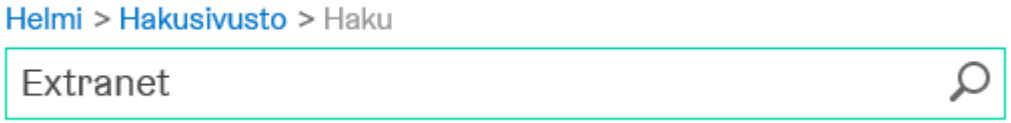


Käyttäjä voidaan yksilöidä tunnistamatta
tai tunnistaa vahvasti (tai vähemmän vahvasti)
tai olla kokonaan yksilöimättä
(anonyymikäyttö, tunnistamaton käyttäjä)

Rajoitetun käyttäjäryhmän yhteistyöskentely

Helmen työtilat ja extranet-työtilat soveltuvat rajoitetun käyttäjäryhmän tiedon jakamiseen ja yhdessä tuottamiseen. Työtilat kaupungin sisäisille ryhmille, extranet-työtilat myös yhteistyökumppaneille.

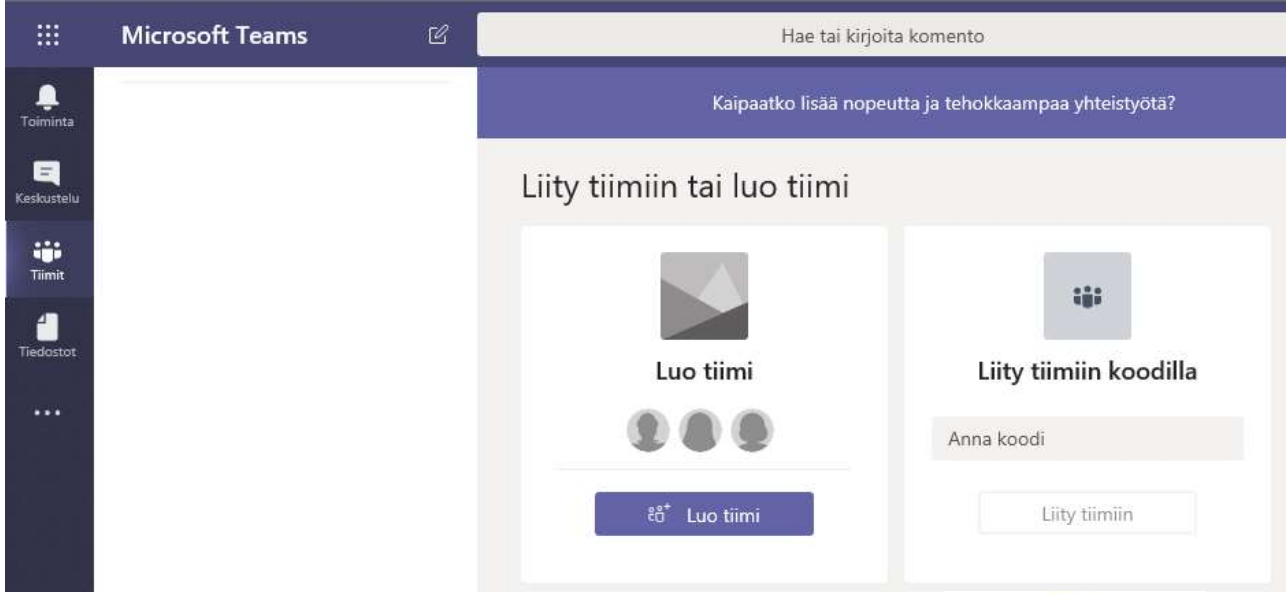
Lisätietoja:



hakusanalla ”extranet” ”työtilat” Helmestä

Microsoft Teams

Toimialalla tai yksiköllä voi olla käytössään myös
Microsoft Teams ryhmätyöympäristö.



Teams-työyhmät voidaan rajata tietyille, kutsutuille osallistujille.
Työryhmään voi kutsua muitakin kuin Helsingin sähköpostin käyttäjiä.

Muut ryhmätyöympäristöt

Jos käytetään muita verkosta löytyviä työvälineitä, niin aina tulee huolehtia, että tiedot joita siellä käsitellään voidaan käsitellä kyseissä ympäristössä. Lopputuotteet (raportit, tekniset piirustukset, videot…) tulee aina huolehtia niille kuuluvalle paikalle kaupungin hallitsemiin ympäristöihin, tietojärjestelmiin ja arkistoihin. Työympäristölle on hyvä olla ainakin kaksi vastuullista pääkäyttäjää.

Internet

julkisen verkon palvelut

Kun internetiä käytetään työpaikalta, työaseman tunnistetiedoista ja käyttäjän sähköpostiosoitteesta selviää, että käyttäjä on Helsingin kaupungin palveluksessa.

Internetin käytöstä jää aina tietoa jonnekin. Kohdepalvelimet pitävät kirjaa siitä, mistä yhteyksiä on otettu. Näitä tietoja saattaa joku taho käyttää esimerkiksi suoramarkkinointiin ja roskapostien lähettämiseen. Niitä saatetaan käyttää myös roskaviestien väärennettyinä lähettäjätietoina. Kaupungin järjestelmät saavat kerätä käyttötietoja siitä, *mihin* kaupungin työasemilta on otettu yhteyksiä. Lokeja saa käyttää mahdollisissa ongelmatilanteissa.

Internetissä on sivuja, jotka pyytävät käyttäjää rekisteröitymään.
Rekisteröitymisissä ei saa käyttää kaupungin järjestelmien käyttäjätunnuksia ja salasanoja.

Työhön liittyvässä rekisteröitymisessä voi kyllä käyttää omaa, julkista työsähköpostiosoitetta, mutta salasanan on oltava kullekin palvelulle omansa.

Internetistä ei pidä tarpeettomasti kopioida tiedostoja. Vaikka aineisto (kuva tms.) on verkossa saatavilla, niin niihin liittyy silti tekijänoikeuksia. Tiedostot voivat myös sisältää haitallista ohjelmakoodia.

Jos verkkosivu ehdottaa lisäosien asennuksia, niin niitä ei pidä asentaa.
Uusien, työssä tarvitsemiesi ohjelmien asentamiseksi pyydä apua lähitueltasi (ICT-tuki).

Internetistä ladattavat suuret tietomassat kuten suoratoisto voivat hidastaa koko tietoliikenneverkon toimintaa. Kaupungin tietoverkko on suunniteltu työtehtävissä tarvittavia tietoliikennemääriä varten, joten vältä työhön liittymätöntä suoratoistoa.

Sosiaalisen median ohjeista

Verkkofoorumeilla (sosiaalisessa mediassa) toimimiseen liittyy samanlaiset tietoturvan ja tietosuojan periaatteet kuin muissakin keskustelu-, tiedonkäsittely- ja ryhmätyöympäristöissä.

Tietoturvan kannalta erityisenä piirteenä on varoa luottamuksellisen tiedon paljastamista verkkokeskusteluissa tai postauksissa (esimerkiksi henkilön yksilöivien tietojen paljastamista, jotka kuuluvat tietosuojan piiriin).

Verkkofoorumeilla on myös hyvä tiedostaa, että foorumin käyttäjiä ei välttämättä ole vahvasti tunnistettu. Verkkokeskustelut voivat myös vääristyä, jos keskustelun osia voi poistaa tai muuttaa.

Ja vaikkakin verkkopalvelut ovat erittäin hyvin saatavilla, niin silti voi olla tilanteita joissa verkon sosiaaliseen palveluun ei pääse kirjautumaan.

Palvelimet voivat sijaita missä päin maailmaa tahansa, ja se voi vaikuttaa mahdollisuuteen osallistua palveluun. Rajatulle käyttäjäryhmälle varattu sosiaalisen median ryhmä ei välttämättä sovellu tietojen luottamuksellisuuden säilyttämiseen kunnolla.

Omasta käyttötunnuksesta tulee pitää hyvä huoli. Jos joku muu pääsee niillä palveluun, niin hän voi esiintyä toisena henkilönä ja aiheuttaa ongelmia esimerkiksi pyrkimällä kaappaamaan käyttäjän muidenkin palveluiden tilejä.

Lisää aiheesta: ”Sosiaalisen median tietoturvaohje” VAHTI 4/2010
https://www.vahtiohje.fi/web/guest/johdanto27

Tietotekniikkaongelmissa kysy paikallisesta ICT-tuestasi apua!

(lähituki, atk-tuki)

Helsinki

Hallinnollinen tietoturva

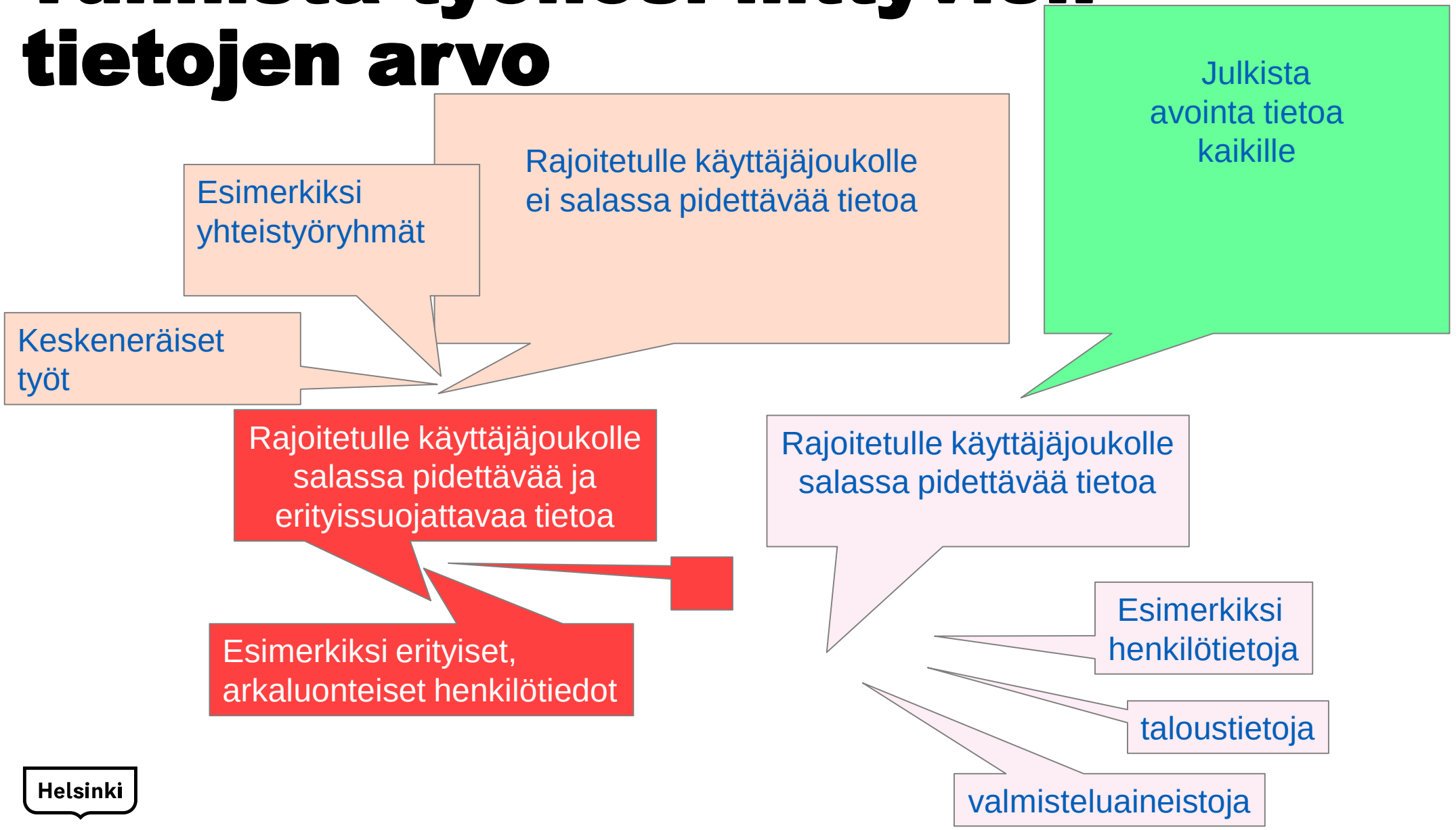
Ohjeet

Organisointi

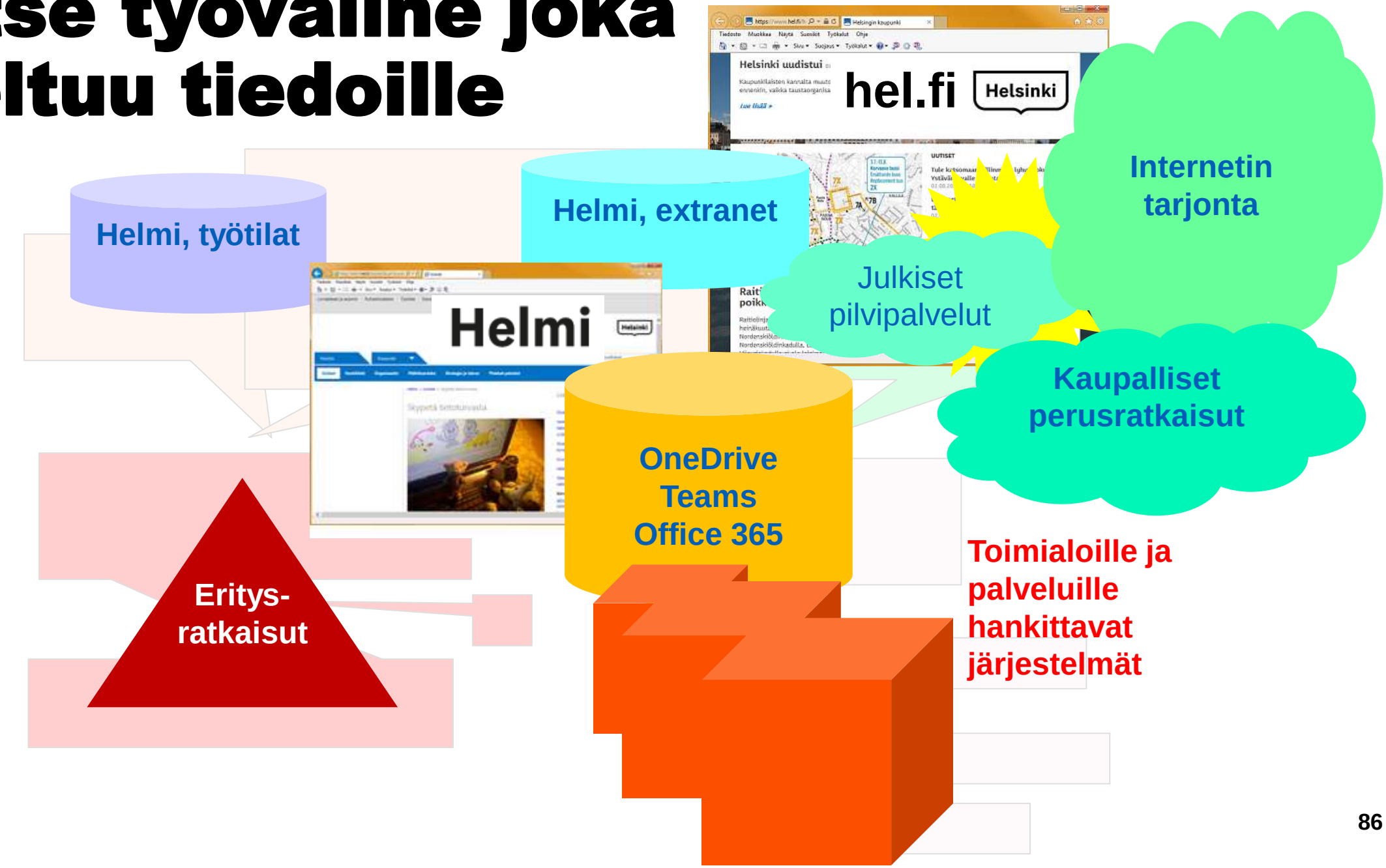
Johtaminen

Helsinki

Tunnista työhösi liittyvien tietojen arvo



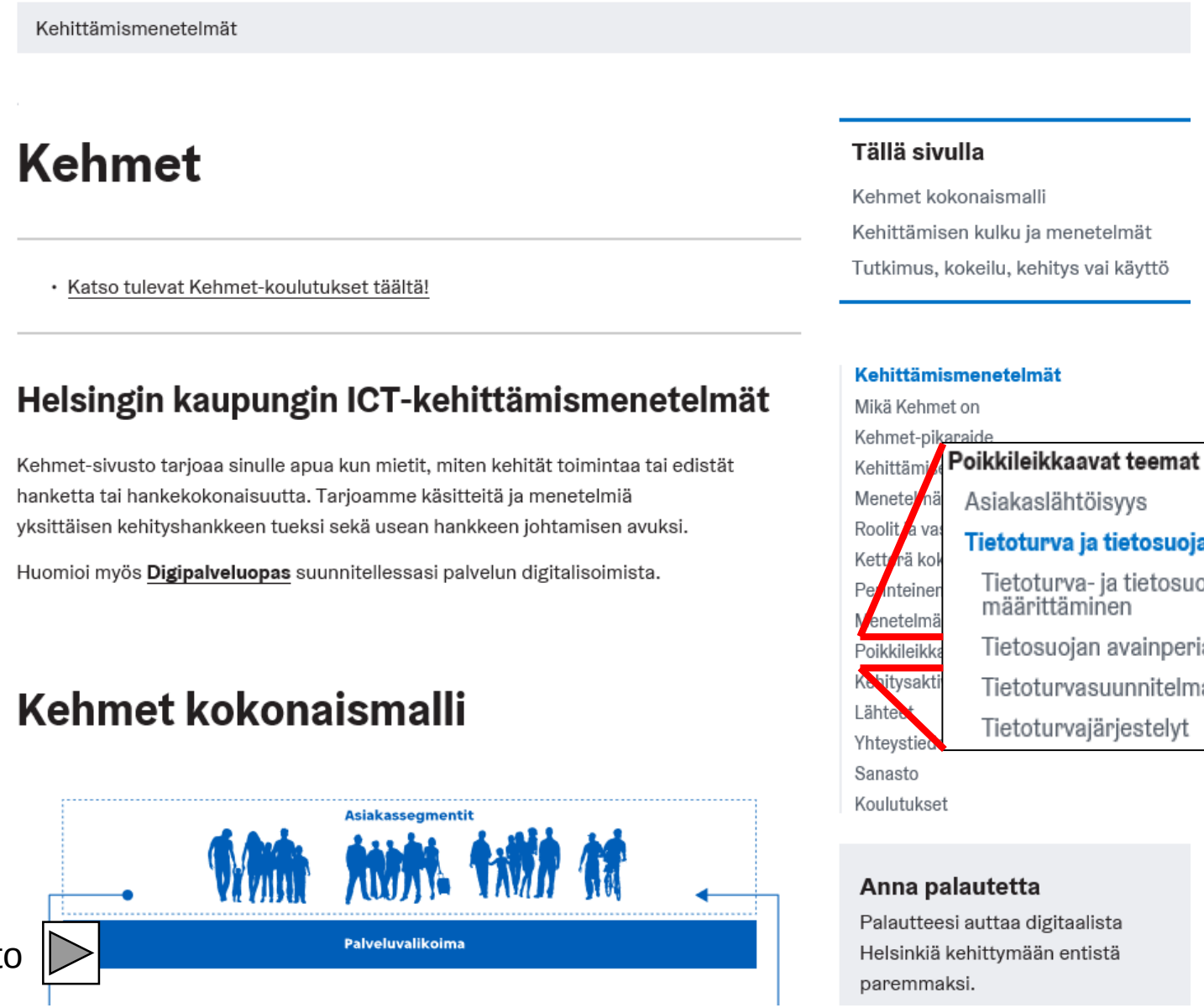
Valitse työväline joka soveltuu tiedoille



Helsingin ICT-kehittämismenetelmät

ICT-järjestelmien kehittäjille löytyy tueksi Helsingin kehittämismenetelmät, joita seuratessa tulee kehitystyön edetessä huomioitua myös tietoturvaan ja tietosuojaan liittyvät kysymykset.

kehmet.hel.fi



Helsingin kaupungin oma yleinen ohjeistus tietoturvasta

Tämä esitelmäkuvasarja on toimitettu Helsingin kaupungin käyttöön yleiseksi henkilökunnan ohjeeksi tietoturvan asioista. Helmessä hae: ”tietoturva”

Nämä ovat yleisiä esimerkkejä hyvistä tietoturvaan liittyvistä työtavoista jokaiselle Helsingin työntekijälle tietoturvan huomioimiseen kaikissa Helsingin työtehtävissä.

Tietoturvaan liittyvää koulutusta löydät Helmen koulutuskalenterista (hae: ”tietoturva”).

Toimialat ja yksiköt antavat omaan tarpeeseensa tarkasti soveltuvat omat toimintaohjeensa.

Helsingin kaupungin ohjeistusta liittyen myös tietoturvaan

Kaupunkikonsernin turvallisuusperiaatteet; tietoturva on yksi organisaatioturvallisuuden osa-alueista
https://dev.hel.fi/paatokset/asia/hel-2017-000339/11010vh1j-2017-14/

Organisaatioturvallisuuden linjaukset; tietoturvan organisointi on osa organisaatioturvallisuuden organisointia
https://dev.hel.fi/paatokset/asia/hel-2017-004903/02100vh2-2017-22/

Sisäisen valvonnan ja riskienhallinnan ohjeistus; ohjeet soveltuvat myös tieto- ja ICT-riskien hallintaan
Kaupunginhallituksen päätös 13.1.2020,
Sisäisen valvonta ja riskienhallinta Helsingin kaupunkikonsernissa -ohje

Tietosuojalinjaukset; linjaus henkilötietojen turvalliseen käsittelyyn
https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/tietoa-helsingista/tietosuoja/

helsinkikanava.fi

Tietoturva työpisteellä

Onnistuvaa tietoturvaa 2020 – perusasioita

ICT riskienhallinta

Tietoturva päivittäisessä työssä

Tietoturva työpisteellä: Salsa-ananas

Tietoturva työpisteellä: Muistitikun elämää

Arkipäivän tietoturva

Helsinki-kanavan
”tietoturva työpisteellä” -sarjassa
on tietoturvaan liittyviä videoita.

https://www.helsinkikanava.fi/fi/web/helsinkikanava/folder?groupItemId=39419608

Ne ovat käytettävissä toimialojen ja
yksiköiden tietoturvan koulutukseen
sekä kaikille aiheen itsenäiseen
tutustumiseen.

Digitaalinen Helsinki Esittely Teemat Ajankohtaista EN SV

Blogi

digi.hel.fi

Helsingin kaupungin julkisilla verkkosivuilla digi.hel.fi blogissa käsitellään erilaisia digitaaliseen kaupunkiin ja sähköisiin palveluihin liittyviä teemoja – välillä tietoturvaakin sivuten.

https://digi.hel.fi/blogikirjoitukset/

Ne ovat luettavissa kaikille aiheesta kiinnostuneille.

hel.fi sivuilta löytyy myös

Sähköinen asiointi > Tietoturva ja tietosuoja
https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/hallinto/palvelut/Verkkoasiointi/tietoturva-ja-tietosuoja/

Helsinki-turva > Turvaa itsesi > Tietoturva
https://www.hel.fi/turva/fi/turvaa-itsesi/tietoturva/

Kaupunki ja hallinto > Tietoa Helsingistä > Tietosuoja
https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/tietoa-helsingista/tietosuoja/

Lisää asiaa tietoturvasta

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

soveltuu myös työpaikan tietoturva-asioista oppimiseen. Julkaisija Turvallisuuskomitea, 2017.

Kyberturvallisuuskeskukselta https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

löytyy yleistajuisia Tietoturva Nyt! -sarjan ajankohtaisartikkeleita sekä ohjeita yksityishenkilöille kuin tietohallinnollekin.

Myös hauskat turvalistit.fi tietoturvavideot.

Monenlaisia tietoturvaan liittyviä ohjeistoja löytyy esimerkiksi julkisen hallinnon digitaalisen turvallisuuden johtoryhmän VAHTI-ohjeista https://www.vahtiohje.fi/ ,

aiemmista julkisen hallinnon suosituksista http://www.jhs-suositukset.fi/

ja tietosuojavaltuutetun toimistolta. http://www.tietosuoja.fi/

Katso myös Digi- ja väestötietoviraston ajankohtaista digiturvallisuudesta https://dvv.fi/digiturva, ja myös linkit VM:n tietoturvan YouTube-videoihin.

Helsinki

TIETOTURVA PÄIVITTÄISESSÄ TYÖSSÄ

Tämän aineiston tuotti Helsingin kaupungin tietotekniikkaohjelman 2015-2017 tietoturvan kehittämisen valmennusryhmä tietoturvan peruspaketiksi kaikille.

2018-2020 sisältö päivitettiin Helsingin kaupungin eri toimintayksiköiden tietoturvan yhdyshenkilöiden kanssa ja se kattaa aiemman tietoturvallisuuden yleisohjeen työasemakäyttäjille (pysyväispäätösten kirje 9.2.2004) sisältämät aiheet.

Aineistossa on tietoturvan tietoiskuihin tarkoitetut esityskuvat, tietoturvan huoneentauluiksi ja kuvitusaiheiksi sopivat aihekuvat sekä tekstisivut, jotka tukevat aineiston itsenäistä selaamista.

Sisältö on julkinen. Aiheet ovat tietoturvan yleistietoa ja kuvien kuvaajatiedot tulee jättää aineistoon sekä viittaus Helsingin kaupunkiin sitä uudelleen käytettäessä.

Yhteyshenkilö:

Aaro Hallikainen
tietoturva-asiantuntija

09 310 25999
aaro.hallikainen@hel.fi

Helsingin kaupunki
Kaupunginkanslia
Pohjoisesplanadi 11–13
PL 1, 00099 HELSINGIN KAUPUNKI

11.2.2020

94 esityskuvaa