


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. 

Tietoturva päivittäisessä työssä

▷ Peruskäsitteitä, johdanto	4-7	... kuvat
▷ Työaseman käyttö, käyttäjätunnus, salasanat	8-25	
▷ Työasemat, tietokoneen ohjelmat, etäyhteydet	26-32	
▷ Puhelin, laitteiden mukana kuljettaminen	33-36	
▷ Toimistolla, tietojäte, tilaturvallisuus	37-50	
▷ Teknisestä tietoturvasta, haittaohjelmat, salaus	51-59	
▷ Muistitikut, tiedostojen jakaminen, varmuuskopiot	60-73	
▷ Viestinnän tietoturva, ryhmätyötilat, verkkopalvelut	74-82	
▷ Hallinnollinen tietoturva, kehittämismenetelmät, ohjeet	84-91	
▷ Lisää asiaa tietoturvasta – verkkoaineistoja	92	
▷ Tekijätiedot	94	



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.

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 tietoiskuista.



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

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

Mistä tiedät kuka käyttää tietoja?



Työasemaan kirjaututaan 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").

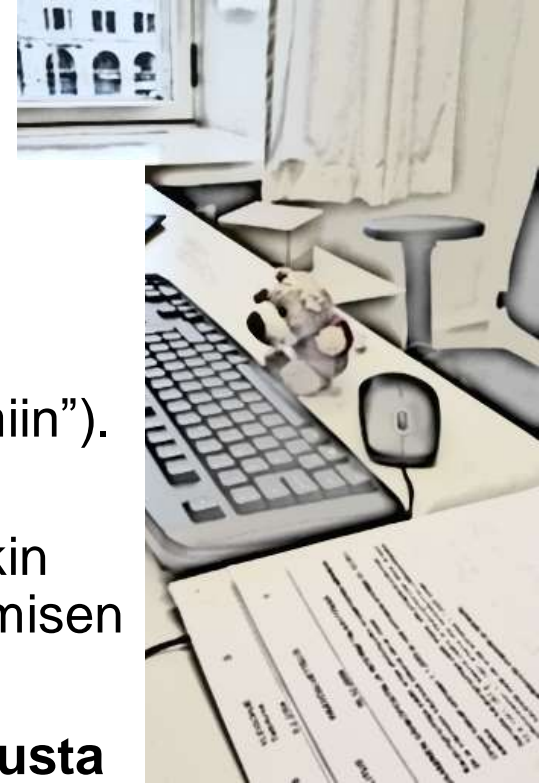
Tunnuksia on useita, koska jotkut järjestelmät eivät käytä kaupungin AD-tunnusta käyttäjän tunnistamiseen. Joihinkin taas kirjaudutaan automaattisesti AD-tunnuksella kirjautumisen jälkeen (kertakirjautuminen; SSO = single sign-on").

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

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

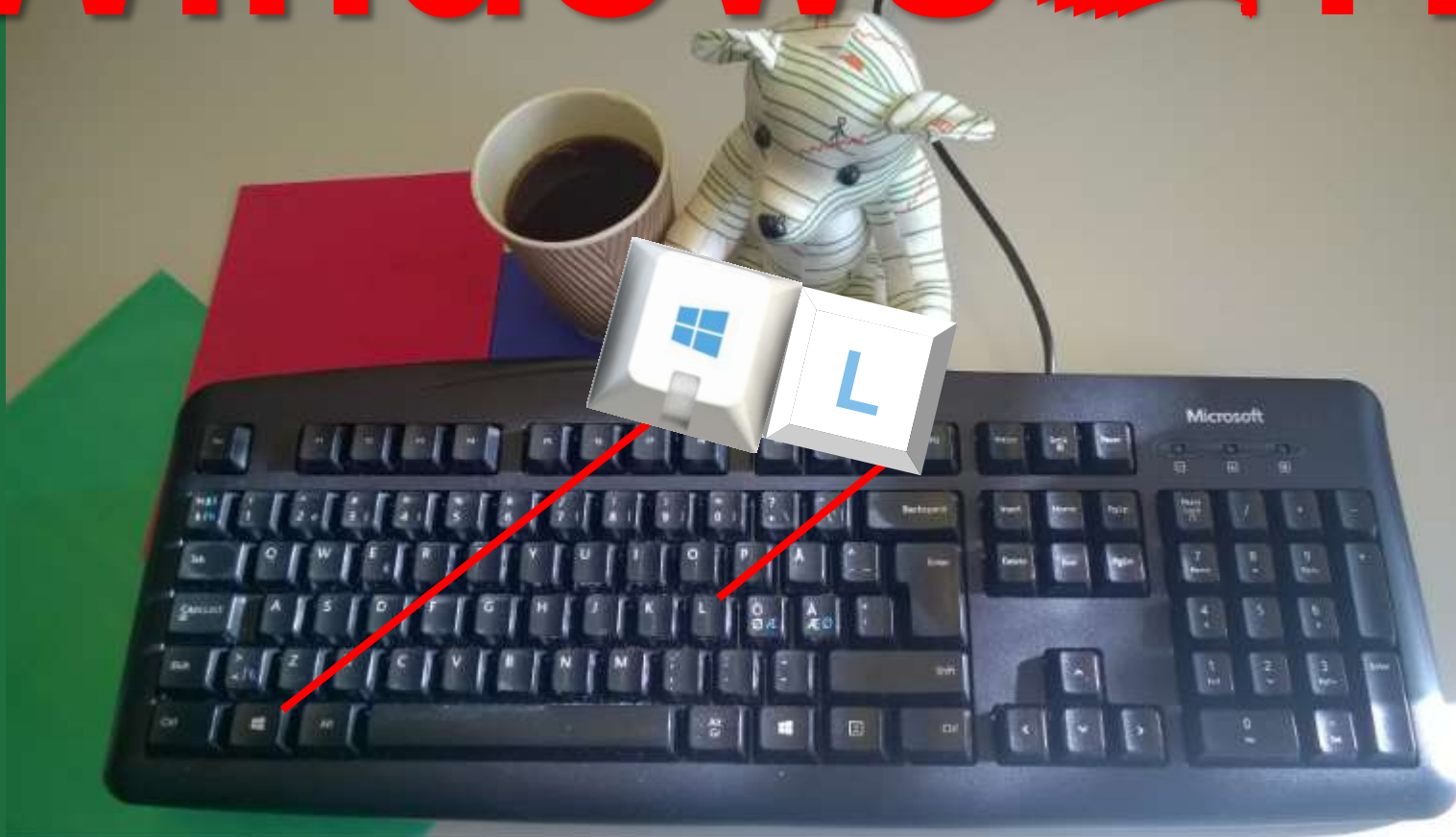
Ylläpitäjät eivät tarvitse eivätkä käytä käyttäjien salasanoja.

Tarvittaessa ylläpitotehtävät tehdään yhdessä käyttäjän kanssa.



Kun poistut työpisteeltä,
lukitse työasema.

Windows  + L



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

Laita myös työpaperit pois näkyviltä.

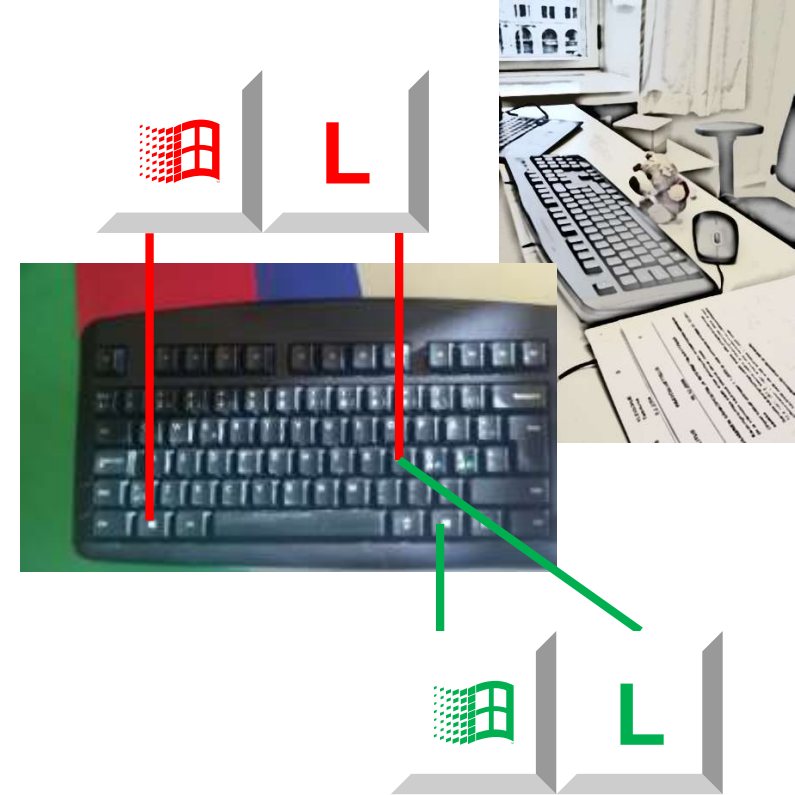
Suojattava aineisto tulee laittaa
lukkojen taakse kun sitä ei tarvita -
lukolliseen pöytälaatikkoon, kaappiin ja/tai
huoneen ovi lukkoon.

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

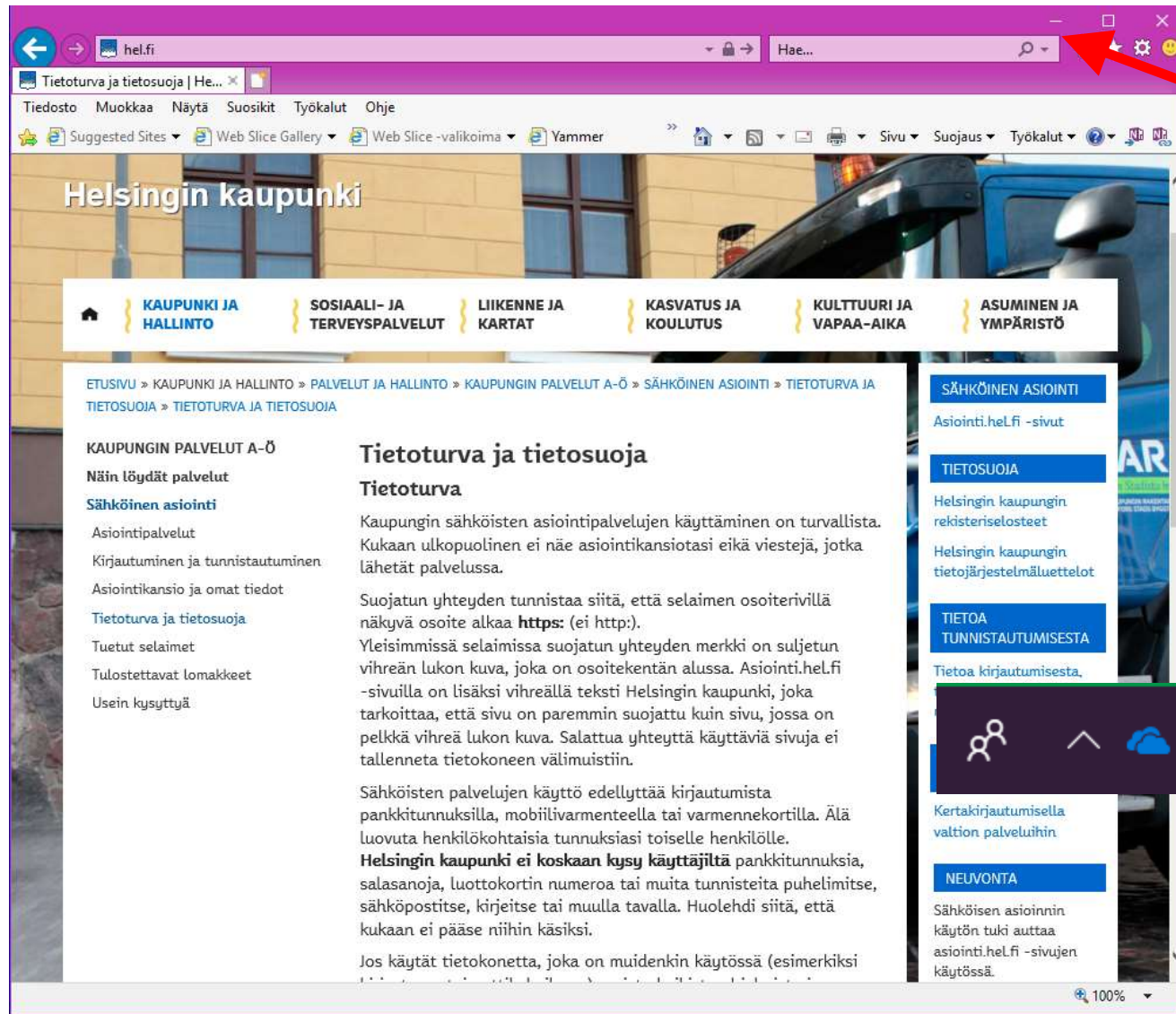
MIKSI:

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.**

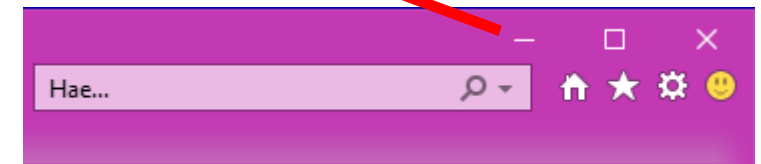


Peitä näyttö olan yli katsojilta



Pienennä yksi ikkuna

-valinnan napauksella



Näytä työpöytä tai

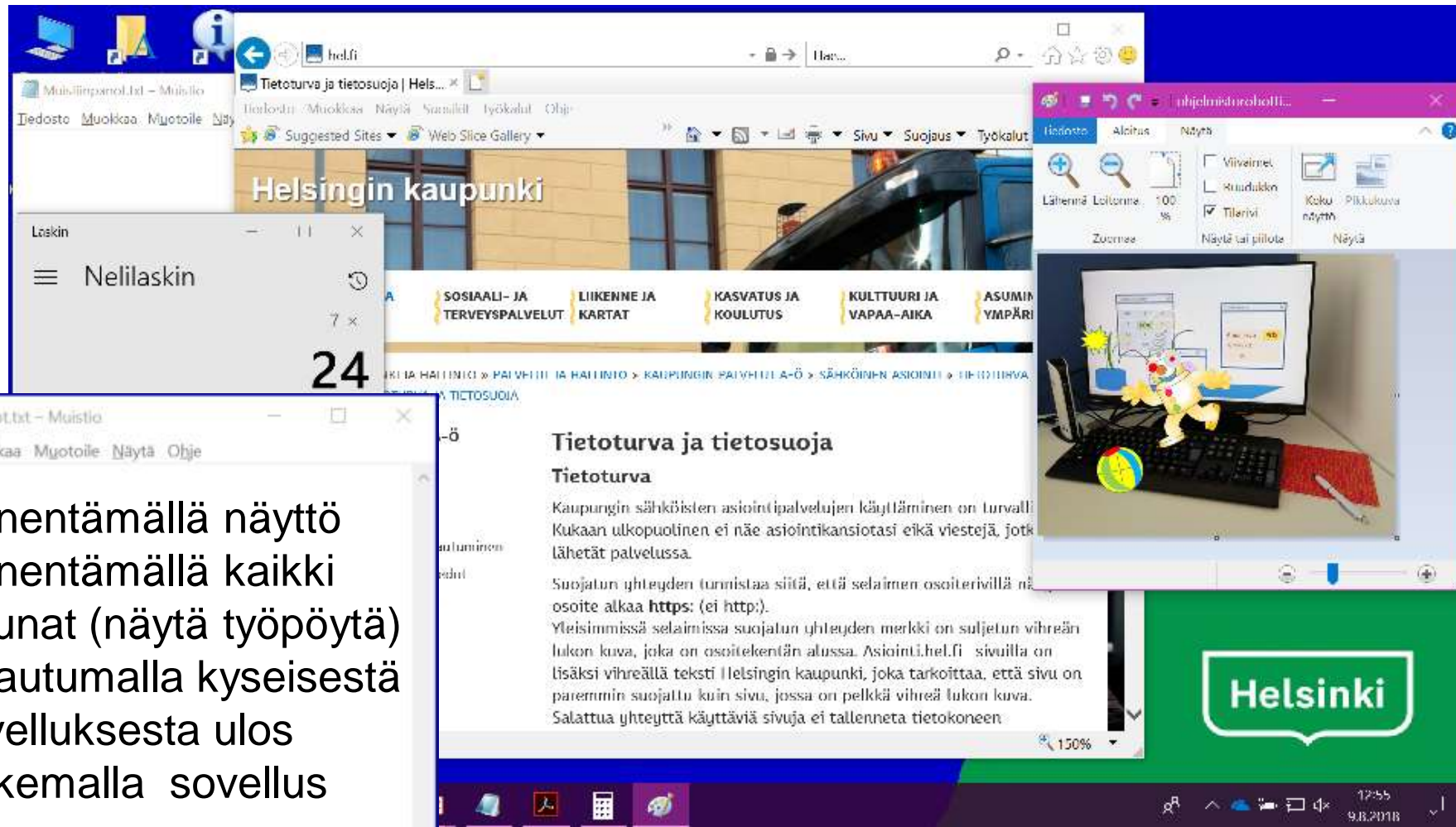
Pienennä kaikki yhdellä napauksella alanurkkaan



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 😊

tai läppärin kansi kiinni



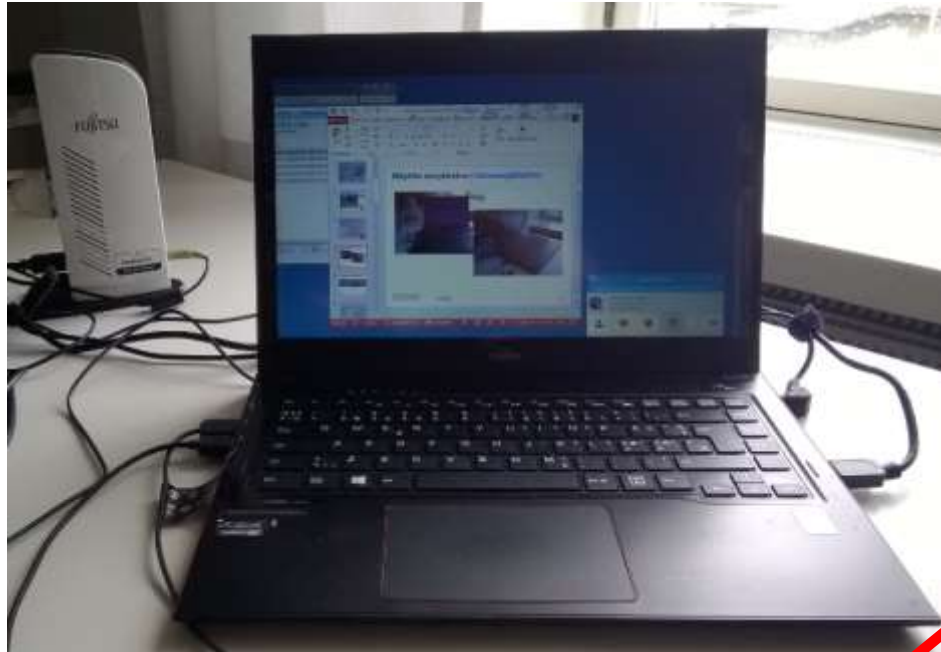
Näyttää tyhjän työpöydän (tai tuo takaisin ikkunat juuri edeltävän Windows+D "desk" näppäilyn jälkeen)

Näytä työpöytä

Pienennä kaikki yhdellä napauksella alanurkkaan



Näytön suojakalvo (tietosuojakalvo)



Estää näytön sisällön
lukemisen sivusta



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

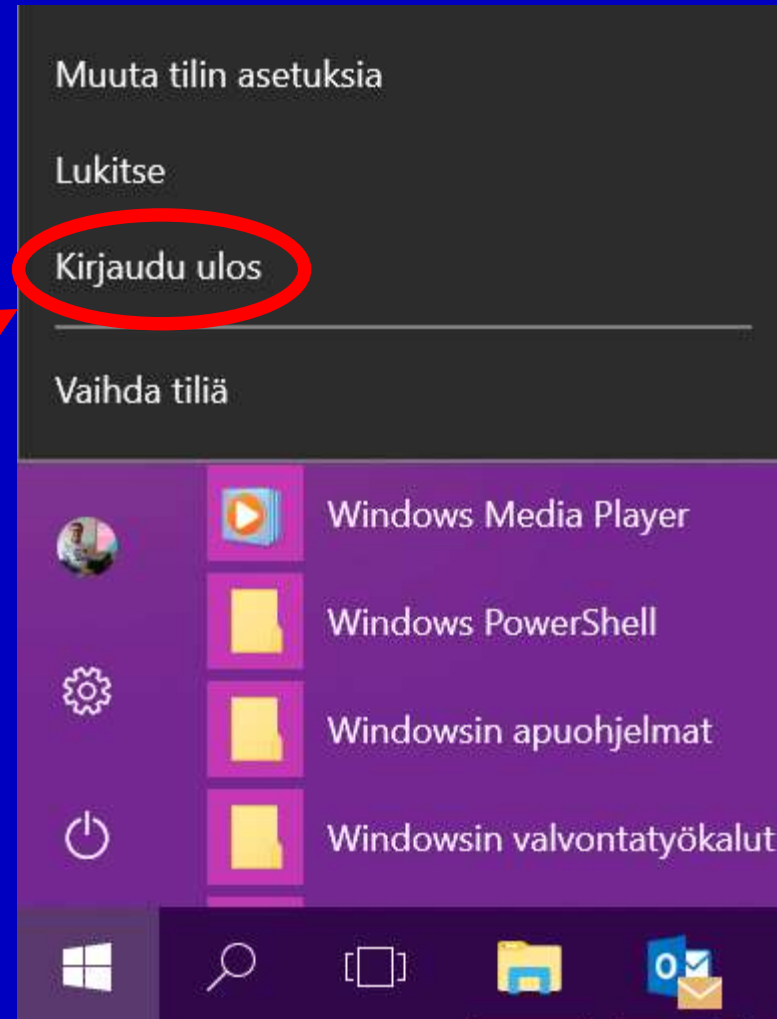
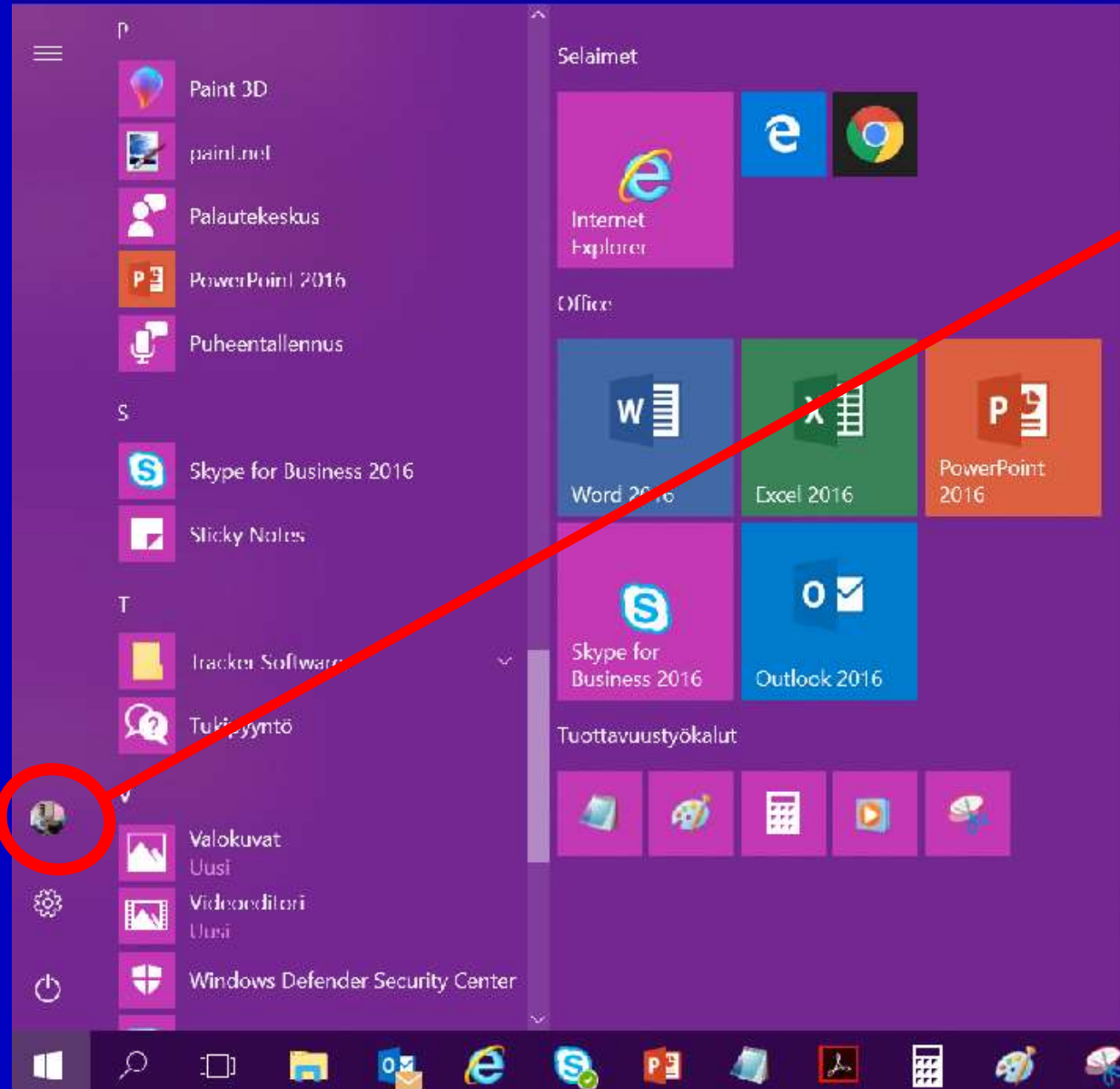


Myös etä- tai matkatöissä
(monipaikkaisessa työssä)
on katsottava että tietoja
ei pääse asiattomille

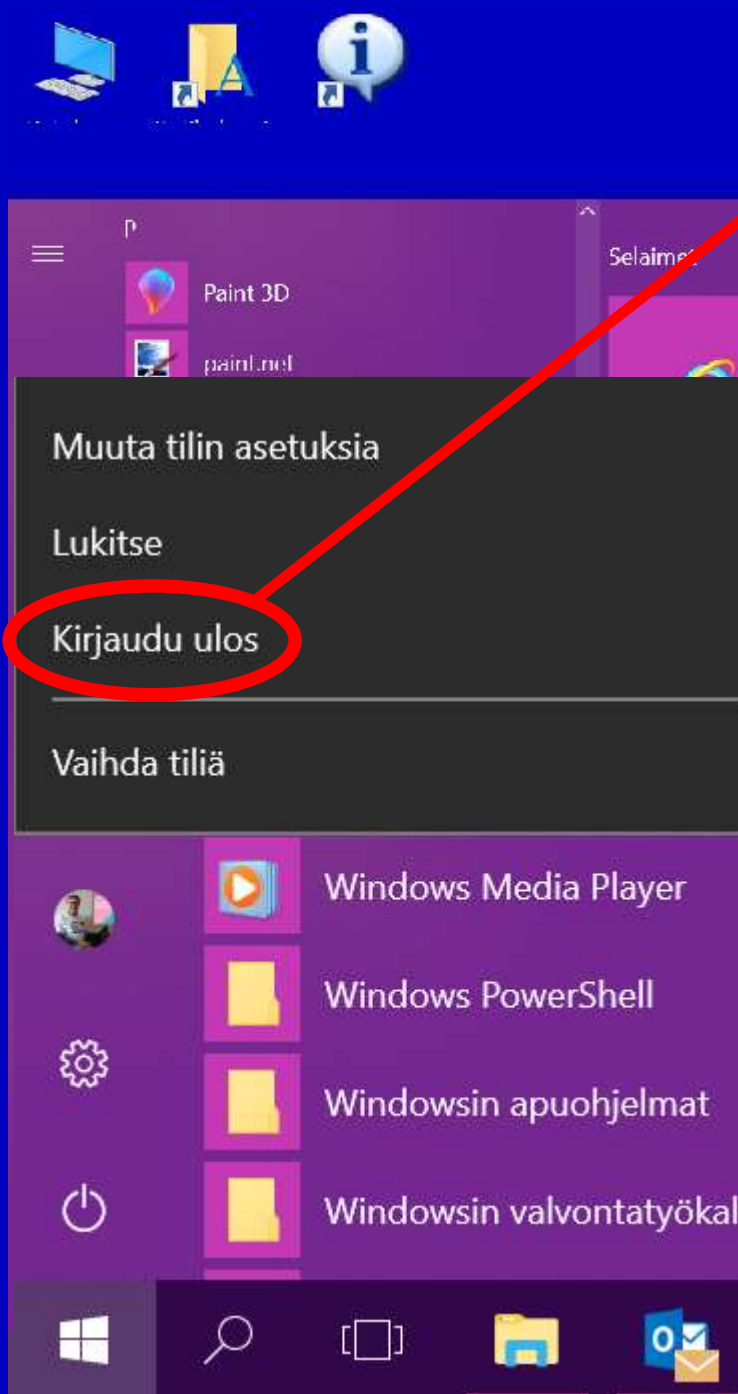
kahvilassa, kirjastossa,
ratikassa, kokoushuoneessa...

Tietosuojakalvoa voi kysyä lähitueltä (ICT-tuki)

Poistuesssa



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 turvallisenä.

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

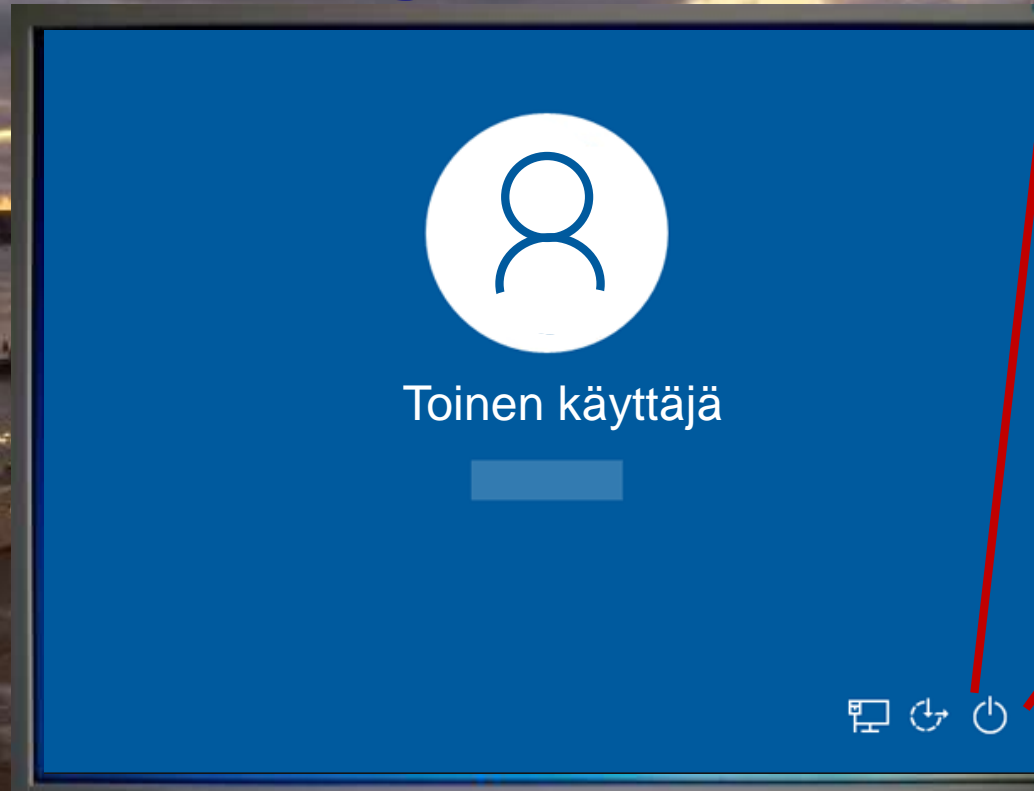
☺ **Energian säästämiseksi**
sähköt voi kytkeä
yöksi pois
näytöstä

Työpaikan
tapana voi
olla myös
tietokoneiden
vieminen
kaappiin
vuoron lopussa

Helsinki

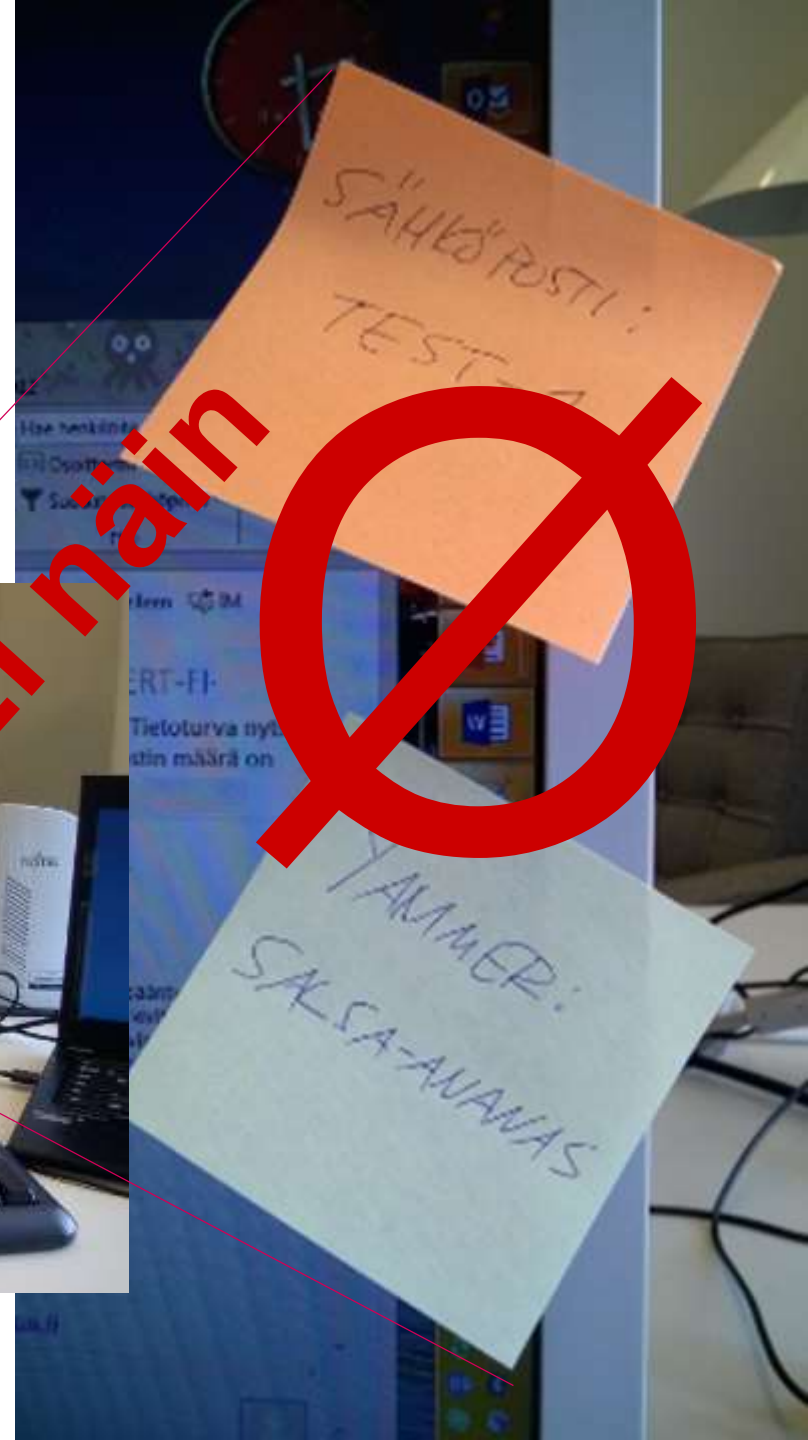
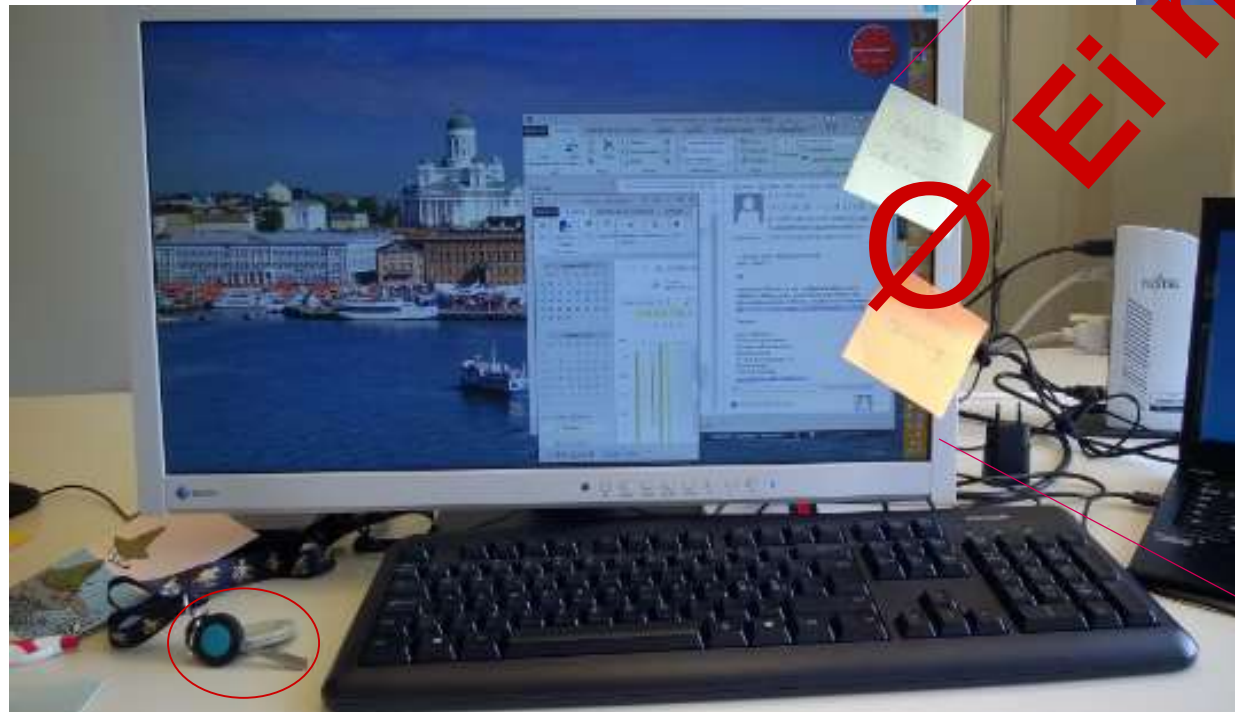
...ja saapuesssa uudelleen käynnistys

Lepotila
Sammuta
Käynnistä uudelleen



Salasanat

Tunnusluvut



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**.

15...	pituus ainakin 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

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 sähköpostisoitteita) 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 lähituelle (ICT-tuelle) ja omalle esimiehelle.

□

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

Jos mahdollista, niin ota käyttöön kaksivaiheinen tunnistus verkkopalveluun. Silloin kirjautumiseen tarvitaan käyttötunnus, salasana ja puhelimeesi lähetetty kertakäyttökoodi.

YAMMER:
SALSA-AUUNAS

15 merkkiä < < 3 kuukautta

Vaihda **salasana** 3 kuukauden välein
tai vaikka useamminkin
ja aina jos järjestelmä pyytää

Käytä ainakin 15 merkkiä pitkiä salasanoja

Älä kierrätä samaa salasanaa uudestaan ja uudestaan ja uudestaan ja uu

**Eri salasananat ja tunnukset töihin
kuin omiin koti/harrastusasioihin**

**Vaihda aina oletussalasanat
ja -numerokoodit**

Monivaiheinen tunnistus on parempi



Työasemat

Digitaaliset työvälineet
Etäyhteys

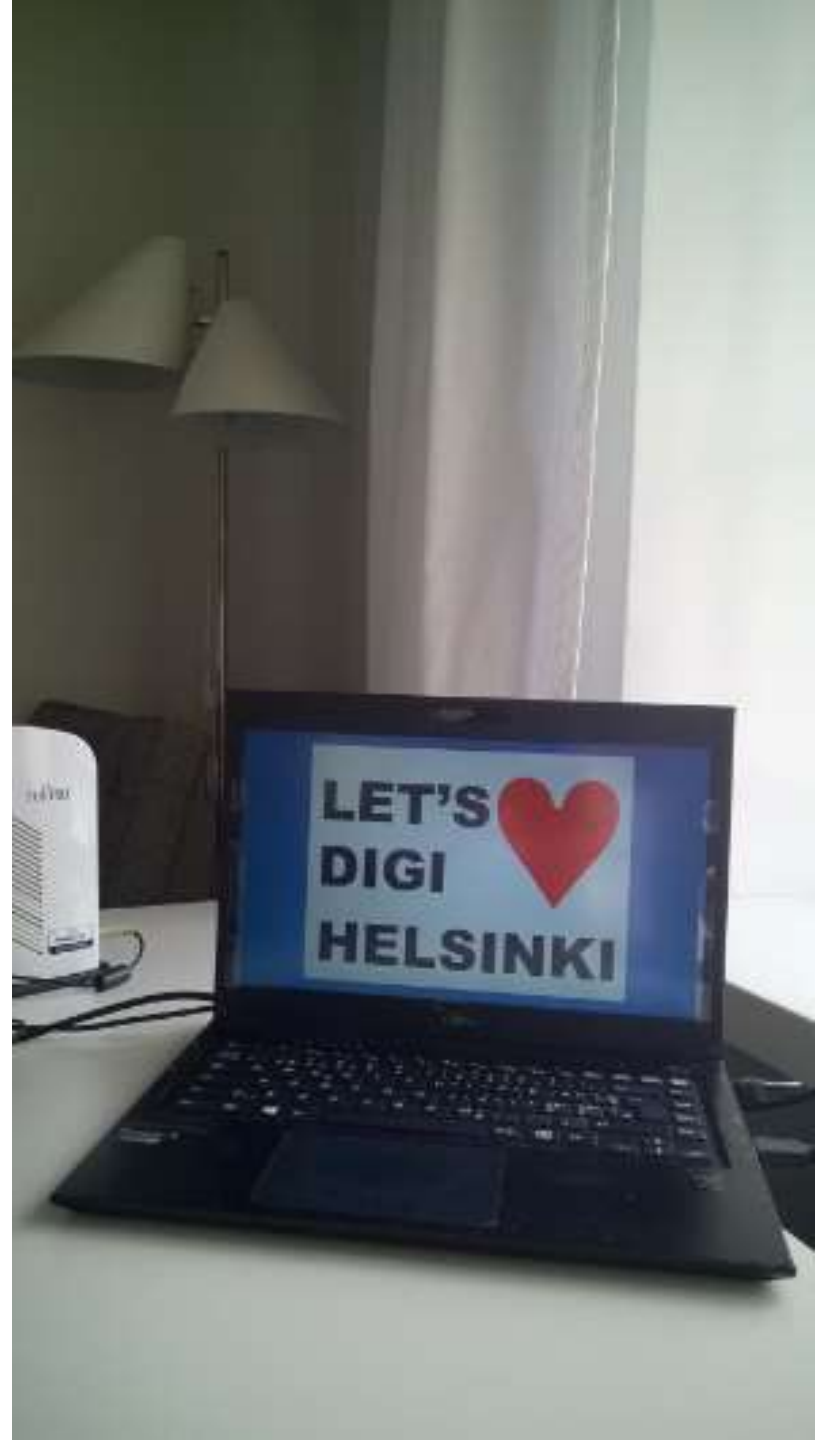
Helsinki
ON



Työasema

Työasemissa käytettävät ohjelmat on standardoitu, 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

Etäyhteyden käyttö - katkaisu

Kun etäyhteys on käynnistetty, niin se katkeaa automaattisesti, jos tietoliikennettä ei ole yhtään pitkäköön 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! Puhelimesta?

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.

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)



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.

Vaihda aina oma PIN
operaattorin oletusnumerosarjan tilalle

Pidä näppäimistön lukittuminen päällä

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.

Toimistolla

Yhteiset työvälineet
Kokoushuoneet
Materiaalien hävittäminen
Lukolliset kaapit

Tyhjän pöydän periaate

*”Tyhjän pöydän periaate”
≈ tiedot ei jää pöydälle*

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 lähitueltä 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.

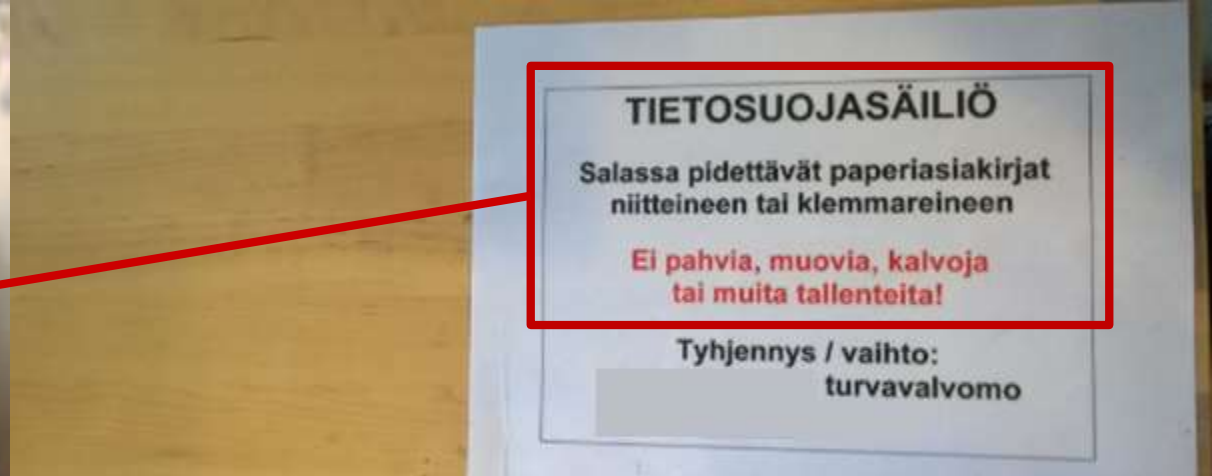




Fläppitaulu **muistiinpanotaulu**

Ota kokouksen muistiinpanot mukaan kokouksen jälkeen
Älä jätä sivullisten näkyville työmuistiinpanoja

Lajittele tietojäte





- 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 tuhoetaan kokouksen jälkeen tietosisältönsä mukaisesti.

Arvokas lukkojen taakse



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

Avaimet Kulikutägit Kulikutunnisteet



**Pidä avaimet mukanas
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/kulcutunnisteet mukanas taskussa tai käsilaussa kuten avaimet.

Erillään henkilökortin ripustuslenkistä tai muista osoitetiedoista.

Tunnusnumero (PIN) pidettävä erillään tågistä.

MIKSI:

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

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



Huolehdiathan, että lukitusta ovesta ei tule mukanas henkilöå, jonka ei tulisi tilaan päästå.

Teknisestä tietoturvasta

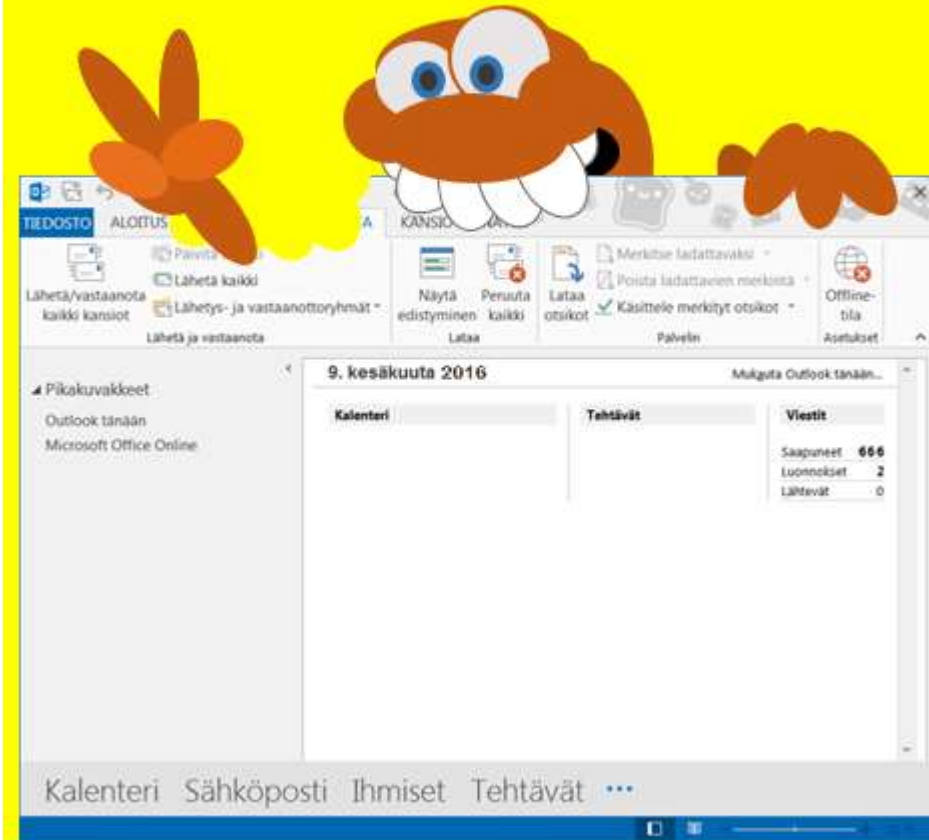
Haittaohjelmien suodatus
Salakirjoittaminen
Varmistukset

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!

Klikkaa ajatuksella



Klikkaa ajatuksella

Selkeästi asiattomat viestit saa poistaa lukematta.

Shift+delete -näppäily

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

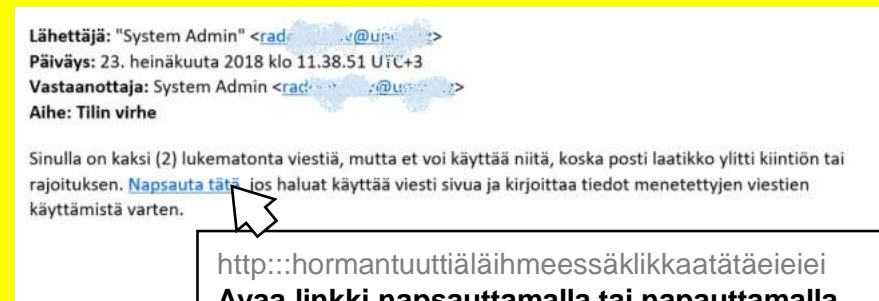
Ei kannata vastata, eikä klikkailla mukana olevia linkkejä.

Roskaa voi tulla viestien sekaan, vaikka postiamme 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.**

Helsinki



Väärennetyt lähettäjä tiedot voivat näyttää oikeilta, jopa työkaverin osoitteelta.



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

Virustorjunta

Työasemissa on keskitetty virustorjunta. Tietokoneen toimintaa häiritsevien haittaohjelmien leviämisenopeus 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 lähettäjiä 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.

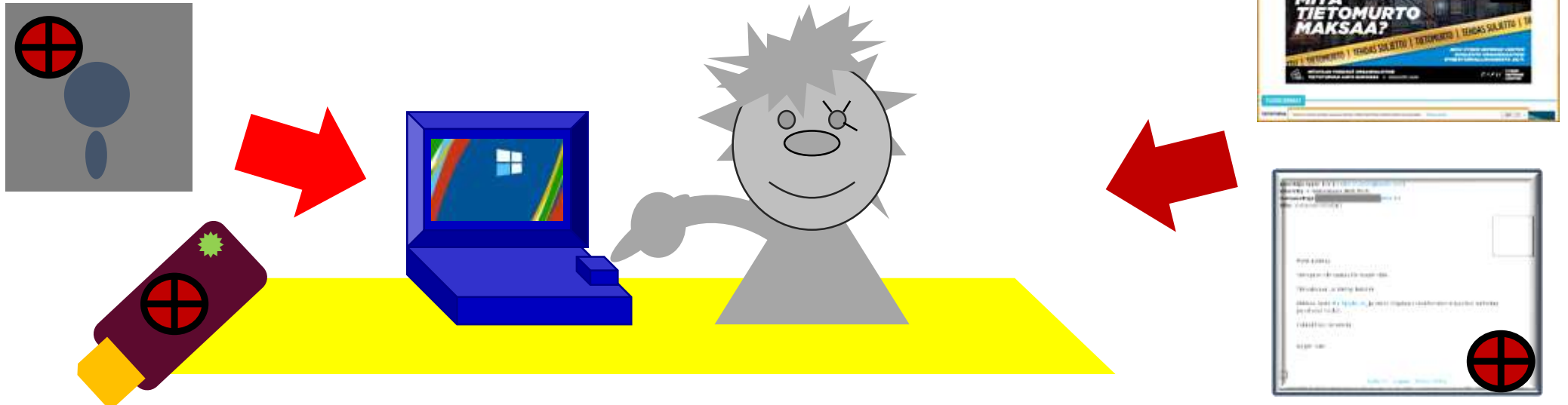
Haittaohjelmia (viruksia) voi tulla tietokoneelle

siirrettäviltä tallennuslaitteilta, vanhoista taltioista ("levyistä"), varmistuksista ("vanhoista tiedostoista"),

sähköpostiliitteinä, viestien klikattavien linkkien päästä, ja ihan asiallistenkin verkkosivujen liitteistä ("mainosliitteistä").



Älä ota sisältöä käyttöön tuntemattomissa Office asiakirjoissa

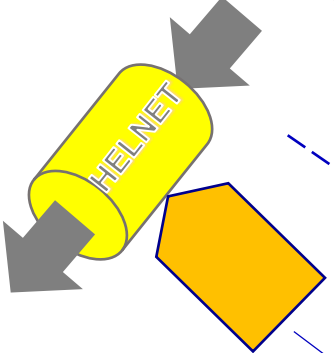
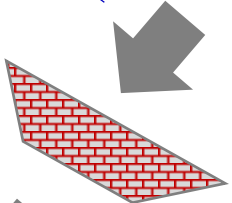


Haitallinen sisältö

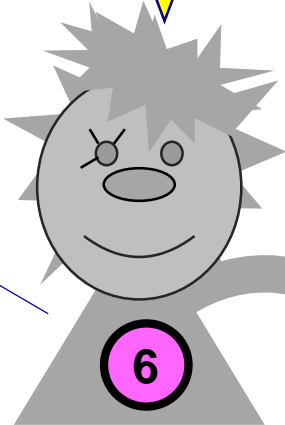


Operaattorin tietoliikenteen suodatus

Haittaohjelmasuodatus sisä- ja ulkoverkon reunalla

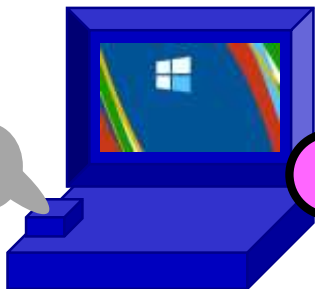


Vastuullinen asenne, oivaltaminen



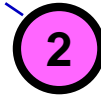
Osaaminen

Helsinki



Haittaohjelmasuojaus ja työaseman palomuuuri

Tietoliikenteen teknisen laadun valvonta



Tietoturvallinen tekniikka

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

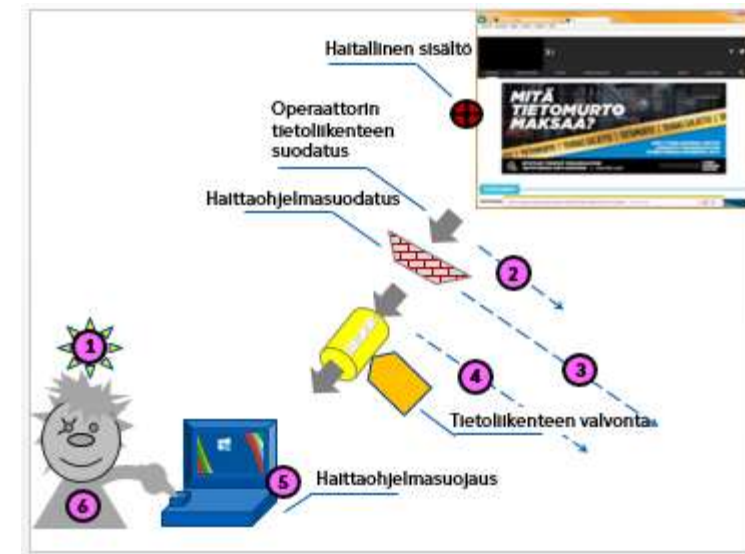
⊕ Haitallinen sisältö voi tulla sinänsä ihan asiallisen tietoliikenteen seassa.

- Tärkein osa tietoturvassa onnistumista on henkilön oma vastuullinen asenne tietojenkäsittelyyn

- ja tehtävissään tarvittava ajantasainen

⑥ osaaminen

③ ④ ⑤



Vastuullisuus Osaaminen

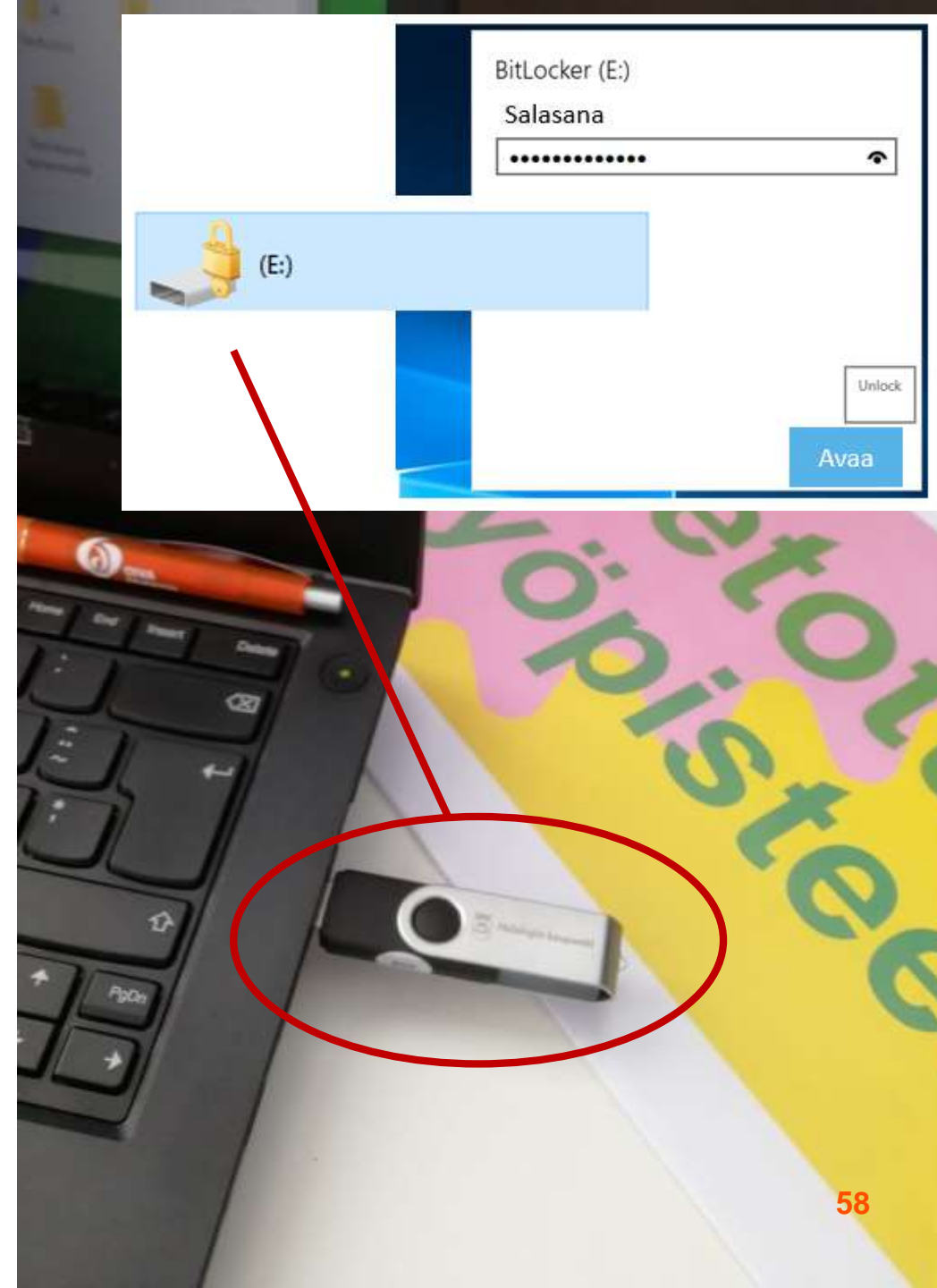
Salakirjoittaminen

Tiedostojen suojaamiseen käytettäviä salakirjoitusohjelmia voi kysyä ICT-tuesta.

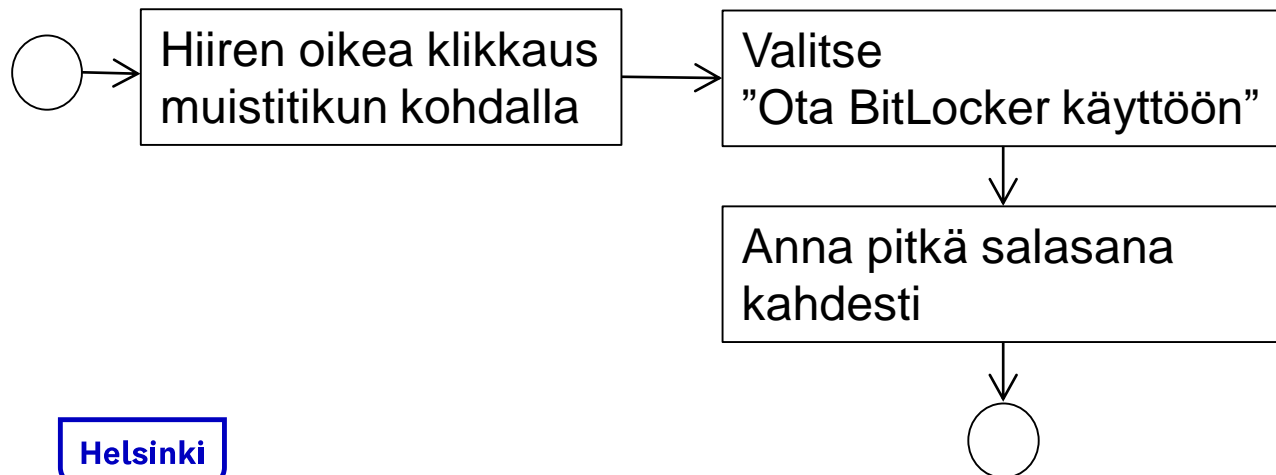
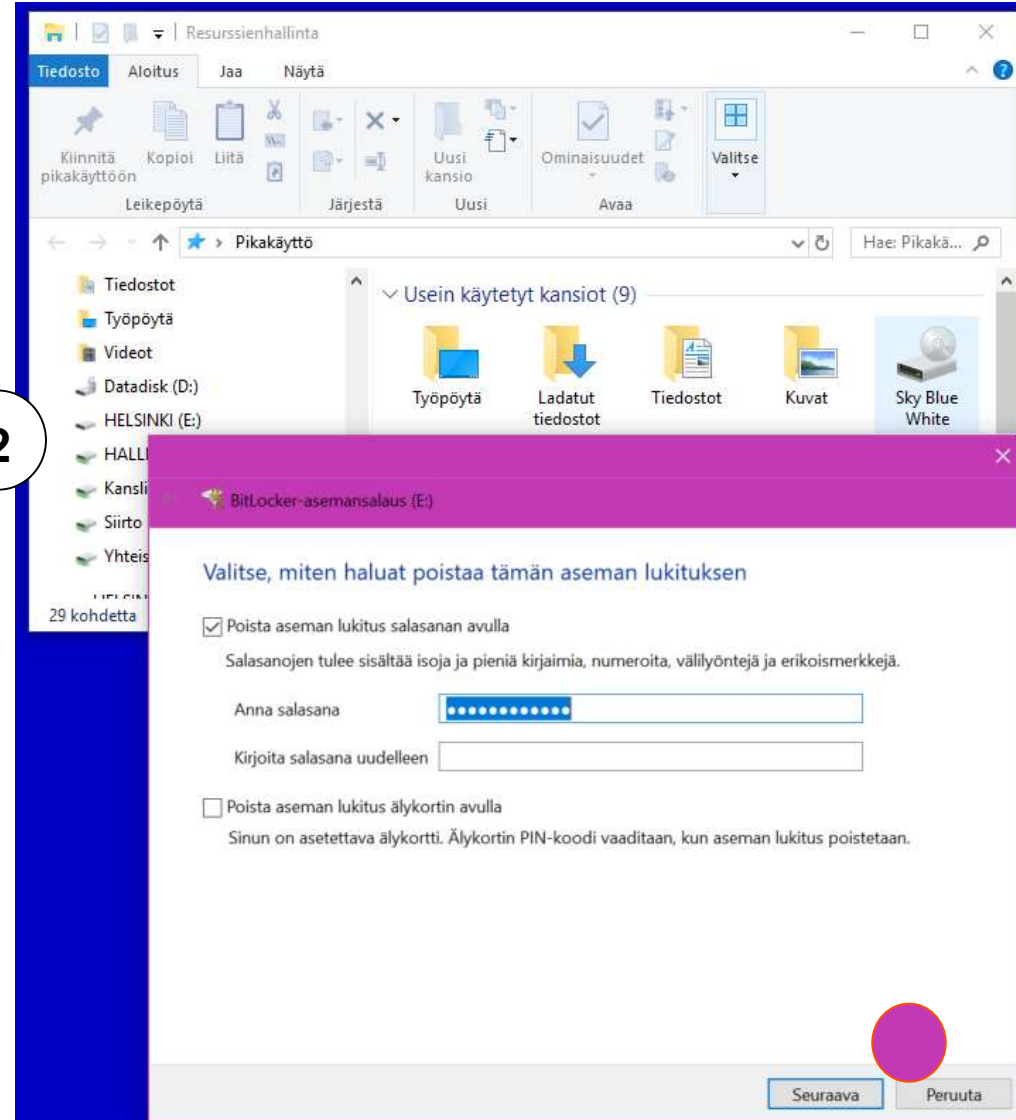
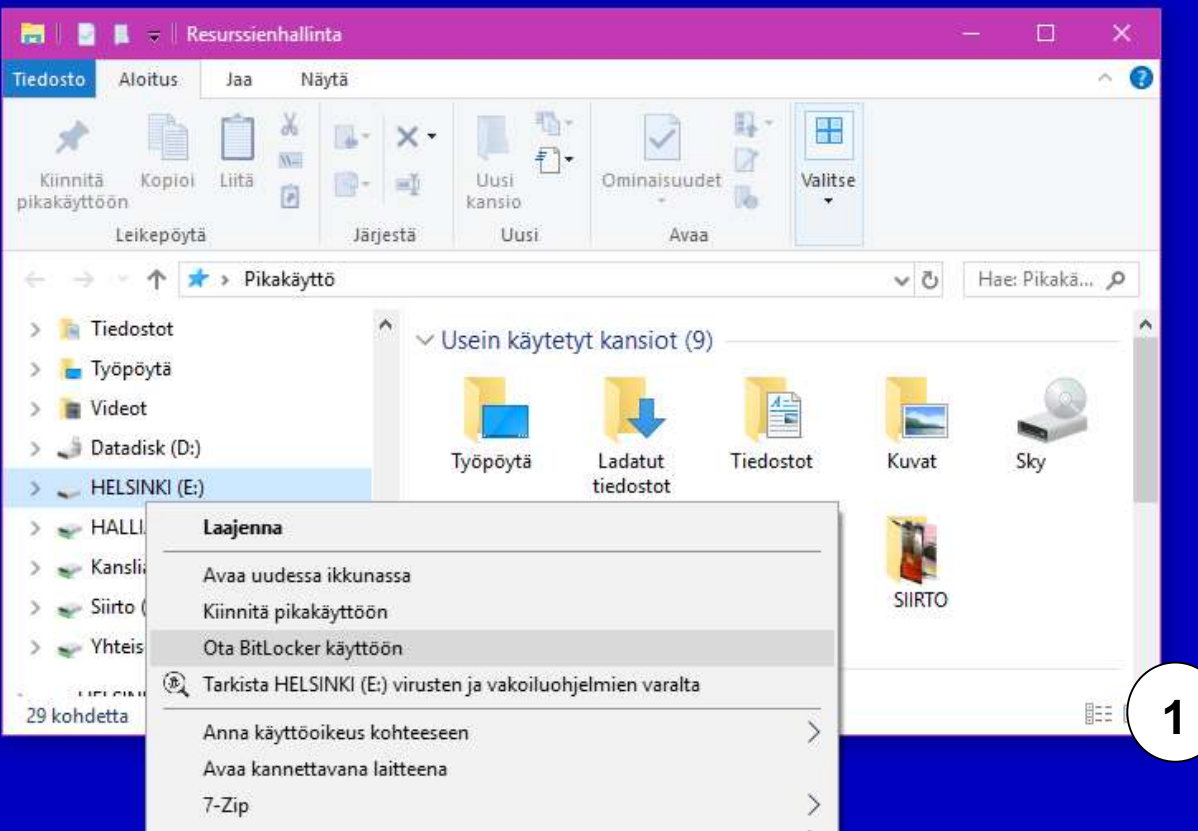
Työpaikan Windows 10 -ympäristössä erillisen muistitikun salaaminen onnistuu käyttöjärjestelmän BitLocker-toiminnolla:

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 muistitikku 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



Muistitikut kaikenlaiset muistilaitteet

Tiedostojen jakaminen



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.



Työkoneeseen liitettäessä

USB-tikku/muistilaite

voi siirtää haittaohjelman mukanaan.

Viruskannaus mieluiten erillisellä tietokoneella.

Korkeampaa turvaa tarvitseva aineisto on salakirjoitettava muistilaitteelle laitettaessa

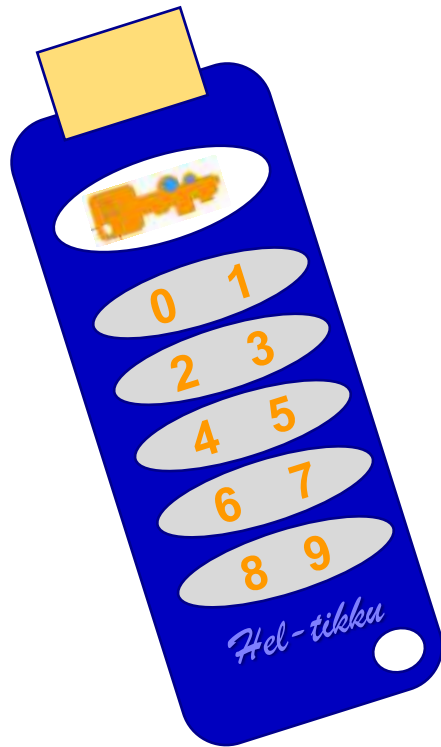
ja samalle tikulle vain saman laatuista aineistoa (ei sekaisin julkista ja salattavaa samalle muistitikulle).

Yksi muistitikku kullekin käyttötärpeelle – 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 ”irralaisia” 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 Office 365-palvelusta (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 lähitueultasi / tietohallinnosta.

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

OneDrive – Ison tiedoston jakaminen

Office 365 | OneDrive

Etsi kaikkialta

Jaa Kopioi linkki Lataa Poista pysyvästi Siirrä kohteeseen Kopioi kohteeseen Nimeä uudelleen 1 valittu

Tiedostot > Videot

Nimi	Muokattu	Muokkaaja	Tiedoston koko	Jakaminen
Microsoft-tuotteiden tietosuoja	8. maaliskuuta	Hallikainen Aaro	268 Mt	Jaettu
tyhjät-huoneet-2018a	3. kesäkuuta	Hallikainen Aaro	261 Mt	Jaettu

1 Lataa tiedostot palvelimeen vetämällä ne tähän

4

5

Lähetä linkki
Microsoft-tuo...

Yrityksen oma organisaatio jäsenet, joilla on linkki, voivat muokata.

Toinen käyttäjä

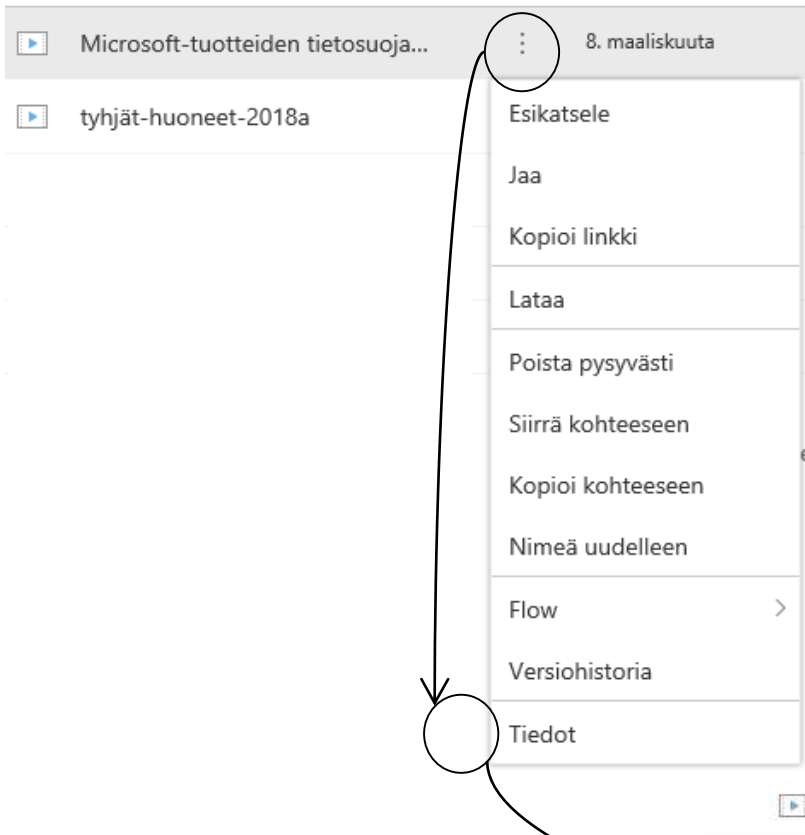
Toinen käyttäjä

Toinen käy Toinein-ei

Kopioi linkki

Helsinki

OneDrive – Tiedoston käyttöoikeudet

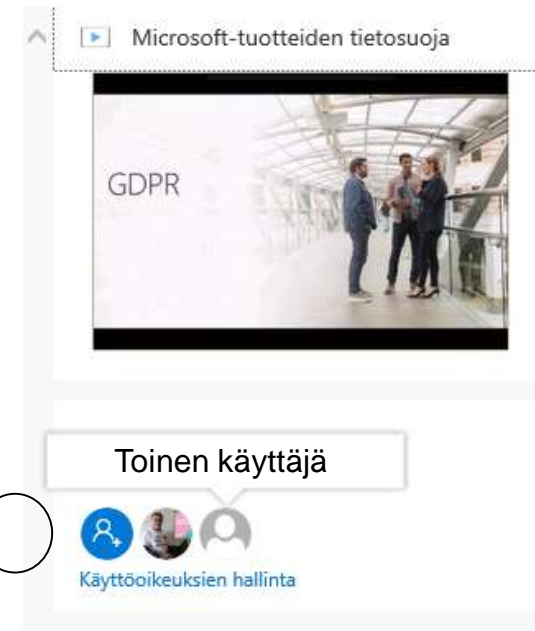


The screenshot shows a OneDrive file named "Microsoft-tuotteiden tietosuoja..." with a context menu open. The menu items are: Esikatselse, Jaa, Kopioi linkki, Lataa, Poista pysyvästi, Siirrä kohteeseen, Kopioi kohteeseen, Nimeä uudelleen, Flow, Versiohistoria, and Tiedot. The "Tiedot" option is circled in red. Below the menu is a table of files:

Nimi	Muokattu	Muokkaaja
Microsoft-tuotteiden tietosuoja	8. maaliskuuta	Hallikainen Aaro
tyhjät-huoneet-2018a	3. kesäkuuta	Hallikainen Aaro

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



The screenshot shows the sharing options for the file "Microsoft-tuotteiden tietosuoja". It includes a video thumbnail with "GDPR" text, a "Toinen käyttäjä" button, and a "Käyttöoikeuksien hallinta" link with user icons.

Varmuuskopio



Korkeasaaren eläintarha korkeasaari.fi / kuvaaja Mari Lehmonen

Helsinki

Tärkeät tiedot varmuuskopioidaan



ja kokeillaan silloin tällöin että ne voidaan tarvittaessa palauttaa takaisin käyttöön.
Työpaikan verkkoaseman kotihakemisto 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 paras vakuutus kiristyshaittaohjelmien varalle

Viime vuosina erilaiset kiristyshaittaohjelmat ovat nousseet uutisiin. 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

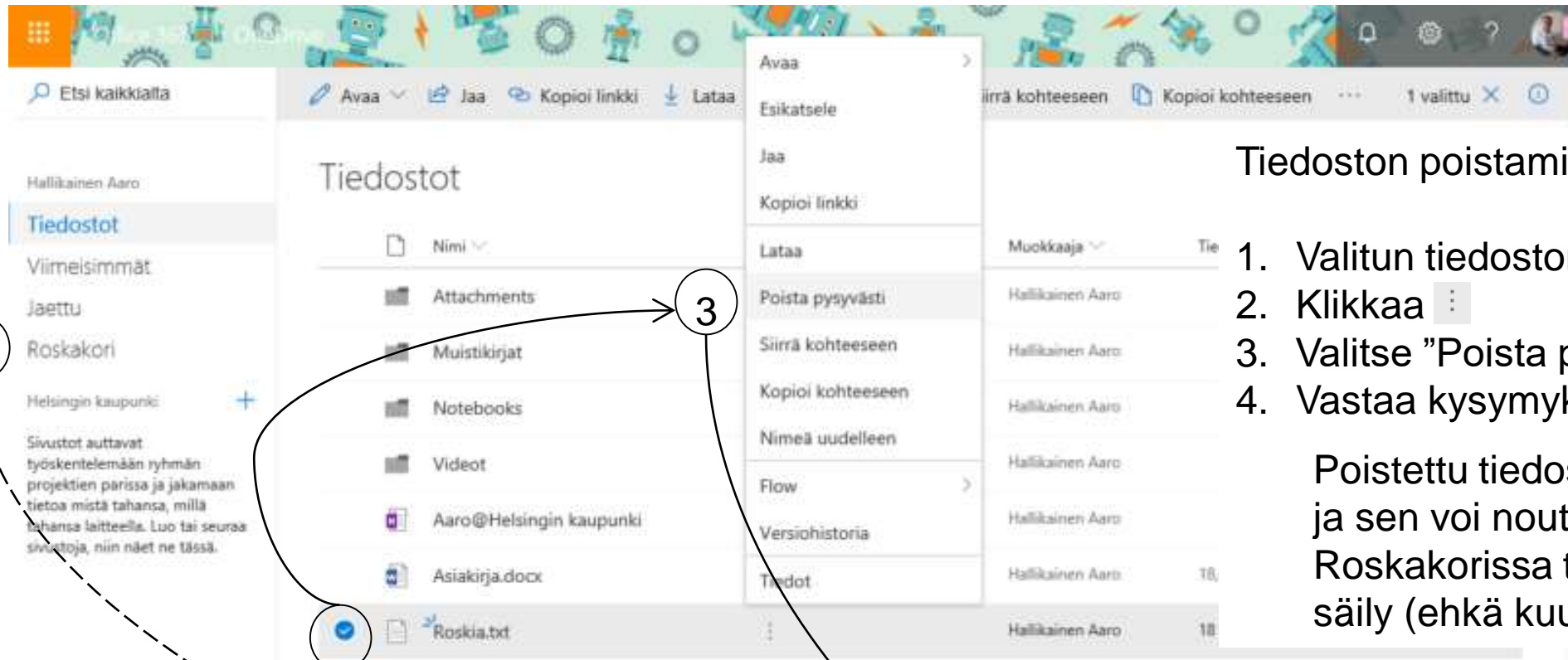
Varmuuskopiot otetaan tietyin säännöllisin ajoin. Tyypillistä on, että kotihakemiston tiedot on mahdollista saada takaisin jonkin rajatun ajan takaa (esimerkiksi vuoden tai muutaman kuukauden). Varsinaisten tietojärjestelmien tiedot taas varmuuskopioidaan yleensä useiden vuosien ajalta.

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

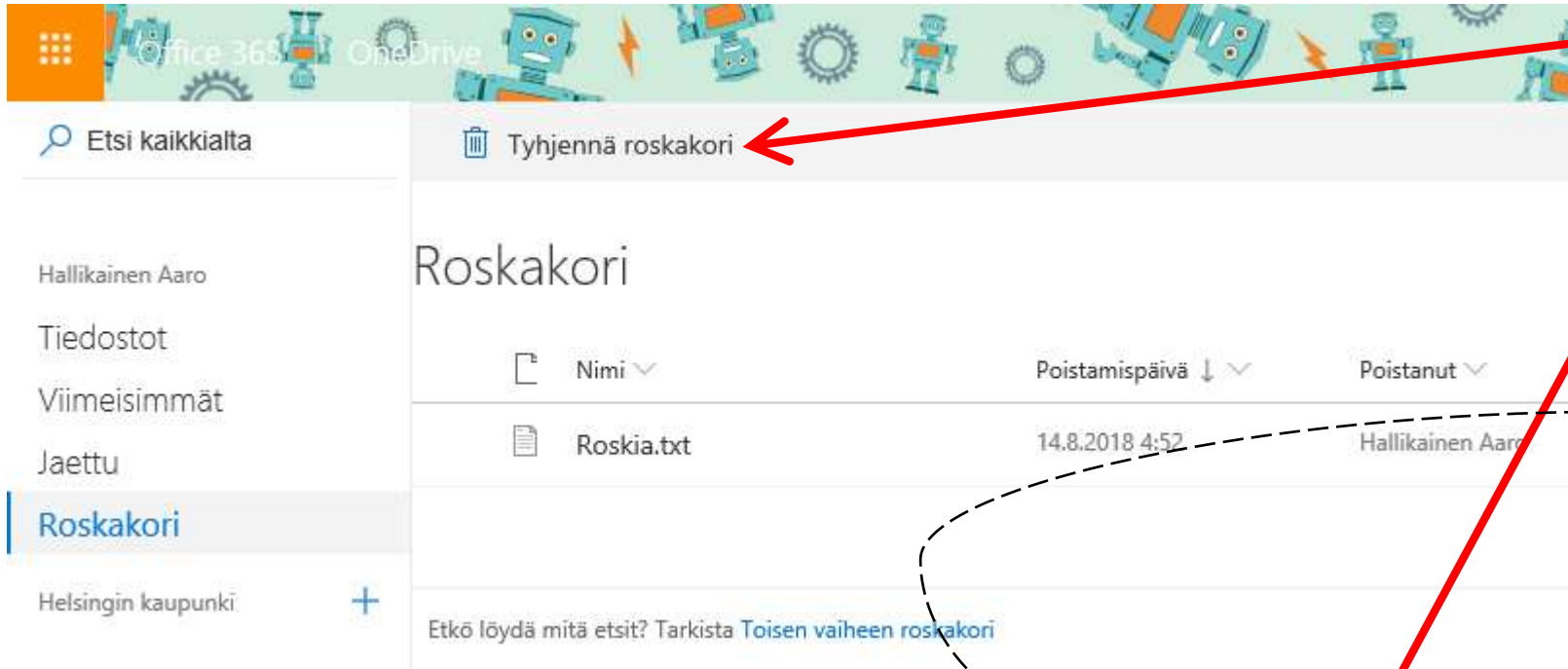


Tiedoston poistaminen vie sen roskiin

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

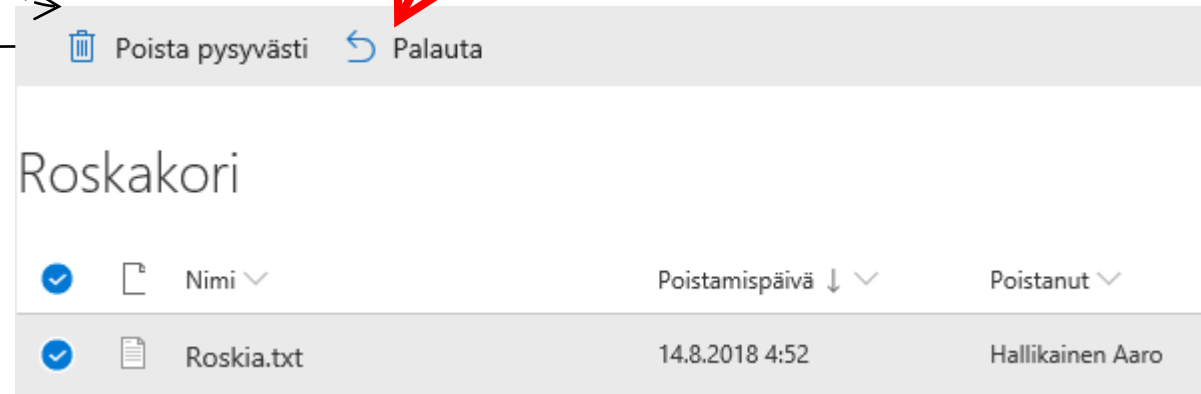
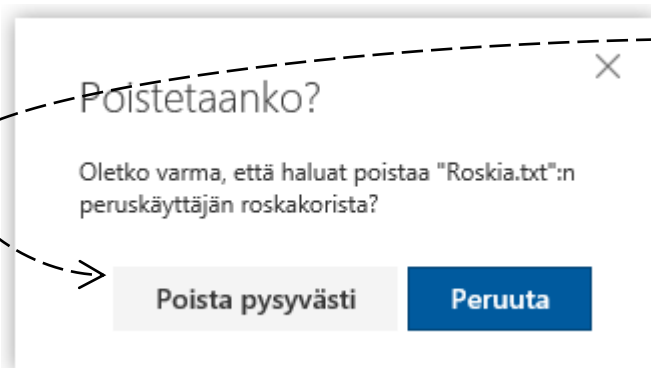


Roskakorin voi tyhjentää
tai valita tiedoston jonka

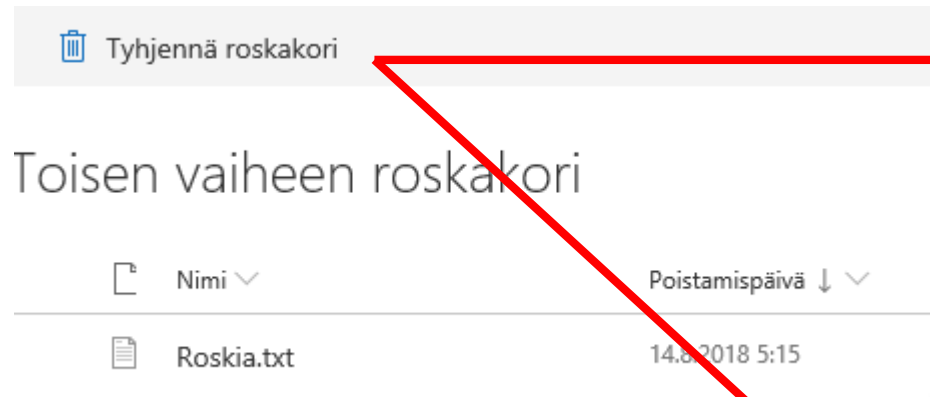
1 palauttaa takaisin sinne
mistä se poistettiin tai

2 poistaa pysyvästi

jolloin roskat menevät
”toisen vaiheen roskakoriin”

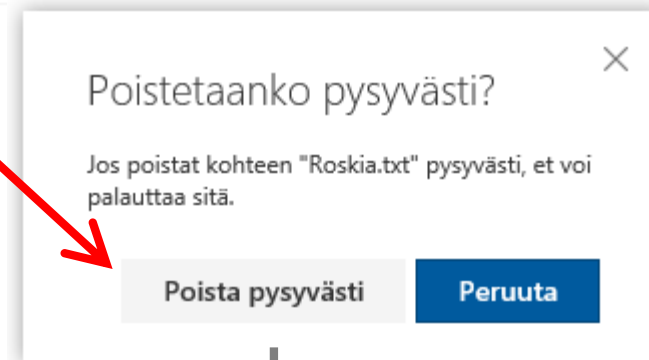


OneDrive - Poista pysyvästi



Toisen vaiheen roskakorin tyhjentäminen tai tiedoston poisto sieltä

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



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>

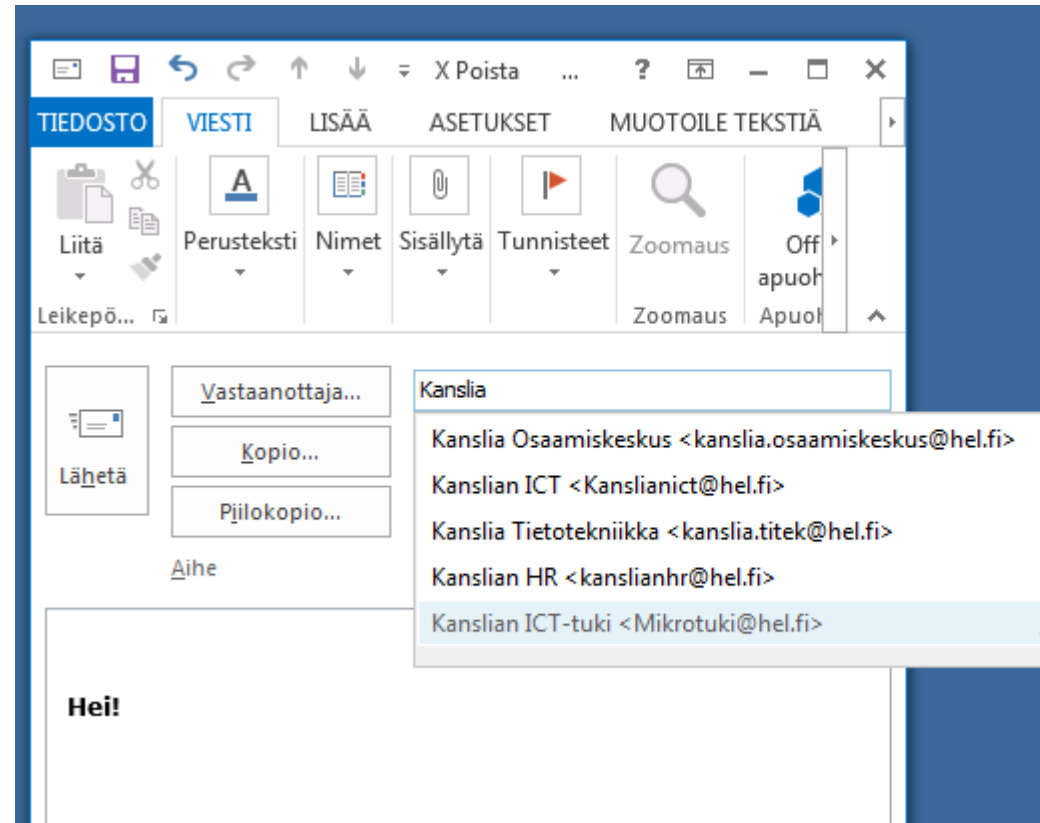
Viestinnän tietoturva

Yhteistyö ja tiedon jakaminen
Sähköposti
Internet
Sosiaaliset mediat

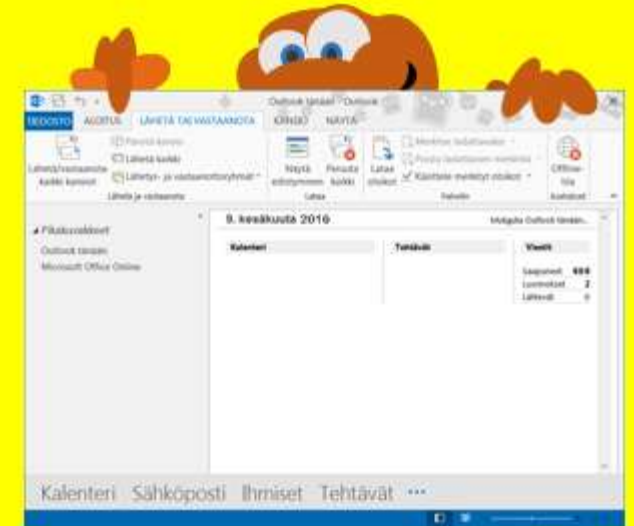
Sähköposti tavanomaiseen viestintään

Älä uudelleen ohjaa työpaikan sähköposteja yksityisiin postilaatikoihin.

Tarkista vastaanottaja huolellisesti.



Klikkaa ajatuksella



Automaattitäydennyksestä saa osoitteen pois klikkamalla X -raksia

Sähköposti

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.

Klikkaa ajatuksella



Suojattu sähköposti

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

Helsingin kaupungilla on tarjolla Viestintäviraston hyväksymää laatua oleva suojatun sähköpostin järjestelmä sitä työssään tarvitseville.



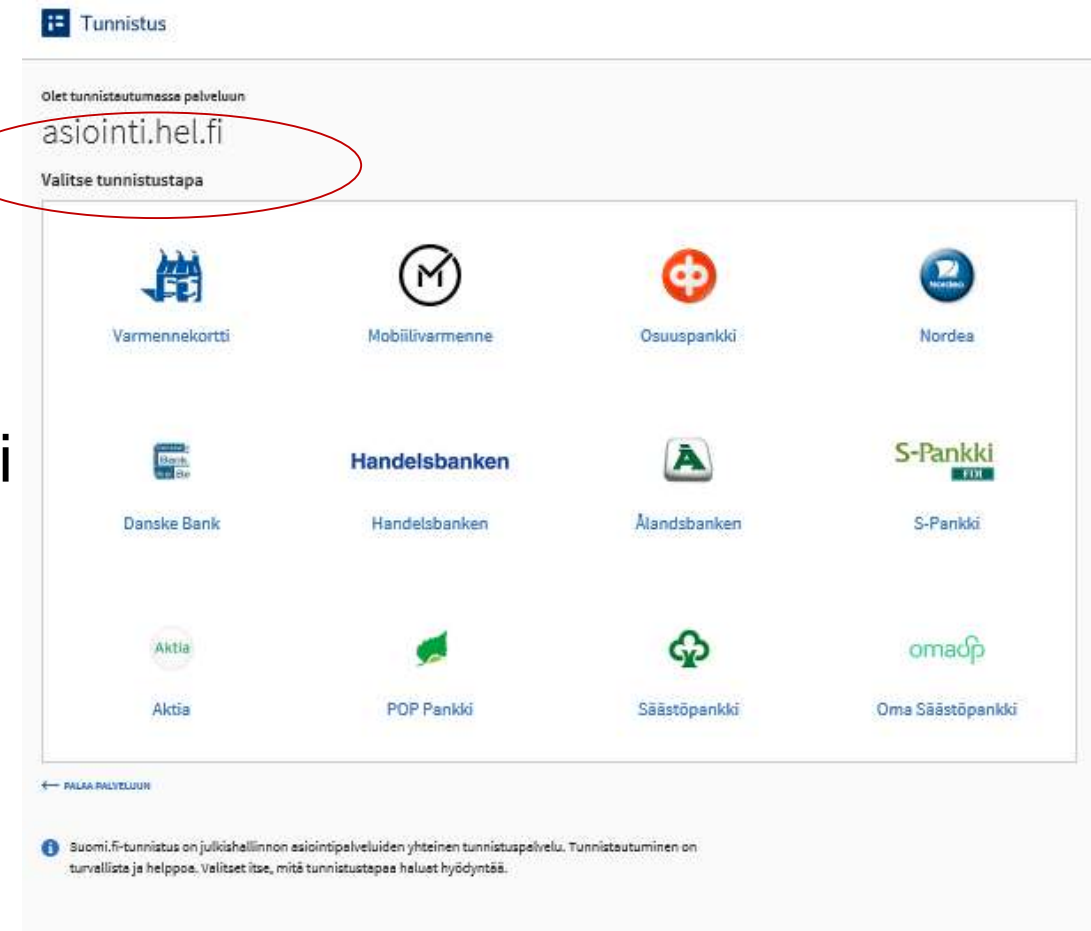
Turvallinen asiointi

Turvallinen tietojen vaihto onnistuu asiointijärjestelmillä.

Niissä vastaanottaja tunnustetaan 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 (anonymikäyttö, tunnistamaton käyttäjä)

Rajoitetun käyttäjäryhmän yhteistyöskenkely

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

Lisätietoja: [Helmi](#) > [Hakusivusto](#) > Haku



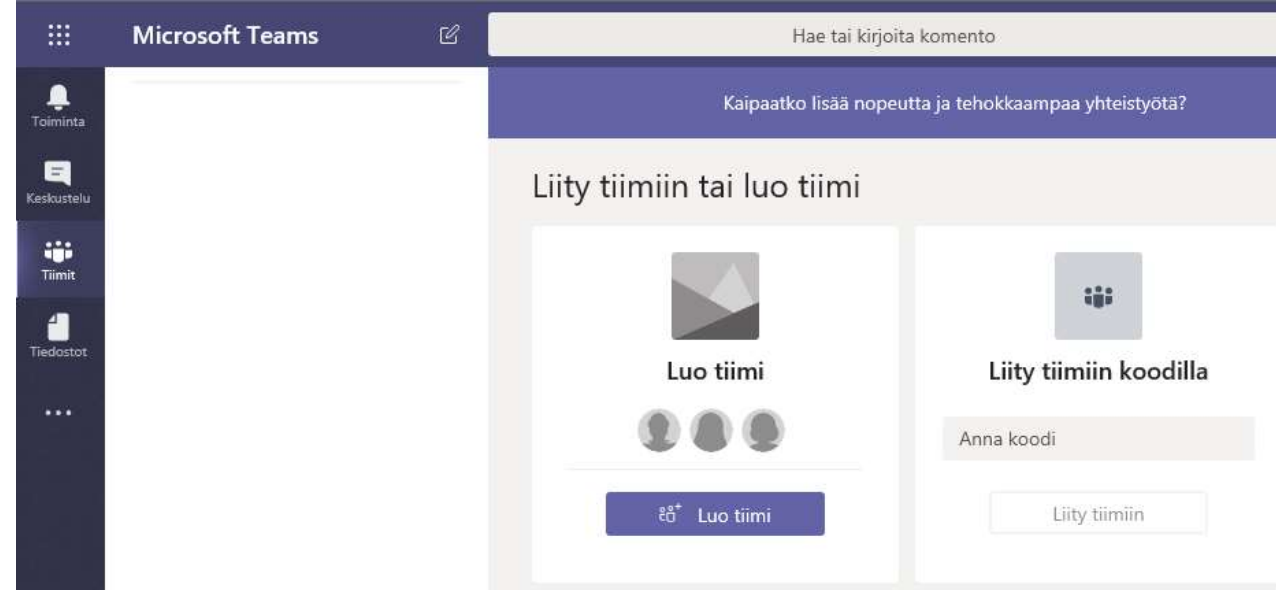
hakusanalla "extranet" Helimestä
"työtilat"

Microsoft Teams

Toimialalla tai yksiköllä voi olla käytössään myös Microsoft Teams ryhmätyöympäristö.

Teams-työryhmät 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 kuuluvalla paikalla 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

Kokeile Helmen hakua...

Helmi > Hakusivusto > Haku

sosiaalisen median ohje



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.

Tietotekniikkaongelmissa kysy paikallisesta ICT-tuestasi apua!

(lähituki, atk-tuki)

Helsinki

TIETOTURVALLISUUSOHJEET



Hallinnollinen tietoturva

Ohjeet
Organisointi
Johtaminen

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 huomioon otettua myös tietoturvaan ja tietosuojaan liittyvät kysymykset.

digi.hel.fi/kehmet

Helsinki

Kehittämismenetelmät

Kehmet

- [Katso tulevat Kehmet-koulutukset täältä!](#)

Helsingin kaupungin ICT-kehittämismenetelmät

Kehmet-sivusto tarjoaa sinulle apua kun mietit, miten kehität toimintaa tai edistät hanketta tai hankekokonaisuutta. Tarjoamme käsitteitä ja menetelmiä yksittäisen kehityshankkeen tueksi sekä usean hankkeen johtamisen avuksi.

Huomioi myös [Digipalveluopas](#) suunnitellessasi palvelun digitalisoimista.

Kehmet kokonaismalli



Tällä sivulla

Kehmet kokonaismalli
Kehittämisen kulku ja menetelmät
Tutkimus, kokeilu, kehitys vai käyttö

Kehittämismenetelmät

Mikä Kehmet on
Kehmet-pikaraide
Kehittämismenetelmä
Roolit ja vastuut
Ketturäkö
Perinteinen menetelmä
Poikkileikkaus
Kehitysaktiivisuus
Lähteet
Yhteystiedot
Sanasto
Koulutukset

Poikkileikkaavat teemat

- Asiakaslähtöisyys
- Tietoturva ja tietosuoja**
- Tietoturva- ja tietosuojatason määrittäminen
- Tietosuojan avainperiaatteet
- Tietoturvasuunnitelma
- Tietoturvajärjestelyt

Anna palautetta

Palautteesi auttaa digitaalista Helsingiä kehittämään entistä paremmaksi.

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
<https://dev.hel.fi/paatokset/asia/hel-2015-010188/khs-2015-41/>

Tietosuojalinjaukset; linjaus henkilötietojen turvalliseen käsittelyyn
<https://dev.hel.fi/paatokset/asia/hel-2017-007001/>



HAE

Tietoturva työpisteellä

Tietoiskut käsittelevät arjen ja työn tietoturvaa. Ne elävöittävät Diggallaan dataa (<https://www.heL.fi/blogit/fi/kirjoitukset/diggallaan-dataa>) -blogin teemoja.

16 videota

Uusimmat

Katsotuimmat



2 min

Näin tehtiin Tietoturva työpisteellä -sarjaa, osa II
05.06.2018



1 min

Tietoturva työpisteellä: Päivitä ohjelmat ja käytä turvaohjelmia
13.11.2017



1 min

Tietoturva työasemalla: Käyttöoikeudet
29.08.2017



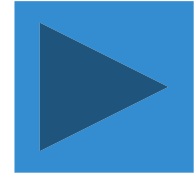
1 min

Saatavuus, eheys ja luottamuksellisuus ovat tietoturvan peruskäsitteitä
21.08.2017

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

<https://www.helsinkikanava.fi/www/kanava/fi/sarjat/sarja?id=309>

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



Diggaillaan dataa

Tietoturva-asiantuntija, Helsingin kaupungin tietotekniikka ja viestintäosasto

Blogissa katsotaan tietoturvan näkövinkkelistä digitalisaatiota, hyvää tiedonhallintaa, tieto- ja viestintäteknikkaa, tietosuojaa sekä muitakin kyberavaruuden asioita. Kuinka ne kuuluvat Helsingin, helsinkiläisten ja kaupungin asiakkaiden elämään.

JAA  



UUSIMMAT KIRJOITUKSET



Tietoturvallinen maksaminen verkkopalvelussa

08.08.2018 15:15 - Diggaillaan dataa

Tietoturvan perusominaisuudet ovat saatavuus, eheys, luottamuksellisuus, todentaminen, kiistämättömyys sekä vaatimusten mukaisuus. Verkkopalvelun maksutapahtumaan ne liittyvät seuraavasti. Vaatimusten mukaisuus Kun verkkopalvelussa käsitellään maksutapahtumia, niin verkkopalvelu täytyy toteuttaa maksupalveluille määriteltyjen turvallisuusvaatimusten mukaiseksi (PCI DS...

[Lue lisää..](#)

<http://www.hel.fi/www/blogit/fi/kirjoitukset/diggaillaan-dataa>

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/>

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.

Viestintäviraston Kyberturvallisuuskeskukselta
<https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet.html>

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

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

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

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

Katso myös Valtiovarainministeriön ajankohtaista digiturvallisuudesta
<https://vm.fi/digiturva>, jossa mm. linkit VM:n tietoturvan [YouTube-videoihin](#).

TIETOTURVA PÄIVITTÄISESSÄ TYÖSSÄ

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

2018 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 tietoisuuteen tarkoitettuja esityskuvia, tietoturvan huoneentauluiksi ja kuvitusaiheiksi sopivia aihekuvia 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