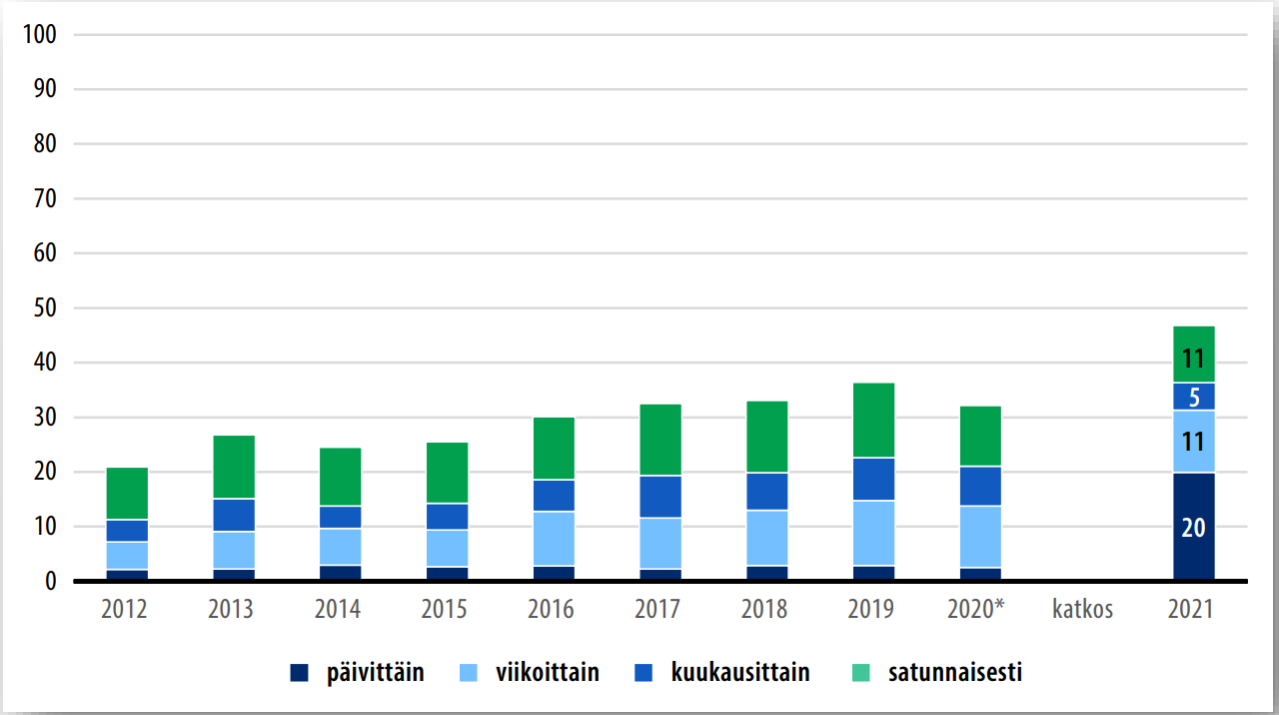
Tietoturva hybridityössä

9.2.2023

Harto Pönkä
Innowise

Kuva: Marvin Meyer @Unsplash, 2018

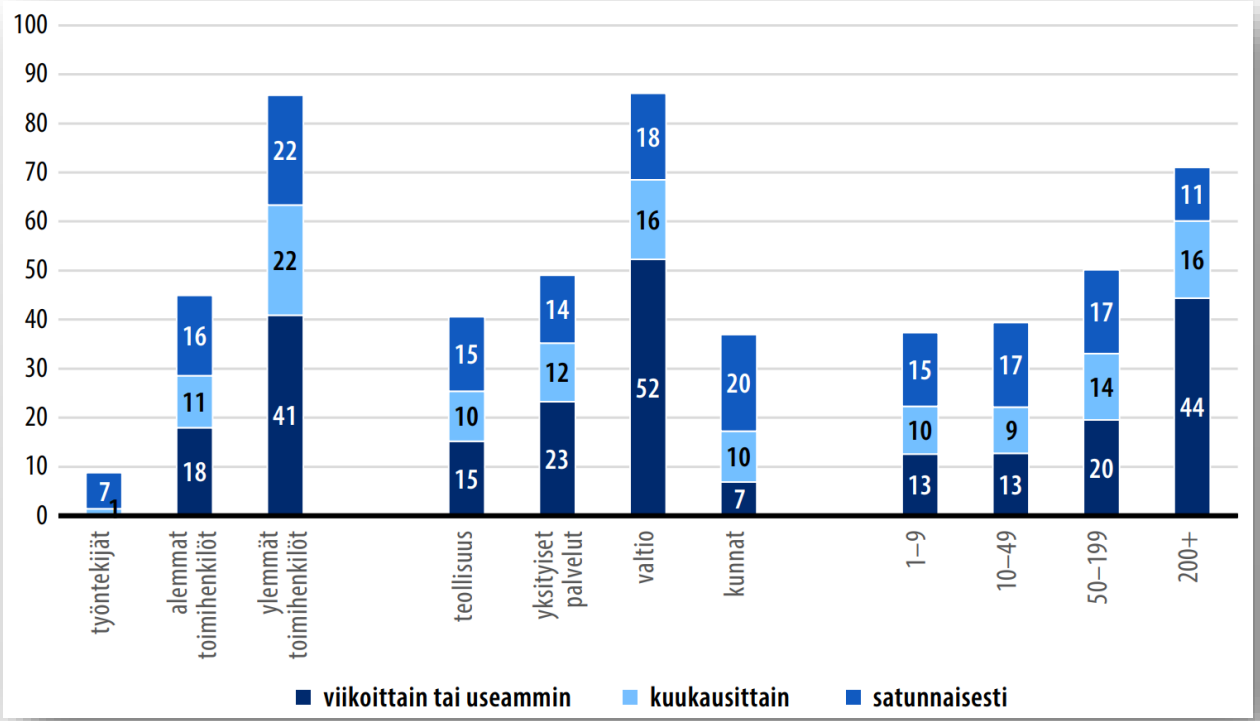
Tehnyt etätyötä viimeisen 12 kuukauden aikana 2012-2021



Korona synnytti etätyöbuumin – aiemmin etätyötä pidettiin monella alalla ”mahdottomana”.

Lähde: TEM, Työolobarometri 2021, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164237/TEM_2022_46.pdf

Tehnyt etätyötä viimeisen 12 kk:n aikana 2021: asema, sektori ja työpaikan koko

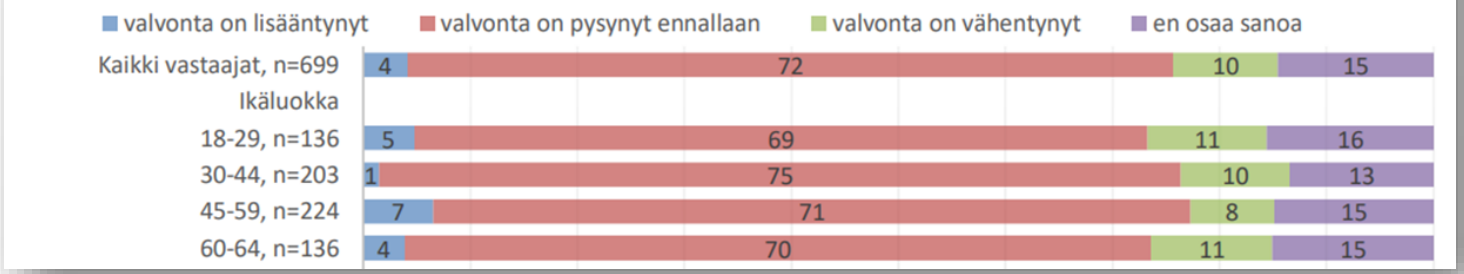


Eniten etätyötä tekevät ylemmät toimihenkilöt, valtion ja isojen organisaatioiden työntekijät.

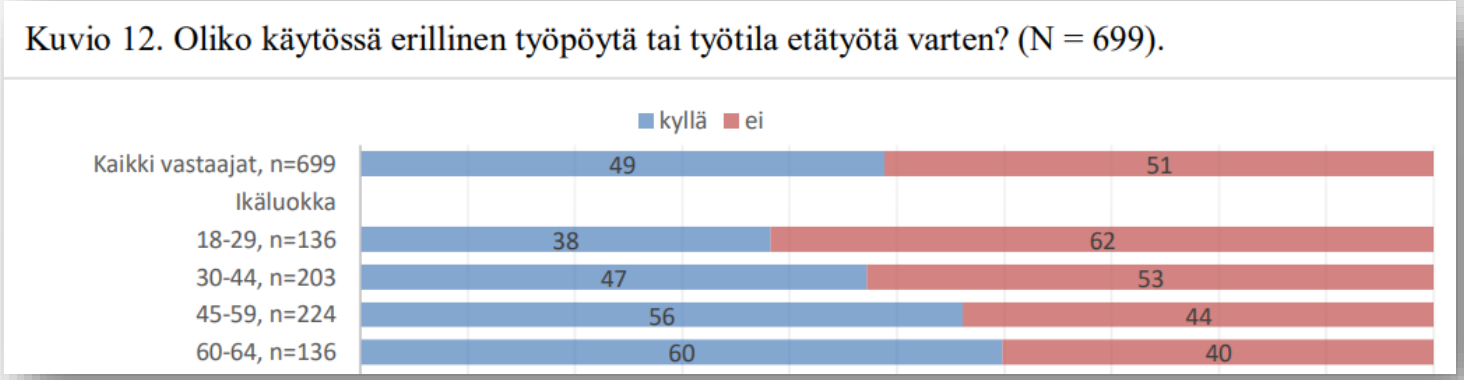
Lähde: TEM, Työolobarometri 2021, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164237/TEM_2022_46.pdf

Etätyötä valvottiin vähemmän ja puolelta puuttui erillinen työtila

Kuvio 6. Työhön liittyvän valvonnan muutos etätyöhön siirtymisen myötä (N = 699).

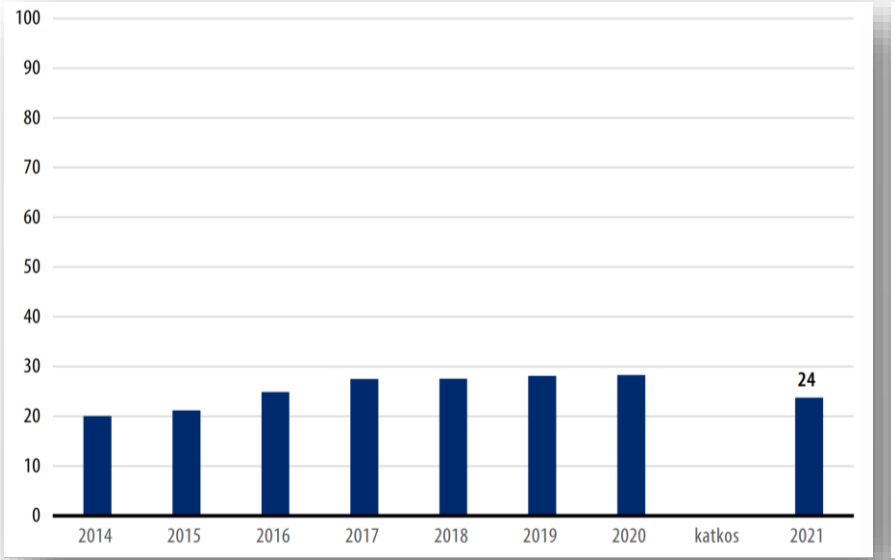


Kuvio 12. Oliko käytössä erillinen työpöytä tai työtila etätyötä varten? (N = 699).

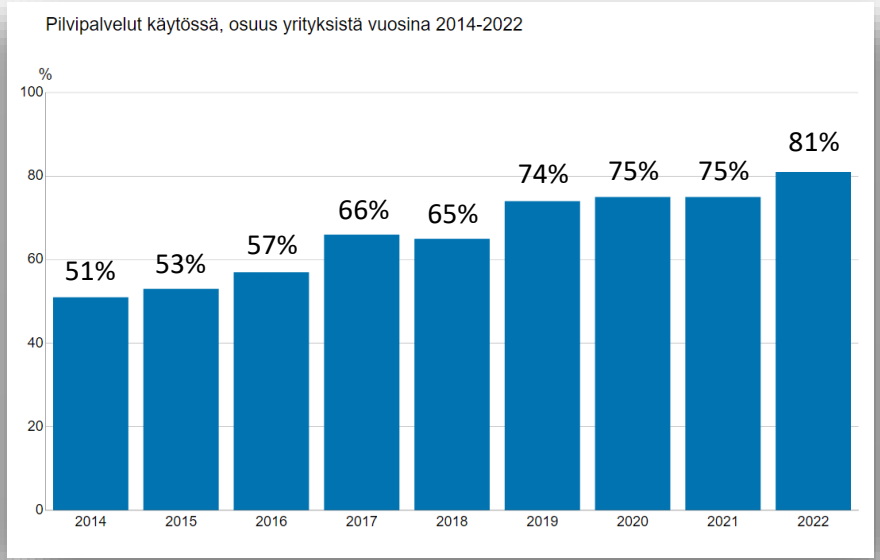


Lähde: Covid-19, luottamus ja digitalisaatio. Tutkimus etätyöstä ja sen järjestymisestä Suomessa keväällä ja syksyllä 2020, Kovalainen, Poutanen & Arvonen, Turun yliopisto, https://www.utupub.fi/bitstream/handle/10024/151453/Covid-19%20luottamus%20ja%20digitalisaatio.pdf (N=1518, 18-64-v. suomalaiset)

Sosiaalisen median käyttö työssä



Pilvipalvelujen käyttö yrityksissä



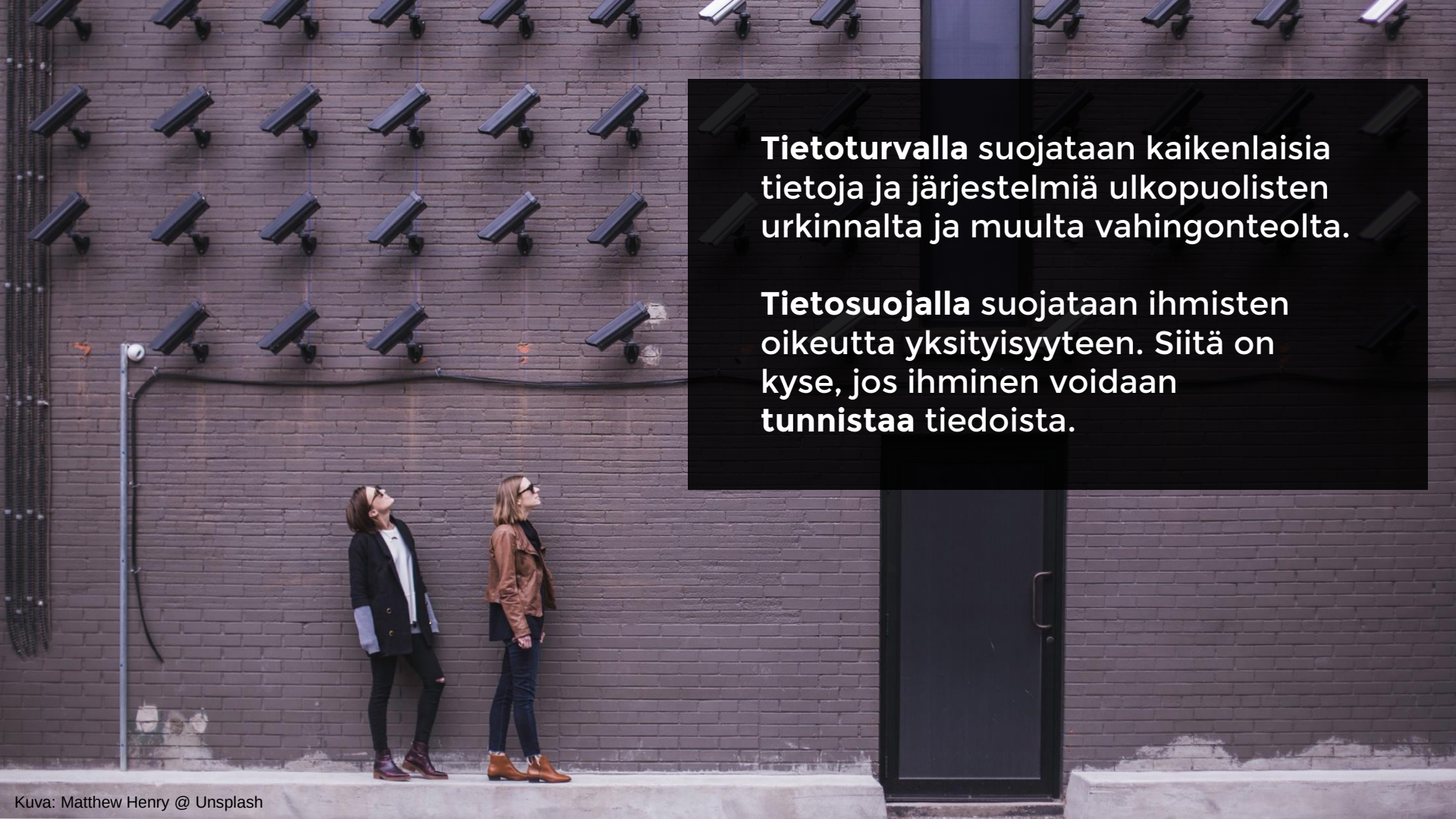
- Somepalvelujen käyttö työssä ei ole juuri kasvanut vuoden 2017 jälkeen, vaan laskenut.
- Yrityksissä käytetään laajasti pilvipalveluja kuten tiedostonjakoa ja toimisto-ohjelmia.

Lähteet: TEM, Työolobarometri 2021, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164237/TEM_2022_46.pdf,
Suomen virallinen tilasto (SVT), Tietotekniikan käyttö yrityksissä, 2022, https://stat.fi/julkaisu/cktvztyy82z790b55dz6j23q3

Organisaatioiden sisäisesti käyttämät viestintäsovellukset

97 %	Sähköposti	**19 %**	Moodle
88 %	Microsoft Teams	**19 %**	Slack
81 %	Microsoft OneDrive	**19 %**	Trello
70 %	Microsoft SharePoint -työtilat	**16 %**	Dropbox
69 %	Verkkolevyt	**16 %**	Google Meet
39 %	Microsoft Yammer	**14 %**	M-Files
36 %	Jira	**13 %**	Howspace
36 %	WhatsApp	**09 %**	Facebook / Workplace by Facebook
31 %	Miro	**09 %**	Mural
28 %	Google Drive	**08 %**	Google Chat
25 %	Confluence	**06 %**	Signal
23 %	Zoom	**05 %**	Microsoft Kaizala

Lähde: North Patrol, Digitaaliset työympäristöt 2022 -selvitys, https://intranet-ostajanopas.fi/2022/08/22/suomalaisten-organisaatioiden-digityon-valineet-2022/
(N=64 vastaajaorganisaatiota)



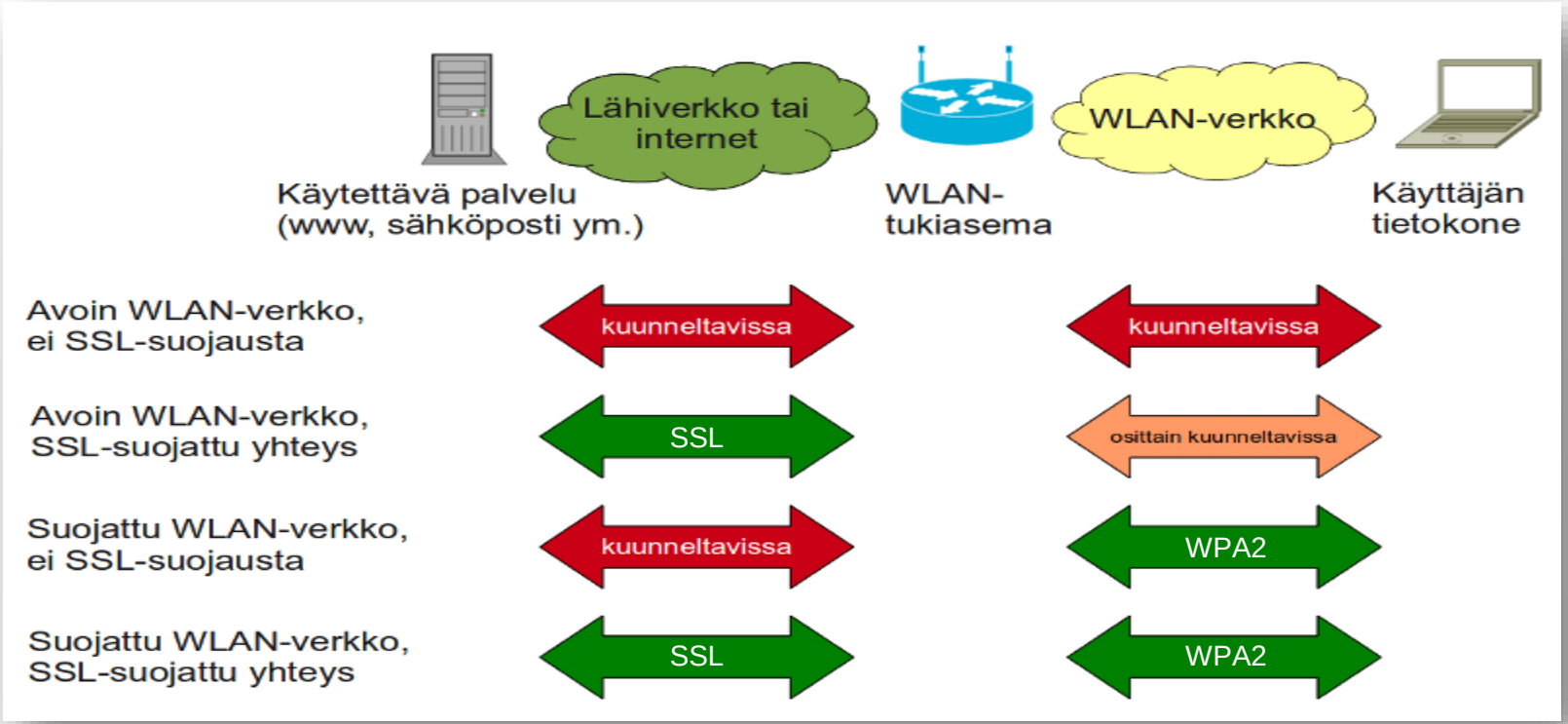
Tietoturvalla suojataan kaikenlaisia tietoja ja järjestelmiä ulkopuolisten urkinnalta ja muulta vahingonteolta.

Tietosuojalla suojataan ihmisten oikeutta yksityisyyteen. Siitä on kyse, jos ihminen voidaan **tunnistaa** tiedoista.

Kuva: Matthew Henry @ Unsplash

Käytä luotettavia ja salattuja verkkoja

Langattoman verkkoyhteyden turvallisuus



Kuva: Viestintävirasto, 2011, lisätietoa:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

WLAN-tukiasemien turvallisuus

1. **Käytä WPA2- tai WPA3-salausta ja verkkoon kirjautumisessa vahvaa salasanaa.**
   - Päivitä tarvittaessa verkkokorttisi ajuri WPA2- tai WPA3-yhteensopivaksi.
   - Älä käytä vanhaa WEP- tai WPA-salausta.
   - Tukiaseman nimen piilottaminen ei paranna sen tietoturvaa.

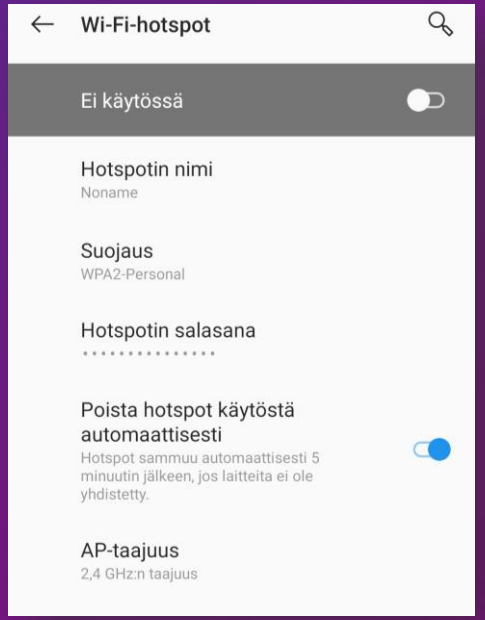
2. Muuta WLAN-tukiasemasi hallintapaneelin asetuksia vain kaapeliyhteyden kautta. Voit estää sen käytön langattoman verkon kautta.
3. Vaihda WLAN-tukiaseman hallintapaneelin käyttäjätunnus ja salasana. Hyökkääjä voi saada tietoonsa tehdasasetuksena olevan tunnuksen ja salasanan.
4. Tee tukiaseman ohjelmiston päivitykset viipymättä.
5. Seuraa verkon käyttöä tuntemattomien käyttäjien (laitteiden) varalta.

Nettiyhteyden jakaminen Android-kännykästä

- Tarkista, että Wi-Fi-hotspotissa on WPA2-suojaus päällä
- Käytä vahvaa salasanaa
- Nimeä hotspot niin, ettei siitä voi päätellä sen omistajaa

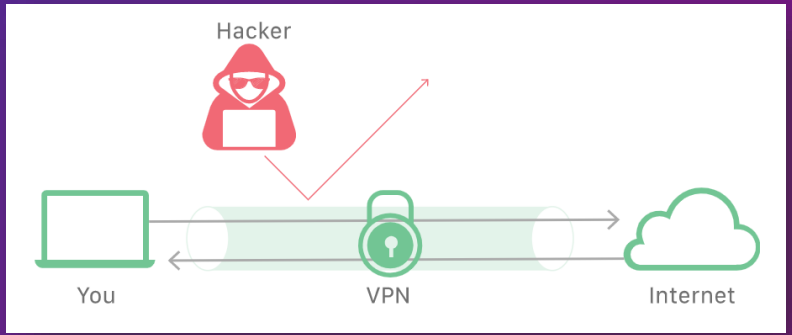
- Jos käytät kännykässä VPN-yhteyttä ja jaat nettiyhteyden tietokoneeseen, ei tietokone ole kuitenkaan VPN:n piirissä.

  → Kytke VPN päälle aina siinä laitteessa, jolla käytät nettiä.



VPN-yhteys salaa nettiliikenteen

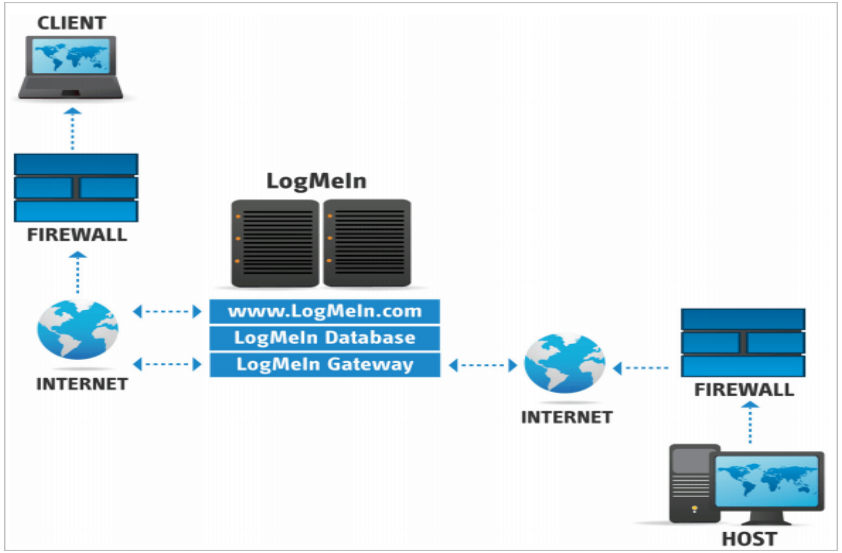
- VPN-yhteydellä nettiliikenne kulkee salattuna palveluntarjoajan palvelimen kautta.
- VPN estää oikean IP-osoitteen ja sijainnin näkymisen verkkopalveluille.
- Käytä työasioissa vain työnantajan VPN-yhteyttä ja hyväksyttyjä sovelluksia.
- Kuluttajille sopivia VPN-palveluita:
  - ProtonVPN, https://protonvpn.com/
  - Opera-nettiselain sisältää VPN:n, http://www.opera.com/fi
  - F-Secure Freedome, https://www.f-secure.com/en/web/home_global/freedome



Lisätietoa ja kuva: https://www.cloudflare.com/learning/access-management/what-is-a-vpn/

Etäyhteyssovellukset

- Etäyhteyssovelluksella voi käyttää esimerkiksi työpaikan tietokonetta muualta.
- Etäyhteyssovellusten tietoturva on yleensä hyvä: salattu yhteys ja vahva salasana.
- Jos mahdollista, käytä kaksivaiheista kirjautumista ja VPN-yhteyttä.
- Älä jätä etäyhteyttä valvomatta ja pidä kirjautumistunnukset suojassa.
- Käytä työasioissa vain organisaation hyväksymiä etäyhteyssovelluksia.
- Ilmainen/edullinen etäyhteyssovellus esim. https://www.teamviewer.com/
- VPN vai etäyhteyssovellus? https://proprivacy.com/vpn/guides/vpn-vs-remote-desktop-comparison



Esimerkki: LogMeIn-sovelluksen toimintaperiaate

Vahva salasana

- **Mieluummin salalause kuin salasana!**

- Mitä pitempi, sen vahvempi (yli 8 merkkiä)
- Kirjaimia, numeroita ja erikoismerkkejä
- Ei ole nimi, sana, päivämäärä tai muuten arvattavissa
- Ei ole käytössä muualla
- Vaihda salasana, jos se on vuotanut

- Käytä kaksivaiheista todennusta aina, kun mahdollista!

Etä- ja hybridityön tietoturvasta

Onko tietokoneesi turvallinen?

Pakollinen kirjautuminen

Virusten ja haitta-ohjelmien torjunta

Ajanmukainen nettiselain

Verkkoyhteys ja palomuuri

Ohjelmat

Varmuuskopiot

Käyttäjä

Kuva: Alkuperäinen IBM PC 5150, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:IBM_PC_5150.jpg (CC-BY-SA)

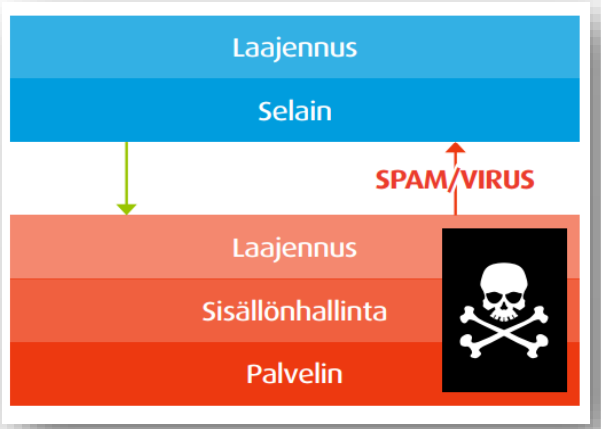
Miksi päivitykset ovat tärkeitä?

1. Hyökkääjä etsii verkkopalveluita ja -sivustoja, joissa on tietoturva-aukkoja.

2. Hyökkääjä saastuttaa haavoittuvan palvelun tai sivuston.

3. Haittaohjelma etsii saastuneen palvelun käyttäjiltä tietoturva-aukkoja:
   a) nettiselaimesta
   b) selaimen laajennuksista/lisätoiminnoista
   c) käyttöjärjestelmästä

4. Jos tietoturva-aukko löytyy, käyttäjän laitteelle voidaan asentaa viruksia ja haittaohjelmia.

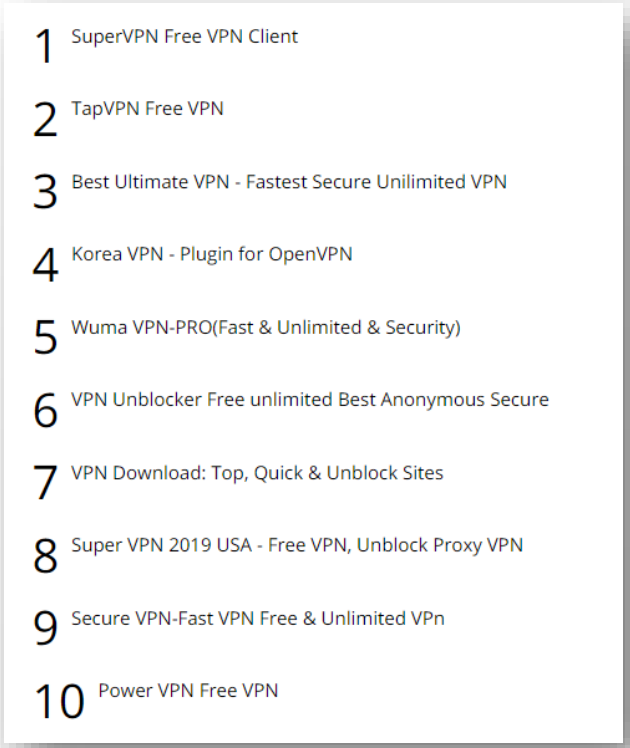


Lähde: Viestintäviraston Kyberturvallisuuskeskuksen vuosiraportti 2015,
https://www.viestintavirasto.fi/attachments/tietoturva/Viestintaviraston_Kyberturvallisuuskeskuksen_vuosiraportti_2015.pdf

Kännyköiden tietoturva

- **Päivittämätön laite tai sovellus on aina riski.**
- Käytä avaukseen PIN-koodia, salasanaa, kuviota tai sormenjälkeä.
- Asenna vain turvallisiksi tietämiäsi sovelluksia.
    - App Storen sovellustarjontaa valvotaan tarkemmin kuin Google Playn.
- Käytä vain turvallisiksi tietämiäsi WLAN-verkkoja.
- Käytä laitteen paikantamista häviämisen varalta.
- Käytä sovelluksissa kaksivaiheista kirjautumista, jos sellainen on tarjolla.
- Jos säilytät työhön liittyviä tiedostoja kännykässä, salaa tallennustila/muistikortti.
- Jos laitteeseen tai sovelluksen ei saa enää päivityksiä, lopeta sen käyttö.
- Tyhjennä vanha kännykkä.

Suositut ilmaiset VPN-sovellukset sisälsivät haavoittuvuuksia



”Nämä haavoittuvuudet antavat hakkereiden katkaista helposti viestinnän vpn-palveluntarjoajan sekä käyttäjän välillä, jolloin hakkerit näkevät kaiken, mitä käyttäjä tekee.

--

85 prosenttia ilmaisista vpn-ohjelmistoista halusi käyttäjältä tarpeettoman paljon tietoa, kuten pääsyn lukea, muokata tai poistaa puhelimessa olevaa dataa, urkkia käyttäjän tai tämän ystävien puhelinnumerot sekä saada selville kännykän sijainnin”

Käytä vain työnantajan hyväksymää VPN-sovellusta!

Lähde: Tivi, 27.2.2020,
https://www.tivi.fi/uutiset/nama-10-vaarallista-android-sovellusta-tulisi-poistaa-heti/d730cffb-50bd-4753-897b-0bf77236822a

5 neuvoa mobiilisovellusten arviointiin

1. **Asenna sovelluksia vain luotetuista sovelluskaupoista.**

2. **Tarkista sovelluksen tekijä ja sovelluksen saama palaute.**
   - Sovelluskaupoissa voi olla myös tunnettujen sovellusten väärennöksiä.
   - Jos sovellukselle ei tule päivityksiä, se voi sisältää haavoittuvuuksia, joita hyökkääjät voivat hyväksikäyttää.

3. **Arvioi sovelluksen pyytämät oikeudet verrattuna sovelluksen käyttäjää palvelevaan toiminnallisuuteen.**
   - Hyväksy mahdollisimman vähän oikeuksia laitteen tietoihin.
   - Tarkista sovellusten oikeudet kännykän asetuksista.

4. **Tutustu sovelluksen käyttöehtoihin.**
   - Mitä tietojen keräämisestä ja käsittelystä kerrotaan?
   - Missä maassa tietoja käsitellään?

5. **Noudata työnantajan ohjeita kännyköiden käytöstä työssä.**
   - Noudata työnantajan ohjeita, jos asennat sovelluksia työssä käytettäviin laitteisiin.

Lähde: Viestintäviraston Kyberturvallisuuskeskus, 2018,
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/11/ttn201811141100.html

Pikaviestintä- ja etäkokoussovellusten ominaisuuksia

TYÖKALU	Pika-viestintä	Etä-kokous	Paikal-linen palvelin	Pilvi-palvelu	Päästä päähän salaus	TLIV-luokitellun tiedon käsittely	Kerta-kirjautuminen	Kaksivaiheinen tunnistau-tuminen
Slack	✓	✓		☁			✓	✓
Mattermost Enterprise	✓	✓	⌂			✓	✓	✓
Teams	✓	✓		☁			✓	✓
Signal	✓			☁	✓		🔍	🔍
WhatsApp	✓			☁	✓			
Zoom Business		✓		☁	✓		✓	✓
Webex		✓	⌂	☁	ⓘ		✓	
BlueJeans		✓		☁	ⓘ		✓	✓
Click Meeting		✓		☁				

🔍 Signal tarjoaa osapuolien vahvan todentamisen ja tiedon paikallisen suojaamisen PIN-koodin avulla.

ⓘ Päästä päähän salaus ei toteudu etäkokouksissa, joihin osallistutaan puhelimitse tai jotka nauhoitetaan (Webex).

Lähde: Huoltovarmuusorganisaatio Digipooli, 2020, Ohjeita turvallisten etätyövälineiden valintaan, https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/07/03140734/Ohjeita-turvallisten-et%C3%A4ty%C3%B6v%C3%A4lineiden-valintaan.pdf

Signal työkäytössä

- Minimaalinen henkilötietojen käsittely: puhelinnumero riittää rekisteröitymiseen
- Tunnus voi olla henkilön tai organisaation
- Vahva päästä-päähän-salaus
- Ei lähetä palvelimelle puhelinnumeroita, vaan niistä muodostetut SHA256-tunnisteet
- Ehdot ja tietosuoja: https://signal.org/legal/

- Ei tarjoa henkilötietojen käsittelyn sopimusta
- Koska Signal käyttää tietoja vain viestien välitykseen, se voisi sisältyä GDPR:n 95 artiklan poikkeukseen viestien välitystietojen osalta.
- Rekisteröidyiltä on syytä pyytää suostumus, jos heille aiotaan viestiä Signalin kautta.

Kuva: Mika Baumeister @Unspalsh (Free to use/Unsplash License)

Ohjelmisto / Palvelu	Signal
Kuvaus ja käyttösuositus	Avoimen lähdekoodin alustariippumaton pikaviestintä- ja puhelusovellus. Sovellusta voidaan käyttää yksityiseen viestinvälitykseen, kun halutaan salata viestit ja puhelut sekä varmistua toisen osapuolen henkilöllisyydestä. Signalin käyttö turvallisesti vaatii käyttäjiltä tavanomaista parempaa tietoturvaosaamista.
Viitteitä	*https://support.signal.org/hc/en-us/articles/360007059792-Signal-PINs* *https://signal.org/en/*

Ohjelmisto / Palvelu	WhatsApp
Kuvaus ja käyttösuositus	Facebookin omistama alustariippumaton pikaviestintä- ja puhelusovellus. Sovellusta voidaan käyttää julkisen tiedon käsittelyyn ja viestintään, mikäli tiedon luottamuksellisuuden vaarantumisesta ei aiheudu vakavia vaikutuksia.
Viite	*https://www.whatsapp.com/security/*

Lähde: Huoltovarmuusorganisaatio Digipooli, 2020, Ohjeita turvallisten etätyövälineiden valintaan,
https://www.huoltovarmuuskeskus.fi/files/57c03f5135e2394fe6c3a442d4348b27d9b48061/ohjeita-turvallisten-etatyovalineiden-valintaan.pdf

TikTokin ongelmia

- Sisältö on voimakkaasti algoritmin ohjaamaa
- Epäasiallista sisältöä, vahingollisia haasteita, kiusaamista, häirintää
- Kerää dataa käyttäjistä monilla tavoilla
- Linkit aukeavat sovelluksen omaan selaimeen, joka seuraa jokaista näppäimen painallusta myös muilla sivustoilla
- Työntekijöiden on kerrottu lukevan käyttäjien henkilötietoja
- Kerrottu aikoneen seurata joidenkin käyttäjien sijainteja epäselviin tarkoituksiin
- Kiinalaistaustainen yritys, henkilötietoja voi päätyä Kiinaan
- Useat tahot ovat kieltäneet TikTokin asentamisen työpuhelimeen

Kuva: myriammira @Freepik (Free license)

Tietosuoja etätyössä

Ohjeita henkilötietojen käsittelyyn

- Henkilötietoja saa käyttää vain rekisterien tietosuojaselosteissa kerrottuihin tarkoituksiin.
- Työntekijä saa käsitellä vain hänen työtehtäviinsä liittyviä henkilötietoja.
- Henkilötietoja ei näytetä tai kerrota sivullisille.
- Henkilötietoja ei julkaista tai luovuteta ilman suostumusta tai laista tulevaa perustetta.
- Tietojen säilytyksessä noudatetaan fyysistä tietoturvaa: valvotaan tiloja ja laitteita.
- Tietojärjestelmissä käytetään henkilökohtaisia tunnuksia sekä huolehditaan käyttöoikeuksista ja seurannasta (lokit).
- Työnantaja huolehtii henkilötietojen käsittelyn ohjeistuksesta, koulutuksesta ja vaitiolovelvollisuudesta työntekijöille.

Security

Mailchimp says it was hacked — again

Zack Whittaker @zackwhittaker / 7:45 PM GMT+2 • January 18, 2023 Comment

Image Credits: Rafael Henrique / SOPA Images / LightRocket / Getty Images

Email marketing and newsletter giant Mailchimp says it was hacked and that dozens of customers' data was exposed. It's the second time the company was hacked in the past six months. Worse, this breach appears to be almost identical to a previous incident.

The Intuit-owned company said in an unattributed blog post that its security team detected an intruder on January 11 accessing one of its internal tools used by Mailchimp customer support and account administration, though the company did not say for how long the intruder was in its systems, if known. Mailchimp said the hacker targeted its employees and contractors with a social engineering attack, in which someone uses manipulation techniques by phone, email or text to gain private information, like passwords. The hacker then used those compromised employee passwords to gain access to data on 133 Mailchimp accounts, which the company notified of the intrusion.

One of those targeted accounts belongs to e-commerce giant WooCommerce. In a note to customers, WooCommerce said it was notified by Mailchimp a day later that the breach may have exposed the names, store web addresses and email addresses of its customers, though it said no customer passwords or other sensitive data was taken.

Esimerkki: MailChimpin tietovuoto

- MailChimp on laajasti käytetty sähköpostimarkkinointityökalu.
- Hakkeri oli päässyt 11.1.2023 Mailchimpin hallintajärjestelmään ”sosiaalisen manipuloinnin” avulla käyttäen työntekijöiden käyttäjätunnuksia.
- Hakkeri pääsi käsiksi 133 Mailchimpin asiakkaan tunnukseen. Yksi vuodon kohteista oli esimerkiksi suosittu verkkokauppajärjestelmä WooCommerce.
- Murtautuja sai käsiinsä yritysten markkinointirekistereissä olevien nimet ja sähköpostiosoitteet.
- Lukumääriä ei ole julkaistu, mutta todennäköisesti kyse on vähintään kymmenistä tuhansista henkilöistä.
- Viimeksi Mailchimpille kävi samalla tavalla elokuussa 2022.

Lähde: TechCrunch, 18.1.2023, https://techcrunch.com/2023/01/18/mailchimp-hacked/
Mailchimpin tiedote: https://mailchimp.com/en-gb/january-2023-security-incident/

28

Henkilötiedot puheluissa

- Henkilö on tunnistettava puhelussa, jos käsitellään hänen henkilötietojaan.
- Vahva tunnistaminen:
  1) jotain mitä olet (nimi, HETU)
  2) jotain mitä sinulla on (puh.nro, s.postiosoite)
  3) jotain mitä tiedät (salasana, asiakastiedot)
- Puhelujen nauhoittaminen on sallittua, kun rekisterinpitäjällä on käsittelyyn oikeusperuste, esim. asiakassuhteessa rek. pit. oikeutettu etu.
- Henkilötietojen käsittelystä on informoitava. Esimerkiksi nauhoituksesta on kerrottava.
- Puhelussa voidaan kertoa, mistä tietosuojaseloste on luettavissa (nettisivut), lukea se ääneen tai se voidaan lähettää esimerkiksi sähköpostitse.

Lisätietoa vahvasta sähköisestä tunnistamisesta esim. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tarjoa-asiakkaillesi-parasta-vahva-sahkoinen-tunnistus

Tietosuoja viestinnässä

- Normaalissa sähköpostissa:
  - Tavalliset henkilötiedot (nimi, osoite jne.)
  - Edellytys: henkilökohtaiset sähköpostilaatikot ja tietoturva kunnossa

- Suojatussa sähköpostissa, turvapostissa tai muussa turvallisessa viestintäkanavassa:
  - Arkaluontoiset henkilötiedot
  - Salassa pidettävät tiedot ja asiakirjat

- Omat laitteet ja somepalvelujen käyttö työnantajan ohjeistuksen mukaan.

Tietosuoja etäkokouksissa ja muissa yhteistyösovelluksissa

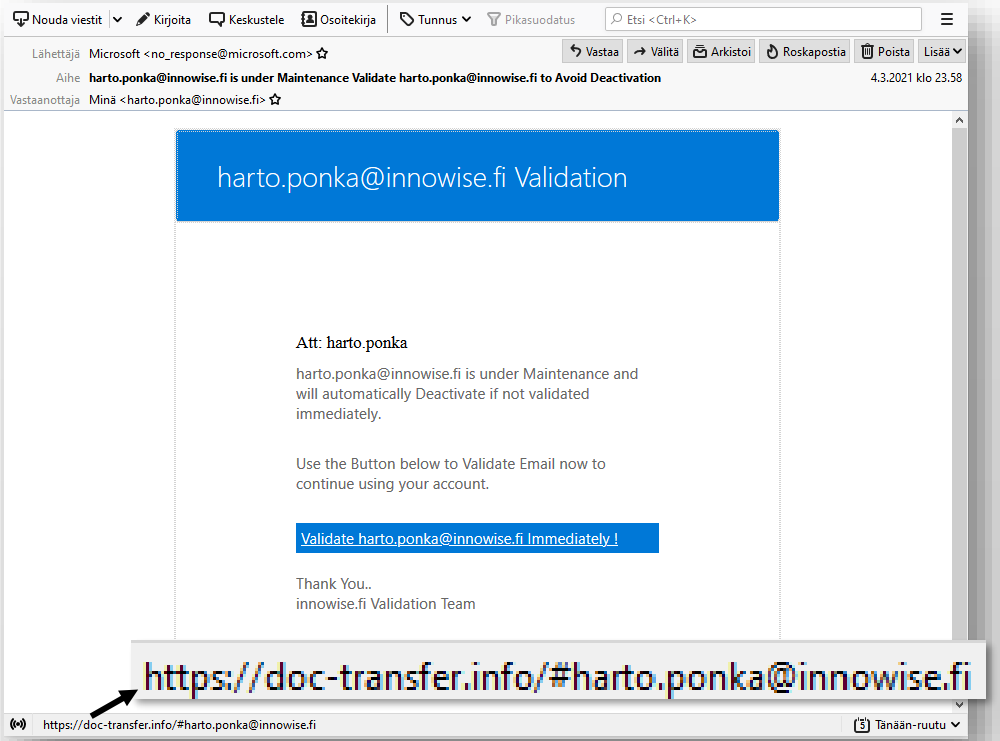
- **Käytä vain organisaation sallimia sovelluksia.**
- Toimita kutsu henkilökohtaisesti osallistujille.
- Informoi osallistujia henkilötietojen käsittelystä.
- Varmista huoneessa olijoiden henkilöllisyys.
- Käsiteltävät henkilötiedot ja asiat riippuvat osallistujien työtehtävistä.
- Varmista esittäjien osaaminen etukäteen.
- Kerro etukäteen, jos kokous tallennetaan, ja näkyvätkö tallenteessa osallistujien nimet ja chat.
- Kotoa osallistuvat: ei sivullisia kuulolla, videon ja mikrofonin käyttö kotirauhan alueella perustuu vapaaehtoisuuteen.
- Lopuksi: päätä kokous, tyhjennä tai sulje huone.
- Suojaa tallenne ja huolehdi sen tietosuojasta.

Älä jaa etäkokouksen linkkiä ulkopuolisille

Kuva: Daniel Veerlan, https://twitter.com/danielverlaan/status/1329799677827551233
Lisää tapauksesta: BBC, 21.11.2020, https://www.bbc.com/news/world-europe-55027641

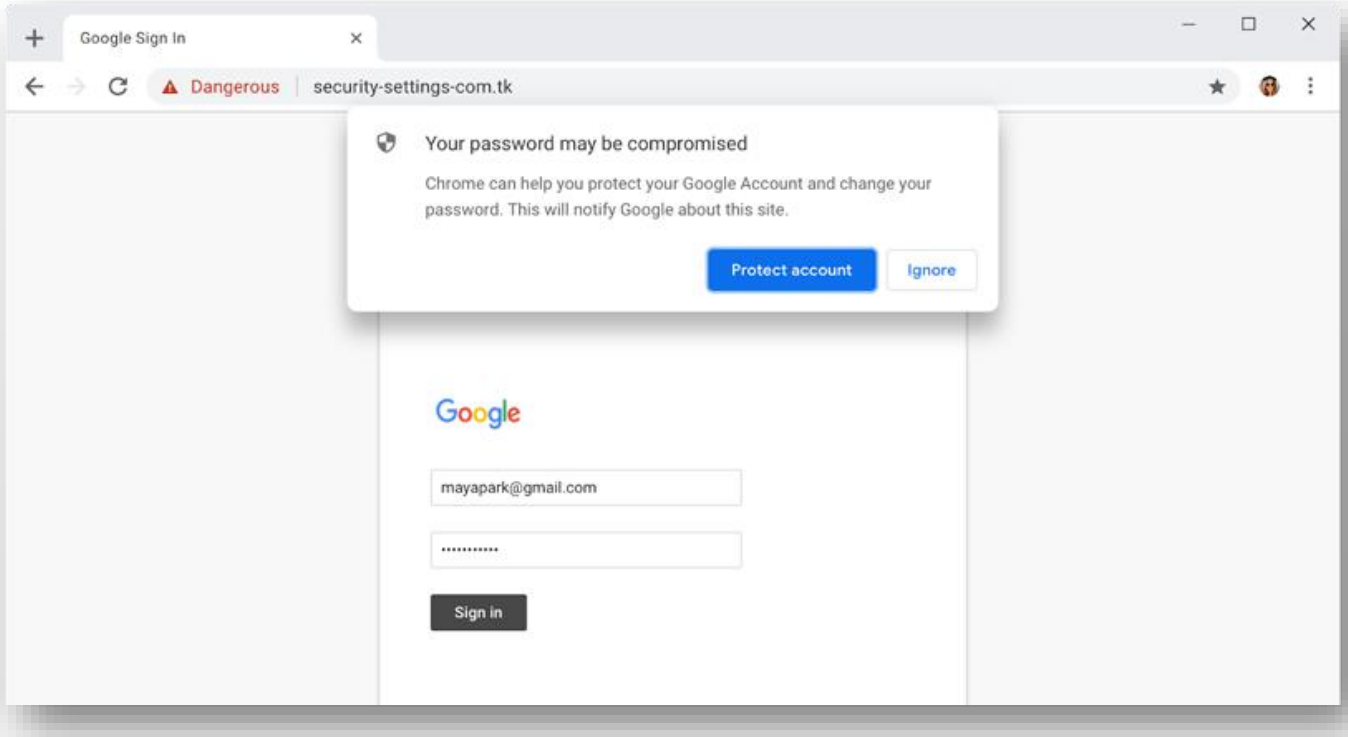
Ajankohtaisia tietoturvariskejä

Huijaus- ja tietojenkalasteluviestit



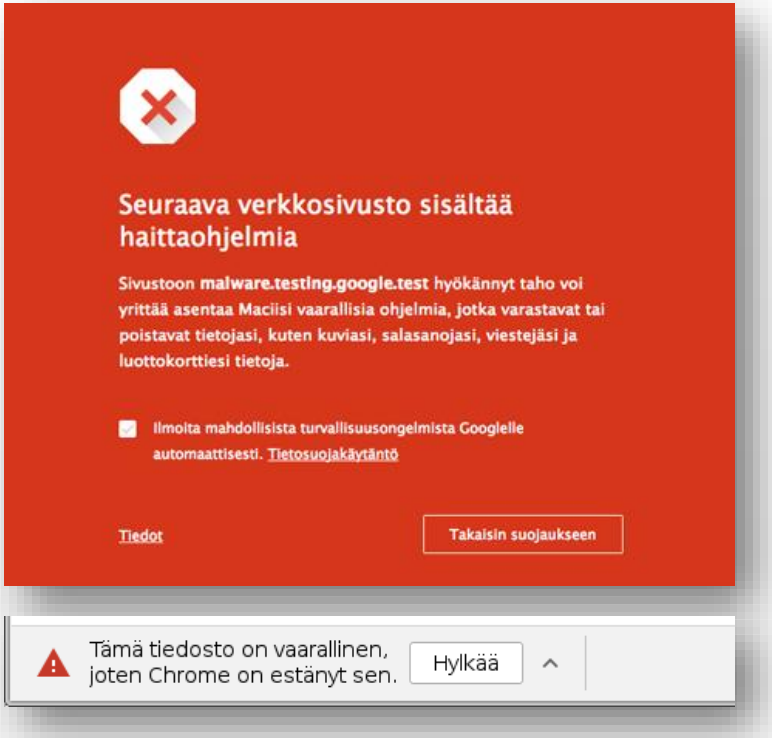
1. Älä luota sähköpostin tai tekstiviestin lähettäjän nimeen tai osoitteeseen/numeroon.
2. Älä koskaan avaa yllätyksenä tullutta liitetiedostoa.
3. Tarkista linkki esim. viemällä hiiri sen päälle.
4. Anna tietojasi vain varmasti luotettaville tahoille.
5. Jos epäilet huijausta, tarkista aitous muuta kautta

Onko tämä aito Googlen kirjautumissivu?



Kuva: Google Chromen tietosuojailmoitus, 2020,
https://www.google.fi/chrome/privacy/whitepaper.html

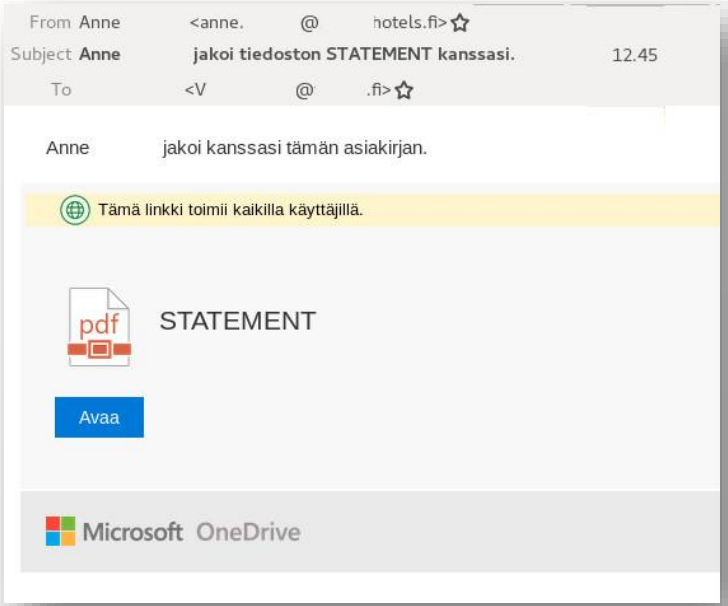
Nettiselaimet pyrkivät tunnistamaan huijaussivustot

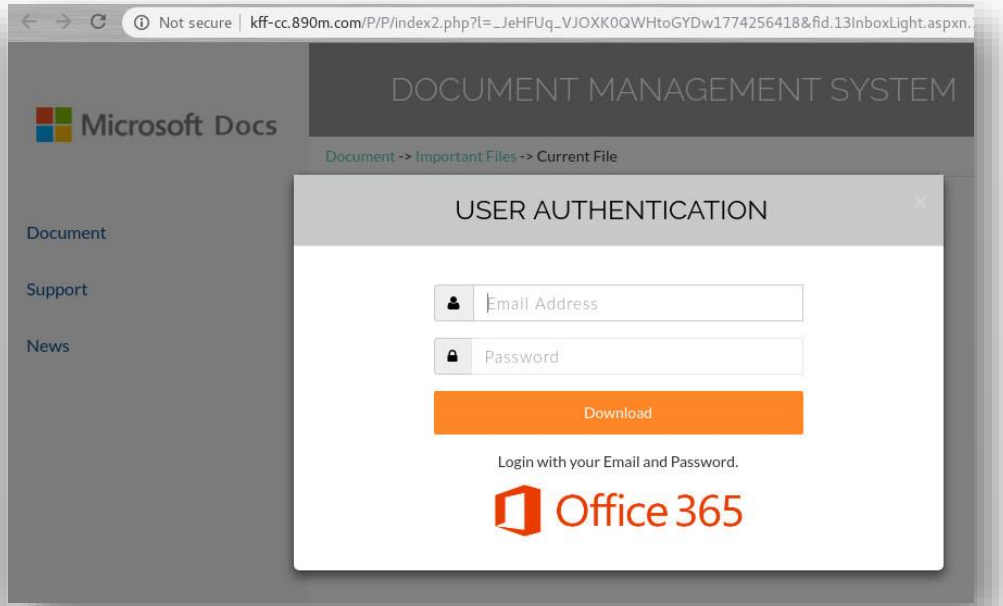


- Yleisimmät nettiselaimet pyrkivät tunnistamaan huijaussivustot ja varoittamaan epäilyttävistä tiedostoista
- Virustorjuntaohjelmat parantavat yleensä nettiselailun turvallisuutta

Kuvat: Google Chromen tietosuojailmoitus, 2017,
https://www.google.fi/chrome/privacy/whitepaper.html

Varo: Office 365 -huijaukset ovat yleisiä!





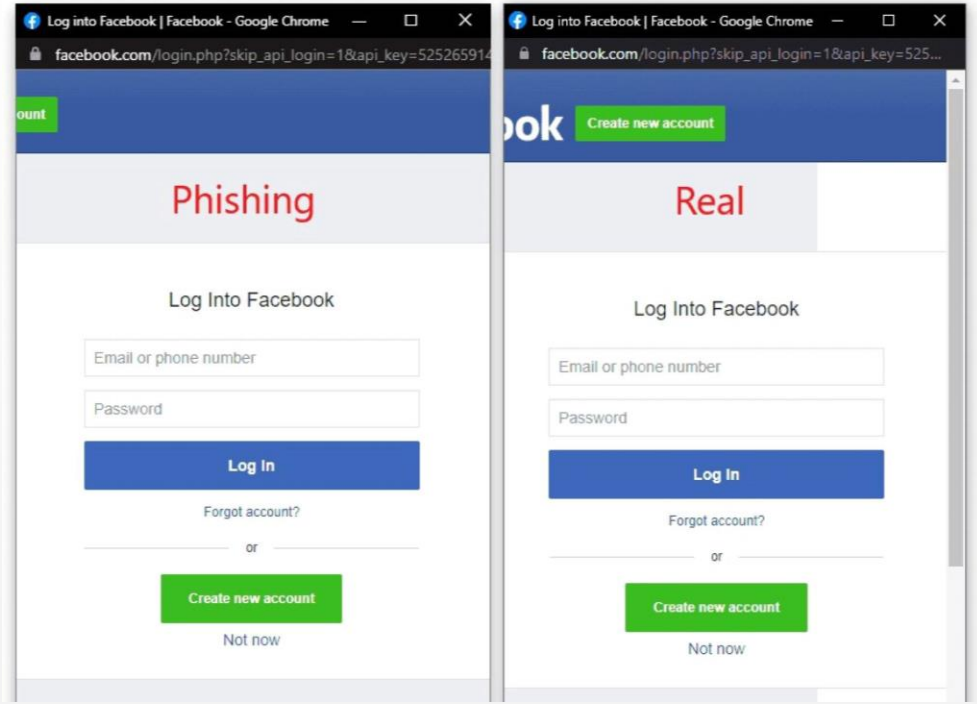
- Rikolliset pyrkivät tietojenkalastelusivun avulla saamaan haltuunsa käyttäjätunnuksia, joilla he voivat päästä käsiksi luottamuksellisiin tietoihin kuten lähetettyihin laskuihin.
- Murretuilla tunnuksilla voidaan lähettää esim. ”korjattuja” huijauslaskuja.

Lähde: Viestintävirasto, 2019,
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusin-microsoft-office-365-huijaus-ohjaa-uhrin-murretulle-sharepoint-tilille

Selain selaimessa –huijaussivu

- Huijari houkuttelee kävijän verkkopalveluun, jossa voi kirjautua sisään käyttäen esim. Facebook-tunnusta
- Aukeava Facebook-kirjatumissivu onkin huijarin tekemä ”kuvakaappaus” oikeasta Facebookin sivusta, mukaan lukien siinä näkyvä selaimen osoiterivi.
- Jos kävijä antaa sivulle tunnuksensa ja salasanansa, ne päätyvät huijarille.

- Helpoin tapa todeta tämä huijaukseksi: klikkaa osoiteriviä ja kokeile toimiiko se oikein.



Lisää aiheesta: https://www.is.fi/digitoday/tietoturva/art-2000008698981.html
Alkuperäinen lähde ja kuva: https://mrd0x.com/browser-in-the-browser-phishing-attack/

Huijauspuhelut

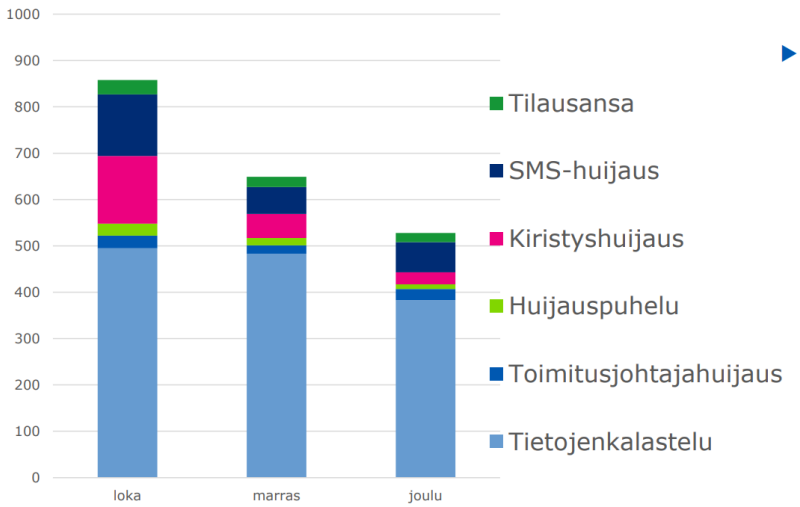
- Käyttäjätunnusten urkintaa, esim. huijari esiintyy IT-tukihenkilönä
- Nigerilaishuijaus: saat rahaa, mutta ensin joudut maksamaan siitä aiheutuvia kuluja
- Pankkitunnusten ja luottokorttitietojen urkintaa pankkien ja viranomaisten nimissä
- Maksulliset numerot takaisin soitettaessa
- Harhaanjohtavat yritykset ja yhdistykset
- Yrityksille suunnatut ylihintaiset verkkomainonta- ja domain-huijauspalvelut
- Hakemistopalvelut: ”jatketaanko aiemmalla näkyvyydellä?”
- Muut tilausansat

Lisätietoa esim. Mikrobitti, 23.5.2020, https://www.mikrobitti.fi/uutiset/mb/455d0762-783c-4f14-8cdc-3d1b1eb96346

Kybersää joulukuu 2022

Käsiteltyjä huijaustapauksia Q4/2022

3kk



- Vuoden 2022 viimeisen neljänneksen ilmiöitä olivat:
  - Vuoden vaihdetta kohden huijausten kokonaismäärä näytti rauhoittuvan. Silti kalasteluhuijarit ovat edelleen hyvin kiinnostuneita erityisesti pankkitunnuksista.
  - Suurin osa tekstiviestihuijauksista kalastelee pankkitunnuksia.
  - Poliisiaiheisia kiristyshuijauksia saadaan edelleen samaan tapaan kuin muuallakin Euroopassa.

TRAFICOM Liikenne- ja viestintävirasto Kyberturvallisuuskeskus

Q4/2022 - tilasto päivitetään kvartaaleittain

12.1.2023

Lähde: Traficomin Kyberturvallisuuskeskus, 12.1.2023, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20joulukuu%202022.pdf

Milloin on syytä epäillä haittaohjelmaa?

- Laite hidastuu ilman selvää syytä.
- Laitteelle ilmestyy yllättäen uusia ohjelmia.
- Laite alkaa näyttää mainoksia, nettiselaimen aloitussivu vaihtuu tai muuta yllättävää.
- Tuttavasi saavat sinulta huijausviestejä.
- Verkkoyhteys siirtää dataa, vaikka et käytä nettiä ja päivityksiä ei ole latautumassa.
  - Windows 10: Asetukset → Verkko & internet → Datan käyttö
  - Applen tietokoneissa: Ohjelmat → Lisäohjelmat → Järjestelmän valvonta ja
  - Iphone ja iPad: Asetukset → Mobiiliverkko
  - Muut kännykät: Asetukset → Datan käyttö

Lisätietoa: https://yle.fi/aihe/artikkeli/2019/06/02/digitreenit-kirotut-haittaohjelmat-kuinka-tunnistaa-onko-kone-saastunut

Mitä tehdä, jos epäilet haittaohjelmaa tai virusta?

1. Etukäteen: varmuuskopioi tärkeät tiedostot työnantajan ohjeen mukaan esim. ulkoiselle kovalevylle.
2. Kun tilanne on päällä: ota laite pois netistä.
3. Jos henkilötietoja on vaarantunut, ilmoita tietosuojavastaavalle.
4. Kysy apua ammattilaiselta/tekniseltä tuelta.
5. Aja virustorjuntaohjelman tarkistus
6. Tarkista selaimen aloitussivu ja asennetut laajennukset (plugins) sekä viimeksi asennetut ohjelmat ja poista epämääräiset.
7. Tarvittaessa palauta laite aiempaan palautuspisteeseen tai asenna käyttöjärjestelmä / alusta laite uudestaan.

Kiitos!

Kysymyksiä tai kommentteja?

Yhteystiedot

Harto Pönkä
0400500315
@hponka
harto.ponka@innowise.fi
https://www.innowise.fi/