Yksinyrittäjän ja mikroyrityksen

KYBER- JA TIETOTURVA OPAS

Kyberturvan abc yrittäjille -hanke

Euroopan unioni
Euroopan sosiaalirahasto

Vipuvoimaa EU:lta 2014–2020

Elinkeino-, liikenne- ja ympäristökeskus

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tiivistelmä

Tietoturva: Keinot, joilla ylläpidetään (digitaalisen) tiedon saatavuus, luottamuksellisuus ja muuttumattomuus (eli eheys).

Kyberturva: Turvallisuuden osa alue, jolla pyritään turvaamaan tietotekniset laitteet sekä yhteydet laitteista ulos ja sisäänpäin.

Kyberturvan ABC yrittäjille -hankkeessa opastetaan kymenlaaksolaisia yksin- ja mikroyrittäjiä käytännönläheisesti parantamaan tieto- ja kyberturvallisuuttaan.

Tässä oppaassa käsitellään kyber- ja tietoturvallisuutta perusteita yksinyrittäjän ja mikroyrityksen näkökulmasta. Aikaisempi kyberturvallisuusosaaminen ei ole lukijalle tarpeen.

Opas antaa yrittäjille selkeitä ohjeita ja omaan liiketoimintaan sovellettavissa olevia tapoja parantaa kyberturvallisuutta. Kun jokainen meistä huolehtii omasta ja yrityksensä kyberturvasta, parantaa se myös asiakkaiden turvallisuutta ja koko alueemme kybervalmiuksia.

Oppaan avulla haluamme tehdä yrittäjät tietoisiksi kyberriskeistä ja siihen liittyvistä sudenkuopista. Opas pitää sisällään myös useita käytännön harjoitteita, jotka tekemällä on mahdollista parantaa verkkoturvallisuuttaan heti. Esimerkkeinä voidaan mainita sosiaalisen median tilit, fyysiset laitteet (mobiililaitteet ja tietokoneet) sekä vinkit siitä,

kuinka käyttää sähköpostia turvallisemmin ja pitää huolta varmuuskopioinnista.

Oppaassa vertaillaan yrittäjän tietoturvaa parantavia ohjelmistoja virustorjuntaohjelmista kaksivaiheiseen tunnistautumiseen, pilvipalveluihin ja salasanahallintaohjelmiin. Olemme valinneet kustakin luokasta muutaman ohjelman, joista on tehty selkeä vertailtu listaten hyvät ja huonot puolet, hinta sekä käytännön huomioita. Oppaasta löytyy myös valmiit pohjat palautussuunnitelman tekemiseen sekä oikeanlaisen pilvipalvelun valintaan.

Hanketta rahoittaa Hämeen ELY-keskus Euroopan sosiaalirahastosta (ESR).

Hanketiimi

Markus Hölsä, kyber- ja tietoturvan asiantuntija

Janine Klauenbösch, kyber- ja tietoturvan asiantuntija (sote- ja hyvinvointiala)

1 Sisällysluettelo

Johdanto

Yhä useampi yrittäjä on siirtänyt toimiaan verkkomaailmaan helpottaakseen työtään ja tehostaakseen yrityksensä toimintaa. Ikävä kyllä nämä digitaaliset työkalut ja prosessit ovat luoneet uusia vaaroja, joita täytyy oppia välttämään. Vaikka kyberturva sanana voi vaikuttaa pelottavalta tai haasteelliselta, on sen parantamiseen liittyvä perustoimet loppujen lopuksi varsin helppoja ja selkeitä.

Miksi sitten parantaa yrityksen kyberturvaa? Vastaus kuuluu, että rikolliset metsästävät väsymättä kohteita verkon välityksellä tehdäkseen rahaa. Rikollisten kohteisiin kuuluvat tavalliset ihmiset, pienet yritykset ja organisaatiot, joiden hakkerointi on nopeaa ja helppoa.

Tämän oppaan avulla luot yrityksellesi ja itsellesi vahvan kybertuvan perustan, joka vaikeuttaa pahantekijöiden elämää. Rikolliset ja satunnaiset hakkerit eivät käytä aikaansa vaikeisiin kohteisiin, joten jo pelkästään tämän oppaan neuvojen soveltaminen käytäntöön tekee sinusta ja yrityksestäsi ajallisesti liian vaikean kohteen monelle toimijalle.

2 Kyberturvan ABC – sanasto

Tietokonemaailman mittayksiköt ymmärrettävästi selitettynä

Bitti: 1 tavu = 8 bittiä = yksi kirjain, esimerkiksi ”a” (älä stressaannu näistä määritelmistä, emme tule keskittymään näihin opetuksessa.)

kbit - Kilobitti: 2–3 kappaletta tekstiä

Mbit – Megabitti: on 873 sivuinen kirja tai noin 1/3 valokuvasta

Gbit - Gigabitti: on noin 1 tuntia Netflixissä tai noin 341 kuvaa

Tbit - Terabitti: on noin 100 tuntia elokuvaa/sarjaa Netflixissä tai 349,525 kuvaa

Tietoturva: Pyritään ylläpitämään tiedon saatavuutta, luottamuksellisuutta ja eheyttä. Nämä tiedot ilmentyvät digitaalisina tallenteina, fyysisinä tallenteina sekä ihmisten, kuten työntekijöiden, tietämyksenä. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana.

Kyberturva: On turvallisuuden osa alue, jolla pyritään turvaamaan sähköiset laitteet sekä yhteydet laitteista ulos ja sisäänpäin. Näillä keinoilla pyritään edistämään laitteiden jatkuvuutta, jotta kaikki toimisi suunnitellusti ja laitteet pysyisivät toiminnassa häiriöistä riippumatta.

Hakkeri: Voidaan jakaa 10 eri kategoriaan, josta tärkeimmät ovat musta-, valko- ja harmaahattu hakkerit, sekä haktivisti.

Mustahattu hakkeri: henkilö, joka käyttää omia tietoteknisiä taitojaan verkkorikollisuuden tekemiseen esimerkiksi: kiristys, verkkoihin murtautuminen ja tietojen myynti.

Valkohattu hakkerit: käyttävät omia tietoteknisiä taitojaan estääkseen verkkorikollisuutta. He pyrkivät etsimään haavoittuvaisuuksia järjestelmistä ja ilmoittamaan niistä eteenpäin, jotta haavoittuvaisuudet korjattaisiin.

Harmaahattu hakkeri: putoaa valkohattu ja mustahattu hakkereiden väliin. Koska harmaahattuhakkeri ei käytä taitojaan henkilökohtaisen hyödyn saamiseksi, häntä ei voida kutsua mustahattuhakkeriksi. Lisäksi, koska hänellä ei ole laillista valtuutusta hakkeroida organisaation tai yrityksen järjestelmiä, häntä ei myöskään voida pitää valkohattuna. Heti kun hakkerit käyttävät hakkerointitaitojaan henkilökohtaisen hyödyn saamiseksi, heistä tulee mustahattu-hakkereita.

Haktivisti: Hakkeri tai hakkeriryhmä, jotka usein hakkeroivat hallituksia ja organisaatioita saadakseen huomiota tai jakaakseen tyytymättömyytensä ajatuksensa vastustamisesta.

Pilvipalvelut: Pilvipalvelut ovat niin sanotusti ”pilvessä” tarjottuja palveluita, nämä ovat joko maksullisia tai määräaikaisesti ilmaisia. Alla olevat termit kuvaavat eri pilven palveluita.

SaaS (Software as a Service): tarkoittaa ohjelmiston jakelua internetin kautta palveluna. SaaS-palveluita käytetään yleensä web-selaimen kautta, esim. Microsoft Office 365 tai Google Docs.

PaaS (Platform as a service): tarkoittaa, että vuokraat tilaa palvelimessa, verkkotallennustilassa, käyttöjärjestelmässä ja tietokannan hallinta- / kehitystyökaluissa. Se ei sisällä applikaatiota kuin Word, Excel, Outlook, jne.

IaaS (Infrastructure as a Service): tarkoittaa, että vuokraat vain tilaa palvelimessa ja verkkotallennustilassa.

A

Applikaatio (äppit): sovellusohjelmaa (esim. Skype, WhatsApp, Instagram, YouTube), se vaatii avaamisen ja käynnistämisen.

B

Bug bounty (Haavoittuvuuspalkkio): Yritykset usein maksavat palkkioita henkilöille, jotka löytävät yrityksen järjestelmistä haavoittuvaisuuksia ja ilmoittavat niistä.

D

Datakeskus: Laitos, jota käytetään tietokonejärjestelmien ja niihin liittyvien komponenttien, kuten tietoliikenne- ja tallennusjärjestelmien, sijoittamiseen.

F

Fyysinen turvallisuus: Myös paikkojen turvallisuus on osa kyberturvaa, tämä voidaan varmistaa lukoilla ja käytännöillä, jotka estävät henkilöiden pääsyn laitteille tai asiakirjoihin.

Fyysinen laitteiden turvallisuus: Verkon päässä olevat tietotekniset laitteet (tietokoneet, tulostimet, puhelimet) ja niiden turvallisuus fyysisiä hyökkäyksiä vastaan. Puhelimen SIM-kortin oletus PIN-koodin (esim. 0000 tai 1234) vaihto on hyvä esimerkki fyysisen laiteturvallisuuden parantamisesta.

H

Haavoittuvuus: Mikä tahansa omaisuuden tai suojauksen heikkous, joka mahdollistaa vahingon aiheuttamisen uhan.

Haittaohjelma: Yleisnimitys haitallisille tietokoneohjelmille, jotka tavalla tai toisella aiheuttavat haittaa henkilölle tai laitteistolle. Kutsutaan usein viruksiksi, mutta haittaohjelmia voi olla myös muunlaisia.

Hybridivaikuttaminen: Valtiollinen toimija pyrkii eri keinoja hyväksi käyttäen, vaikuttamaan kohdemaahan. Hybridivaikuttamisen tavoitteena on hyväksikäyttää kohdevaltion haavoittuvuuksia ja vaikuttaa siten että se ei ole päältäpäin näkyvää. Keinoja on useita aina poliittisesta vaikuttamisesta tekniseen häirintään.

K

Kaistaleveys: Tarkoittaa verkon niin sanottua kantokykyä. Yksinkertaisesti selitettynä siis verkon tai verkkolaitteen kykyä tuoda tai lähettää internet sisältöä. Kaistanleveyden vähyys voi aiheuttaa internet selailun hidastumisen tai videoiden pätkimistä.

Kyberhygienia: Tarkoittaa hyviä kyberturvallisuuteen liittyviä toimintatapoja, jotka parantavat kyberturvaa. Näitä tapoja voi olla esimerkiksi uniikkien salasanojen käyttö eri palveluissa tai se, että lukitsee tietokoneensa siltä poistuessaan.

Käyttöjärjestelmä: Tietokoneiden ja puhelimien hallintajärjestelmä, joka mahdollistaa laitteiden käytön. Esimerkkejä: Windows, Linux, Android, Apple iOS.

Kryptovaluutta: Digitaalista valuttaa, jolla on arvoa oikeassa rahassa. Rikolliset usein suosivat kyseistä valuuttaa sen tuoman yksityisyyden takia. Esimerkkejä ovat Bitcoin ja Etherium.

M

Modeemi: Se kotisi nurkassa valoja vilkuttava laatikko, joka taikoo internetin yhteydet eli verkon kotiisi tai yritykseesi. Modeemin liikenne ei ole salattua. Vanhentunutta teknologiaa, jota kuitenkin käytetään usein markkinointikielessä. Suurella todennäköisyydellä, modeemista puhuttaessa tarkoitetaan reititintä.

Meta-tiedot: Tietoja, joita ei näe päältäpäin tiedostoista tai kuvista. Esimerkiksi kuva usein sisältää erilaisia paikkatietoja, milloin kuva on otettu ja millä laitteella. Näihin on helppo päästä käsiksi ja useat eivät edes ole tiedä, että nämä tiedot on sisällytetty kuviin ja tiedostoihin.

O

Ohjelmisto: Ryhmä ohjelmista, jotka käskevät tietokoneen suorittamaan tehtävän. Ohjelmisto on laitteiston vastakohta. Mikään laitteisto ei toimi yksin vaan tarvitsee toimiakseen ohjelmiston. Näin ollen ei myöskään ohjelmistosta ole mitään hyötyä ilman laitteistoa.

Ohjelmointikoodi: Tietokonelaitteiden ymmärtämä ohjelmointikieli, jotka ovat periaatteessa käskyjä laitteille. Nämä käskyt saavat laitteet toimimaan niille tarkoitetulla tavalla. Ohjelmointikieliä on monenlaisia, mutta sinun ei tarvitse välittää niistä.

P

Palomuuri: Laite tai sovellus, jonka tarkoituksena on suodattaa liikennettä ulkoverkosta sisäverkkoon ja pyrkiä estämään haitallinen liikenne.

Pilvipalvelu: Tarkoittaa palvelua, joka tarjoaa tietoteknisiäpalveluita verkon välityksellä. Microsoft Office 365 tai Google Drive on esimerkki tämänkaltaisesta palvelusta.

Ponnahdusikkuna: Usein netissä surffatessa esiin ponnahtava, yllättävä ja huomion vievä ikkuna, esim. ‘Olet sivun miljoonas kävijä, klikkaa painiketta voittaaksesi palkinto tai ‘Osallistu ilmaisen iPhonen arvontaan’. Useimmiten visusti varottavia ja vaarallisia.

Pääkäyttäjä: Voidaan tarkoittaa kahta asiaa. Puhekielessä tarkoitetaan usein laitteen sen hetkistä käyttäjää. Teknisessä kielessä pääkäyttäjä tarkoittaa laitteelle tai järjestelmään kirjautunutta käyttäjää, jolla on täydet oikeudet toimia laitteella. Hän pystyy antamaan muille käyttäjille eri tasoisia käyttäjäoikeuksia.

Q

QR-koodi: Eli ruutukoodi on kuvakoodi, jonka voi lukea esimerkiksi puhelimen kameralla.

R

Reititin: Laite, joka myös taikoo verkon kotiin tai yritykseen, mutta erona reitittimen ja modeemin välillä on reitittimen kyky salata liikennettä ja sen sisään rakennettu palomuuri. Suosi tätä ostaessa.

Roskaposti: ei-toivotut, yleensä kaupalliset viestit (kuten sähköpostit, tekstiviestit, tai internet-ilmoitukset), jotka on lähetetty suurelle määrälle vastaanottajia tai julkaistu suuressa määrässä paikkoja.

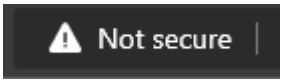
S

Salaus: Tarkoittaa sähköisten dokumenttien tai verkkoliikenteen muuttamista sellaiseen muotoon, joka estää ulkopuolisten toimijoiden yritykset nähdä dokumenttien tai liikenteen sisältö. Käytetään luottamuksellisen tiedon lähettämiseen (asiakkaan henkilötiedot, liikesalaisuudet).

Sisäinen laitteiden turvallisuus: Suojataan tietoteknisetlaitteet verkon kautta tulevilta hyökkäyksiltä. Suojauskeinoja voi olla esimerkiksi virustorjunnan asentaminen tai vahvat salasanat.

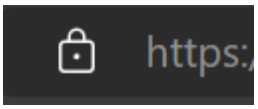
Sosiaalinen manipulointi: Keino saada ihminen tekemään asioita, jotka eivät ole hänen etunsa mukaisia. Kuuluisin näistä ehkä on ns. toimitusjohtajahuijaus. Siinä kohde saa sähköpostin, joka näyttää tulevan toimitusjohtajalta ja siinä vaaditaan kiireellisesti siirtämään rahaa liikekumppanille. Rahat katoavat yleensä iäksi.

Salaamaton web liikenne: Nettisivut tarvitsevat väylän, joka mahdollistaa tiedon välittämisen nettisivulta. Ilman lukon kuvaa tämä on salaamatonta liikennettä, eikä silloin tulisi ikinä syöttää kyseiselle sivulle omia sensitiivisiä



henkilötietoja. Sivu on itsessään aivan normaali eikä lukon puuttuminen suurenna riskiä saada haittaohjelma.

Salattu web liikenne: Helposti tunnistettavissa sivun yläkulmassa olevasta lukon kuvasta.



T

Tietomurto: Yritys tai organisaatio joutuu kyberhyökkäyksen kohteeksi, jonka seurauksena hyökkääjä saa haltuunsa arvokkaita henkilö-, yhteystietoja tai liikesalaisuuksia. Näitä tietoja myydään usein eteenpäin muille rikollisille. Myös valtiolliset toimijat voivat hyödyntää tällaisia rikollisten vapaasti myymiä tietokantoja.

Tietojen kalastelu: Tarkoittaa keinoja, joilla pyritään keräämään kohteesta arkaluontoista tai yleistä tietoa. Tehdään usein sähköpostitse mutta lähestyä voidaan myös some-tilien kautta.

Tietovuoto: Luottamuksellisten, arkaluonteisten tai suojattujen tietojen jakaminen luvattomalle henkilölle. Tietomurron kohteena olevia tiedostoja tarkastellaan ja / tai jaetaan ilman lupaa.

Tietoväline: Fyysinen laite niin kuin Atk-magneettinauha, levyke, CD-levy, lomake tai muuta väline, jolla säilytetään tietoa.

U

URL (Uniform **R**esource **L**ocator**)**: tietyn (ainutlaatuisen) resurssin osoite verkossa. Helpommin selitettynä tarkoittaa nettisivun osoitetta, jonka kirjoittamalla tai kopioimalla pääsee käymään kyseisellä nettisivulla. Esimerkki tästä on *https://www.xamk.fi/tutkimus-ja-kehitys/kyberturvallisuuden-abc-yrittajille/*

V

Verkko: Tarkoittaa ympäristöä, jossa tieto liikkuu. Verkot jaetaan ulko- ja sisäverkkoon. Sisäverkko on tarkoittaa yrityksen/organisaation tai kodin sisällä tapahtuvia yhteyksiä, esimerkiksi tietokoneen ja tulostimen välinen yhteys tai modeemin ja äly TV:n välinen yhteys. Ulkoiset verkkoyhteydet ovat kaikki muut yhteydet sisäverkon ulkopuolella.

Valtiollinen toimija: Usein valtion sisäinen organisaatio (esim. tiedusteluun perustuva), joka saa rahallista ja laite tukea valtion eri organisaatioilta. Näiden toimijoiden tehtävä on toteuttaa valtion mielenkiinnon mukaisia toimia, joilla pyritään aiheuttamaan haittaa muita valtioita kohtaan. Toimijat harjoittavat vakoilua, sabotaasia ja häirintää.

W

Wi-Fi: Wi-Fi on radiosignaali, joka lähetetään langattomasta reitittimestä lähellä olevaan laitteeseen, joka muuntaa signaalin näkyväksi ja käytettäväksi dataksi. Laite lähettää radiosignaalin takaisin reitittimeen, joka muodostaa yhteyden internetiin johtoa tai kaapelia pitkin.

3 Internet ja sen kyberuhat

Moni meistä ajattelee, että eri laitteet ovat omia yksiköitään, jotka toimivat itsenäisesti verkossa. Tämä ajatus on vaarallinen, sillä käytännössä aina, kun laitteet yhdistyvät verkkoon, ne kommunikoivat keskenään sen verkon sisällä, jossa ne ovat. Jos yhteen laitteeseen, kuten tietokoneeseen, tulee haittaohjelma, voi haittaohjelmat levitä tässä verkossa kaikkiin siinä oleviin laitteisiin.

Jos kotiverkossasi on siis tabletti, oma ja puolison tietokone, pari puhelinta, pelikone, äly-tv, pelikonsoli, robotti-imuri ja lemmikkivahtina käytettävä kamera, riittää kaikkien saastumiseen se, että yksi näistä laitteista on saanut itseensä haittaohjelman. Kun tällainen laite sitten viedään työpaikan verkkoon, voi se saastuttaa myös työpaikan verkon.

Tämä on tärkeä muistaa myös siksi, että verkossa käy myös usein vierailijoita. Olet varmasti itse kysynyt monessa paikkaa ‘mikä teidän wifin salasana on’ tai sitä on saatettu kysyä sinulta, kun vaikka sukulaiset ovat tulleet vierailulle. Myös lapset käyttävät usein toistensa wifi-yhteyksiä vierailujen aikana. Nämä tilanteet luovat riskin haittaohjelman leviämiselle sisäisessä verkossa.

Riskitöntä ei myöskään ole se, että monet meistä antavat lastensa pelata tai asentaa tuntemattomia ohjelmia (tai tekevät sen itse) jopa työkoneelle tai työpuhelimeen. Kun saastuneen ohjelman sisällä oleva haittaohjelma leviää työpaikan muihin laitteisiin, on soppa jälleen valmis.

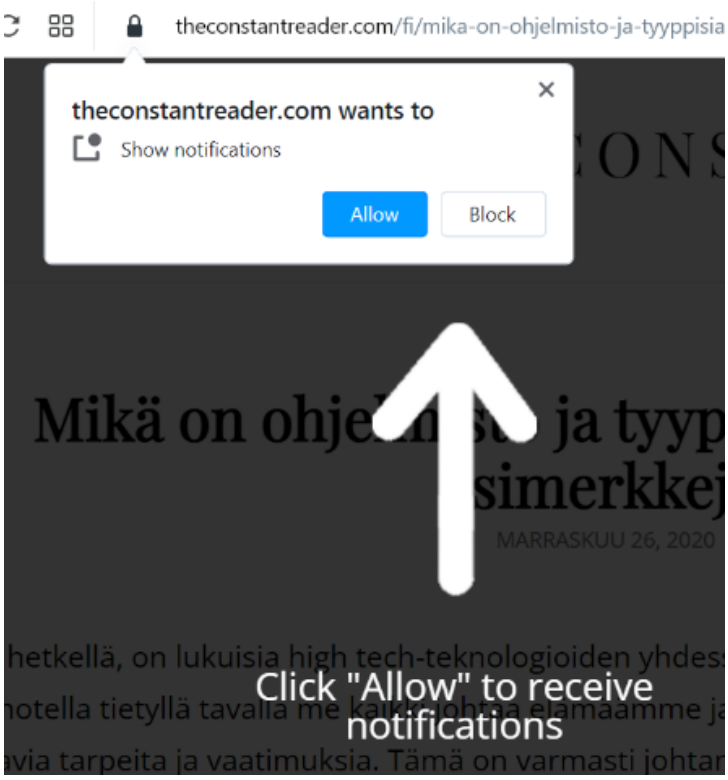
Helpoin tapa välttää tämä on käyttää työkonetta esimerkiksi vain työkännykän verkon kautta (ei lainkaan oman wifin kautta, mikäli mahdollisuutta kahteen erilliseen internet-liittymään ei ole) ja hankkia kotikäyttöön, vaikka käytetty tietokone, jossa on kuitenkin ajantasainen virustorjunta.

3.1 Mikä on haittaohjelma?

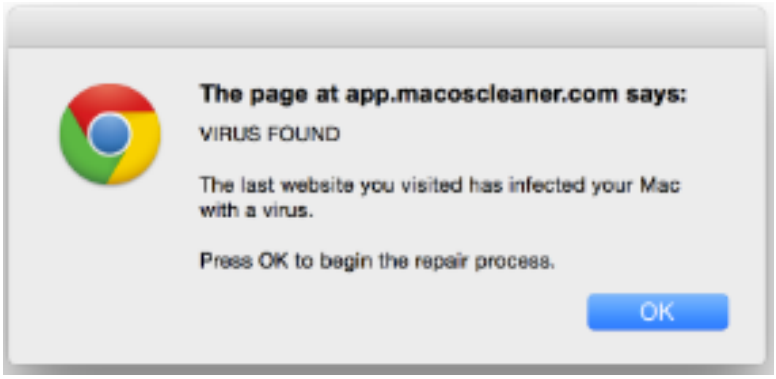
Virus

- Virus on haittaohjelma, joka syöttää laitteeseen haitallista ohjelmointikoodia. Tämä haitallinen koodi saa laitteen usein toimimaan sille epätyypillisellä tavalla.
    - Epätyypillisiä tapoja voi olla esimerkiksi laitteen käyttöjärjestelmän hidastuminen/jäätyminen, tuntemattomien ohjelmien ilmestyminen, verkkotoiminnan (datan) lisääntyminen.
    - Myös tietokoneen sovellusten avaamisen ja käytön äkillinen hidastuminen voi olla hälyttävä merkki haittaohjelmasta, joka käyttää tietokoneen tehoja omiin tarkoituksiinsa kuten esimerkiksi kryptovaluutan louhimiseen.
- Viruksen voi saada haitallisista nettisivuista, linkeistä tai ulkoisista tallennusasemista kuten esimerkiksi USB-tikuista.

- Viruksille on kuitenkin tyypillistä se, että ne tarvitsevat pääkäyttäjältä jonkin toimen asentuakseen laitteelle.
    - Esimerkkejä tällaisista toimista ovat erilaiset ponnahdusikkunat, jotka saattavat pitää sisällään pyynnön painaa painiketta.
    - Jos päädyt sivulle, joka näyttää paljon ponnahdusikkunoita, älä sulje niitä painamalla ruksin kuvaa yläkulmassa. Usein haitalliset ponnahdusikkunat toimivat siten, että niihin lisätään päälle näkymätön ikkuna, jota painamalla antaakin luvan johonkin toimintoon (esim. tiedoston lataamiseen.) On turvallisempaa painaa Windows laitteella **ALT + F4** näppäinyhdistelmää. Tämä sulkee koko selaimen, jotta pääsee sivulta turvallisesti pois.

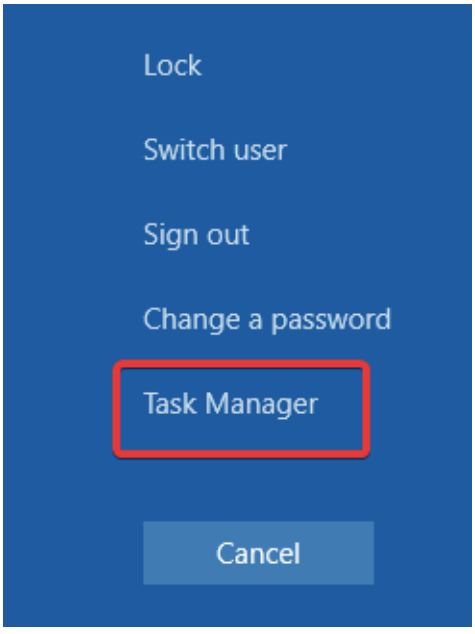


Sivusto pyytää lupaa ponnahdusikkunoille

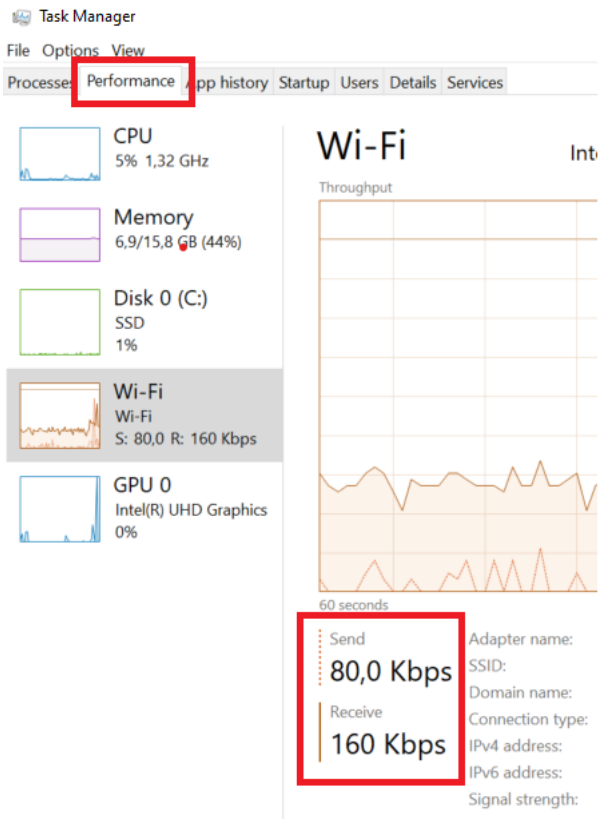


Kuvassa esimerkki vaarallisesta ponnahdusikkunasta. Se esittää olevansa Googlen ilmoitus, joka auttaa poistamaan koneella olevan viruksen. Tosiasiassa siitä painamalla tulee kuitenkin asentaneeksi viruksen omalle koneelleen ihan itse.

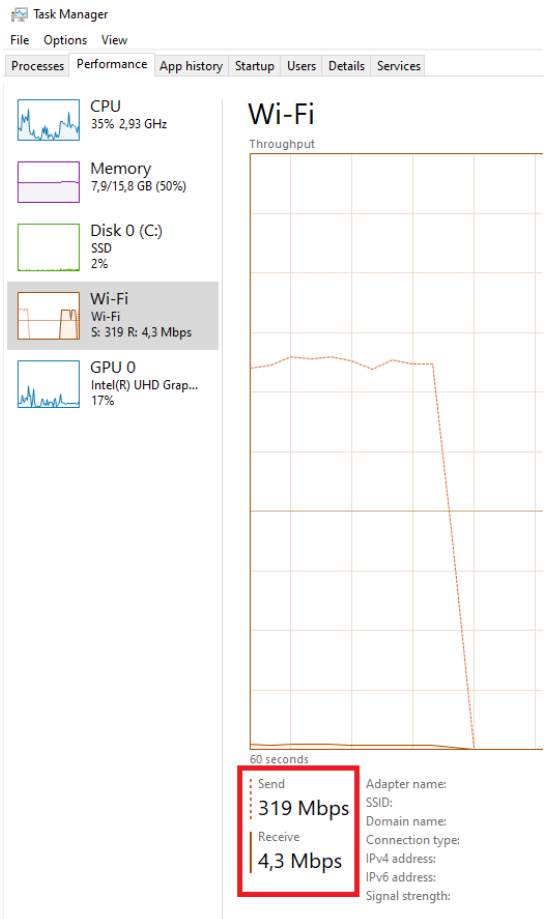
Alla ohjeet kuinka voit helposti tarkistaa verkkotoiminnan lisääntymisen tietokoneella:



1. Painamalla **Ctrl+Alt+Delete** samanaikaisesti saat auki asetusvalikon. Painamalla **Tehtävänhallinta/Task Manager** pääset hallinta ikkunan etusivulle.



2. Valitsemalla vasemmasta yläkulmasta kohdan **Suorituskyky/Performance** pääset tarkastelemaan tietokoneen eri prosesseja ja niiden tehonkulutusta. Tässä tarkastelemme **Wi-Fi** kohtaa, joka pitää sisällään verkkoliikenteen. Kuvassa näkyy miten paljon verkkoliikennettä verkko lähettää ja vastaanottaa.



3. Kuvista voi verratta liikenteen määrää. Älä huoli, jos numerot ja lyhenteet vaikuttavat vaikeasti ymmärrettäviltä, tärkeää on kiinnittää huomiota liikenteen laajuuteen.

Haittaohjelmat lähettävät dataa usein ulospäin, jonka takia **Lähetä/Send** kohta usein nousee tiedonsiirto määrässä.

Kuinka paljon data käyttää elokuvien katseleminen ja musiikkien kuunteleminen netissä:

Youtube: noin 560 Mb per tunti

Netflix: noin 3 Gb per tunti

Amazon Prime Video: noin 2 Gb per tunti

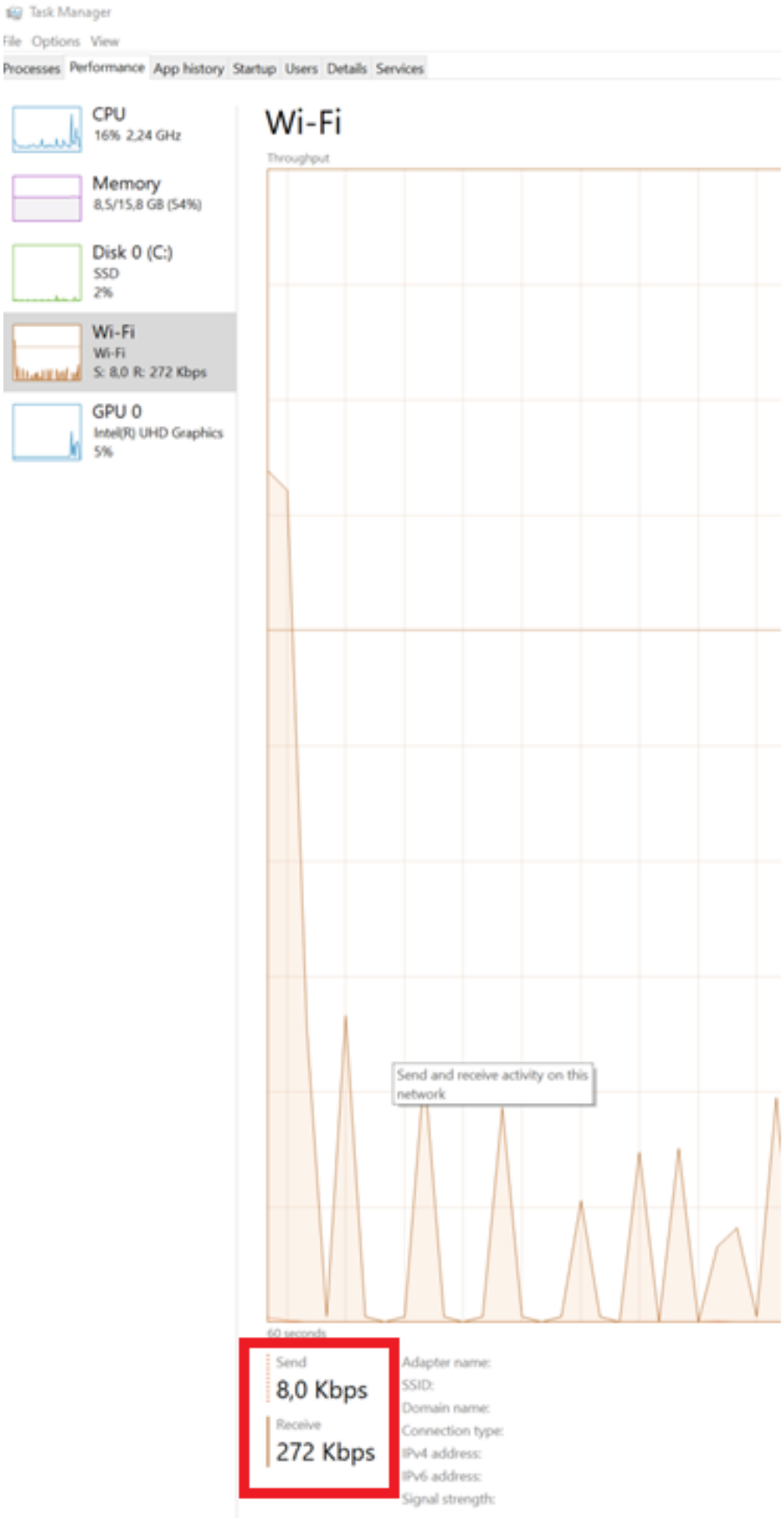
Hulu: noin 2.7 Gb per tunti

Spotify: 1.5 GB per tunti (video), 70 Mb per tunti (musiikki)

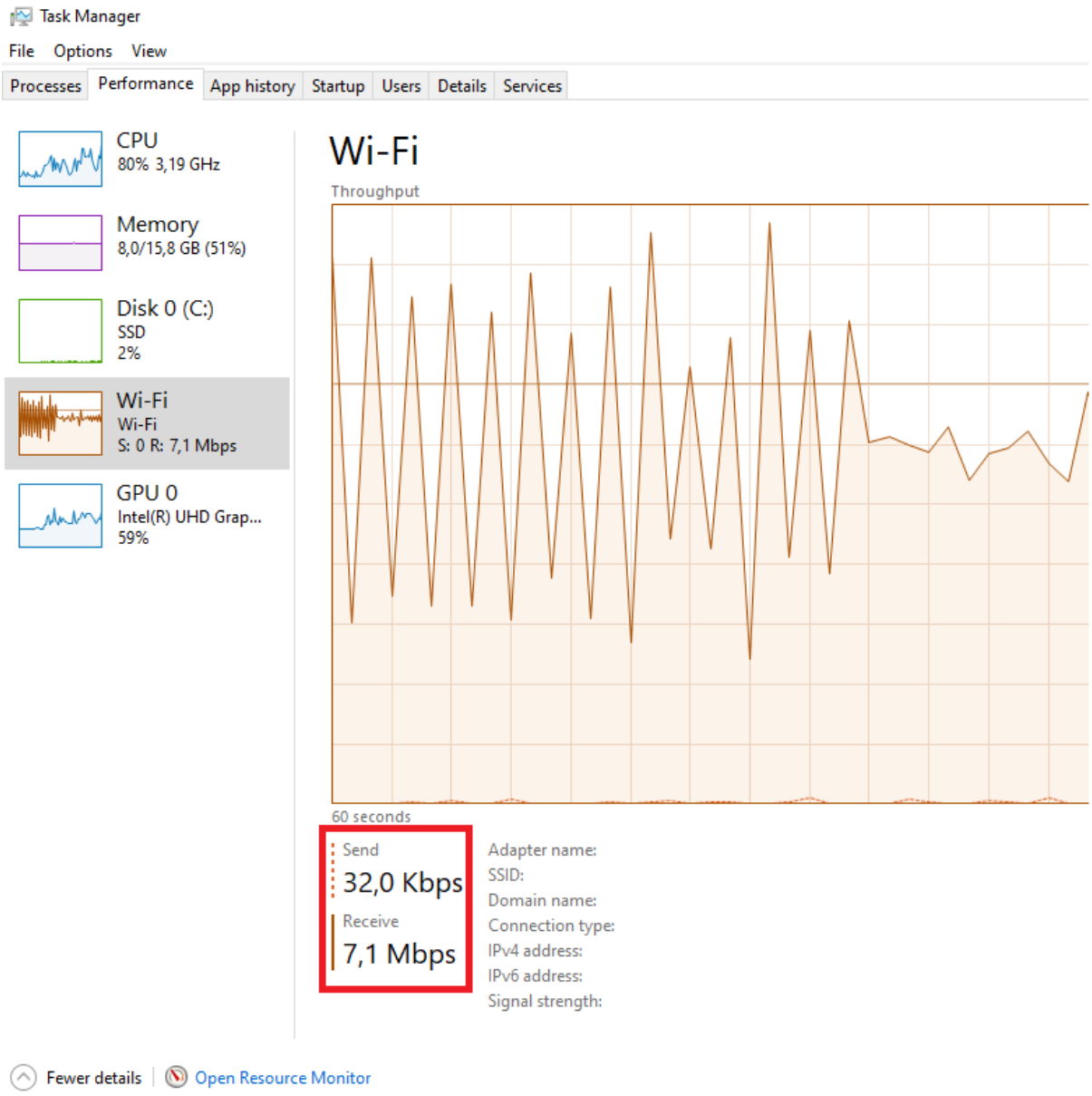
Instagram: 0.5 Gb per tunti

Facebook: Normaali fiidin selailu vie keskimäärin 80-150 Mb tunnissa

Sarjan striimaus Amazonissa näyttää vuoristoradalta:



Keskimääräinen live videon katseluun käytetty kaista:



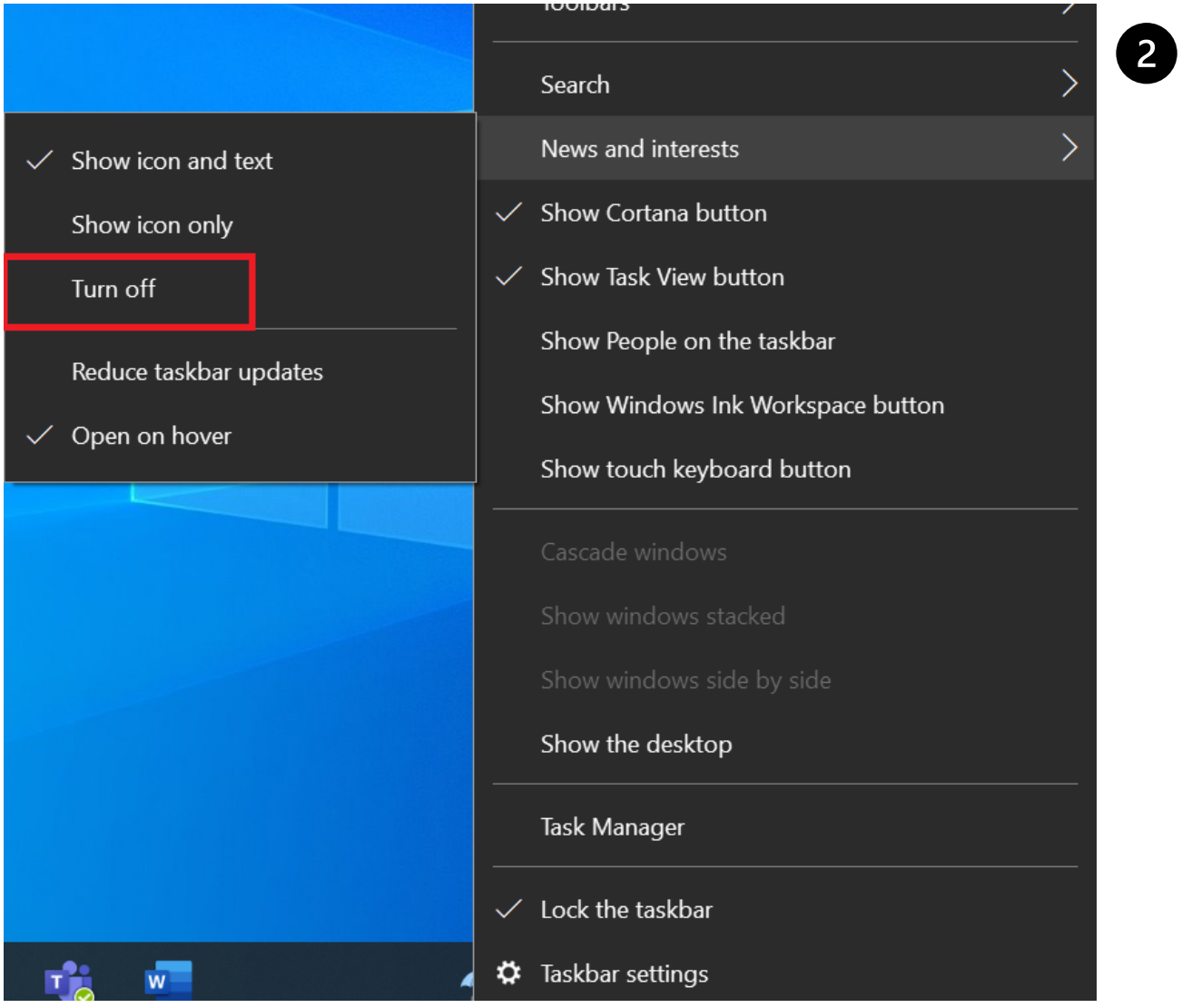
Tältä sivulta voit laskea kuinka paljon kaistaleveyttä tarvitset kotonasi / yrityksessäsi:

https://www.btel.com/bandwidth-calculator/

Windows käyttöjärjestelmässä on tällä hetkellä haavoittuvaisuus, joka mahdollistaa haitallisen ohjelmointikoodin suorittamisen mainoksien kautta. Olet varmaan huomannut alla olevan kohdan Windows

tietokoneessasi, joka avaa uutisia ja mainoksia, kun hiiren kursori osuu siihen. Kun nämä mainokset tai uutiset ovat latautumassa. On mahdollisuus, että siihen yhteyteen on liitetty ohjelmointikoodi, joka toimii haittaohjelman tavoin. Tämän takia kyseinen toiminto kannattaa ottaa pois käytöstä.

1. Vie kursori palkin päälle ja paina hiiren oikean puolista näppäintä.



2. Sinulle avautuu valintavalikko, josta etsi kohta **News and interests/Uutiset ja kiinnostuksen kohteet** ja sitten **Turn off/Poista käytöstä**

Kiristysohjelma

- Kiristyshaittaohjelma on haittaohjelma, joka lukitsee tietokoneessa olevat tiedot siten että niihin ei pääse käsiksi. Näiden tiedostojen avaamiseen täytyy käyttäjän maksaa lunnasvaatimus.
    - Lunnasvaatimus täytyy usein maksaa Bitcoineilla, joka on kryptovaluutta. Rikolliset suosivat Bitcoinin kaltaista kryptovaluuttaa, koska valuutan liikettä on todella vaikea jäljittää.
    - Viestissä saattaa myös olla mukana hupeneva aikalaskenta. Useissa kiristyshaittaohjelmissa pelotellaan tiedostojen tuhoamisella, kun aika loppuu, mutta tämä saattaa usein myös olla vain pelottelutaktiikka.
- Kiristyshaittaohjelmat ovat usein liitettyinä sähköposteihin ja niissä esiintyviin haitallisiin linkkeihin ja tiedostoihin. Ole siis hyvin, hyvin varovainen siinä, millaisia sähköpostin linkkejä klikkaat! Kun kiristysohjelma on koneessa, on käytännössä mahdotonta päästä siitä eroon.

Mato

- Mato on tuhoisa haittaohjelma, jolla on kyky monistaa itseään. Tämän takia madot leviävät usein todella nopeasti verkossa.
    - Madot ovat erityisen tuhoisia silloin, jos ne levittävät kiristyshaittaohjelmaa. Näiden kahden yhdistelmän ansiosta kiristyshaittaohjelma voi salata kokonaisen yrityksen kaikki tietokoneet ja mobiililaitteet.
- Madot leviävät usein sähköpostin välityksellä, mutta myös haitallisten nettisivujen kautta.

Vakoiluohjelma

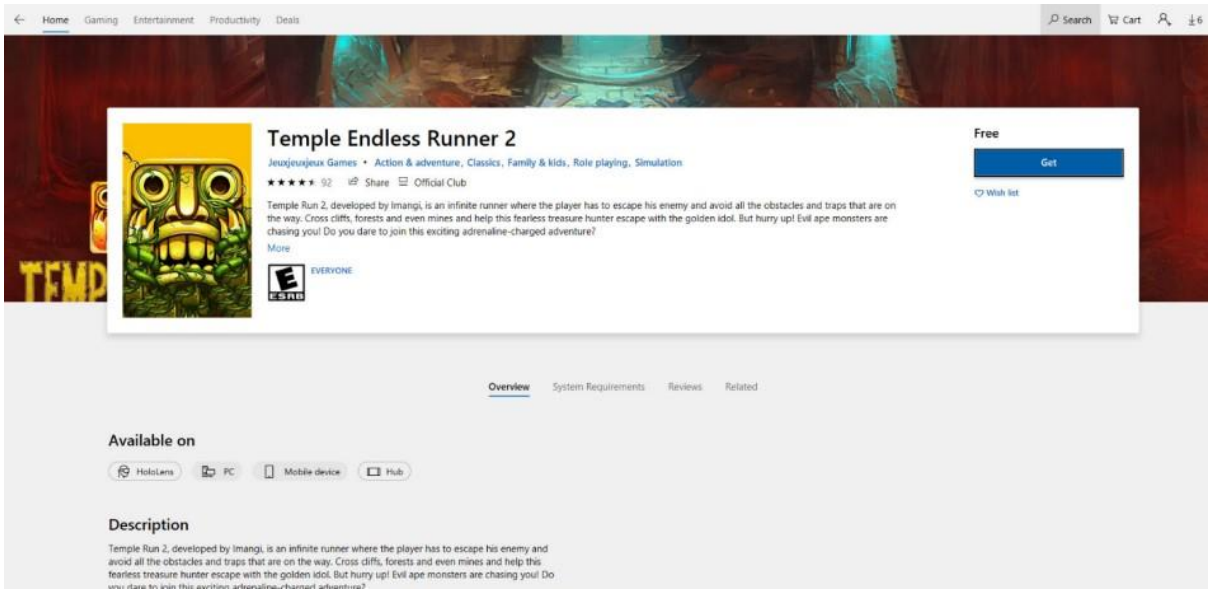
- Vakoiluohjelmat ovat usein vaikeasti havaittavia haittaohjelmia, jotka pyrkivät pysymään piilossa ja keräämään tietoja kohdelaitteesta.
    - Tietoihin kuuluu esimerkiksi webkameran kautta saadut kuvat, näppäinten painallukset (mikä mahdollistaa esimerkiksi salasanojen selvittämisen), ruutukaappaukset tietokoneen työpöydästä ja yleisiä tietoja laitteesta ja sen verkko ympäristöstä.
- Tiedot lähetetään uhkatekijälle, joka käyttää saatuja tietoja omiin hyökkäyksiinsä.

Troijalainen

- Troijalainen on haittaohjelma, joka pyrkii naamioimaan itsenä oikeaksi ohjelmaksi.
    - Usein troijalaiset suorittavat niiden lupaavan tehtävän, mutta tekevät sivussa haitallisia toimia kuten esimerkiksi keräävät tietoja siitä mitä laitteella tehdään tai käyttää laitteen resursseja kryptovaluutan louhimiseen.
- Troijalaiset leviävät ladatun ohjelman mukana, jonka takia ne voi saada vain silloin kun lataa tuntemattomia ohjelmia laitteelle.

Seuraavaa kaksi kuvaa on esimerkki troijalaisesta applikaatioista:

Yllä on kuva troijalaisesta, mikä naamioituu virustorjuntaohjelmaksi sekä pystyy myös estämään koronavirukseen sairastumisen.



Kaikki ”Laced games” peliyhtiön pelit toimivat odotettusi, kun taas haitalliset toiminnot paljastuivat taustalla. Tämä johti positiivisiin käyttäjäarvosteluihin Microsoft Storessa. Esim. Temple Endless Runner 2:lla, oli lähes täydellinen viiden tähden luokitus 92 arvostelun perusteella.

Niin sanottu ”peliyritys” päivitti jatkuvasti pelejään ja käyttivät erilaisia pelinimikkeitä ja sovelluksia haittaohjelmien toimittamiseen uhreille.

Julkaisijat, jotka julkaisuttanut haitallisia pelisovelluksia seuraavilla nimillä:

- Lupy Games
- Crazy 4 Games
- Jeuxjeuxkeux Games
- Akshi Games
- Goo Games
- Bizzon Games

3.2 Haitalliset sähköpostit

Tietoteknisten laitteiden heikoin lenkki on usein ihminen itse. Sähköposti on rikollisten pääsääntöinen tapa murtaa yritysten sekä organisaatioiden suojamuurit ja päästä käsiksi sisäiseen verkkoon.

- Massa sähköpostit eli spam-viestit ovat varmasti monille tuttuja, näiden sisältö vaihtelee usein tyhjien lupausten ja äkkirikastumisen väliltä.
    - Monet spam-viestit sisältävät usein paljon haittaohjelmia, jotka voivat olla usein tuhoisia laitteille ja verkoille.

    - Spam-viestejä ei yksilöidä vaan niitä lähetetään miljoonittain eri sähköposteihin klikkausten toivossa.
    - Jopa 94 % kaikista maailman haittaohjelmista tulee sähköpostin kautta.
    - Tämän takia ei ole suositeltavaa klikata liitteitä tai linkkejä sähköpostissa, ellei ole 100 % varma siitä, että liite on asiallinen. Jos olet epävarma - soita tai ota yhteyttä lähettäjään suoraan erillisessä viestissä. Jotkut yritykset ovat jopa kieltäneet tästä syystä sähköpostitiedostojen lähettämisen kokonaan.
- Tietojen kalastelu ja sosiaalinen manipulointi (Phishing)
    - Sähköpostien kautta voidaan myös yrittää saada arkaluontoista tietoa henkilöstä tai yrityksestä tai saada lukija suostuteltua tekemään jokin toimi.
    - Usein uhkatekijät pyrkivät saamaan käsiinsä salasanoja ja käyttäjätunnuksia, jonka takia ei mitään tietoja tulisi koskaan antaa, vaikka niitä pyydetäänkin.

3.3 Haitalliset nettisivut

Haitalliset nettisivut voivat asentaa laitteille haittaohjelmia tai varastaa laite tai verkkotietoja. Monet haitalliset nettisivut on myös saatu näyttämään virallisilta yrityksen nettisivuilta kuten esimerkiksi erilaisilta nettipankkipalveluilta. Asiansa osaava rikollinen pystyy tekemään täydellisen kopion yrityksen verkkosivuista noin 5–10 minuutissa, joten on syytä olla tarkkaavainen. “Hoono soomi” näillä sivuilla käy yhä harvinaisemmaksi.

- Rikolliset ovat keksineet keinoja, joilla nettisivuille saa liikennettä.
    - Hakukoneen myrkytys on yleinen keino saada käyttäjä päätymään haitallisille nettisivuille. Hakukoneen myrkytyksessä hakukonetta manipuloidaan sillä tavalla, että se suosittelee käyttäjille haitallisia nettisivuja. Rikolliset siis maksavat noustakseen Googlen hakutuloksissa ylös.
    - Esimerkiksi kirjoittamalla hakukenttään nettipankin saa tulokseksi identtisen nettipankki nettisivun, joka kuitenkin varastaa sinne syötetyt tiedot.
    - Sähköpostin kautta saadut linkit voivat viedä myös haitallisille nettisivuille.
- Rikolliset ovat myös murtautuneet oikeille ja turvallisille nettisivuille, tehden näihin sivuihin muutoksia.

3.4 Miltä näyttää turvallinen nettisivun osoitetta?

Esimerkki:

https://www.xamk.fi/tutkimus-ja-kehitys/kyberturvallisuuden-abc-yrittajille/

https:// - s lopussa tarkoittaa salattua, yhteys on siis turvallinen

xamk. - internetsivun nimi

fi - ilmaisee, minkä tyyppiseen kokonaisuuteen verkkosivusto kuuluu, usein maa (Suomi – fi, Ruotsi – se, Norja – no)

/tutkimus-ja-kehitys/kyberabc/ - antaa vierailijoille tiedon siitä, millä verkkosivuston osassa tai sivulla he ovat

3.5 Kuinka tunnistan väärennetyt nettisivun osoitteet?

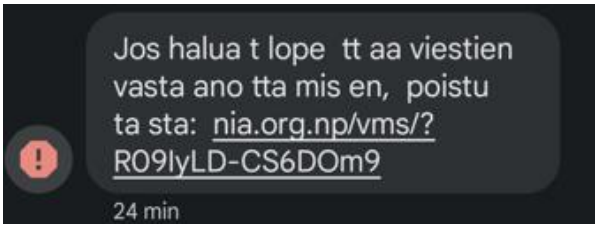
- Fake buttons - klikkaa oik. hiiren näppäimellä, jolla voit kopioida linkin ja tarkistaa
- Kirjoitusvirheet - Netflix.com / Netlfix.com
- Ylimääräiset URL-sanat - netflix.com.movies.com
- Lyhennetyt URL-osoitteet väärennettyjen verkkosivustojen tarkistus https://transparencyreport.google.com/safe-browsing/search

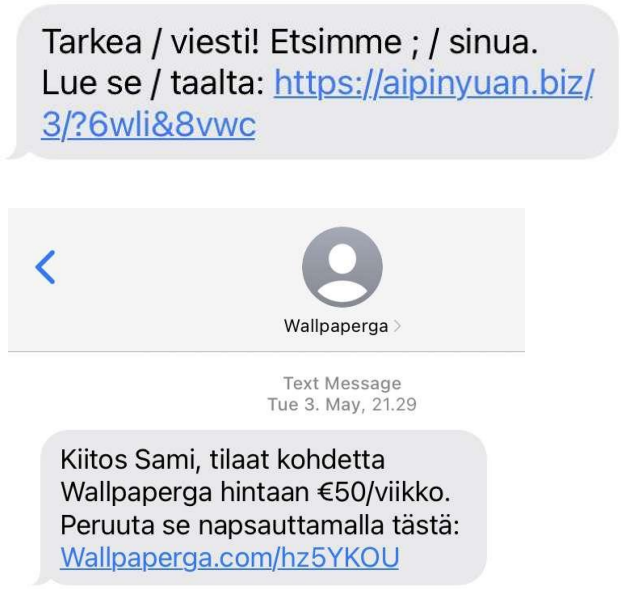
3.6 Haitalliset tekstiviestit

Haitallisten tekstiviestien tehtävänä on:

- On hyötyä taloudellisesti.
- Varastaa tietoja käyttämällä joko apunaan sosiaalista manipulointia tai laitteisiin asentuvalla haittaohjelmalla, joka kerää ja lähettää henkilökohtaisia tietoja.
    - Haittaohjelmat saattavat pyrkiä keräämään pankkitietoja tai salasanoja puhelimesta.
- Asentaa erilaisia haittaohjelmia, jotka usein pyrkivät levittämään itseään eteenpäin käyttäen hyödykseen puhelimessa olevia puhelin numeroita ja sähköposti tilejä.

Alla muutamia esimerkkejä haitallisista tekstiviesteistä:





3.7 Haitalliset sovellukset ja sovelluksien käyttöoikeudet

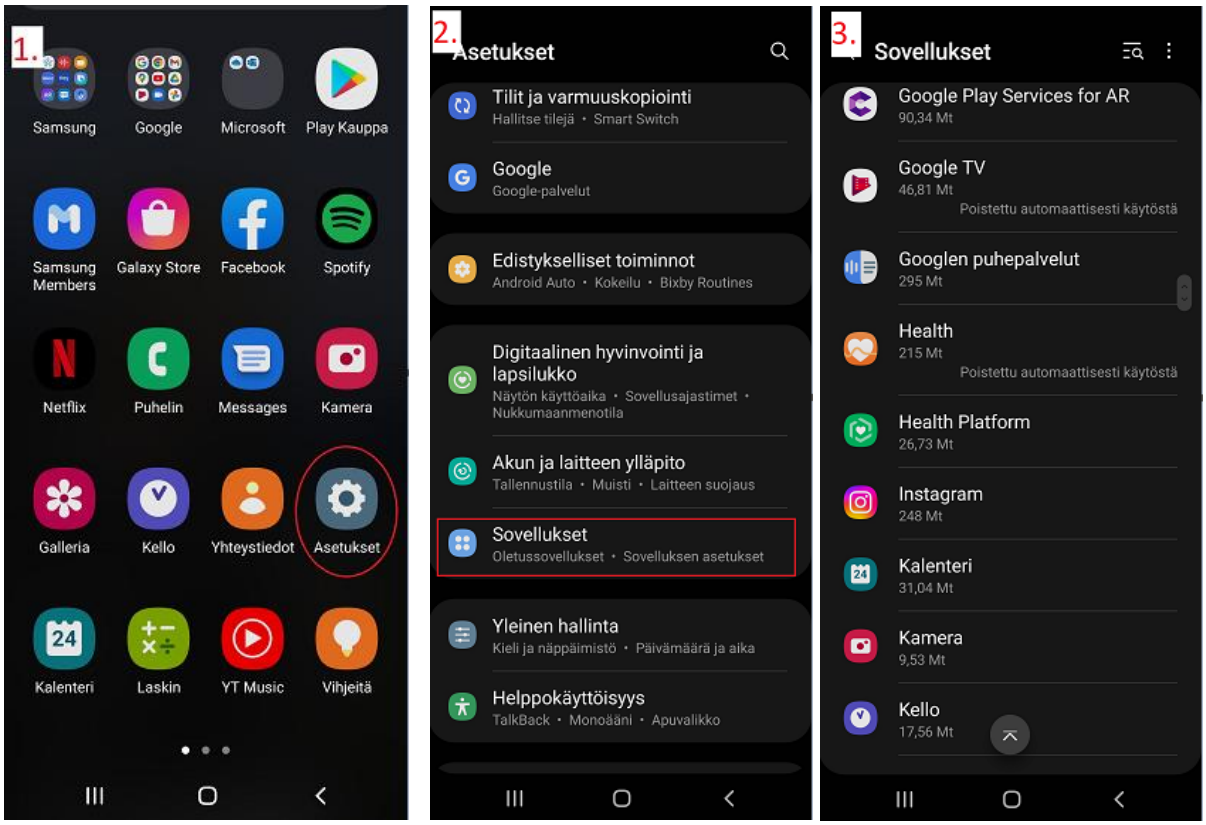
Puhelimille ladattavat sovellukset pyytävät usein lupaa käyttää tiettyjä puhelimen oikeuksia, kuten kameraa tai yhteystietoja. Moni sovellus tarvitsee näitä lupia toimiakseen kunnolla, mutta osa sovelluksista pyytää omaan tarpeeseensa liikaa vapauksia liikkua puhelimessa. Nämä sovellukset usein keräävät ylimääräistä tietoa käyttäjistään.

- Tietoja saatetaan myydä eteenpäin, tai käyttää markkinoinnissa.
    - Muistiinpano sovellus ei varmaankaan tarvitse oikeuksia kameraan, yhteystietoihin tai sijaintiin. Myöskään valokuvien muokkaamiseen tarvittava sovellus ei tarvitse oikeuksia

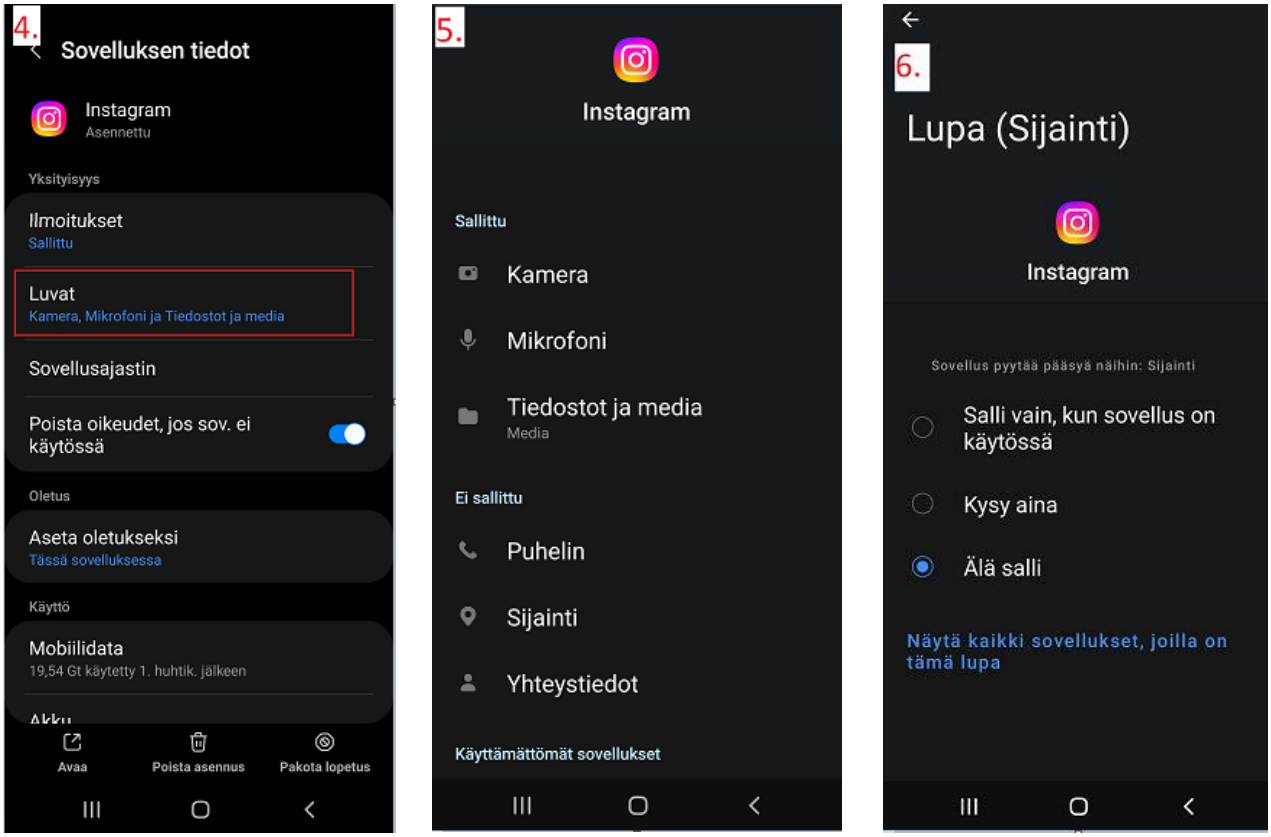
osoitekirjaan, sijaintiin ja mikrofoniin. Sen sijaan se tarvitsee oikeudet kameraasi voidakseen toimia.

- On hyvä pysyä perillä siitä mitä oikeuksia eri sovelluksilla on puhelimeen.

Alla on ohjeet Android puhelimen sovelluksien oikeuksien tarkistamiseen:

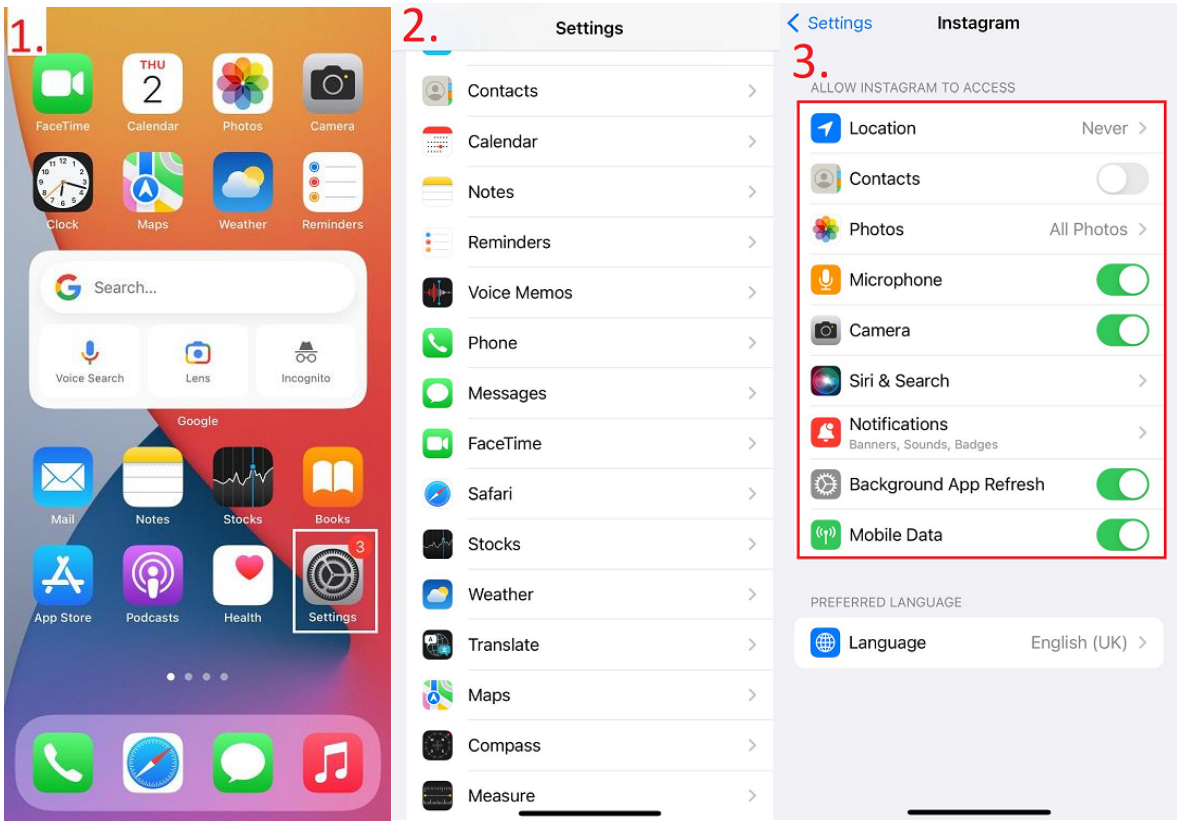


1. Aloita etsimällä **Asetukset/Settings** painike valikosta.
2. Etsi **Sovellukset/Apps** asetus.
3. Sovellukset asetuksesta löydät kaikki sovellukset, jotka on asennettu puhelimeesi. Valitse valikosta sovellus, jonka oikeuksia haluat muuttaa.



4. Sovelluksen asetuksista löydät **Luvat/Permissions** painikkeen, tämän kautta pääset muokkaaman sovelluksen lupia.
5. Luvat osiosta löydät **Sallittu/Allowed** ja **Ei sallittu/Not allowed** osiot sovellukselle, painamalla oikeuksia voit lisätä tai poistaa niitä.
6. Voit valita miten sovellus saa oikeuksia käyttää.

Alla on ohjeet Apple puhelimen sovelluksien oikeuksien tarkistamiseen:



1. Apple laitteilla sovellusten oikeuksien asettaminen on hiukan helpompaa kuin Android laitteilla. Aloita ensin **Asetukset/Settings**.
2. Etsi Asetukset valikosta sovellus, jonka oikeuksia haluat muuttaa.
3. Päätä oikeudet sovellukselle.

3.8 Minkälaisia tietoja puhelimessa ladattu sovellukset keräävät?

	Face-book	Insta-gram	Spoti-fy	Lidl Plus	WhatsApp	Twitter
Sähköposti	x	x	x	x	x	x
Nimi	x	x	x	x	x	x
Ikä	x	x	x	x		x
Sukupuoli	x	x				x
Seksuaalinen suuntautuminen	x					
Siviilisääty	x					
Rotu	x					
Usko	x					
Sijainti	x	x		x		x
Kotiosoite	x	x	x	x		
Työllisyystilanne	x	x				
Työnimike	x	x				
Lemmikki	x	x		x		
Puhelinnumero	x	x	x	x	x	
Lankapuhelinnumero	x		x	x		
Puhelimen tyyppi	x	x	x	x	x	x
Harrastukset	x	x				
Kiinnostuksen kohteet	x	x	x			
Pituus		x				
Paino		x				
Lähiomainen	x					
Äidin tyttönimi						

Nykyinen työnantaja	x	x				
Entiset työnantajat	x	x				
Pankkitilin tiedot			x			
Palkka				x		
Sosiaalinen profiili (ystävät)	x	x	x			x
Sosiaalinen profiili (Harrastukset)	x	x	x			
Sosiaalinen profiili (Kiinnostukset kohteet)	x	x	x			
Terveystiedot	x	x		x		
Poliittinen suuntautuminen	x	x				

3.9 Haitalliset laitteet

Haittaohjelmat ja huijarit eivät ole ainoita uhkia verkkomaailmassa. Monien internetyhteyden vaativien laitteiden turvallisuus on usein kyseenalainen, joko tahallisesti tai tahattomasti.

- Näitä internetyhteyksiä vaativia laitteita kutsutaan IoT-laitteiksi (Internet Of Things) ja ne voivat olla usein iso tietoturvariski yrityksen tai kodin sisäverkolle.
- Monet valmistajat eivät tuotetta suunnitellessa ota ollenkaan huomioon sitä miten turvallinen tuote on verkossa.
    - Tämän takia IoT-laitteet voivat olla hakkereille keino murtautua verkkoon.
- Wishistä, Aliexpressistä ja Alibabasta ei ole suositeltavaa tilata IoT-laitteita, johtuen usein laitteiden väärinkäytöstä valmistajan toimesta. Ne ovat usein halpoja, koska mahdollisimman moni halutaan houkutella luovuttamaan yksityisyytensä laitteelle.
    - Valvontakamera (esim. lemmikkikamera/itkuhälytin) voi lähettää kuvamateriaalia tai ääntä takaisin valmistajalle tai kerätä tilanne/paikka dataa. Monet kamerat voivat esimerkiksi skannata kaikki pöydälläsi olevat asiakirjat ja lähettää niistä kuvat ulkomailla olevaan tietokantaan.
    - Usein laitteiden tietoturva on myös olematon ja pahimmissa tapauksissa kuka tahansa verkossa pääsee hallitsemaan laitteita tai katselemaan kotisi tapahtumia reaaliajassa.
- Tämänhetkisten IoT toimintamallien takia isotkin yritykset ovat jääneet usein kiinni laitteiden tietoturvan laiminlyönnistä. Jos kuitenkin tarvitsee kyseisen laitteen, ota seuraavat asiat huomioon ostopäätöstä tehdessäsi:

- Lue arvosteluja ja kokemuksia, näistä voi usein selvitä ovatko laitteet minkälaisia ja kuinka ne toimivat.
- Suosi isoja, tunnettuja yrityksiä, sillä isot yritykset todennäköisemmin päivittävät laitteitaan haavoittuvaisuuksia vastaan ja niillä voi todennäköisemmin olla asiakaspalvelu, joka neuvoo pulmatilanteissa.
- Etsi laitteista Tietoturvamerkkiä, joka on Traficomin myöntämä sertifioitu merkki kyberturvasta laitteessa:

3.10 Hyödyllisiä linkkejä

Lisää tietoa Tietoturvamerkistä:

Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja | Traficom (kyberturvallisuuskeskus.fi)

YLE:n hyvä uutinen IoT laitteiden turvallisuudesta:

Kodin älylaitteet yleistyvät vauhdilla, mutta tietoturva ja lainsäädäntö laahaavat perässä – "Kameralla varustettua laitetta voidaan seurata"

Tietoturvapäällikön blogi: asetelma yrityksen ja kyberrikollisen välillä on epäreilu - siksi henkilöstöä on koulutettava:

https://www.epressi.com/tiedotteet/energia/tietoturvapaallikon-blogi-asetelma-yrityksen-ja-kyberrikollisen-valilla-on-epareilu-siksi-henkilostoa-on-koulutettava.html

Muutama hyvä YLE:n uutinen haittaohjelmista:

Suomalaisia diplomaatteja vakoiltu haittaohjelmalla – ulkoministeriö: Vakava tapaus, tulkitsemme laittomaksi tiedusteluksi (yle.fi)

Poliisi Hyrylän koulu-uhkauksesta: Epäilty latasi oppilaan koneelle viruksen nettipelissä, vei Wilma-tunnukset ja lähetti koululle pommiuhkauksen (yle.fi)

Alla on Ylen hyvä artikkeli, kuinka sovellukset voivat väärinkäyttää oikeuksiaan eri tietokoneissa ja puhelimissa:

Tiedätkö minkälaisia oikeuksia annat sovelluksille? Jokainen sovellus voi napata näppäinlyöntisi tai ottaa ruutukaappauksia näytöstäsi (yle.fi)

Alla on Iltasanomien uutinen Flubot nimisestä puhelinhaittaohjelmasta, uutisessa on myös hyvä ja informoiva video.:

FluBot leviää satojen tuhansien viestien voimin päivässä - Tietoturva - Ilta-Sanomat (is.fi)

Alla on Traficomin tietoturvaoppaita yksityishenkilöille ja yrityksille:
Ohjeita ja oppaita tietoturvasta | Kyberturvallisuuskeskus

Tältä sivulta voit laskea kuinka paljon kaistaleveyttä tarvitset kotonasi / yrityksessäsi: https://www.btel.com/bandwidth-calculator/

Ylellä on useita hyviä digitreeni oppaita niille, jotka haluavat harjoitella omia tietoteknisiä taitojaan: Digitreenit – yle.fi

4 Työasemat eli pöytätietokoneet ja kannettavat tietokoneet

4.1 Miten haittaohjelmilta voi suojautua?

Ennakoiminen on hyvä taito oppia kyberturvallisuudessa, mutta tosiasia on, että kaikille voi sattua virheitä ja ongelmia, joihin ei voi aina varautua. Ongelmatilanteisiin on hyvä varautua suojaamalla päätelaite eli pöytätietokone tai kannettava tietokone.

4.2 Virustorjunta-ohjelmat

Virustorjunta ohjelmat ovat jokaisen päätelaitteen turvallisuuden yksi kulmakivistä. Virustorjunta ohjelmat tarkastelevat tietokoneen tiedostoja ja sillä käynnissä olevia ohjelmia löytääkseen jotain, mikä voisi olla haitallista.

- Monet eri yhtiöt tekevät omia virustorjunta ohjelmia, joista osa on ilmaisia ja osa maksullisia. Alle on listattu muutama vaihtoehto, jotta saa kuvan eri virustorjuntaohjelmien ominaisuuksista.

	Microsoft Defender	F-secure Safe	Bitdefender	Norton
Tiedot	Microsoftin virustorjunta ohjelma, joka löytyy kaikista Windowsin käyttöjärjestelmän laitteista. • Tarjoaa aktiivisen virustorjunnan ja perussuojan haitallisempia haittaohjelmia kohtaan	Suomalaisen yrityksen F-securen suunnittelema virustorjunta ohjelma. • Tarjoaa aktiivisen virustorjunnan, pankki palveluiden suojan, selailun suojan ja lapsilukon laitteisiin ja sovelluksiin	Alun perin Romaniassa perustettu Bitdefender on yksi maailman suosituin virustorjunta ohjelma. • Ilmaisversio tarjoaa aktiivisen virustorjunnan ja web identiteetin suojan	Yhdysvalloissa perustettu Norton on suuri kyberturva ohjelmia tekevä yritys. Perusversio tuo kaikki kyberturva palvelut käyttäjälle, kuten VPN ja salasanahallintaohjelman

Hyvää	• Todella helppo asentaa ja tulee Windows laitteissa tehdasasetuksena päällä • Varsin toimiva virus tarkastuksen kanssa • Sopii hyvin perustason turvalliseen internet toimintaan	• Helppo ja käyttäjäystävällinen käyttöliittymä • Tehokas estämään haittaohjelmat laitteissa • 30-päivän ilmainen kokeilu • Paljon hyödyllisiä lisäpalveluita	• Helppo ja yksinkertainen käyttöliittymä • Virussuoja on tehokas ja toimiva. Ilmaisversion virustorjunta on sama kuin maksullisen eli tehoissa ei ole eroa • Monin tavoin palkittu asiantuntijoiden toimesta	• Käyttäjäystävällinen käyttöliittymä

Huonoa	• Kehittyneet haittaohjelmat saattavat päästä läpi ilman suurempia ongelmia • Ei verkkoselaimen suojaa	• Ei ilmaisversiota • Laitteiden rekisteröinti on vähän jäykkää	• Voi olla liian tiukka toiminnaltaan ja estää oikeiden ohjelmien toimimisen	• Tekee paljon ilmoituksia, joka voidaan nähdä tunkeilevana • Varsin hintava
Hinta	Ilmainen	• 3 laitetta vuodeksi 59,90 € • 5 laitetta vuodeksi 79,90 € • 7 laitetta vuodeksi 99,90 €	• Ilmaisversio • Bitdefender antivirus plus yhdelle laitteelle vuodeksi 29,90 €	• Norton 360 Standard 79,90 € yhdelle laitteelle vuodeksi • Norton 360 Deluxe 94,90 € viidelle laitteelle vuodeksi

				• Norton 360 Premium 104,90 € kymmenelle laitteelle vuodeksi
Saatavuus	Löytyy Windows laitteista	F-Secure SAFE — Award-winning internet security | F-Secure	Bitdefender Antivirus Free - Download Free Antivirus Software	Norton-ohjelmistot 2022 | Norton-tuotteet ja -palvelut

4.3 Fyysisten laitteiden turvallisuus

Fyysisten laitteiden turvallisuus on tärkeä osa-alue, kun puhutaan kyberturvallisuudesta. Laitteen varastaminen ja siihen käsiksi pääseminen helpottaa siihen murtautumista, tämän takia laitteiden niin sanottu koventaminen on tärkeää.

- Aina kun nouset pois koneelta, lukitse näyttö (Windows laite: Windows näppäin + L, Applekone: Control + Command + Q). Varmuuden vuoksi kannattaa myös laittaa kone lukitsemaan itsensä automaattisesti esimerkiksi 10 minuutin päästä.
- Kaikissa laitteissa tulisi olla vahva kirjautumissalasana.
    - Monia biometrisiä tunnustautumiskeinoja (esim. kasvojentunnistus ja sormenjälki) voidaan huijata eri tavoilla. Vaikka nykyään biometriset tunnustautumiskeinot ovat jo melko luotettavia tulisi silti näiden sijaan suosia vahvaa PIN-koodia tai kuviota.
- Automaattista kirjautumista eri nettisivuille ei suositella, kun kyse kannettavasta. tietokoneesta tai mobiililaitteesta, tämän avulla on hyökkääjän helppo päästä käsiksi tärkeisiin tileihin.
- Ulkoiset tallennusasemat tulisi suojata sillä tavalla, että niitä ei saisi irti tai niihin pääsisi ulkopuoliset käsiksi.
- Yleisissä tiloissa olevat tietokoneet tulisi suojata sillä tavalla, että niihin ei pääsisi liittämään ulkopuoliset omia laiteitaan.
- Älä koskaan liitä laitteisiisi tuntemattomia laitteita ja tallennusasemia, kuten USB-tikkuja tai mitään muutakaan laitetta.

4.4 Salasanahallintaohjelmat

Hyvän kyberhygienian mukaan kaikilla tileillä ja palveluissa tulisi olla uniikki ja vahva salasana. Ikävä kyllä salasanojen muistaminen vaikeutuu mitä enemmän niitä syntyy. Tähän on nykyaikana keksitty ratkaisu nimeltään salasanojenhallintaohjelma.

- Salasanahallintaohjelmalla voi luoda vahvoja ja uniikkeja salasanoja eri palveluihin.
    - Näitä salasanoja ei tarvitse muistaa, koska ohjelma tallentaa ne ja syöttää automaattisesti salasanan kirjautumisen yhteydessä.
- Alla on taulukko eri salasanahallintaohjelmista, jotta salasananhallintaohjelmien eri ominaisuudet olisivat selviä.

	1Password	Bitwarden	F-secure ID PROTECTION	LastPass
Tiedot	Kanadalaisen yhtiön valmistama 1Password on yksi tämän hetken turvallisimmista salasananhallinta ohjelmista	Amerikkalaisen yhtiön valmistama Bitwarden on tällä hetkellä paras ilmainen salasananhallinta ohjelma	Suomalaisen F-securen valmistama ID PROTECTION tuo suomalaisen tietoturvaosaamisen salasanoihin	LastPass on yhdysvaltalaisen yhtiön tekemä salasananhallintaohjelma, joka on varmasti myös tällä kaikista suosituin.
Hyvää	• Tämän hetken turvallisin salasananhallinta ohjelma	• Ilmaisista salasananhallinta ohjelmista pätevin	• Helppo ja yksinkertainen käyttöliittymä • Varsin turvallinen	• Pimeän verkon tarkkailu, joka ilmoittaa heti kun omat tiedot vuotavat

	• Ilmainen kokeilu 14 päiväksi • Ei sisällä yhtään evästeitä, jotka jäljittäisivät	• Ei sisällä yhtään evästeitä, jotka jäljittäisivät • Hyvin turvallinen		• Helppo ja yksinkertainen käyttöliittymä • Laitteiden välillä tapahtuva salasanojen jakaminen helppoa
Huonoa	• Turvallisuus vie pois käytännöllisyyttä	• Turvallisuus vie pois käytännöllisyyttä	• Hallintaohjelma voi olla hieman kankea	• Ilmaisversioon saa vain yhden laitteen rekisteröityä • Sisältää paljon seurantaa käyttäjästä
Hinta	• Yksityishenkilö 2,99 $	• Ilmainen • Premium 1 $	Viidelle laitteelle	Ilmainen yhdelle laitteelle

	• Perhe 4,99 $ • Yritys 19,95 $	• Perhe 3,33 $ • Yritys 3 $	• 3,99 € kuukausi • 39,90 € vuosi Kymmenelle laitteelle • 5,99 € kuukausi • 59,90 € vuosi	Premium 2,90 € kuukaudessa Family 3,90 € kuukaudessa
Saatavuus	Pricing & free trial | 1Password	Install and Sync All of Your Devices | Bitwarden	F-Secure ID PROTECTION — Secure passwords and online identity | F-Secure	LastPass Premium vs Families | What plan is best for you?

Vaikka salasanahallintaohjelmat tekisivät suurimman osan salasanoista, on tärkeää tietää tämänhetkisen hyvän salasanan tunnusmerkit.

- Sanojen sijaan suosi lauseita, näitä lauseita voivat olla esimerkiksi laulun sanat tai runo. Murrelauseet ovat erityisen tehokkaita.
- Älä käytä salasanoissa mitään henkilötietoja kuten omaa nimeä, läheisten nimiä tai syntymäaikoja. Näiden kaltaisia tietoja voi löytyä yleisesti sosiaalisesta mediasta ja verkosta.
- 12–15 merkkiä pitkät salasanat, mitä pidempi sitä turvallisempi.
- Suosi useita erikoismerkkejä, kuten huuto- ja kysymysmerkkiä.
- Älä kierrätä samoja salasanoja.
- Esimerkki: kissa+koira=8jalkaa

4.5 Yleisimmät käytetyt salasanat Suomessa

Alla on tällä hetkellä Suomen suosituimpien salasanojen lista, jos salasanassasi on jokin seuraavista sanoista, on salasana melko turvaton:

Salasana	Arvaamisaika	Salasana	Arvaamisaika
111111	< 1 sekunti	kissa	10 sekuntia
123123	< 1 sekunti	lol123	3 tuntia
1234	< 1 sekunti	lollero	17 minuuttia
12345	< 1 sekunti	lollipop	< 1 sekunti
123456	< 1 sekunti	makkara	17 minuuttia
1234567	< 1 sekunti	mansikka	3 tuntia
12345678	< 1 sekunti	moi123	11 sekuntia
123456789	< 1 sekunti	moikka	2 minuuttia
1234567890	< 1 sekunti	moimoi	< 1 sekunti
123qwe	< 1 sekunti	n-sana	17 minuuttia

1q2w3e	< 1 sekunti	paska	10 sekuntia
1q2w3e4r	< 1 sekunti	paska123	17 minuuttia
abc123	< 1 sekunti	password	< 1 sekunti
akuankka	3 tuntia	perkele	17 minuuttia
asd123	2 tuntia	perkele1	3 tuntia
asdasd	17 minuuttia	petteri	17 minuuttia
asdasd123	3 sekuntia	qwe123	< 1 sekunti
aurinko	17 minuuttia	qwerty	< 1 sekunti
dragon	< 1 sekunti	qwerty1	< 1 sekunti
jeejee	< 1 sekunti	qwerty123	< 1 sekunti
johannes	< 1 sekunti	saatana	17 minuuttia
kakka	10 sekuntia	salasana	< 1 sekunti
kakka123	17 minuuttia	salasana1	9 sekuntia
kamari	2 minuuttia	tietokone	24 tuntia
kikkeli	17 minuuttia		

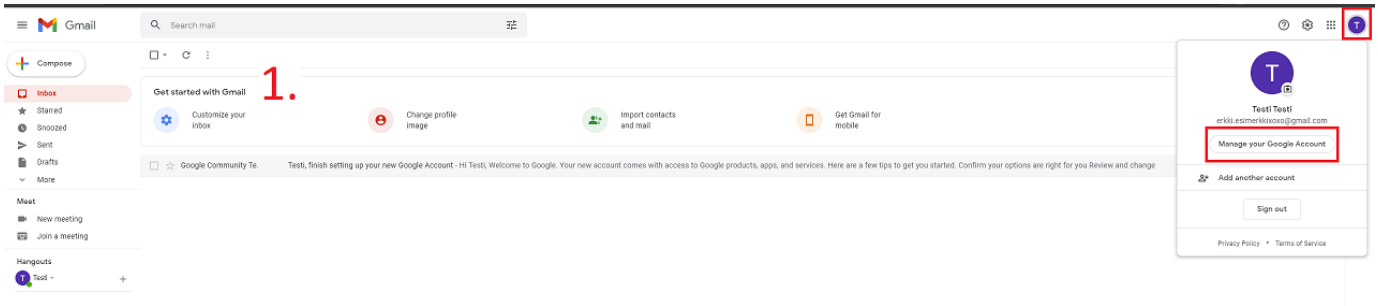
5 Sähköpostin käyttö / kaksivaiheinen tunnistautuminen

Sähköposti on yleistynyt ja lähes kaikilla on jonkinlainen tili sähköpostipalvelussa. Yritysten välinen viestintä tapahtuu myös usein sähköpostin välityksellä ja se sisältää paljon arvokasta tietoa yrityksestä sekä yrityksen toiminnasta. Monet rikolliset tietävät tämän ja pyrkivätkin tämän takia murtautumaan sähköpostiin ja saamaan sen hallintaansa. Tässä kappaleessa opastetaan sähköpostin turvallisuuteen näyttämällä, kuinka sähköpostin sisäisillä asetuksilla voi parantaa turvallisuutta, kuinka salasananhallintaohjelman voi saada toimimaan ja kuinka ottaa käyttöön kaksivaiheinen tunnistautuminen.

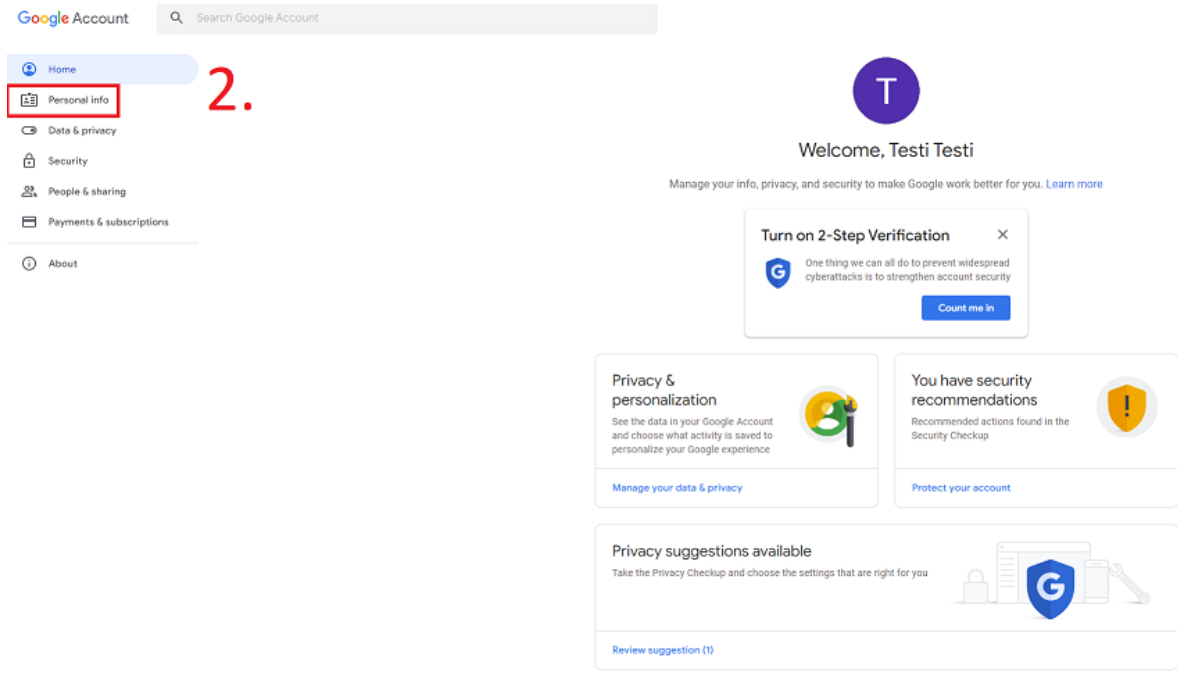
5.1 Sähköposti

Sähköpostin sisäisillä asetuksilla voi parantaa turvallisuutta merkittävästi, alla on muutamille sähköpostipalveluille ohjeet siitä mitä asetuksia suositellaan.

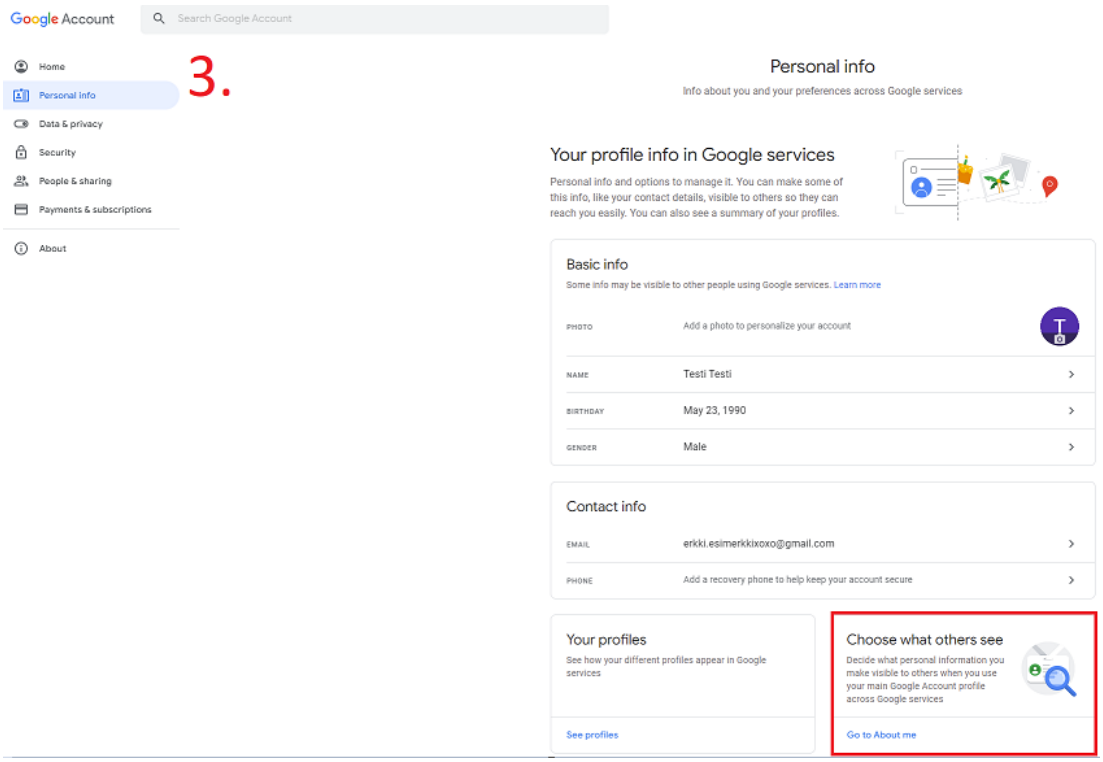
Google:



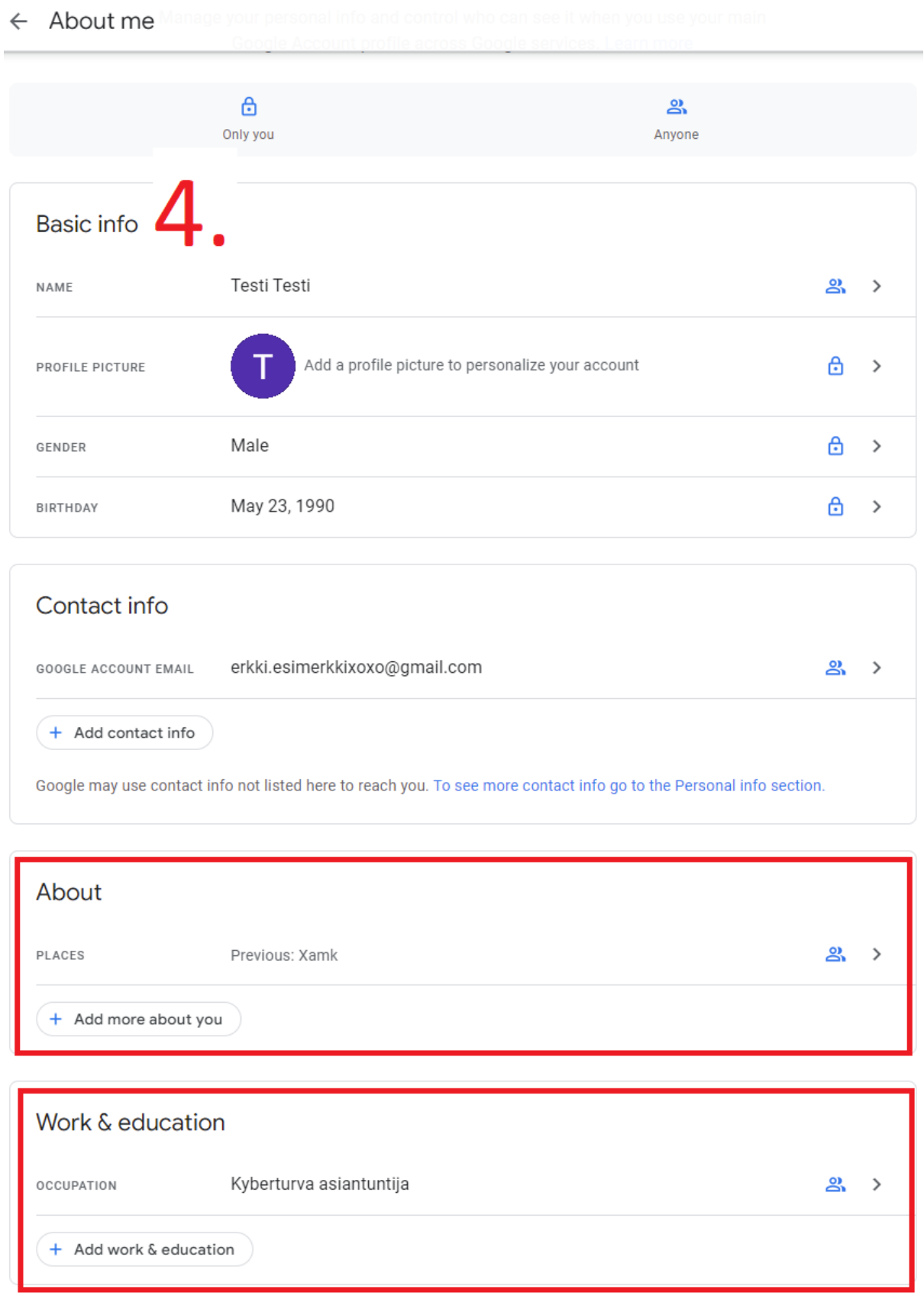
1. Omalta gmail-tililtä voi avata asetus valikon painamalla oikealla yläkulmassa olevaa käyttäjäkuvaketta, josta valitsee **Hallinoi Google-tiliäsi/Manage your Google Account.**



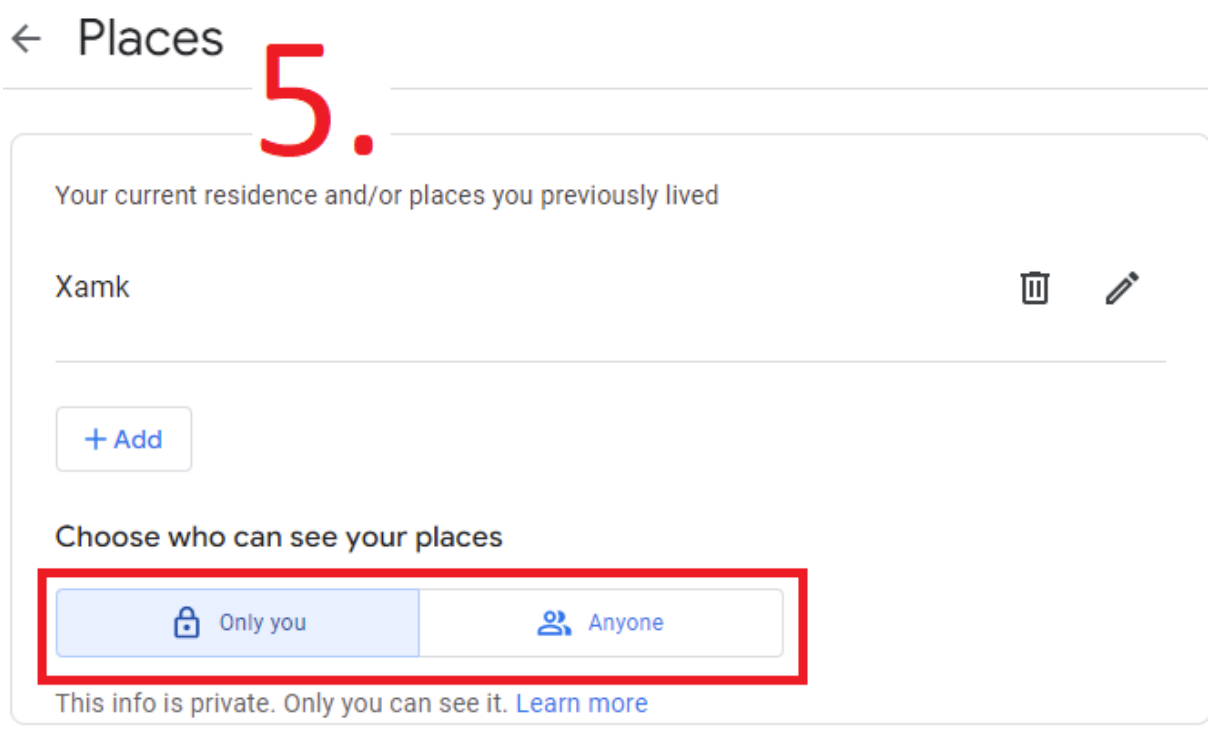
2. Yleisnäkymästä pääsee helposti muuttamaan useita asetuksia Google-tiliin liittyen, aloitetaan **Henkilökohtaiset tiedot/Personal info** muokkaamisella.



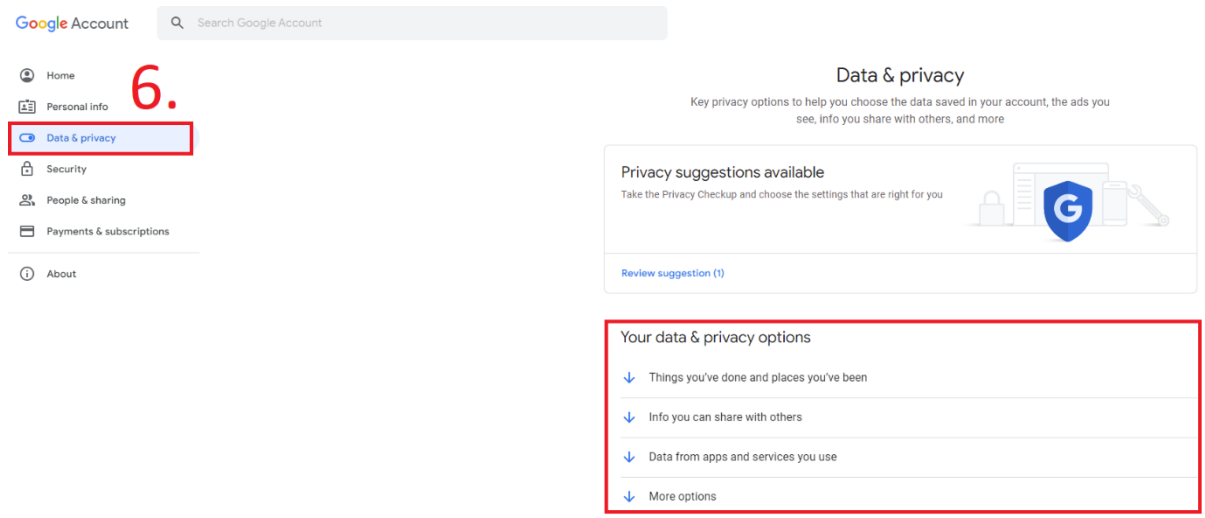
3. Sivulta löydät tietoa tiliisi liittyen, haluamme kuitenkin rajat näiden tietojen näkyvyyttä. Etsi **Valitse, mitä muut näkevät/ Choose what others see**.



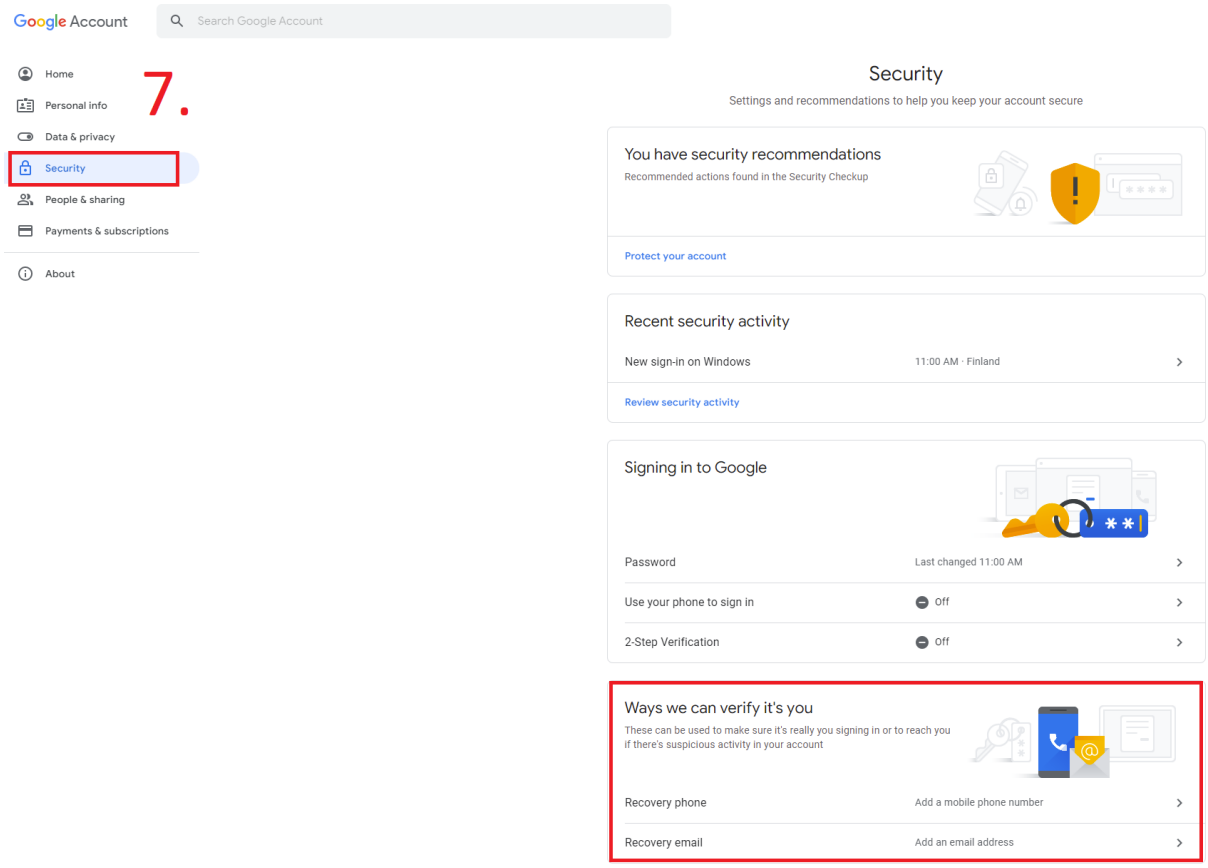
4. On suositeltavaa piilottaa muilta tietoja, joita ei ole pakko jakaa. Eri henkilökohtaisia tietoja voidaan käyttää tileille murtautumisessa.

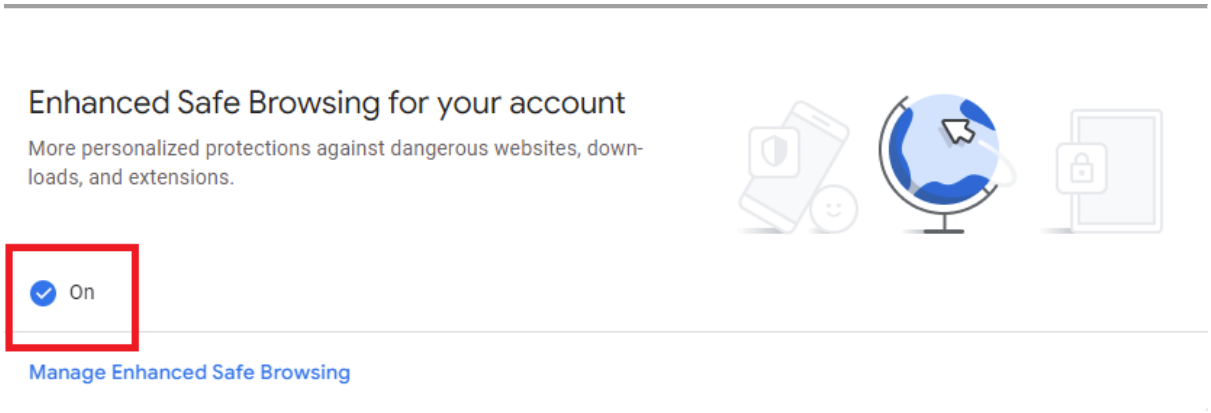


5. Nämä tiedot voidaan piilottaa kaikilta muilta, kun itseltään. Jos kuvassa on lukko tarkoittaa se sitä, että muut eivät näe tietoja.



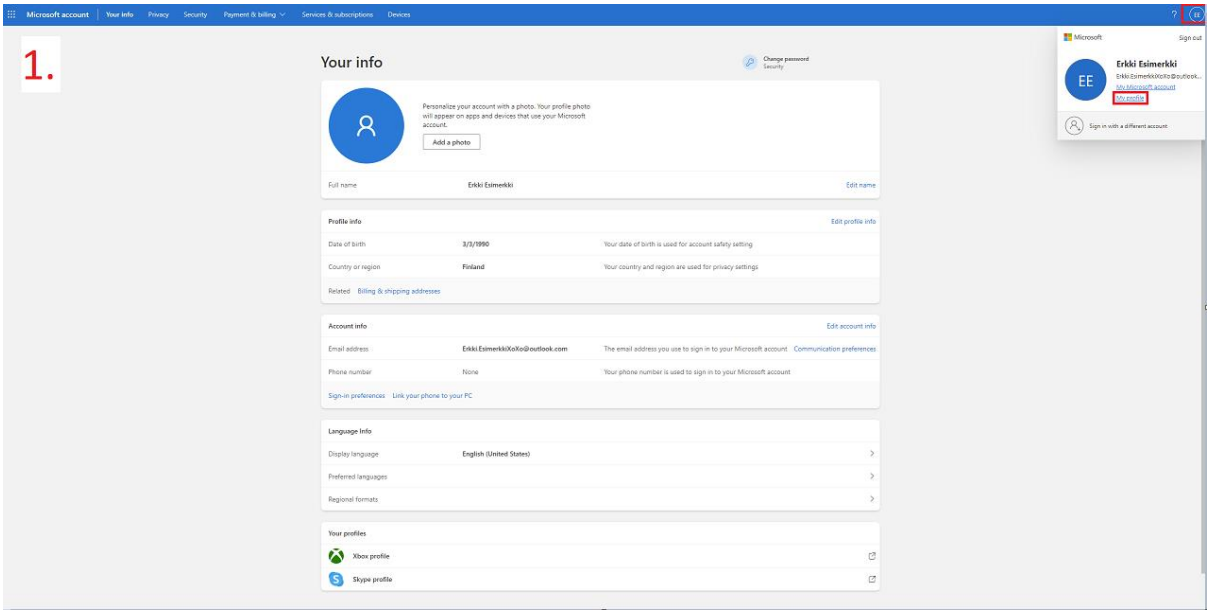
6. **Data ja yksityisyys/Data & privacy** välilehdeltä löydät asetukset sille mitä tietoja Google saa kerätä. Voit muokata näitä itse ja oman harkinnan mukaan päättää tietojesi jakamisesta.



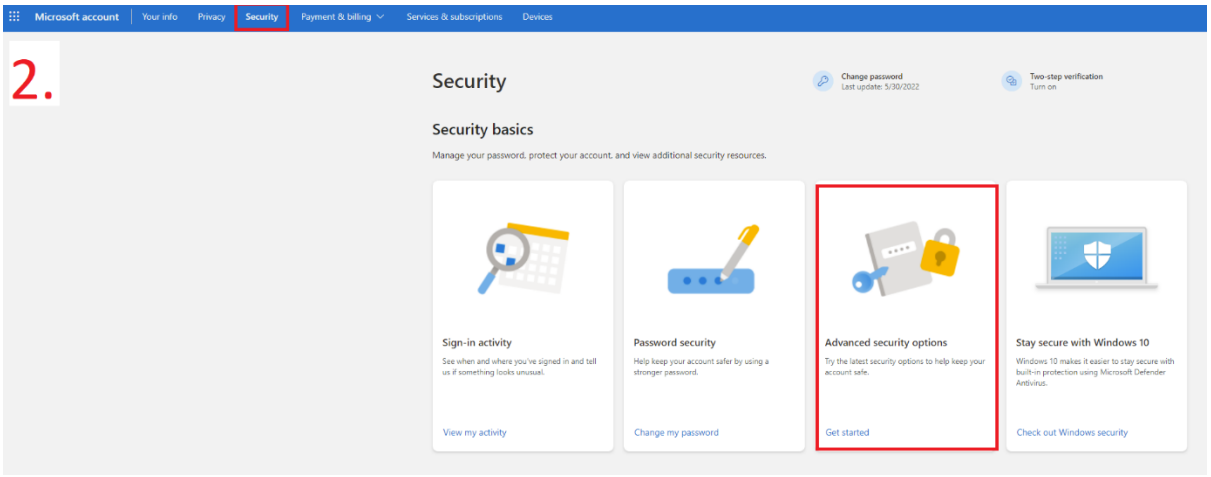


7. **Tietoturva/Security** välilehdeltä löydät kaikki asetukset yleiseen turvallisuuteen liittyen. Sähköposti tilille olisi todella suositeltavaa liittää palautus puhelinnumero tai toinen sähköpostitili, jotta tili pahimmassa tapauksessa saadaan takaisin haltuun/toimimaan. On myös suositeltavaa laittaa päälle **Parannettu selaussuoja/Enhanced Safe Browsing**.

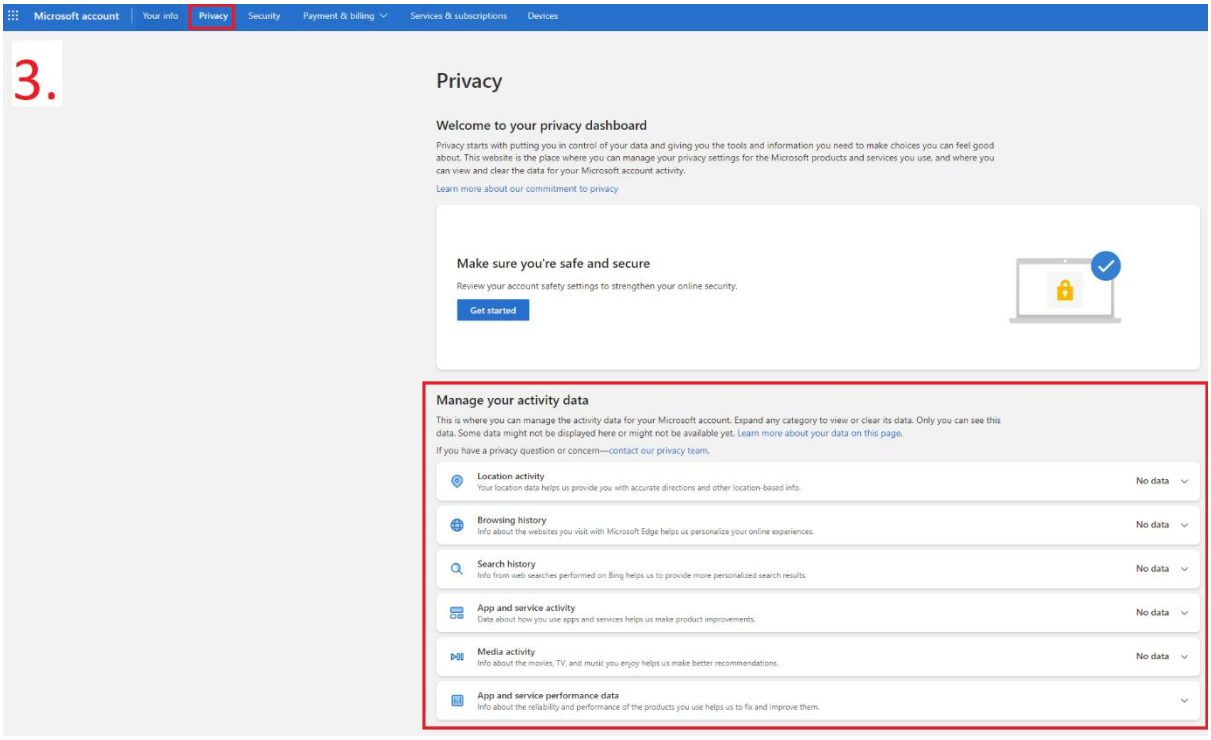
Outlook (selain-versio):

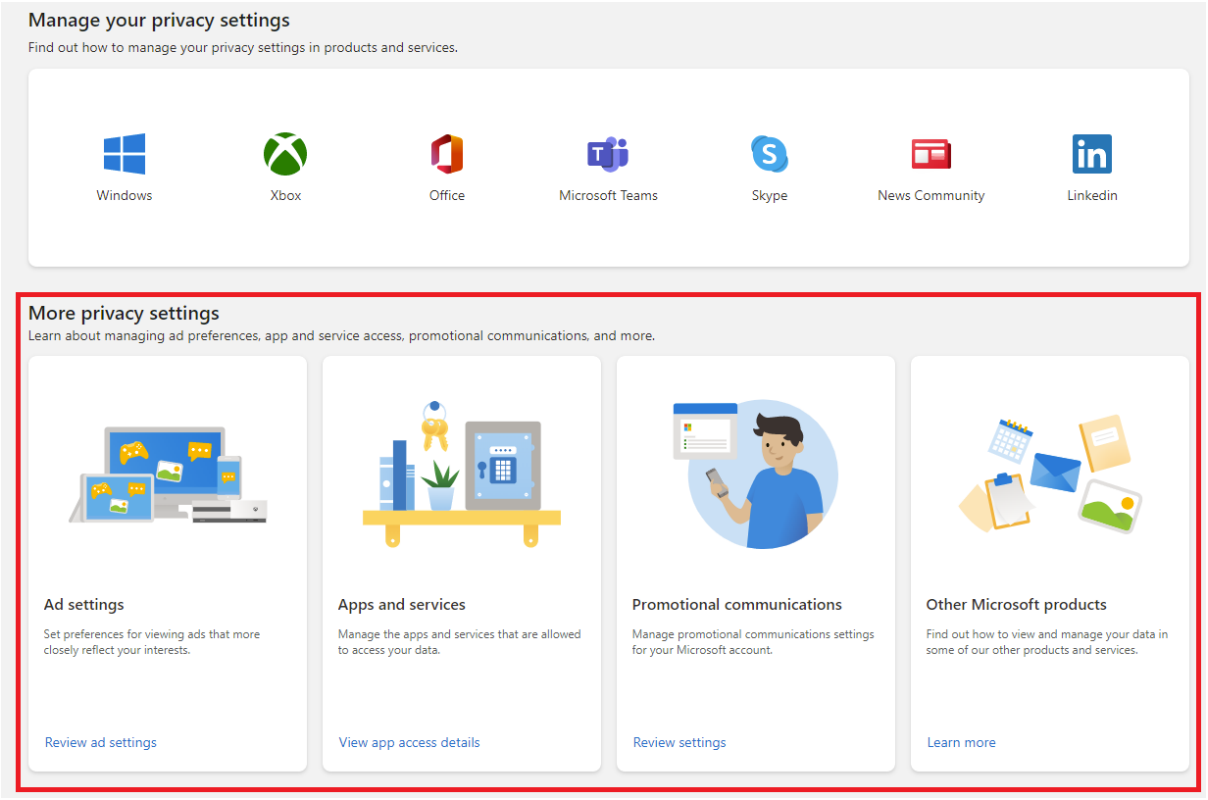


1. Pääset Outlookin asetuksiin oikeassa yläkulmassa olevasta käyttäjä painikkeesta ja painamalla **My Profile/Oma profiili.**



2. Outlook pitää sisällään muutaman välilehden, joista ensimmäisenä tarkastellaan **Security/Tietoturva** painiketta. Täältä löydät kaikki tilin turvallisuuteen liittyvät toimet, joista suositellaan käymään läpi **Advanced security options/Edistyneet suojausasetukset**. Täältä löydät kaksivaiheiseen tunnistautumiseen liittyvät asetukset.

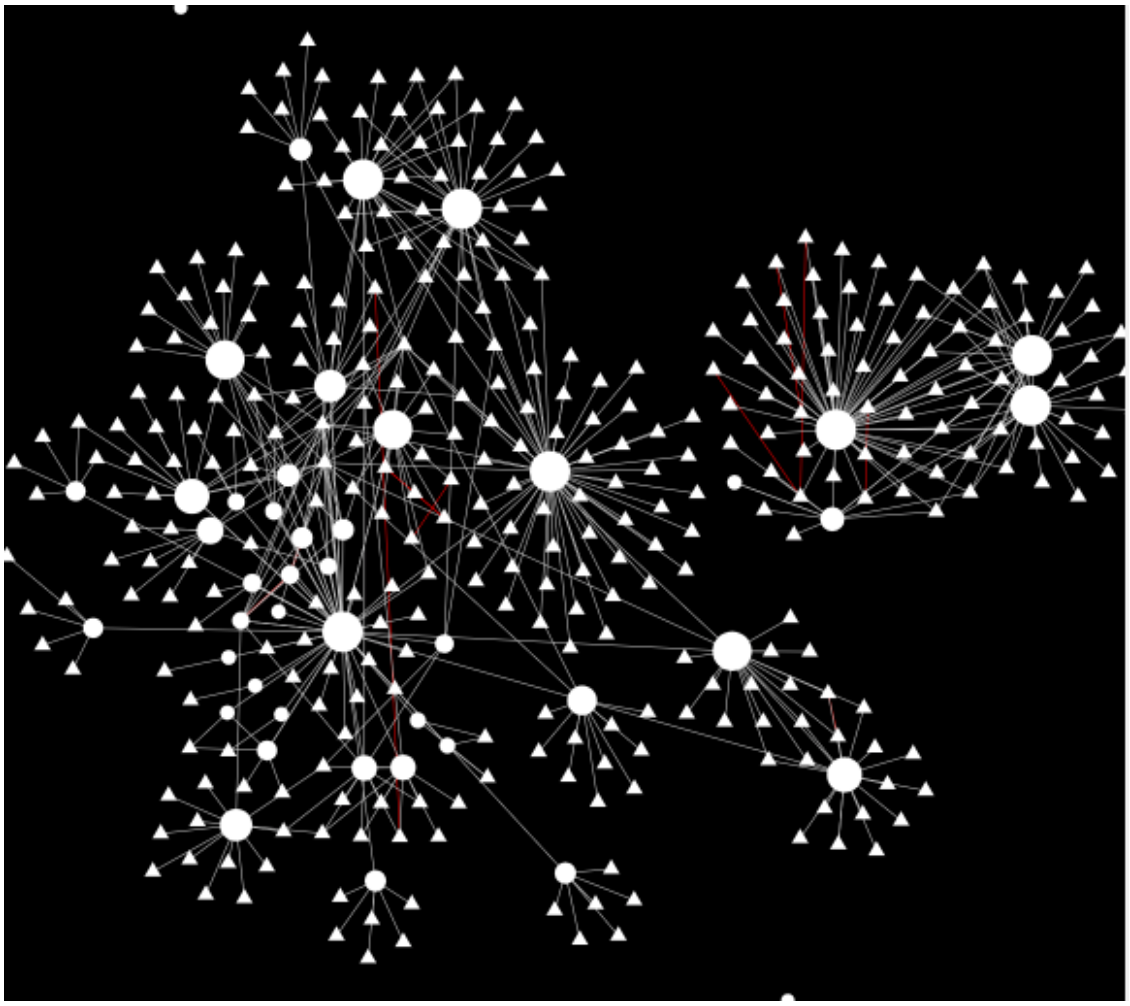




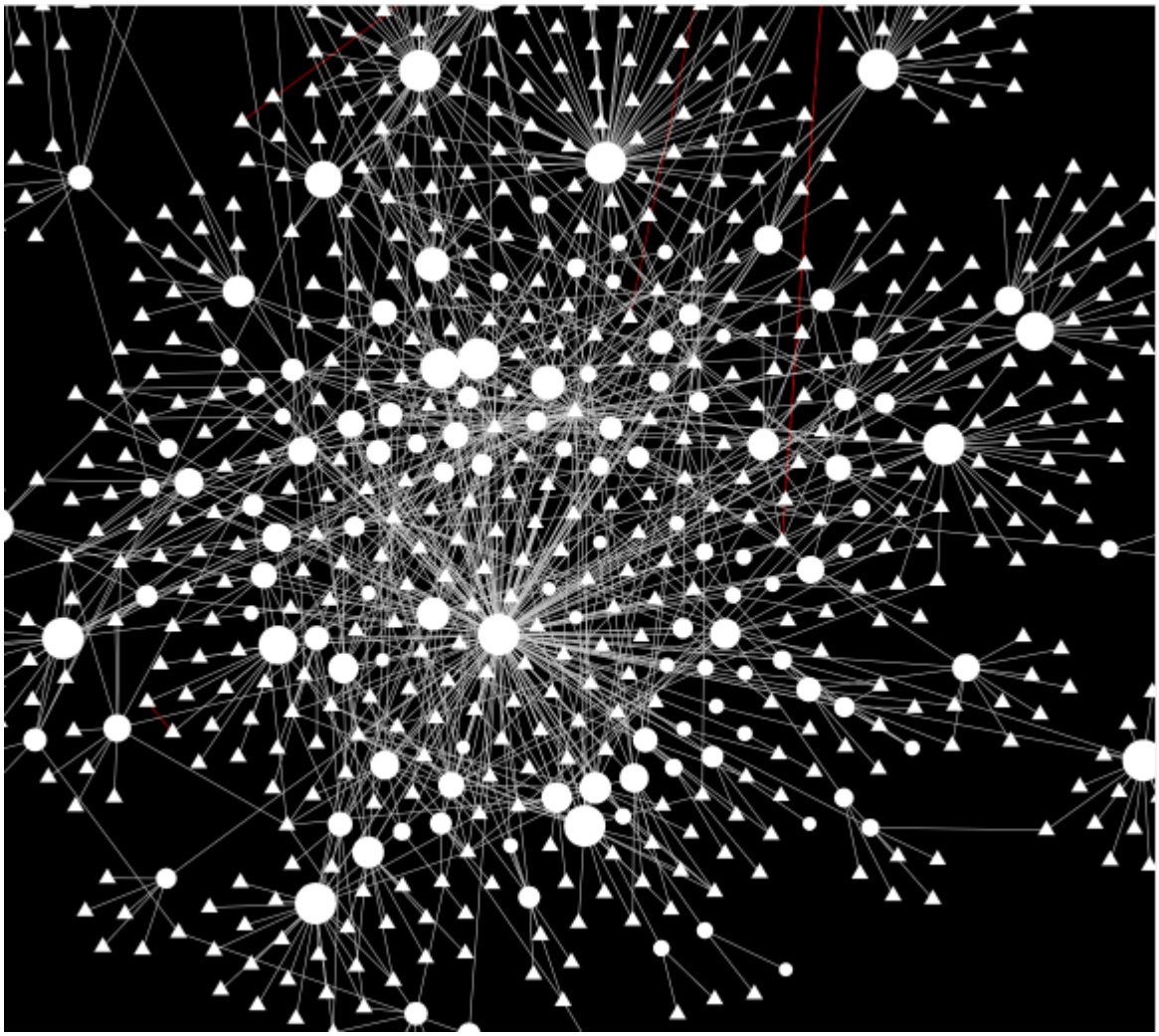
3. **Privacy/Tietosuoja** välilehti pitää sisällään omien tietojen hallinnan, voit tätä kautta muokata sitä, miten Microsoft käyttää sinusta kerättyä tietoa. Nämä asetukset ovat kaikille melko henkilökohtaisia, jonka

takia on suositeltavaa tutustua välilehtiin ja arvioida sitä haluaako omien tietojensa jakamisen.

Alla on esimerkki, joka näyttää miten eri nettisivut keskustelevat keskenään ja jakavat evästeitä sekä tietoja Google Chrome selaimessa. Ensimmäisessä kuvassa on estetty evästeiden käyttö sivuilla, kun niitä kysytään. Toisessa kuvassa on hyväksytty kaikki evästeet.



1



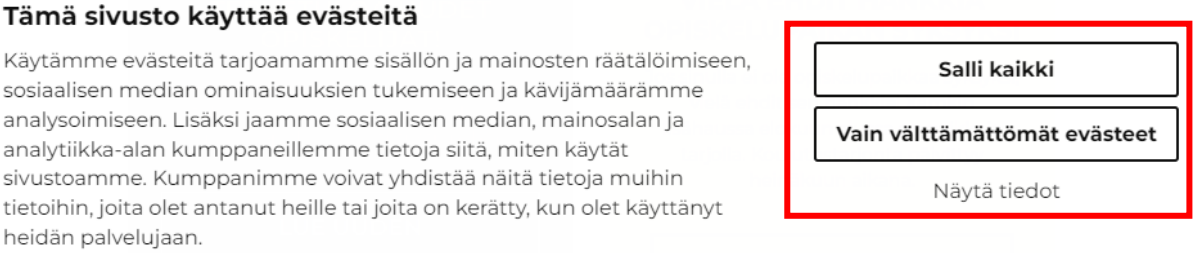
2

Evästeet ovat yksinkertaisimmillaan tietoja, jotka tallennetaan selaustoiminnoistasi ja mieltymyksistäsi verkossa. Tämä on tärkeä tietoa yrityksille, jotka haluavat lisätä todennäköisyyttä, että ostat jotain, kun vierailet niiden sivustoilla. Miten verkkosivustot luovat kolmannen osapuolen evästeitä, jotka seuraavat sinua ympäri internetiä? Esimerkiksi, vierailet helsinkiläisen hotellin verkkosivustolla, saatat nähdä mainoksia samasta hotellista myös sen jälkeen, kun menet pois sivustolta ja vierailet muilla verkkosivustoilla. Tavoitteena on saada sinut palamaan kyseisen hotellin verkkosivustolle ja varaamaan huone. Evästeiden takana oleva koodi ei saastuta tietokonettasi, asenna laitteeseesi mainos- tai haittaohjelmia tai muuta laiteittasi. Näiden

evästeiden avulla verkkosivustot voivat seurata toimintaasi, vaikka et käyttäisikään niiden sivustoja.

Valkoiset pallot kuvaavat nettisivuja kuten esimerkiksi Iltalehti, Iltasanomat, Helsingin Sanomat, Facebook. Mitä isompi pallo on, sitä enemmän kyseinen sivu on kerännyt ja jakanut nettiselailusta tullutta tietoa. Pienet valkoiset kolmiot ovat evästeitä ja erilaisia valmiita tietopaketteja, jotka sisältävät informaatiota yleisesti sivuista tai käyttäjistä. Viivat kaikkien näiden välillä tarkoittavat yhteyksiä ja tietojen jakoa. Punaiset viivat ovat evästeiden jakoa sivujen välillä

- Kuvista voi nähdä miten paljon nettisivut jakavat tietoja, kun niille antaa siihen luvan.
- Evästeet ovat useille nettisivuille niiden pääelinehto. Mitä enemmän ihmisiä käy sivulla sitä enemmän tietoja voidaan käyttäjäkunnasta kerätä, tämä tieto voidaan myydä eteenpäin mainosyhtiöille, jotka käyttävät tietoja hyväkseen suositellessaan ihmisille mainoksia. Kaikki tieto ei kuitenkaan mene mainostajille, vaan tietoja saatetaan myös myydä huijareille, jotka tietojen avulla aloittavat puhelin ja sähköposti huijaus operaatioita ihmisiä kohtaan.
- Näet varmasti usein alla olevan ilmoituksen, kun menet nettisivuille. Asiaa ei välttämättä mieti sen suuremmin, kun painaa hyväksy painiketta, mutta on hyvä pitää mielessä, että painamalla hyväksy annat sivulle luvan tietojen keräämiseen ja jakamiseen.



Alla on linkki, jolla voit ladata websovelluksen Chromelle ja Firefoxille, jos olet itse kiinnostunut näkemään omien tietojesi jaon.

Google Chrome:

Thunderbeam-Lightbeam for Chrome - Chrome Web Store (google.com)

Firefox:

Lightbeam – Get this Extension for 🦊 Firefox (en-US) (mozilla.org)

5.2 Kaksivaiheisen tunnistautumisen käyttöönotto

Tilin käyttäjänimen ja salasanan vuotaminen ei aina ole kiinni tilin käyttäjän omista teoista, vaan monissa tietosuojamurroissa nämä kriittiset tiedot voivat vuottaa verkkoon ja niitä myydään eniten maksavalle. Kaksivaiheisen tunnistautuminen antaa tarvittavan suojan siksi aikaa, kun salasana on paljastunut ja sitä ei ole vaihdettu.

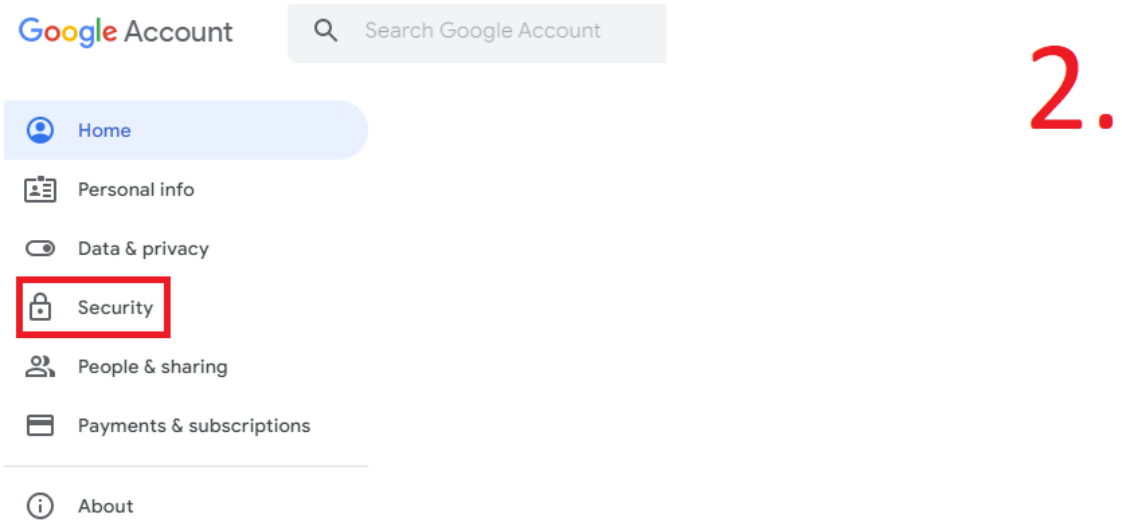
Esimerkki tietovuodosta, joka vuosi noin 6,5 miljoonan ihmisen käyttäjänimen ja salasanan oli vuoden 2012 LinkedIn tapaus. Neljä vuotta myöhemmin LinkedIn huomasi vielä noin 100 miljoonan sähköposti osoitteen ja salasanan vaarantuneen tietomurron yhteydessä. Tämänkaltaisessa tapauksessa kaksivaiheinen vahvistus suojaa sen ajan, kun vaihtaa vuodetun salasanan turvalliseen. Koko tietomurto sai alkunsa, kun hakkeri sai käsiinsä työntekijän käyttäjänimen sekä salasanan ja pääsi kirjautumaan yrityksen palvelimelle. Kaksivaiheisella tunnistautumisella tämä olisi pystytty suurella todennäköisyydellä estämään.

Nettisivussa https://haveibeenpwned.com voit tarkistaa onko sinun sähköpostisi ja/tai salasanasi vuotanut nettiin.

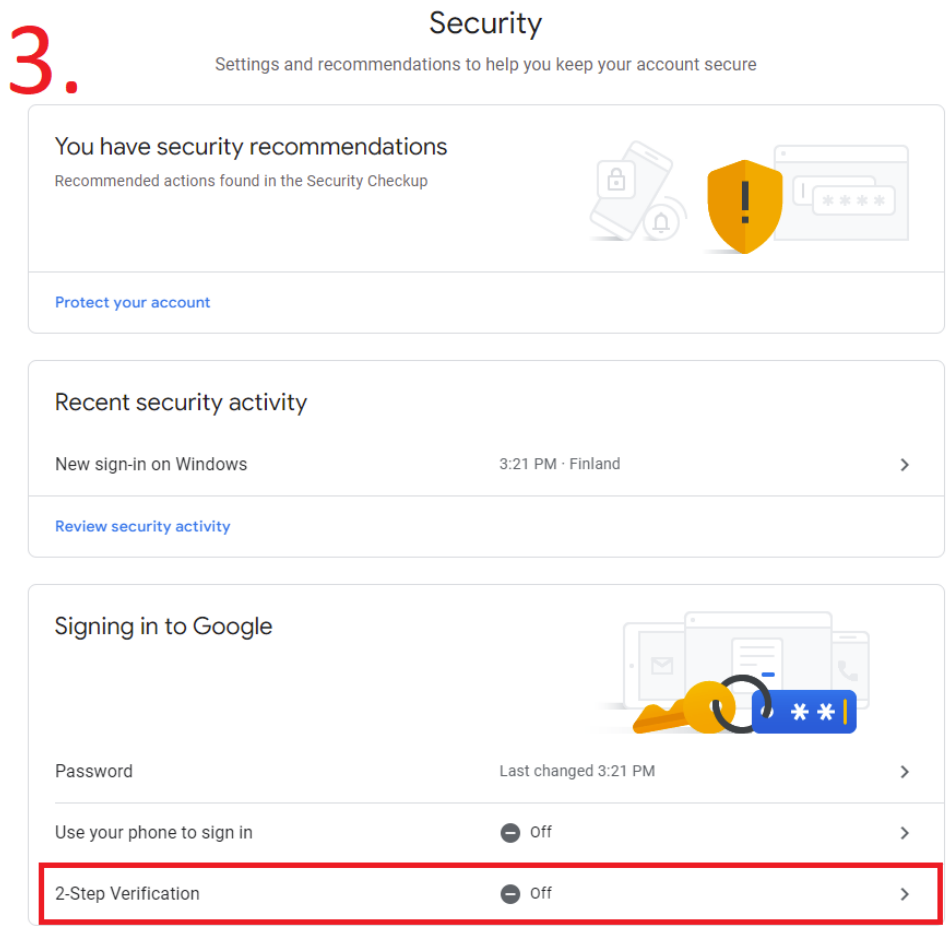
Alla on ohjeita kaksivaiheisen tunnistautumisen käyttöönottoon eri palveluilla:

5.2.1 Kaksivaiheinen Tunnistautuminen Googlessa

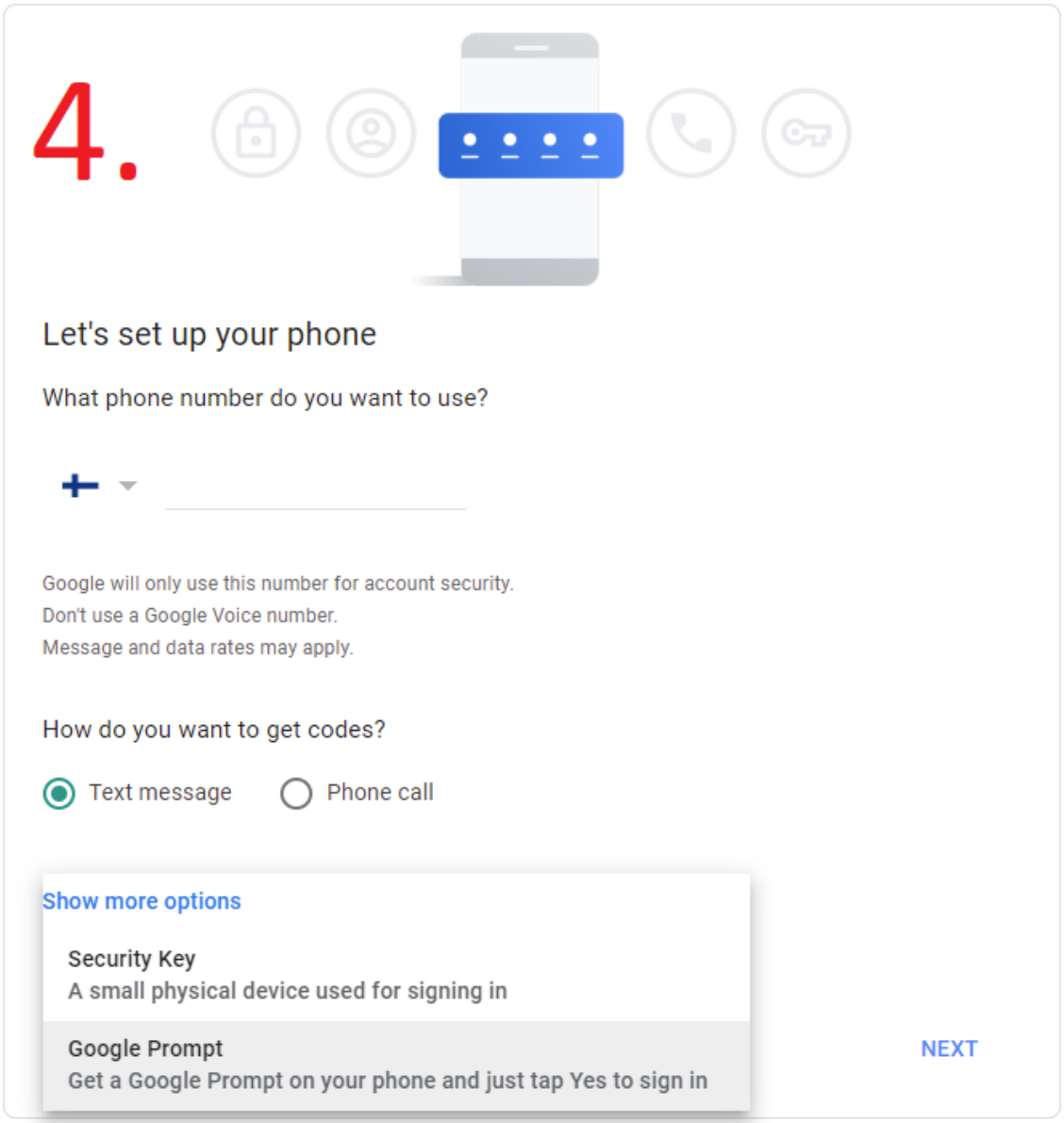
1. Omalta gmail-tililtä voi avata asetus valikon painamalla oikealla yläkulmassa olevaa käyttäjäkuvaketta, josta valitsee **Hallinoi Google-tiliäsi/Manage your Google Account.**



2. Siirrytään **Tietoturva/Security** välilehdelle.

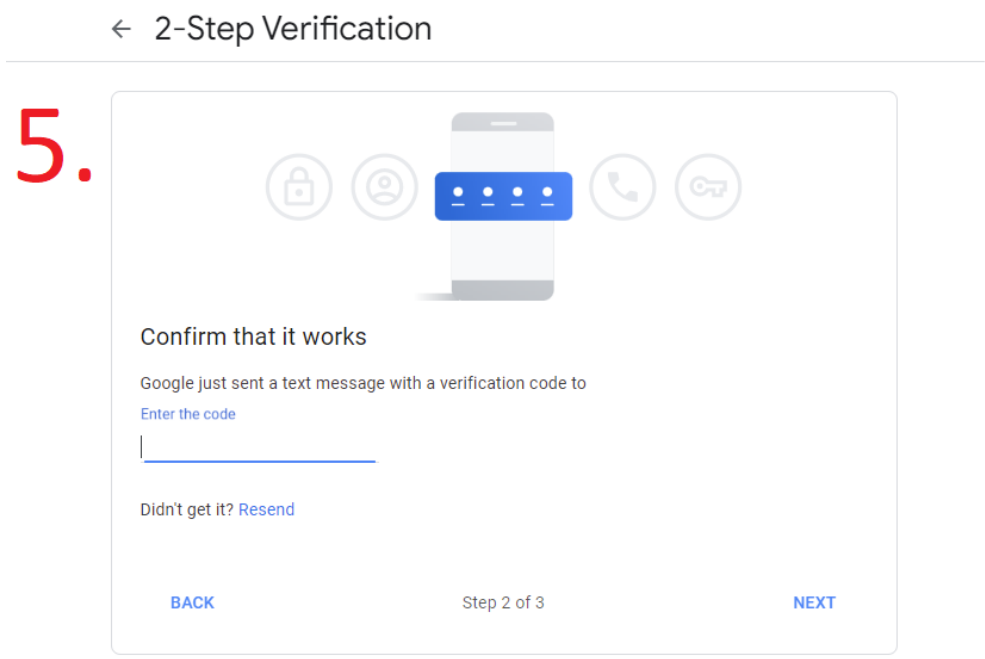


3. **Tietoturva/Security** välilehdeltä löydät **Kaksivaiheinen vahvistus/2-Step Verification** kohdan, jota painamalla pääset aloittamaan kaksivaiheisen vahvistuksen käyttöönoton.



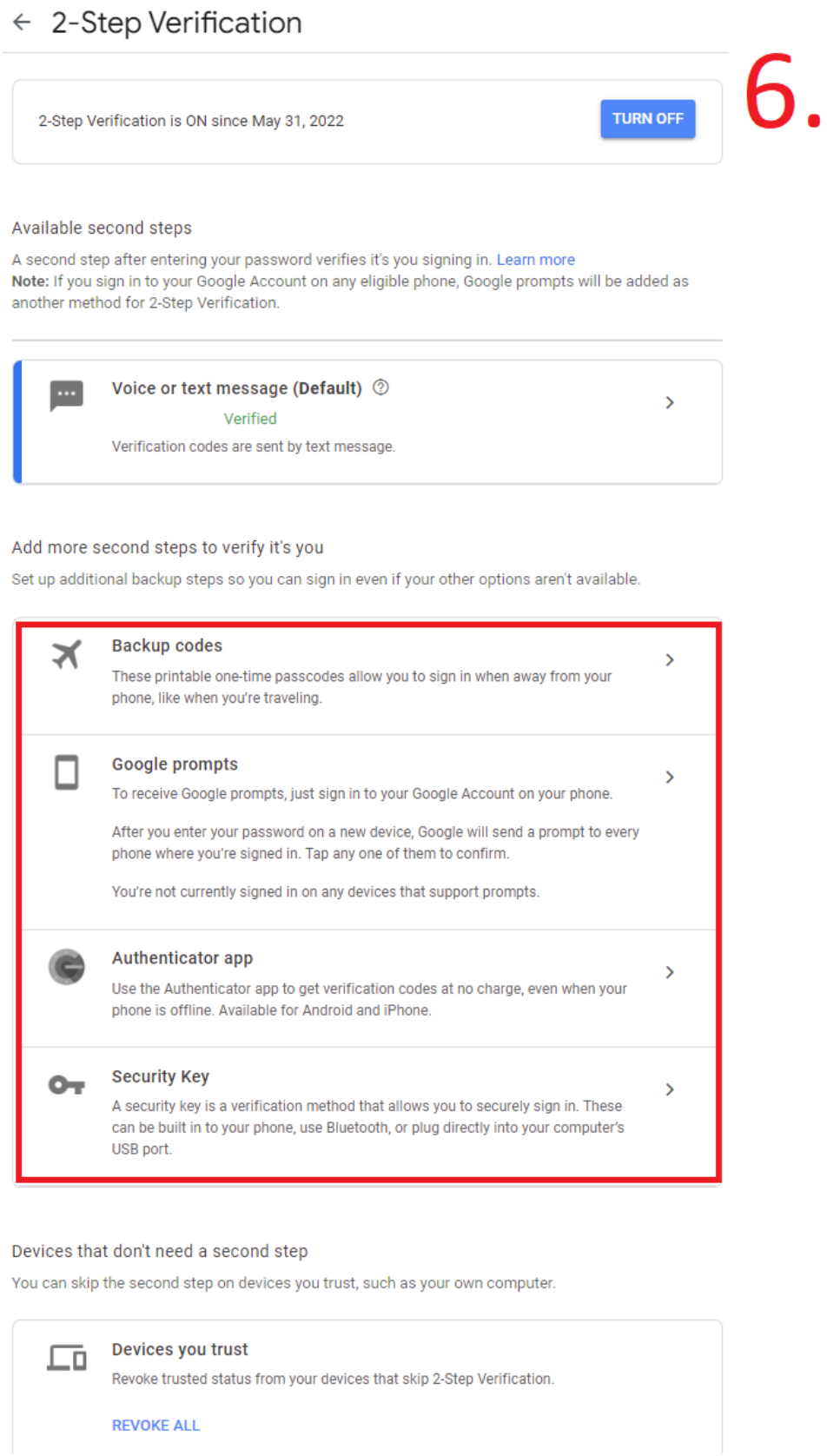
4. Sinun tulee laittaa toimiva puhelinnumero, jotta Google pystyy vahvistamaan tilin omistajan ja samalla aktivoimaan perustason kaksivaiheisen tunnistautumisen. Aina kun kirjaudut tilillesi, saat tekstiviestin, joka sisältää Google vavistuskoodin.

5.

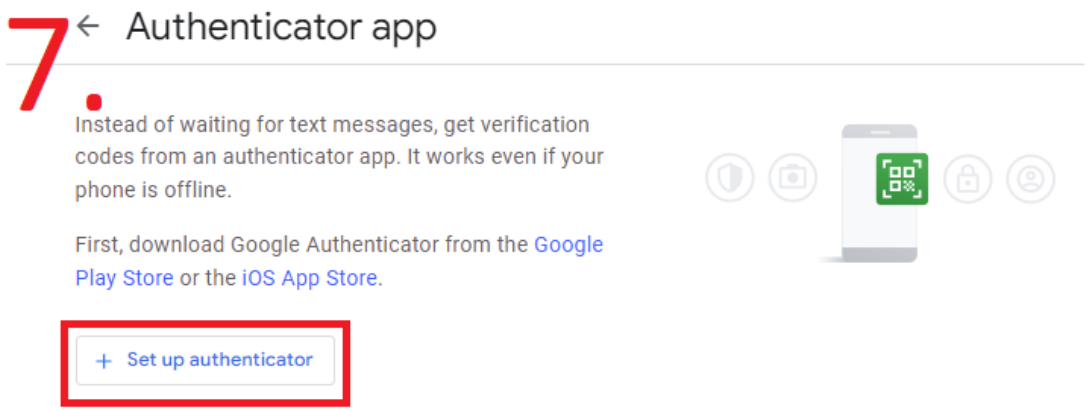


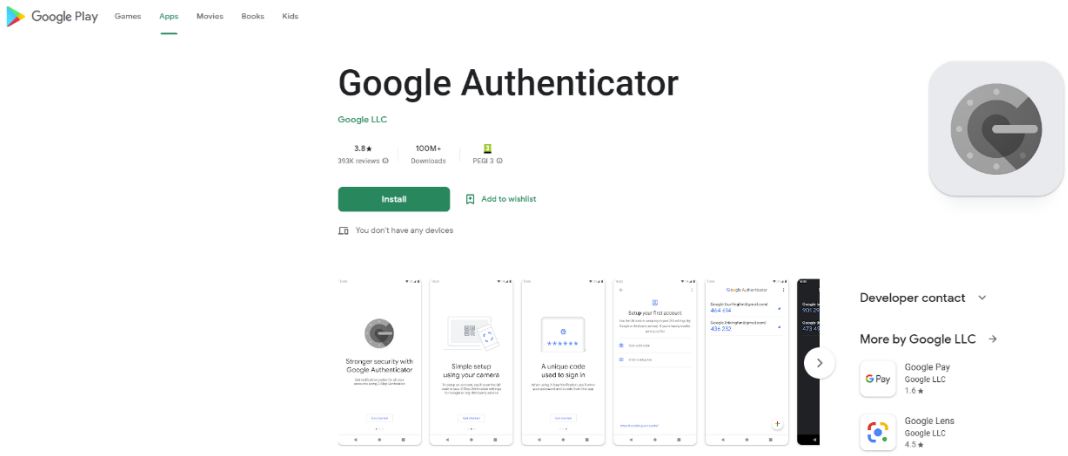
5. Kun saat vahvistuskoodin puhelimeesi, syötä siinä näkyvä numerosarja kenttään. Älä koskaan jaa kyseistä vahvistuskoodia kenenkään kanssa, vaikka sitä pyydettäisiin.

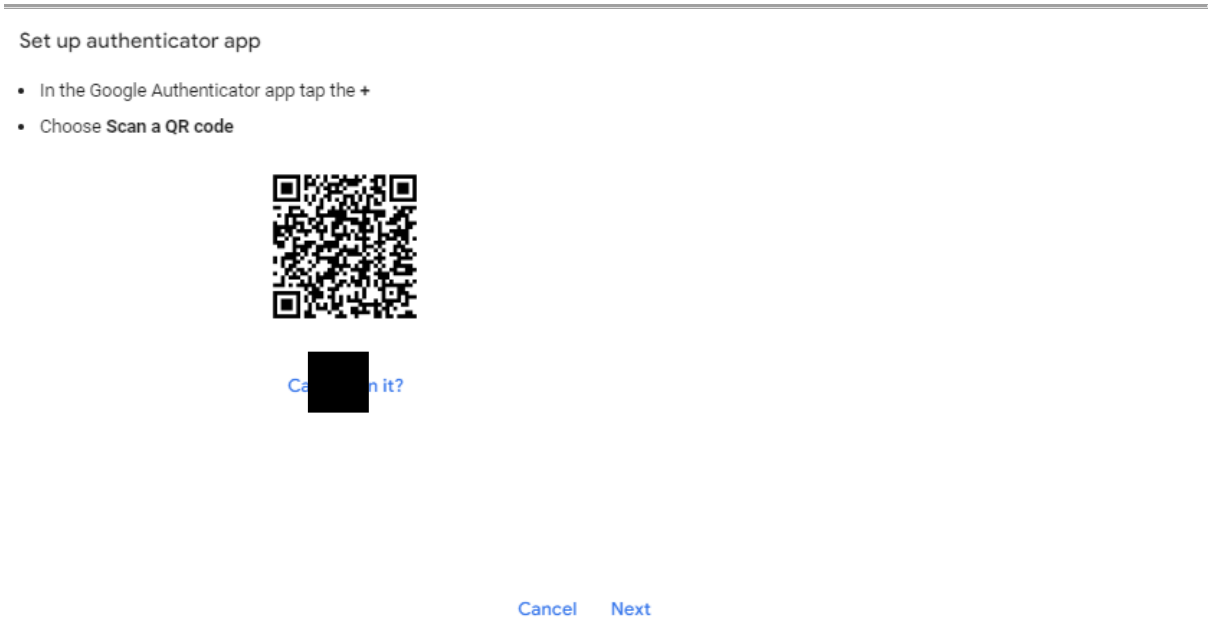
6.


2-Step Verification
2-Step Verification is ON since May 31, 2022
TURN OFF
Available second steps
A second step after entering your password verifies it's you signing in. Learn more
Note: If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.
Voice or text message (Default)
Verified
Verification codes are sent by text message.
Add more second steps to verify it's you
Set up additional backup steps so you can sign in even if your other options aren't available.
Backup codes
These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.
Google prompts
To receive Google prompts, just sign in to your Google Account on your phone.
After you enter your password on a new device, Google will send a prompt to every phone where you're signed in. Tap any one of them to confirm.
You're not currently signed in on any devices that support prompts.
Authenticator app
Use the Authenticator app to get verification codes at no charge, even when your phone is offline. Available for Android and iPhone.
Security Key
A security key is a verification method that allows you to securely sign in. These can be built in to your phone, use Bluetooth, or plug directly into your computer's USB port.
Devices that don't need a second step
You can skip the second step on devices you trust, such as your own computer.
Devices you trust
Revoke trusted status from your devices that skip 2-Step Verification.
REVOKE ALL

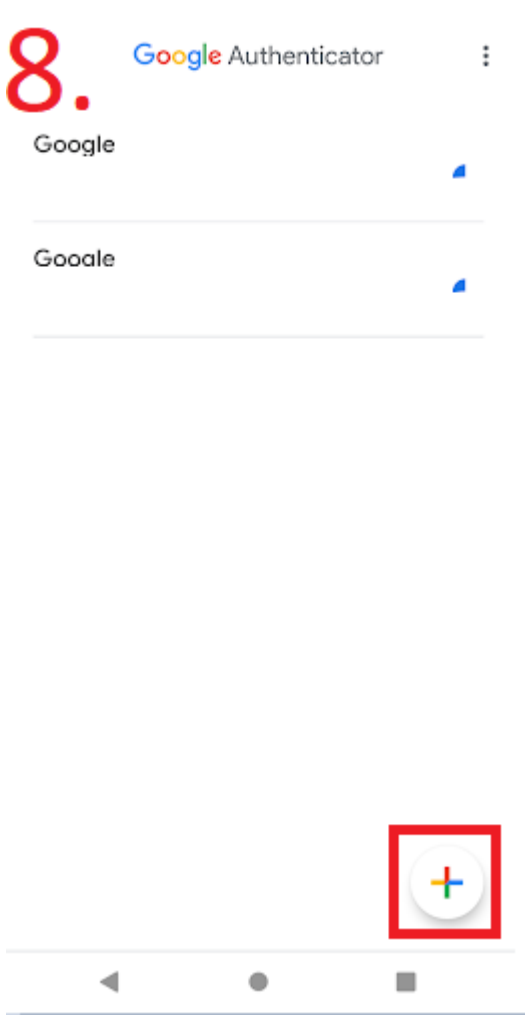
6. Googlella on useita eri keinoja tehdä kaksivaiheinen vahvistus tilille. Näistä voi valita itselleen kaikista mieleisimmän.



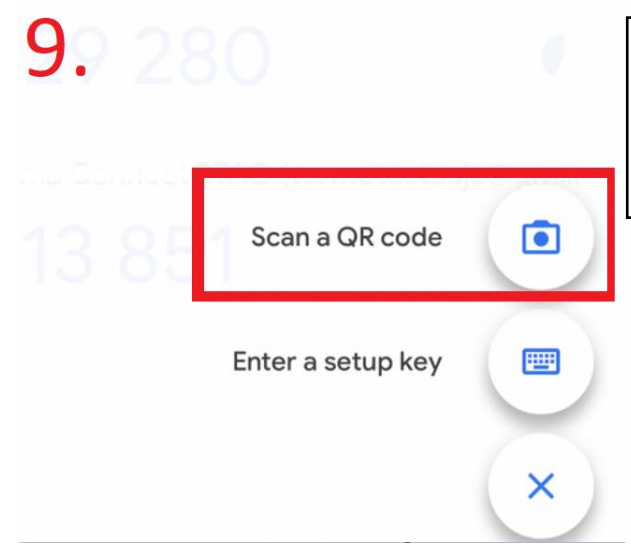




7. Käymme näistä valinnoista läpi sovellus version, joka edellyttää **Google Authenticator** sovelluksen latauksen **Google play** sovelluskirjastosta puhelimelle. Valitse vaihtoehdoista **Authenticator sovellus/Authenticator app** ja paina **Ota todennussovellus käyttöön/Set up authenticator.** Sivulle avautuu QR-koodi, joka tulee kuvata **Google authenticator** sovelluksella.

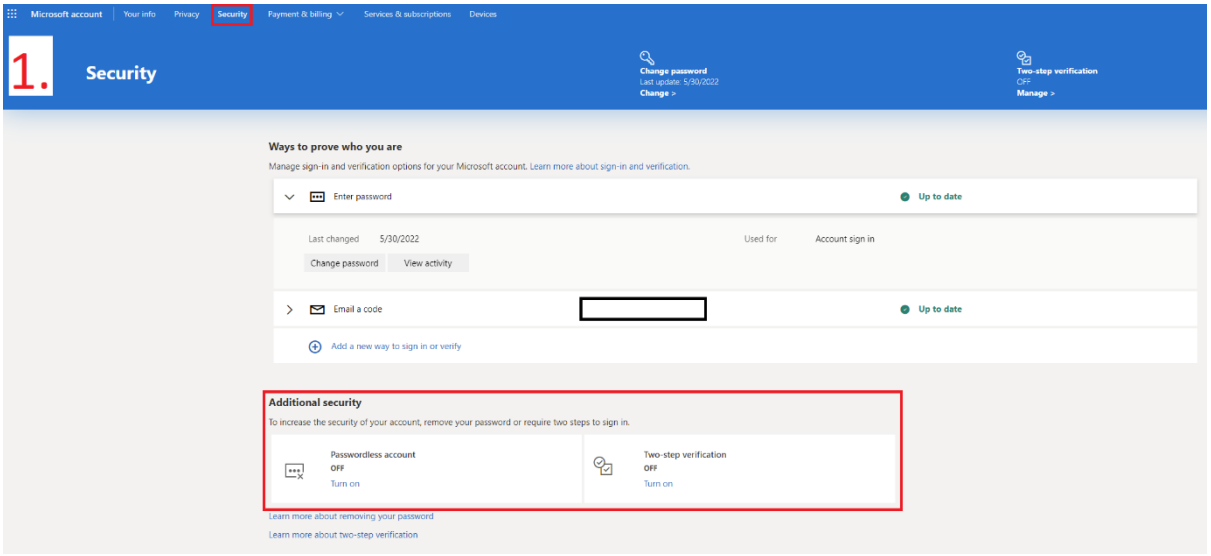


8. Oikeassa alakulmassa on plus merkki, painamalla sitä voit lisätä uuden tunnistautumisen.

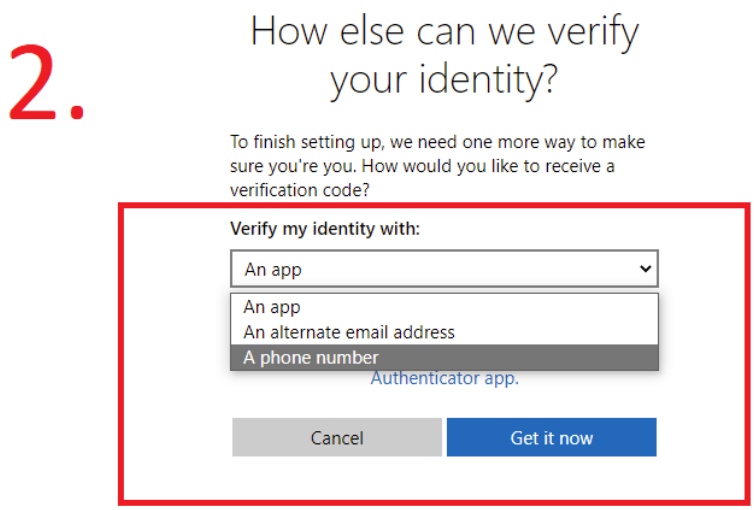


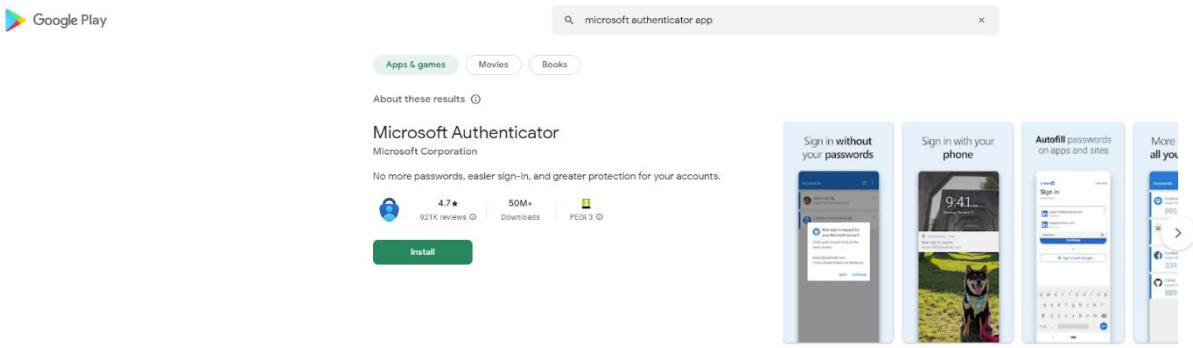
9. Sinulle avautuu valikko, josta valitse **Lue QR-koodi/Scan a QR code**

5.2.2 Kaksivaiheinen Tunnistautuminen Outlookissa

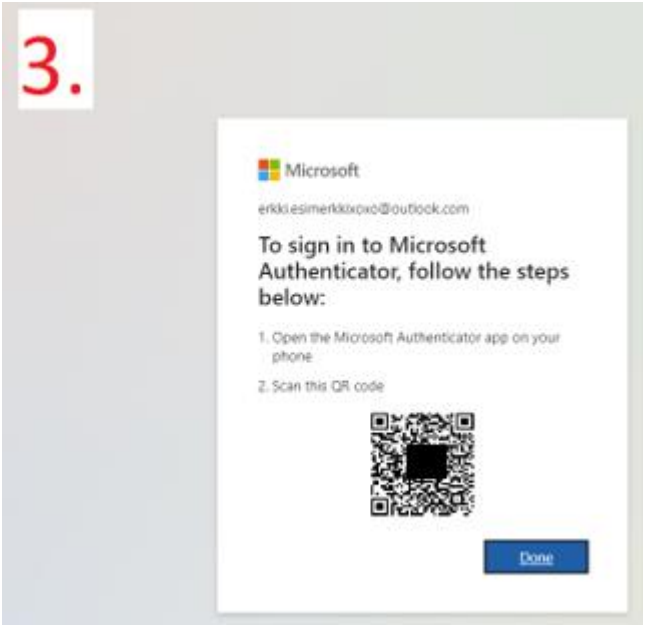


1. Kaksivaiheisen tunnistautumisen käyttöönotto aloitetaan **Security/Tietoturva** välilehden kautta, etsi sivun keskivaiheilta kohta **Additional security/Edistyneet suojausasetukset** ja valitse **Two-step verification/Kaksivaiheinen tarkistaminen** painike.

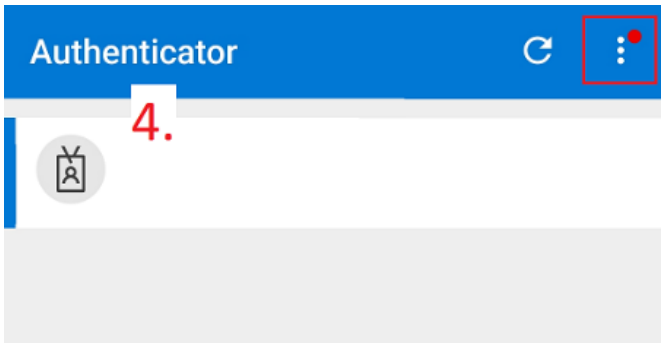




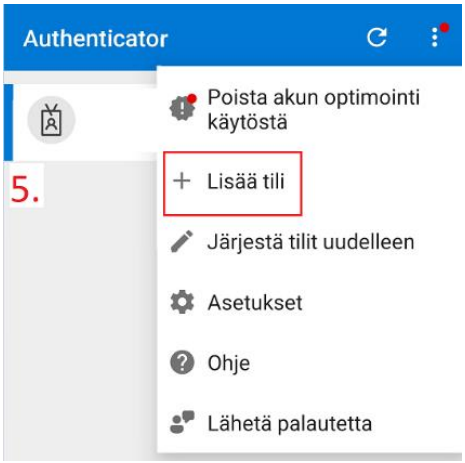
2. Tämä vie sinut sivulle, josta voit valita itsellesi sopivimman vaihtoehdon sähköpostin, puhelinnumeron ja sovelluksen väliltä. Sähköposti ja puhelinnumero ovat näistä vaihtoehdoista helpoimmat mutta jossain määrin vähemmän turvallisia. Jos kuitenkin valitset jommankumman näistä vaihtoehdoista, sinulta kysytään tällä hetkellä käytössä olevaa sähköpostiosoitetta tai puhelinnumeroa. Antamalla jommankumman näistä saat aina kirjautuessasi vahvistusviestin sähköpostiisi tai puhelimeesi, joka sisältää koodin mikä täytyy syöttää.



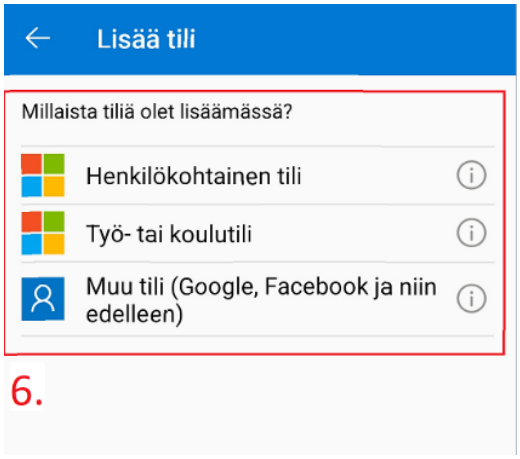
3. Sovellus vaihtoehto vaatii **Microsoft Authenticator** sovelluksen, jonka voi ladata Android laitteilla Google play kaupasta tai Apple laitteilla **App Storesta**. Kun valitset sovellus vaihtoehdon sinulle annettaan QR-koodi, joka sinun tulee kuvata kännykän kameralla.



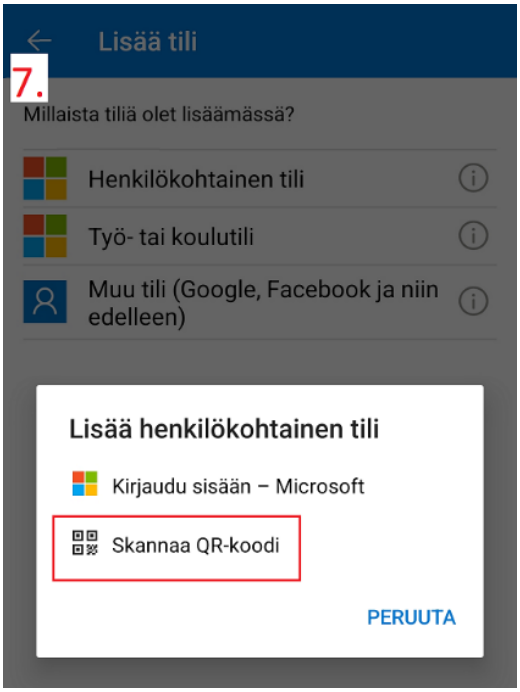
4. Voit kuvata QR-koodin avaamalla **Microsoft Authenticator** sovelluksen puhelimellasi ja painamalla kolmea valkoista palon kuvaketta oikeassa yläkulmassa.



5. Valitse **Lisää tili**.



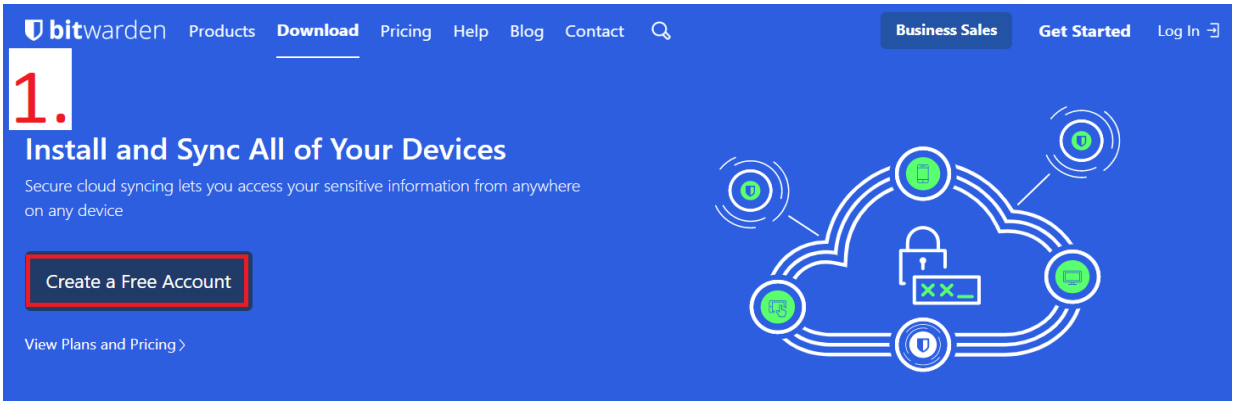
6. Valitse tili, jolle haluat ottaa kaksivaiheisen tunnistautumisen.



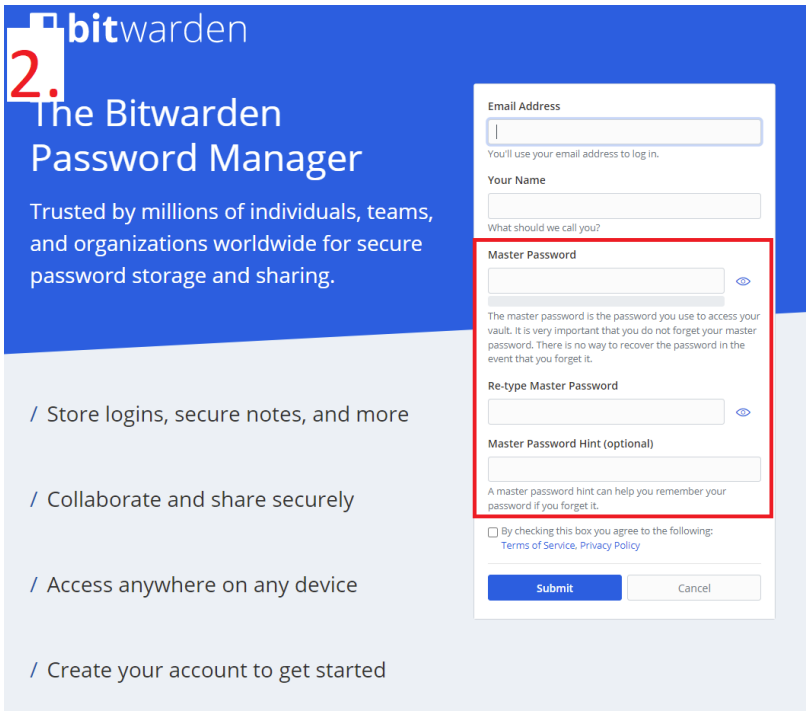
7. Paina **Skannaa QR-koodi**.

5.3 Salasanahallintaohjelmien käyttöönotto

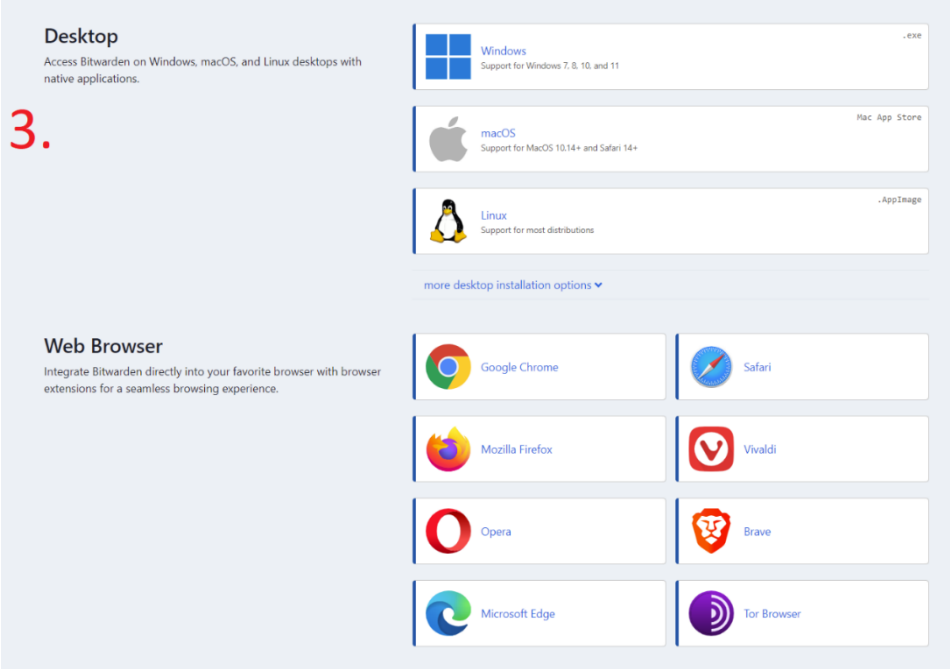
Bitwarden:

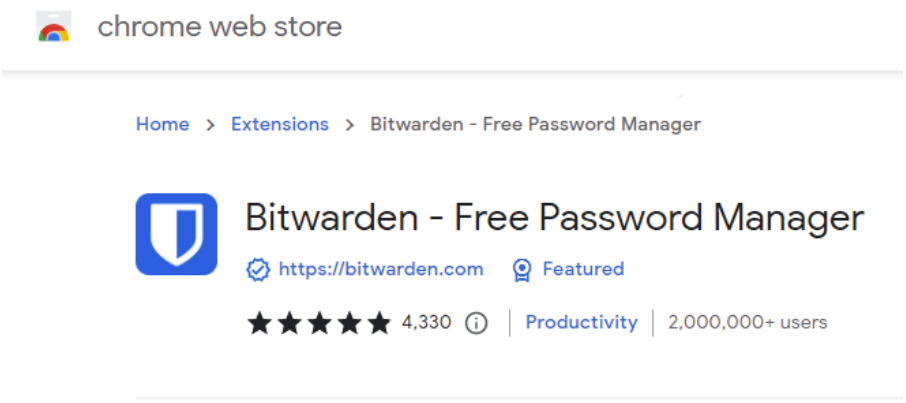


1. Bitwarden on tällä hetkellä salasanahallinta ohjelmien parhaimmistoa. Käymme läpi vähän sen asentamisesta päätelaitteelle ohjeiden avulla. Voit luoda käyttäjän palveluun painamalla **Create Free a Account**.

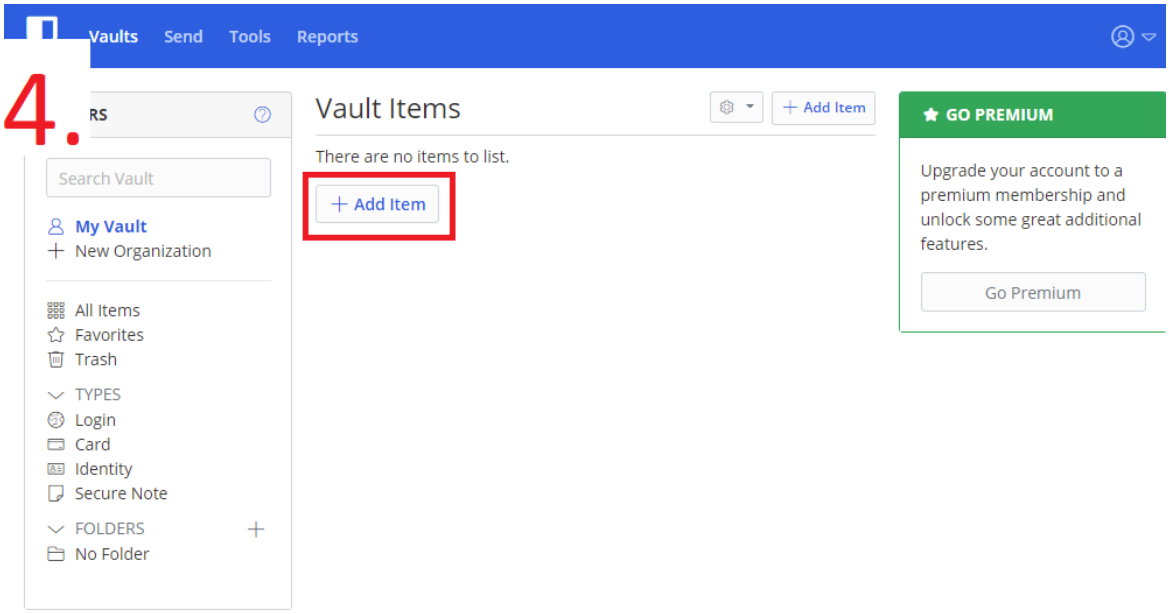


2. Sinun täytyy luoda tunnus, jotta voit käyttää Bitwardenin salasanahallinta ohjelmaa. **ON TODELLA TÄRKEÄÄ, että muistat Master salasanan/Master password**. Tätä salasanaa ei voi luoda uudestaan mitenkään jos sen unohtaa, on siis suositeltavaa kirjoittaa salasana paperille ja piilottaa paperi hyvin. Jos salasanan kadottaa, et todennäköisesti pääse enää käyttämään mitään tilejäsi tai niiden palauttaminen on hyvin vaikeaa. Voit asettaa alussa vinkin salasanaan muistamiseen (Huom. vinkistä kannattaa tehdä vaikeasti arvattavan, johon ei löydy vastausta sosiaalisesta mediasta tai verkosta ylipäätänsä

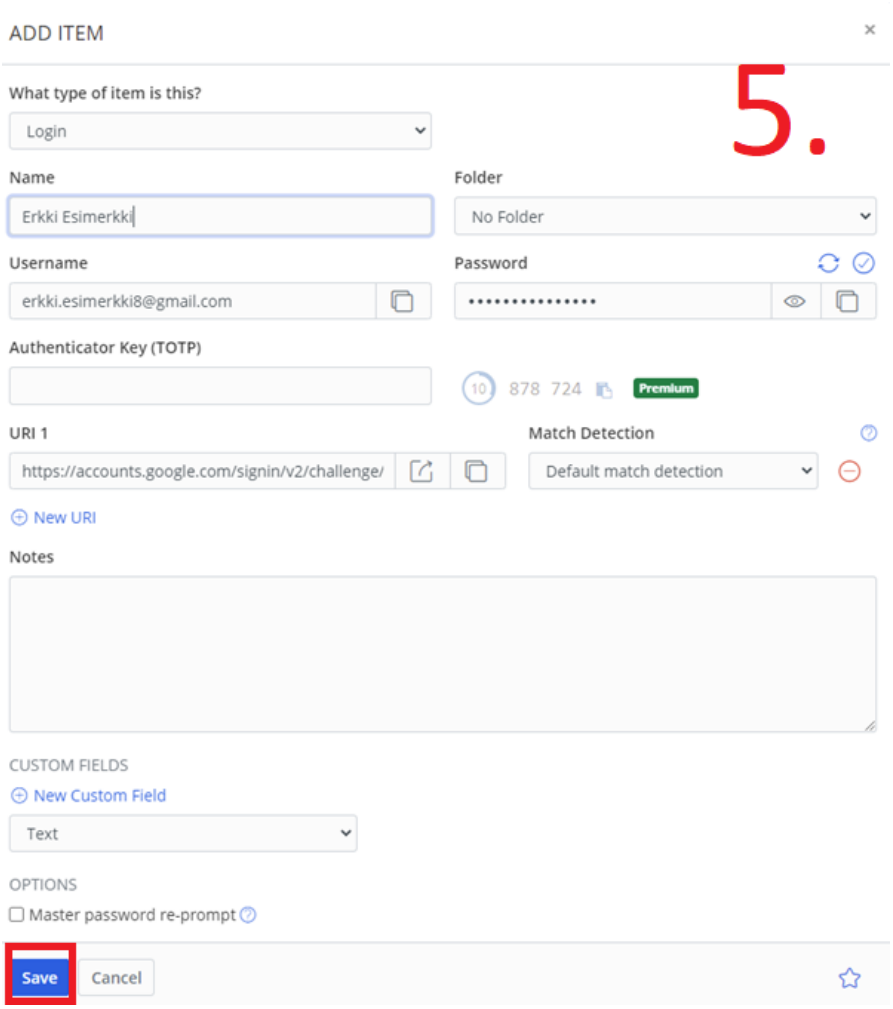


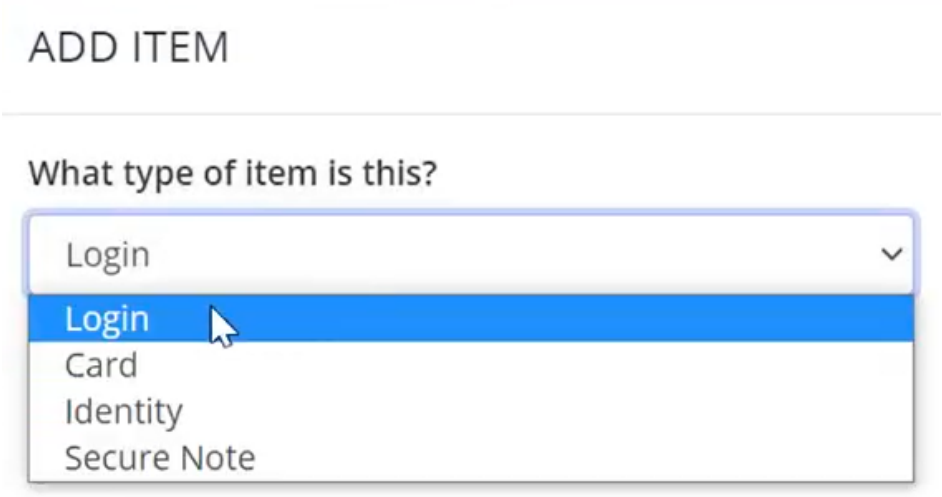


3. Nyt kun tunnus on luotu, ladataan samalla Bitwardenin websovellus. Valitse käyttöselaimesi ja liitä Bitwarden websovellus selaimeen. Voit myös ladata laitteelle sovelluksen Bitwardenin sivulta.



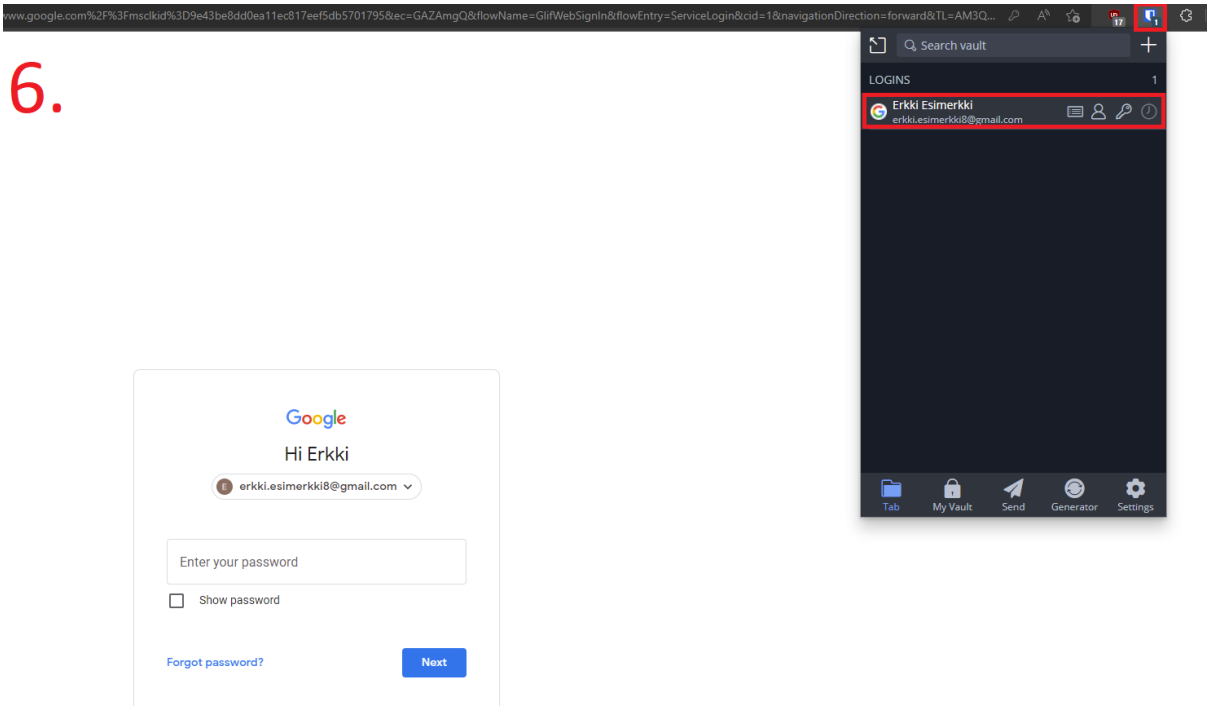
4. Nyt kun tunnus on luotu ja websovellus ladattu, voidaan alkaa lisäämään salasanoja palveluun. Paina **Add item**.


ADD ITEM
5.
What type of item is this?
Login
Name
Erkki Esimerkki
Folder
No Folder
Username
erkki.esimerkki8@gmail.com
Password
Authenticator Key (TOTP)
878 724
Premium
URI 1
https://accounts.google.com/signin/v2/challenge/
Match Detection
Default match detection
New URI
Notes
CUSTOM FIELDS
New Custom Field
Text
OPTIONS
Master password re-prompt
Save
Cancel


ADD ITEM
What type of item is this?
Login
Login
Card
Identity
Secure Note

5. Eteesi avautuu tietojen syöttö laatikko, se voi aluksi näyttää monimutkaiselta mutta on lopuksi varsin helppo operoida.
    a. **Add item:** Voit valita minkä tyyppisen tiedon haluat tallentaa. **Login** tarkoittaa kirjautumista, **Card** tarkoittaa maksukorttia, **Identity** tarkoittaa usein laskutusosoitteiden tai sähköposti ja posti tietojen täyttämistä, **Secure notes** tarkoittaa salattua vapaamuotoista tekstikenttää.
    b. **Name:** tähän voi laittaa sivun nimen, jotta se on itse helppo tietää mihin palveluun salasana kuuluu
    c. **Username:** Käyttäjätunnus sivulle, jolle haluat kirjautua.
    d. **Password:** Salasana, jota käytät sivulla tai palvelussa.
    e. **URI 1:** kirjautumissivun URL-osoite
    f. Kaikki muut kohdat ovat vapaaehtoisia, voit täyttää niitä helpottaaksesi kirjautumista tai tehden siitä vielä turvallisemman.

6.



6. Kun olet saanut kirjautumistiedot täydennettyä, siirry haluamallesi kirjautumissivulle, jolle teit kirjautumisen ja paina oikeassa yläkulmassa olevaa Bitwardenin logoa. Valitse oikea kirjautuminen valikosta, Bitwarden täyttää tiedot automaattisesti.

6 Sosiaalinen media ja verkkokauppa

6.1 Sosiaalinen media

Monet käyttävät sosiaalista mediaa nykypäivänä moniin tarkoituksiin, kuten oman yrityksen mainostamiseen tai vain yhteydenpitoon läheisten tai sukulaisten kanssa. Moni ei kuitenkaan tiedä, että rikolliset käyttävät sosiaalista mediaa hyödyksi keräämällä tietoa uhreistaan tai kohteistaan. On siis tärkeää miettiä tarkkaan, mitä asioita kannattaa jakaa ja mitä ei.

- On tärkeää muistaa, että itselle pieni ja vähäpätöinen tieto voi olla rikolliselle arvokas pala informaatiota.
    - Monet turvakysymykset voivat kysyä koiran nimeä, ensimmäisen opettajan nimeä tai peruskoulun lempiainetta.

    - Rikolliset etsivät tämäntyyppisiä tietoja kahdesta syystä. Ensimmäinen on turvakysymyksiin vastaaminen ja toinen on löytää vihjeitä salasanan arvaamisen suhteen. Salasananmurto ohjelmiin voi syöttää esimerkki sanoja, joita apuna käyttäen salasanamurto ohjelma käy läpi miljoonia eri salasana yhdistelmiä, kunnes salasana murtuu.
    - Yksi tosielämän esimerkki tapahtui vuoden 2008 Yhdysvaltojen presidentinvaalien aikaan. 20-vuotias yliopisto-opiskelija hakkeroi vaaliehdokkaan Yahoo -sähköpostitilin, käyttämällä turvakysymyksiä, joihin sai vastaukset Wikipediasta ja sosiaalisesta mediasta. Tämän avulla yliopisto opiskelija sai haltuunsa sähköposti tilin ja pääsi tutkimaan sen sisältöä. Osa tästä sisällöstä vuodettiin yleisille keskustelufoorumeille.
- Hyvä nyrkkisääntö sosiaalisen median suhteen on pysähtyä hetkeksi ja miettiä kahteen kertaan onko tämän kuvan tai tilannepäivityksen laittaminen sosiaaliseen mediaan järkevää. Pidä nämä mielessä, kun julkaiset itsestäsi jotain:
    - Sisältääkö kuva tai tilannepäivitys liikaa informaatiota? (työpaikka, läheiset ja ystävät). Huom! Valokuvien metatiedoista voi paljastua enemmän tietoa, kuin haluaisit.
    - Sisältääkö julkaisu tunnistustietoja (osoite, kadunnimi, auton rekisteriote)
    - Kaikki minkä verkkoon julkaiset, pysyy siellä.

Alla on Valkohattuhakkerin vinkkejä itsensä suojaamiseen verkossa:

Hakkeri Laura Kankaala ei halua kertoa edes ikäänsä julkisuuteen – nyt hän vinkkaa, miten omia tietoja kannattaa suojata netissä | Oppiminen | yle.fi

Videoissa ihmiset kertovat salasanojensa osia, kun niitä kysytään:

What is Your Password? - YouTube

6.2 Verkkokauppa

Monet yritykset pyörittävät verkkokauppaa lisätäkseen myyntiä ja samalla monet yritykset sekä yksityishenkilöt ostavat verkkokaupoista tuotteita itselleen. Verkkokauppa on hieno tapa myydä ja tilata, mutta siinäkin on omat vaaransa.

- Oman verkkokaupan pyörittämisessä tulisi ottaa sivun tietoturva huomioon.
    - Jos käyttää kolmannen osapuolen websivu palveluita (esim. Wordpress, Squarespace) tulisi näissä pyrkiä suojaamaan omat käyttäjätunnukset mahdollisimman hyvin. Tästä kerromme lisää koulutuksissamme.
- Verkkokaupasta ostaessa tulisi ottaa muutama asia huomioon, jotta osto tapahtuu turvallisesti.
    - Sivun nimi kannattaa aina tarkistaa nopealla Google haulla ja sivusta tulisi etsiä kolmannen osapuolen arvosteluja.
    - Kaupasta kannattaa etsiä sosiaalisen median profiileja ja tutkia ovatko nämä aidon näköisiä.
    - Ovatko maksutavat erikoisia? Jos maksut pyydetään suorittamaan maksusovelluksilla (esim. Venmo, Zelle, Cach App), lahjakorteilla tai kryptovaluutalla, on sivu melko suurella todennäköisyydellä rikolliseen toimintaan liittyvä. Näitä rahanmaksu keinoja ei voi jäljittää helposti tai ne eivät tarjoa mahdollisuutta uhrille saada rahojaan takaisin.

- Verkkokaupat saattavat myös varastaa pankki- ja maksutietoja, tämän takia kannattaa tutkia huolellisesti verkkokauppaa ennen ostopäätöstä.

Käymme vielä läpi hyviä kolmannen osapuolen websivu palveluita ja listaamme turvallisuuden ja GDPR:än suosituimpien palveluiden välillä:

WiX:

Turvallisuus:

- Turvallisuus on hyvä laatuista ja WiX tekee paljon turvallisuuden eteen.
  - Bug Bounty ohjelma
  - Penetraatio testaukset
  - Useat datakeskukset Amerikassa, Irlannissa ja Israelissa
  - Käyttäjätunnusten salaus
- Käyttäjät pystyvät käyttämään kaksivaiheista tunnistusta ja muita turvallisuus palveluja käyttäjätunnusten turvaamiseen

GDPR:

- WiX noudattaa GDPR:än kaikkia pykäliä.
  - Tietojen muokkaus ja saaminen on mahdollistettu joko suoraan WiX tilin kautta tai asiakaspalveluun yhteyttä ottamalla.
  - Omien henkilökohtaisten tietojen poistaminen ei ole mahdollista ilman koko Wix tilin poistamista. WiX tilin poistaminen tarkoittaa WiX palvelujen menettämistä ja palvelun käytön lopettamista.

  - Jos pyörität omaa websivua WiX:in kautta, voit käyttää palvelun omia työkaluja asiakkaittesi tietojen antamiseen, muokkaamiseen ja poistamiseen.
  - WiX kerää tietoja käyttäjistä, jotka käyvät WiX:in tarjoamassa ostetussa nettisivussa. Näihin tietoihin lukeutuu esim. sähköposti ja evästeet sivujen välillä.

- Mitä tietoja WiX kerää:
  - Sähköposti
  - Postiosoite
  - Laskutus tiedot
  - IP-osoite
  - Web selain
  - Käyttöjärjestelmä
  - Painallukset
  - Paikkasijainti

- Huomioitavaa:
  - Tietojen siirtäminen WiX:in ja muiden samankaltaisten palveluiden välillä on todella haastavaa. Kaikkea mitä olet WiX:in omassa palvelussa tehnyt tai luonut ei siirry tai tallennu, jos WiX tilin menettää tai WiX syystä tai toisesta lopettaa toimintansa.

Squarespace:

Turvallisuus:

- Turvallisuus on yleisesti hyvällä tasolla
  - Penetraatio testaukset
  - Useita datakeskuksia ympäri maailmaa, joilla varmistetaan palvelujen jatkuvuus
  - Käyttäjätunnusten salaus
- Käyttäjät pystyvät käyttämään kaksivaiheista tunnistusta ja muokkaamaan sivun oikeuksia

GDPR:

- Squarespace noudattaa todella hyvin GDPR:n sääntöjä
  - Tietojen muokkaus, saaminen ja poisto onnistuu osaksi palvelun kautta tai asiakaspalvelun kautta
  - Tietoja voi poistaa ilman koko tilin poistamista
  - Kaikkia tietoja ei kuitenkaan välttämättä poisteta, vaikka tili poistettaisiin tai palvelu sopimus päättyisi. Tähän syyksi annettaan lainvaatimat määräykset tai myöhempi palaaminen palveluun.
  - Sivusi kävijöiden tietojen antaminen, muokkaaminen ja poistaminen pitää tehdä Squarespacen:in kautta, ottamalla heihin yhteyttä suoraan.

- Mitä tietoja Squarespace kerää:
  - Sähköpostiosoitteen
  - Etu ja sukunimen

- Osa maksutiedoista (maksukortin 4 viimeistä numeroa, maan jossa kortti on myönnetty sekä vanhentumispäivämäärä maksukortille)
- Yhteystietoja, jotka on sivulle annettu
- IP-osoite, aikaisemmin vierailemasi sivut, selaintiedot, verkkotiedot ja laite tiedot

Wordpress:

Turvallisuus:

- Wordpress ei tietosuojaselosteessaan selitä avoimesti turvallisuus käytännöistään, mutta käyttäjälle on selitetty omat turvallisuus asiansa varsin hyvin.
- Käyttäjällä on paljon mahdollisuuksia parantaa omaa turvallisuuttaan palvelussa esim:
  - Omien tietojen jakamisen rajoittaminen (palvelulle sekä mainostamiselle ja markkinoinnille)
  - Mobiililaitteiden tietojen jako palvelulle
  - Käyttäjät pystyvät käyttämään kaksivaiheista tunnistusta ja sitä suositellaan käytettäväksi

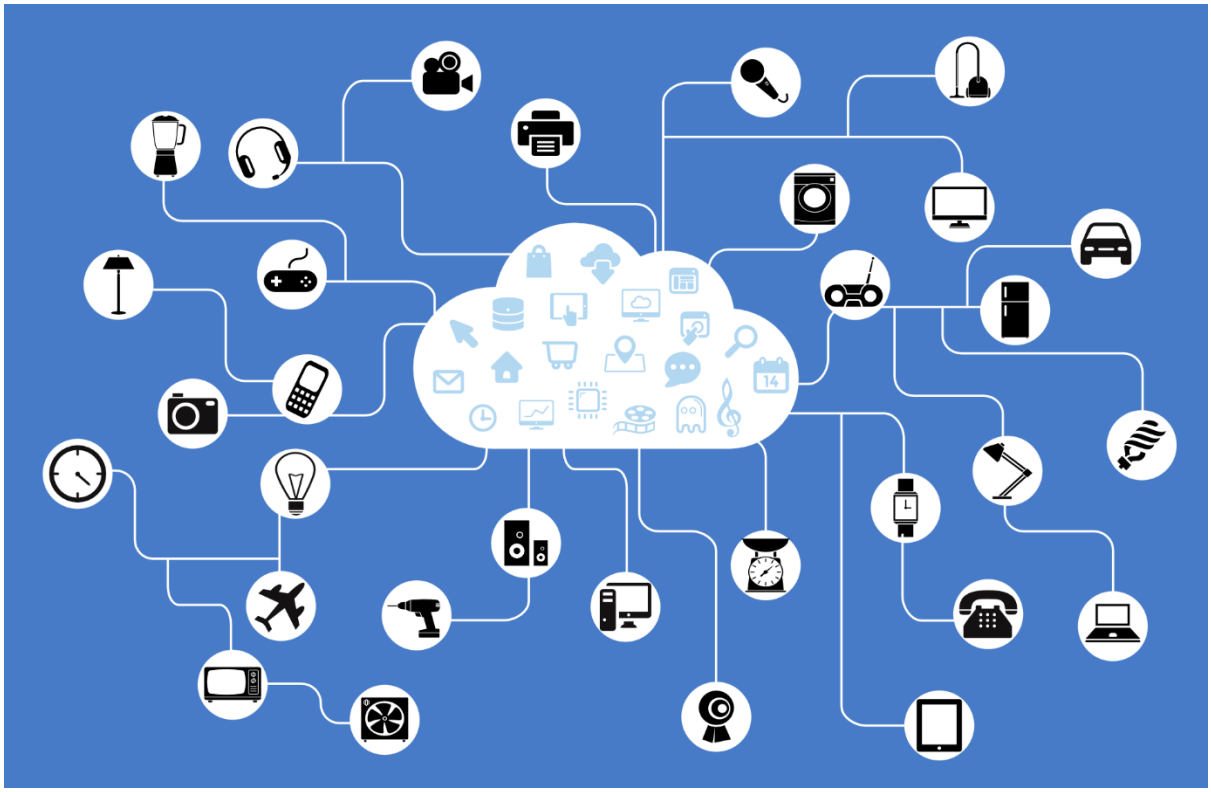
GDPR:

- Wordpress on todella avoin siitä mitä tietoja palvelu kerää ja siitä, miten tiedot kerätään. Kaikkia tietoja pystytään muokkaamaan, saamaan ja poistamaan ilman vaikutusta palveluun.
  - Palvelun sisäisillä asetuksilla pystyy saamaan, muokkaamaan ja poistamaan tietoja itseltä tai käyttäjiltä, jotka käyttävät tekemääsi Wordpress sivuasi.

- Jos palvelun lopettaa, tietoja säilytetään 30 päivää, jonka jälkeen tiedot poistetaan. Sama pätee myös tietoihin, jotka eivät ole tärkeitä palvelun toimivuuden kannalta.

- Mitä tietoja Wordpress kerää:
  - Tilin luomiseen tarvittavat tiedot (nimi, sähköposti, salasana)
  - Maksutietoja
  - Mahdolliset yritys tai yhtiö tiedot
  - Joitain suojaus tietoja tiliin liittyen
  - IP-osoite, selain, laitekohtaiset tiedot
  - Sijaintitiedot
  - Mobiililaitteiden tiedostoja (sovellukselle pitää antaa lupa)

7 Mobiililaitteet ja internetiin kytketyt laitteet osana yrityksen kyberturvallisuutta



7.1 Mobiililaitteiden turvallisuus

Mobiililatteiden yleistymisen myötä on niissä olevan tiedon määrä samalla kasvanut. Tämä tieto on houkutteleva kohde kyberrikollisille. Onkin tärkeää osata varautua uhkiin ja hoitaa mobiililaitteiden turvallisuus ajan tasalle.

- Vuonna 2022, 75 % kaikista tietojenkalastelu sivuista kohdistui pääsääntöisesti mobiililaitteisiin.
- Haittaohjelmat leviävät nykyään puhelimissa lähes yhtä tehokkaasti kuin tietokoneissa
    - Syitä ovat useat haavoittuvuudet sekä puhelimien vanhempien mallien päivitystuen loppuminen.

7.2 Kuinka suojata mobiililaitteet

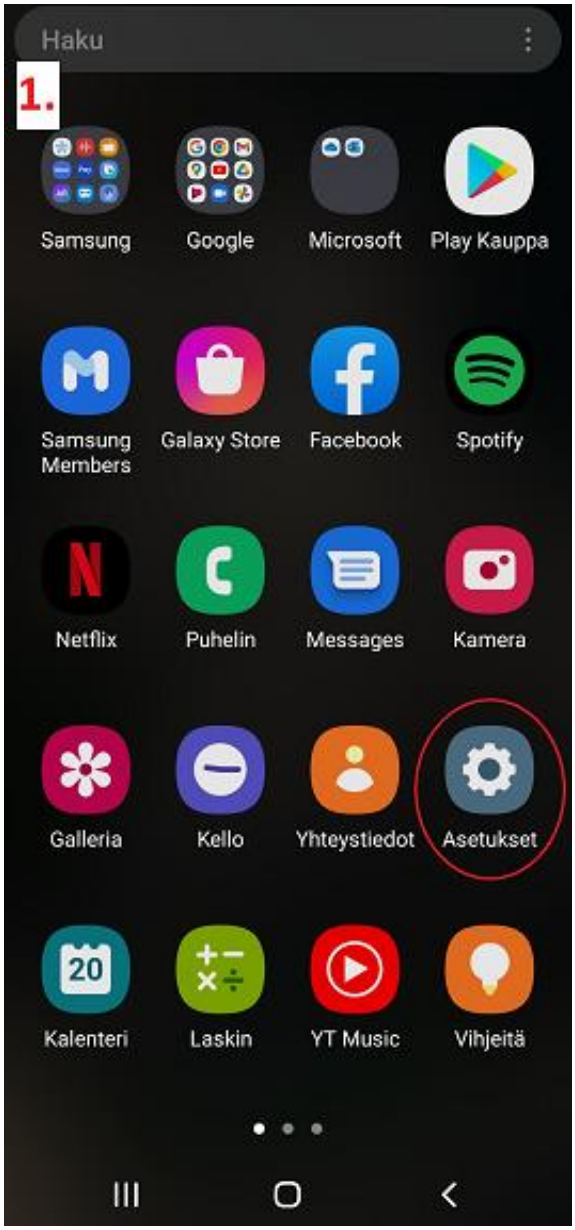
- Jos puhelimessa on SIM-kortti, tulisi sen oletus PIN-koodi vaihtaa.

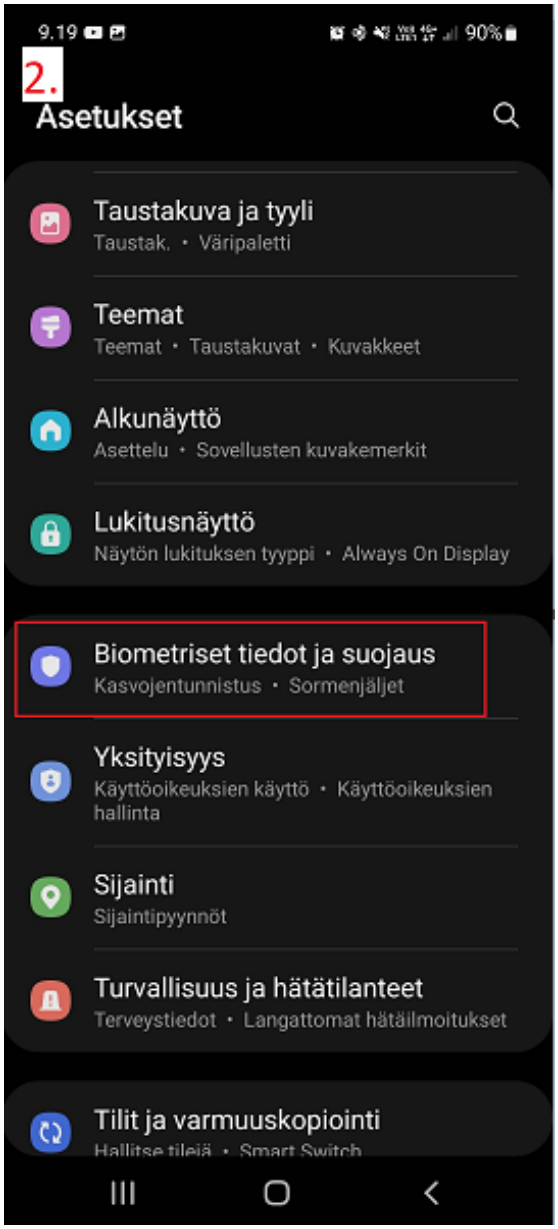
- Varmista puhelimen näytönlukitus joko PIN-koodilla tai kuviolla, pyri tekemään lukituksesta mahdollisimman vaikeasti arvattava.

- Muista myös, että haittaohjelmat tarttuvat myös herkästi mobiililaitteisiin. Tämän takia mobiililaitteita tulisi kohdella kuten tietokoneita.
    - Älä avaa tekstiviestien kautta tulevia linkkejä tai lataa ohjelmia.
    - Sama pätee myös sähköpostiviesteihin.
    - Muista myös, että sovelluskaupat eivät ole aina täysin turvallisia. Monet haittaohjelmat ovat päässeet livahtamaan tarkastuksien välistä ja päätyneet saastuttamaan puhelimia haittaohjelmilla.

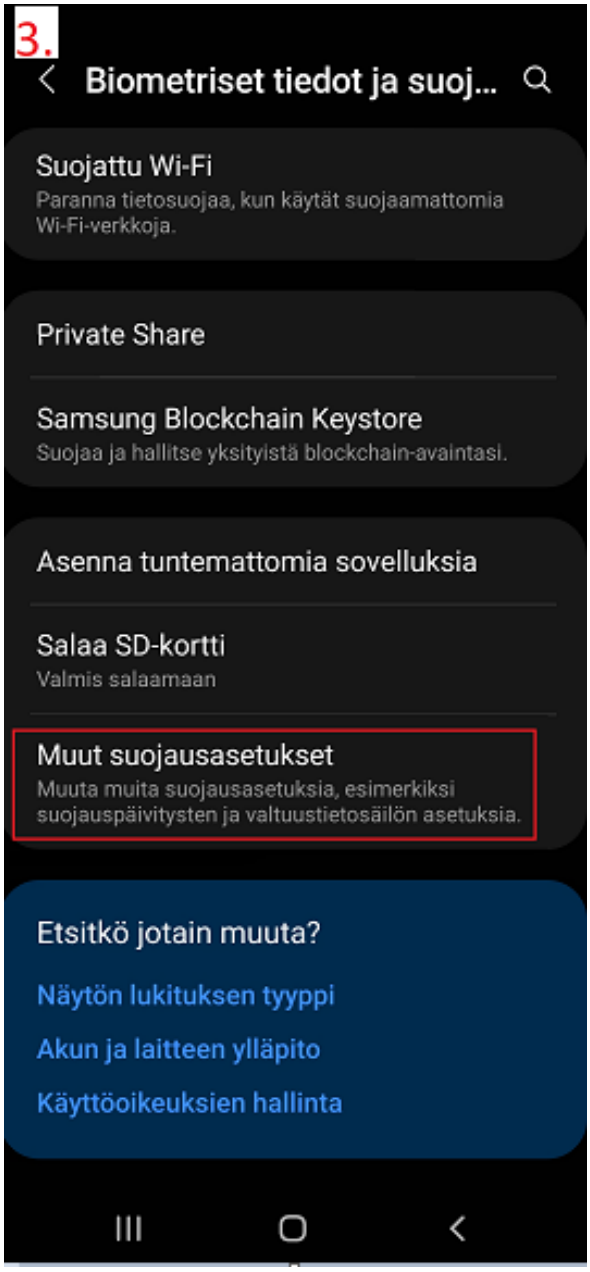
- Vaikka puhelimeen ei pääsisi sisään, on SIM-kortin irti ottaminen silti helppoa. SIM-kortin avulla voi tehdä lukuisia eri hyökkäyksiä eri henkilökohtaisia palveluja kohtaan.
    - SIM-kortin irti ottamisella on mahdollisuus päästä SIM-korttiin tallennettuihin yhteystietoihin.
    - Jos sähköpostiin tai sosiaalisen median tiliin on yhdistetty palautus puhelinnumero, SIM-kortin irti ottamisella voi pyytää varmistuksen tulemaan puhelimeen tekstiviesteillä.

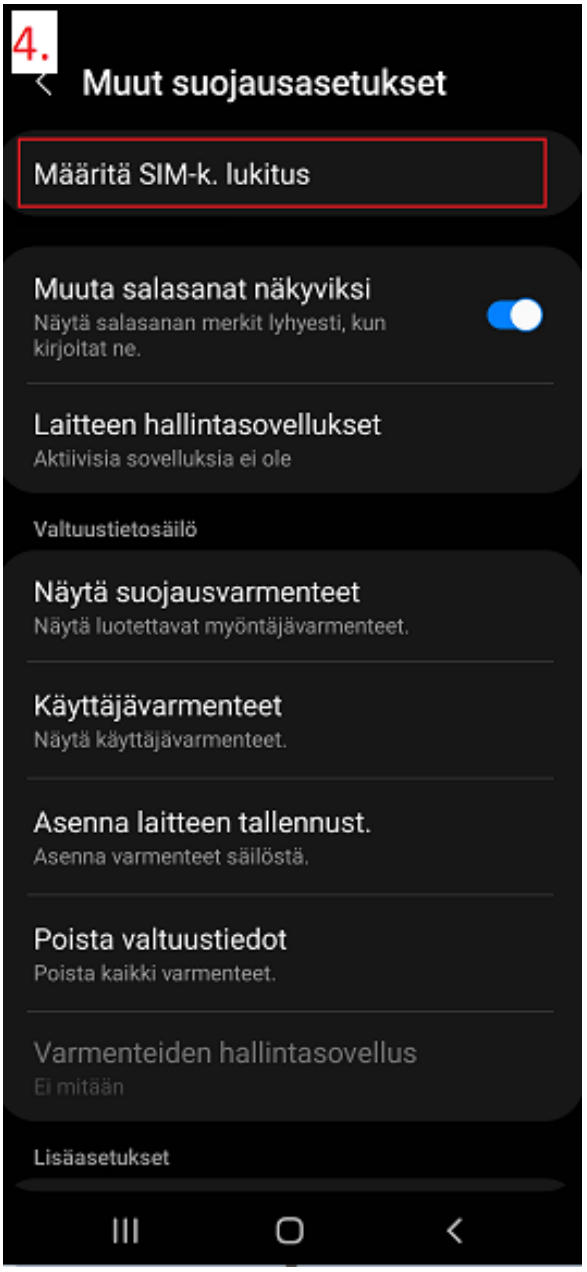
Ohjeet miten SIM-kortin lukitus vaihdetaan Android puhelimessa:





1. Aloita etsimällä **Asetukset/Settings** painike valikosta.
2. Etsi asetuksista kohta **Biometriset tiedot ja suojaus/Biometrics and security.**

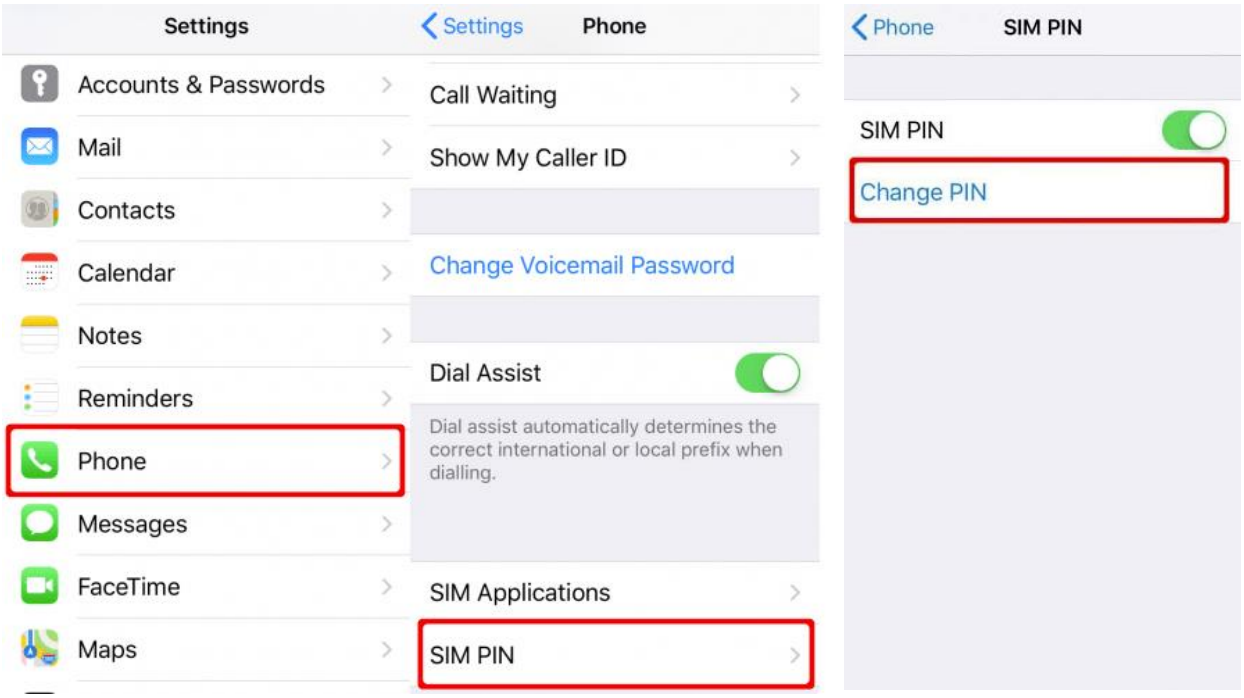




3. Selaa alas ja valitse **Muut suojausasetukset/Other security settings.**
4. Valitse **Määritä SIM-k. lukitus/Set up SIM card lock.**

5. Valitse **Vaihda SIM-k. PIN-koodi/Change SIM card PIN**, tämän kautta voit vaihtaa SIM-kortille tarkoitetun nelinumeroisen PIN-koodin. Pidä tämä PIN-koodi muistissa, koska sitä tarvitaan aina silloin kun puhelin käynnistetään uudelleen.

Ohjeet miten SIM-kortin lukitus vaihdetaan Apple puhelimessa:



1. Etsi valikosta **Settings/Asetukset**
2. Asetuksista löytyy kohta **Puhelin/Phone**, jota painamalla pääsee käsiksi SIM-kortin asetuksiin
3. Valikosta löytyy asetus **SIM-kortin PIN/SIM PIN**
4. Painamalla **Vaihda PIN/Change PIN** voi vaihtaa PIN koodia

Puhelimiin erikoistuneet haittaohjelmat ovat yleistyneet jo pitkään kybermaailmassa. Samoin kuten tietokoneille, myös puhelimiin on saatavilla virustorjunta ohjelmia. Vaikka virustorjunta ohjelmista puhelimille ei puhuta yleisesti, voivat ne olla hyvä lisä parantamaan yksittäisten laitteiden kyberturvaa. Teimme taulukon, johon vertasimme suosituimpia virustorjunta ohjelmia puhelimille ja keräsimme niistä plussat ja miinukset.

	Bitdefender Mobile Security	Norton 360: Mobile Security	F-Secure SAFE Mobile Antivirus
Tiedot	Bitdefender tuo virustorjunnan myös puhelimiin. Tilaus tuo puhelimeen: • Sovelluksien lukituksen, jolla pystyy asettamaan PIN-koodin sovellukselle, jos sitä haluaa käyttää puhelimessa • Keinon löytää kadonnut/varastettu puhelin • Sovelluksien skannaus	Nortonin virustorjunta ohjelmalla saat puhelimeesi: • Haittaohjelmien ja sovelluksien luokittelu niiden haitallisuuden mukaan esim. akun kulutus • Verkon tarkkailu • Vaarallisten sivujen tarkkailu • VPN-palvelu • Salasanahallinta palvelu	F-Securen luoma Safe virustorjuntaohjelma, antaa puhelimelle: • Salasanahallinta ohjelman • Verkkoselailun suojan • Lapsilukko • VPN-palvelu

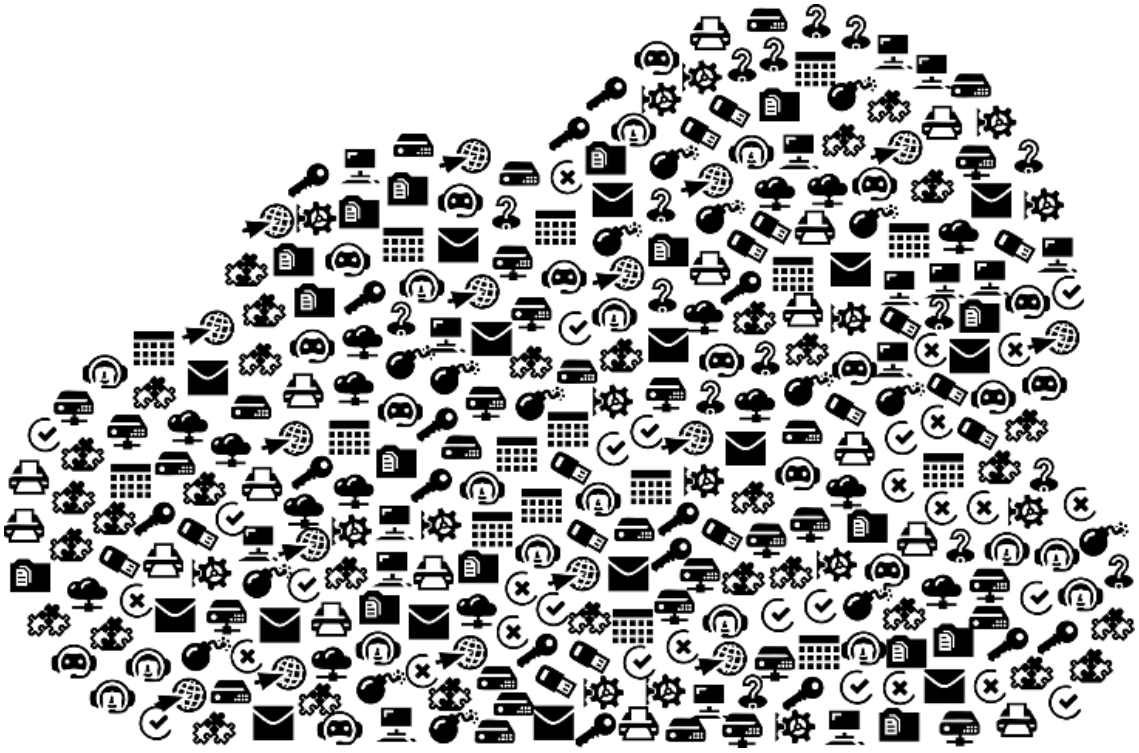
	• VPN-palvelu	• Lapsilukko	
Hyvää	• Nopea puhelimen tarkastus viruksien varalta • Kamera ottaa kuvan kohteesta, jos PIN-koodin kirjoittaa kolme kertaa väärin • Nopea asiakaspalvelu	• Nopea asiakaspalvelu • Todella yksinkertainen ja helppo käyttöliittymä	• Selkeä ja yksinkertainen käyttöliittymä
Huonoa	• Vaatii verkkoyhteyden puhelimen skannausta varten	• VPN, salasananhallinta ohjelma sekä lapsilukko täytyy ladata erikseen • Ei ilmaisversiota	• Palvelusta puuttuu ominaisuuksia, joita kilpailijoilla on

		• Tilaus yhdelle laitteelle on varsin hintava • Puhelimen skannaus voi olla hieman jäykkä ja hidas	• Puhelimelle ei pysty ostamaan yksittäistä tilausta, pitää tilata pakettina • Ei ilmaisversiota
Hinta	• Ilmaisversio • Maksullinen versio yhdelle puhelimelle 9,90 € vuodessa • Total security, joka pitää sisällään suojan viidelle laitteelle, mukaan lukien puhelimet ja tietokoneet 34,99 € vuodessa	• Tilaus yhdelle puhelimelle vuodeksi 29,90 € • Norton 360 Deluxe, joka pitää sisällään suojan viidelle laitteelle vuodeksi 94,90 €	• Vuodeksi 3 laitteelle 59,90 € • Vuodeksi 5 laitteelle 79,90 € • Vuodeksi 10 laitteelle 99,90 €

Saatavuus	Bitdefender Mobile Security for Android Devices Bitdefender Antivirus Free for Android	Norton Mobile Security for Android | Malware Protection & Antivirus App	F-Secure SAFE — Award-winning internet security | F-Secure

Jos sinulla on paketti palvelun kaltainen tilaus virustorjuntaohjelmaan, joka kattaa ohjelman asentamisen usealle laitteelle, on viisaampaa hinnan puolesta asentaa puhelimeen paketin tuoma virustorjuntaohjelma.

8 Verkkolevyt / palvelimella olevat tiedostokansiot



8.1 Mitä pilvi on?

Pilvi alkoi teknologiateollisuuden slangitermistä. Internetin alkuaikoina tekniset kaaviot edustivat usein palvelimia ja verkkoinfrastruktuuria, jotka muodostavat Internetin pilvenä. Pilvi ei ole yksi paikka. Se koostuu palvelimista datakeskuksissa ympäri maailmaa. Pilvi on yksinkertaistetusti sanottuna jonkun muun iso tietokone, jossa tietosi ovat.

8.2 Millaisia pilviä ovat olemassa?

Pilvi	Julkinen pilvi (Public cloud)	Yksityinen pilvi (Private cloud)	Hybridi pilvi (Hybrid cloud)
Kuvaus	Monilla asiakkailla on yhteinen infrastruktuuri	Yhdelle asiakkaalle tarkoitettu infrastruktuuri	Käyttää yhdistelmä yksityisiä ja julkisia pilveä
Edut	• SaaS (Software as a Service) * • PaaS (Platform as a Service) ** • IaaS (Infrastructure as a Service) *** • Kustannus-tehokkuus • Saatavuus • Luotettavuus • Vaivaton ylläpito • Hinta	• Turvallisuus • Täysi kontrolli • Tehokkuus • Datan sijainti (vain kun tarjolla) sopii arka-luonteisiin tietoihin	• Voi helposti lisää tilaa • Kustannus-tehokkuus • Tietoturvallinen • Helposti muokattava

Haasteet	• Ei sopiva arkaluonteisiin tietoihin • Datan sijainti (GDPR-yhteen-sopiva) • Tietoturvallinen	• Hinta • Ylläpito • Suunnittelu	• Aikaa suunnitella • Vaatii API yhteen-sopivuuden ja verkkoyhteyden • Yhteensopivuus ongelma
Toimittaja (esimerkkejä)	• Dropbox • Google Cloud Platform • Microsoft Office 365 • MyCashflow • Kymijoen ICT	• Kaita • TNNet • Valtti	• Google Cloud • TNNet • Contrasec

- * SaaS (Software as a Service) tarkoittaa ohjelmiston jakelua internetin kautta palveluna. SaaS-palveluita käytetään yleensä web-selaimen kautta, esim. Microsoft Office 365 tai Google Docs.
- ** PaaS (Platform as a service) tarkoittaa, että vuokraat tilaa palvelimessa, verkkotallennustilassa, käyttöjärjestelmässä ja tietokannan hallinta- / kehitystyökaluissa. Se ei sisällä applikaatiota kuin Word, Excel, Outlook, jne.
- *** IaaS (Infrastructure as a Service) tarkoittaa, että vuokraat vain tilaa palvelimessa ja verkkotallennustilassa.

8.3 Miten valitsen minulle sopivan pilvipalvelun?

Kun valitset pilvipalvelun, on hyvää tarkistaa, mitä kuuluu palveluun. Pilvipalvelut toimivat siten, että maksamalla enemmän palveluun kuuluu enemmän. Pitää miettiä, mitä kaikkea tarvitset yritykseesi. Kallein palvelu ei välttämättä ole aina paras vaihtoehto.

Taulukossa vertaillaan Google Driven, OneDriven, Dropboxin ja iCloudin ominaisuuksia yritysversiossa.

	Google Drive	OneDrive	Dropbox	iCloud
Yrityssähköposti	Kyllä	Kyllä	Ei	Kyllä
Kalastelu (phishing) ja roskaposti (spam) suojaus	Kyllä	Kyllä	Ei	Kyllä
Video ja äänipuhelut	Kyllä	Kyllä	Ei	Ei
Kokouksen tallenteet	Kyllä	Kyllä	Ei	Ei
Pilvitallennus	2 TB	1 TB / käyttäjä	3 TB	2 TB
Jaetut asemat tiimeille	Kyllä	Kyllä	Kyllä	Kyllä
Chat / viestit	Kyllä	Kyllä	Ei	Ei
Jaetut kalenterit	Kyllä	Kyllä	Ei	Ei
verkkosivujen rakentaja	Kyllä	Ei	Ei	Ei

kyselyn rakentaja	Kyllä	Kyllä	Ei	Ei
Yhteen toimivuus Office-tiedostojen kanssa	Kyllä	Kyllä	Kyllä	Kyllä
Perusapplikaatiot kuten Word, Excel jne.	Kyllä (Google Doc)	Kyllä	Ei	Ei
Kaksivaiheisen tunnistautuminen	Kyllä	Kyllä	Kyllä	Kyllä
Salasanahallinta-ohjelma	Kyllä	Ei	Kyllä	Kyllä
Salausalgoritmi	Hyvä AES 128-bit tai AES 256-bit ja TLS	Hyvä AES 256-bit ja SSL/TLS	Hyvä AES 256-bit ja SSL/TLS	OK AES 128-bit ja TLS
Oikeuksien hallinta	Kyllä	Ei	Ei	Ei
Varmuuskopio	Ei	Kyllä	Kyllä	Kyllä
Tukipalvelu	Sähköposti	Sähköposti / Puhelin	Sähköposti / Puhelin / Chat	Sähköposti / Puhelin

Seuraavassa sivussa oleva lomake auttaa tekemään päätöksen siitä minkälainen pilvipalvelu sopisi yrityksellesi.

Pilvipalvelun nimi			
Minun käyttöjärjestelmäni			
Minkälaisia käyttöjärjestelmävaatimuksia pilvipalvelulla on?			
Kuinka paljon palvelu maksaa?	/kuukausi /vuosi	/kuukausi /vuosi	/kuukausi /vuosi
Kuinka paljon tilaa minä saan?	Gigabitti Terabitti	Gigabitti Terabitti	Gigabitti Terabitti
Kuinka monta käyttäjää on sallittu?			
Onko pilvipalvelu optimoitu mobiililaiteisiin?	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei
Kuuluuko varmuuskopiointi palveluun?	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei
Kuinka kauan tietoja säilytetään varmuuskopioinnissa (esim. 30 päivää)?			
Mitä sovelluksia kuuluu palveluun?	☐ Word / Excel ☐ Sähkö-postisovellus (esim.	☐ Word / Excel ☐ Sähkö-posti sovellus (esim.	☐ Word / Excel ☐ Sähkö-posti sovellus (esim.

	Outlook, Thunderbird) ☐ Muita sovelluksia (esim. palkkalaskelma)	Outlook, Thunderbird) ☐ Muita sovelluksia (esim. palkkalaskelma)	Outlook, Thunderbird) ☐ Muita sovelluksia (esim. palkkalaskelma)
Missä maassa tiedot ovat tallennettu?	☐ Suomi ☐ EU ☐ Muualla maailmassa	☐ Suomi ☐ EU ☐ Muualla maailmassa	☐ Suomi ☐ EU ☐ Muualla maailmassa
Pystynkö määrittämään tiedostojen / kansioiden käyttöoikeudet?	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei
Pystynkö suojaamaan jakamislinkit salasanalla?	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei	☐ Kyllä ☐ Ei
Minkälainen tuki kuuluu palveluun?	☐ Tuki ei kuuluu palveluun. ☐ Tuki sähköpostin kautta ☐ Chat-tuki ☐ Tuki puhelimessa	☐ Tuki ei kuuluu palveluun. ☐ Tuki sähköpostin kautta ☐ Chat-tuki ☐ Tuki puhelimessa	☐ Tuki ei kuuluu palveluun. ☐ Tuki sähköpostin kautta ☐ Chat-tuki ☐ Tuki puhelimessa

8.4 Yleisimmät ongelmat ja riskit pilvipalvelussa

Kun valitset pilvipalvelun, on tärkeä tietää, minkälainen tuki on saatavissa ja kuinka kauan yleensä kestää, ennen kuin asiakaspalvelu pystyy vastaamaan. Sähköpostitukea usein mainostetaan 24/7 tueksi, mutta vastauksen nopeudesta ei ole takeita. On myös hyvä huomioida, millä kielellä palvelua on saatavilla.

Pilvipalvelun riskit:

- Tietosi vuotaa internetiin
- Tietosi katoavat
- Pilvipalvelun tarjoaja menee konkurssiin
- Pilvipalvelun tilaa loppuu kesken

8.5 Linkit

Valtti Tietopankissa on hyvä opas ”Miten valitset yrityksellesi parhaat pilvipalvelut?”.

Tältä sivustosta voit ladata: https://tietopankki.valtti.com/pilvipalvelut

Pieni yhteenveto parhaista ilmaisistä pilvipalveluista: https://www.internetopas.com/parhaat-ilmaiset-pilvipalvelut/

Microsoft - Henkilökohtainen OneDrive-pilvitallennus: https://www.microsoft.com/fi-fi/microsoft-365/onedrive/online-cloud-storage

Google – Google Drive: https://www.google.com/intl/fi/drive/

Apple – iCloud: https://www.apple.com/fi/icloud/

Dropbox: https://www.dropbox.com

9 Varmuuskopiointi

Varmuuskopiointi on osa toimivaa tietoturvaa ja yksi digitaalisen maailman tärkeimmistä asioista. Pidä enemmän kuin yksi varmuuskopio, joista yksi ei ole omassa kodissasi tai toimistollasi. Jos kodissasi syttyy tulipalo, tai vesivahinko tapahtuu, se ei vaikuttaa kodin ulkopuolella olevaan kopioon.

Yleisin tallennusväline varmuuskopiointiin on ulkoinen kiintolevy, mutta myös DVD-levyt, Cd-levyt tai USB-tikut ovat suosittuja. Puhelimessa tallennetut tiedot ei ole varmuuskopio. Tässä kappaleessa käsitteellään mikä varmuuskopio on ja yleisimmät varmuuskopiomahdollisuudet.

9.1 Mitä on Varmuuskopiointi?

Varmuuskopio on käytännössä vain kopio laitteeseesi tallennetuista tiedoista. Varmuuskopiointi on toistettava, jotta tietoihin tehdyt muutokset tallennetaan viimeisen kopion jälkeen.

Varmuuskopiotiedot tietokoneen kiintolevyltä voidaan yleensä tallentaa mille tahansa useista tietovälineistä, niin kuin:

- Muut kiintolevyt (paikalliset tai verkossa olevat kiintolevyt)
- Ulkoiset tallennuslaitteet (USB-tikut, USB-kiintolevyt)
- Verkko- tai pilvitallennustilit
- Toinen kiintolevyosio (levyosio on erillinen osa samalla kiintolevyllä)

Tietojen varmuuskopiointiin on monia tapoja. Mikä sitten ei ole varmuuskopio? Kun käytät pilvitallennusratkaisun sovellusta, kuten Google Drivea tai Dropboxia, synkronoidaksesi tietyssä kansiossa olevat tiedostot pilvitilisi kanssa, sitä ei pidetä varmuuskopiona koska tiedostoista on vain yksi versio. Heti kun päivität synkronoidussa kansiossa olevan tiedoston, myös pilvitallennussivustolla oleva tiedosto muuttuu. Varmuuskopioiden tiedostoversiot eivät muutu aina, kun luot uuden varmuuskopion – ellet korvaa ja poista edellistä varmuuskopiota uudella.

9.2 Miksi varmuuskopiot ovat välttämättömät

Tietokoneen kiintolevyn varmuuskopiointi on tärkeää laitteeseen tallennettujen arvokkaiden tietojen ja tiedostojen suojaamiseksi.

- **Tietosuoja**
  Varmuuskopioinnit pitävät tärkeät tiedostosi turvassa tietojen katoamiselta. Voit myös salata varmuuskopiotiedoston tai tallennusvälineen turvallisuuden lisäämiseksi.

- **Helppo palauttaa**
  Varmuuskopiointi on luotettava, helppo ja turvallinen tapa palauttaa kadonneet tiedostot. Varmuuskopiointi voi palauttaa jopa 100 % tiedostoista. Tätä varten tarvitset tietojen palautusohjelmiston. Varmuuskopiointijaksojen välillä luotuja, päivitettyjä tai järjestelmään lisättyjä tiedostoja ei kuitenkaan palauteta. (Lisää palautusohjelmista alhaalla.)

- **Pitää yrityksen toimintakuntoisena**
  Data on yrityksen tärkein voimavara. Säännöllisen varmuuskopioinnin avulla voidaan varmistaa tietoturva ja liiketoiminnan jatkuvuus tietojen katoamisen sattuessa.

- **Mielenrauha**
  Kun teet varmuuskopioita säännöllisesti, sinun ei tarvitse huolehtia useista tekijöistä, jotka usein johtavat tietojen katoamiseen.

- **Säästä aikaa ja rahaa**
  Varmuuskopiointi säästää huomattavan määrän resursseja, jotka muuten joutuisit käyttämään kadonneiden tietojen palauttamiseen. Oikealla varmuuskopioilla palautusprosessi on helpompaa ja vaatii vähemmän vaivaa. Muussa tapauksessa saatat joutua viettämään useita päiviä tai viikkoja saadaksesi takaisin kadonneet tietosi ammattimaisen palautuspalvelun avulla.

9.3 Kuinka varmuuskopioida tietoja?

Erilaisten varmuuskopioiden plussat ja miinukset alla olevassa taulukossa:

Vaihtoehtoja	**Plussa**	**Miinus**
Pilvi	• Vapaata tilaa ja edullisia päivityksiä. • Tiedot suojattu etäpaikassa. • Voit käyttää sitä missä tahansa, josta pääset Internetiin. • Turvallinen tiedonsiirto.	• Ilmaisen tallennustilan kapasiteettirajoitukset. • Sivuston sulkemisen riski. • Varmuuskopiotiedostojen käyttäminen edellyttää yhteyden Internetiin.
Ulkoinen kiintolevy	• Helppokäyttöinen. • Ohjelmiston avulla voit ajoittaa varmuuskopiot etkä koskaan enää murehdi niistä.	• Kiintolevyasemat voivat epäonnistua. • Puolijohde-asemilla on pienempi riski, mutta ne voivat olla kalliita suurikapasiteettisille asemille. • Säilytettävä muualla tulipalon tai muun katastrofin varalta.

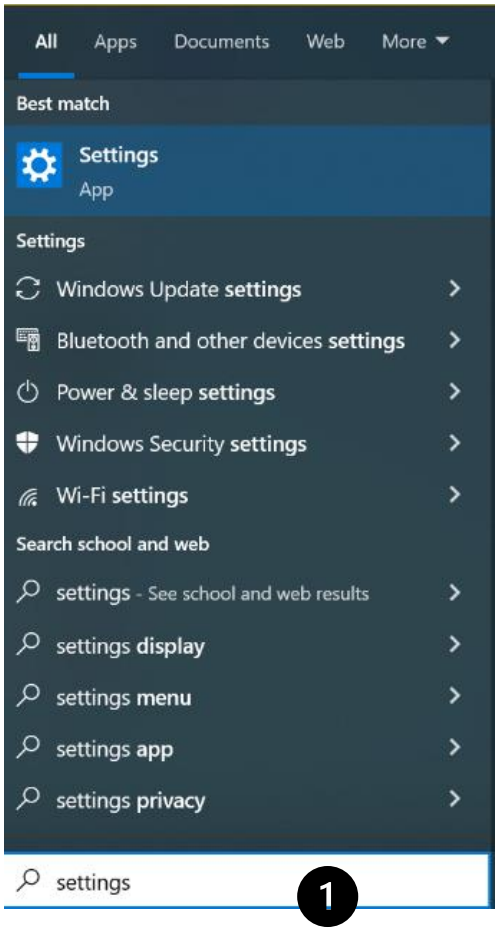
USB-tikku	• Tietokoneen vika ei ole ongelma. • Voidaan säilyttää turvallisesti toisessa paikassa.	• Varmuuskopioiden hallinta vie aikaa. • Oletuksen CD-yhteensopivan tekniikan tulevaisuus. Joissakin laitteissa ei enää ole asemaa tätä tarkoitusta varten. • Suuret tietomäärät voivat tulla kalliiksi, kun ostat lisää levyjä.
CD, DVD, Blue-Ray	• Kannettava. • Helppo vaihtaa.	• Hintava • Helppo hävittää (ei suositella tärkeän tiedon pitkäaikaiseen säilytykseen tämän riskin vuoksi). • Ei aina kestävä. • Kapasiteettirajoitukset. • Sopivan väliaineen hankinta.
NAS	• Voi varmuuskopioida useita tietokoneita kerralla. • Voidaan asettaa automaattiseen varmuuskopiointiin.	• Hintava • Aseman vian mahdollisuus.

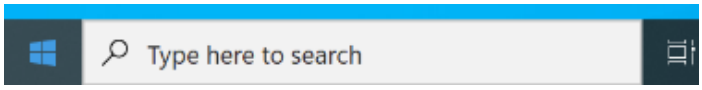
9.4 Mitä pitää varmuuskopioida?

Voit tallentaa tiedot, jotka haluat varmuuskopioida itse toiselle tietovälineelle säännöllisin väliajoin. Vaikka tämä tehtävä ei ole liian vaikea, tietojen tallentaminen yhä uudelleen ja uudelleen voi olla myös vaivalloista. Lisäksi monet käyttäjät unohtavat tehdä tämän tehtävän, joten kaikkia tietoja ei aina varmuuskopioida.

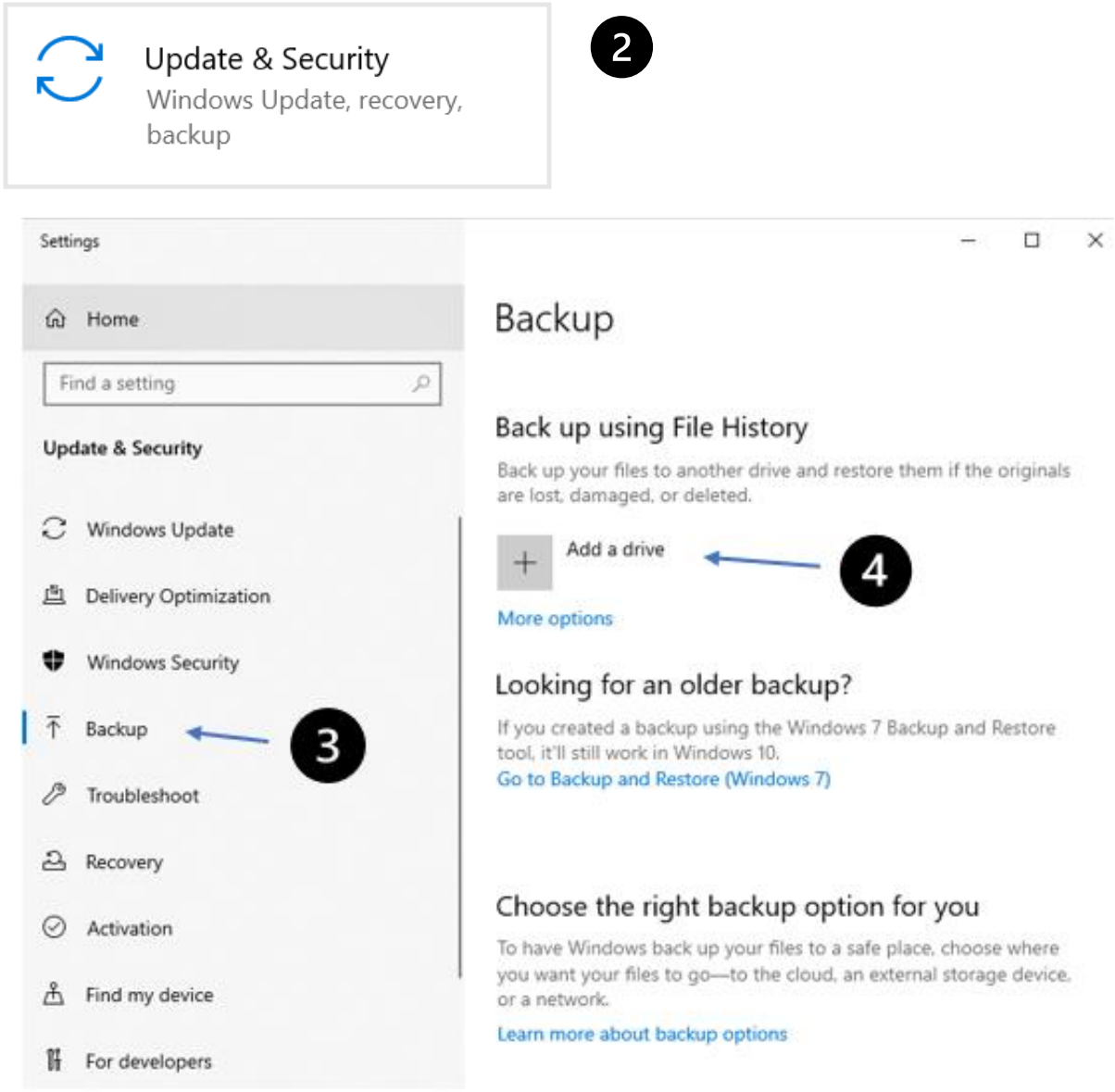
Voit myös luoda varmuuskopion automaattisella ohjelmalla. Kun olet asentanut tämän, se tallentaa automaattisesti kaikki tiedot uudestaan ja uudestaan. Tämä ei ainoastaan helpota tätä tehtävää, vaan yleensä myös suorittaa sen luotettavammin tämän ohjelman kanssa.

9.5 Kuinka teen varmuuskopiointi Windows koneella ulkoiseen kiintolevyyn?

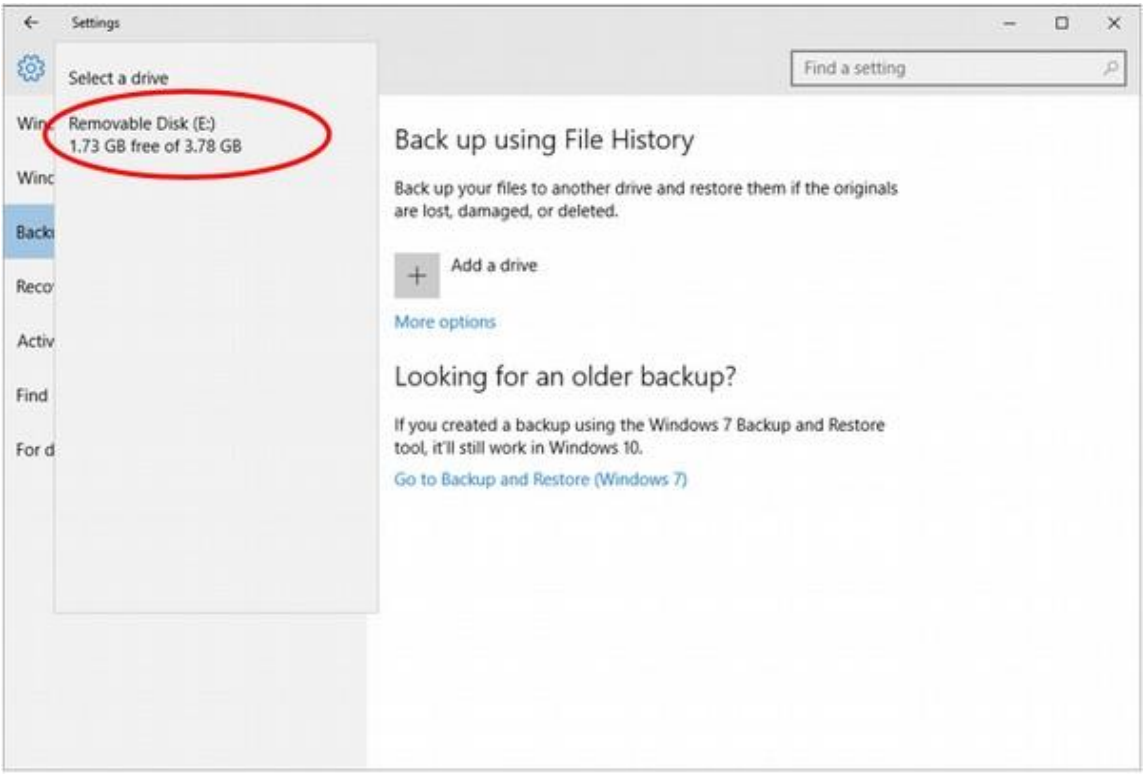




1. Näytön vasemmassa alanurkassa löytyy kohta ”**Type here to search/Kirjoita tähän hakeakseksi kohteista**”. Klikkaa palkkia, ja kirjoita ”**Settings/Asetukset**” ja paina ”Enter”.



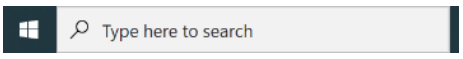
1. Skrollaa alas, kunnes löytyy ”**Update and Security/Päivittäminen ja suojaus**” ja paina painiketta.
2. Klikkaa ”**Backup/Varmuuskopioi**”.
3. Valitse oikealla puolella ”**Back up using File History/Varmuuskopioi tiedostohistorian avulla**” alapuolella plussa ja valitse ulkoinen kiintolevy.



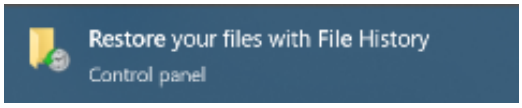
9.6 Kuinka palautan ulkoisella levyllä olevat varmuuskopiot (Windows 10-järjestelmä)?

Näin toimit, kun tiedostot ovat poissa ja varmuuskopiot sijaitsevat ulkoisella levyllä.

1. Kirjoittaa hakukenttään ”**Restore Files / Varmuuskopioi ja palauta**”



2. Valitse ”**Restore your Files with File History/Palauta tiedostot Tiedostohistoria-toiminnon avulla**”



3. Etsi tarvitsemasi tiedosto ja käytä sitten nuolia nähdäksesi kaikki sen versiot.
4. Tallenna se alkuperäiseen sijaintiinsa valitsemalla Palauta.

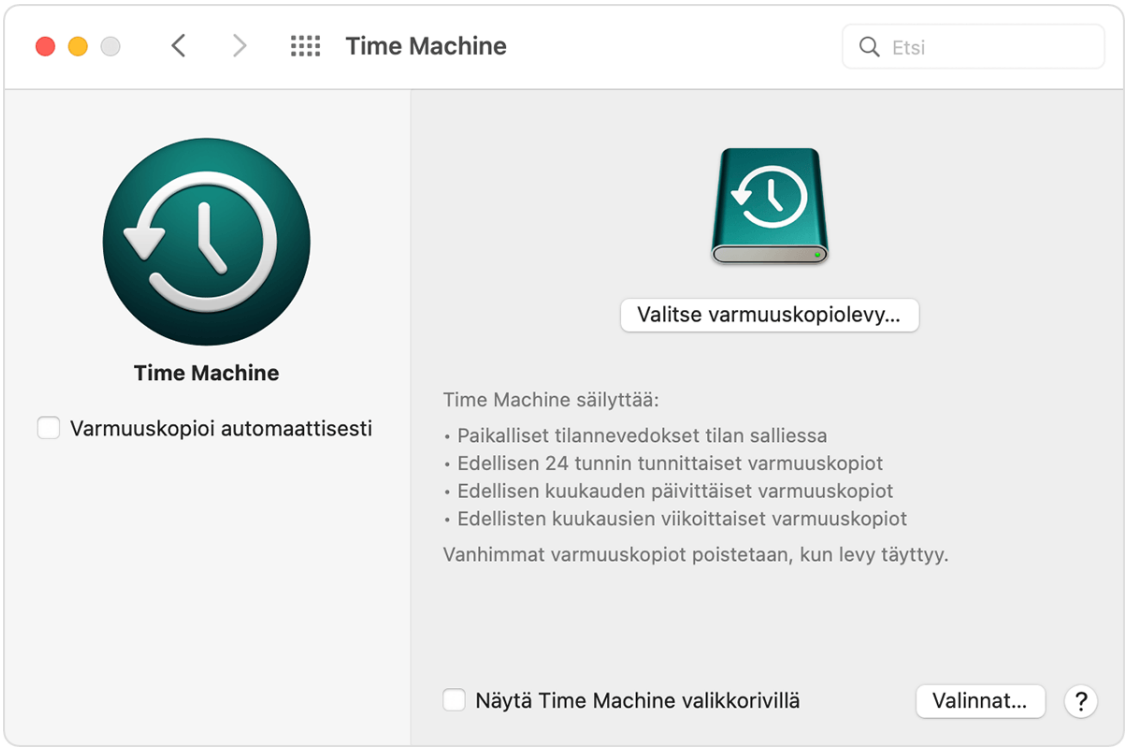
5. Jos haluat tallentaa sen toiseen paikkaan, napsauta hiiren kakkospainikkeella Palauta, valitse Palauta kohteeseen ja valitse sitten uusi sijainti.

9.7 Kuinka palautan tiedostoja varmuuskopiointista ulkoisesta levystä (Windows 11-järjestelmä)?

1. Yhdistä ulkoinen kovalevy, joka sisältää varmuuskopiotiedostot.
2. Kirjoittaa tehtäväpalkin hakukenttään: ohjauspaneeli. Valitse se näkyvistä tuloksista.
3. Valitse se tulosluettelosta ja valitse sitten Varmuuskopioi ja palauta (Windows 7).
4. Valitse toinen varmuuskopio, jos haluat palauttaa tiedostoja kohteesta, valitse ulkoisen tallennuslaitteen sijainti ja palauta tiedostot noudattamalla ohjeita.

9.8 Kuinka teen varmuuskopiointi Mac koneella Time Machinella?

1. Liitä Maciin ulkoinen tallennuslaite, kuten USB- tai Thunderbolt-asema.
2. Avaa Time Machine -asetukset valikkorivin Time Machine -valikosta . Voit myös valita Omenavalikko () > Järjestelmäasetukset ja paina Time Machine.
3. Paina Valitse varmuuskopiolevy.



4. Valitse levyn nimi ja klikkaa sitten Käytä levyä. Time Machine aloittaa heti säännöllisen varmuuskopioimisen automaattisesti, eikä sinun tarvitse tehdä mitään.

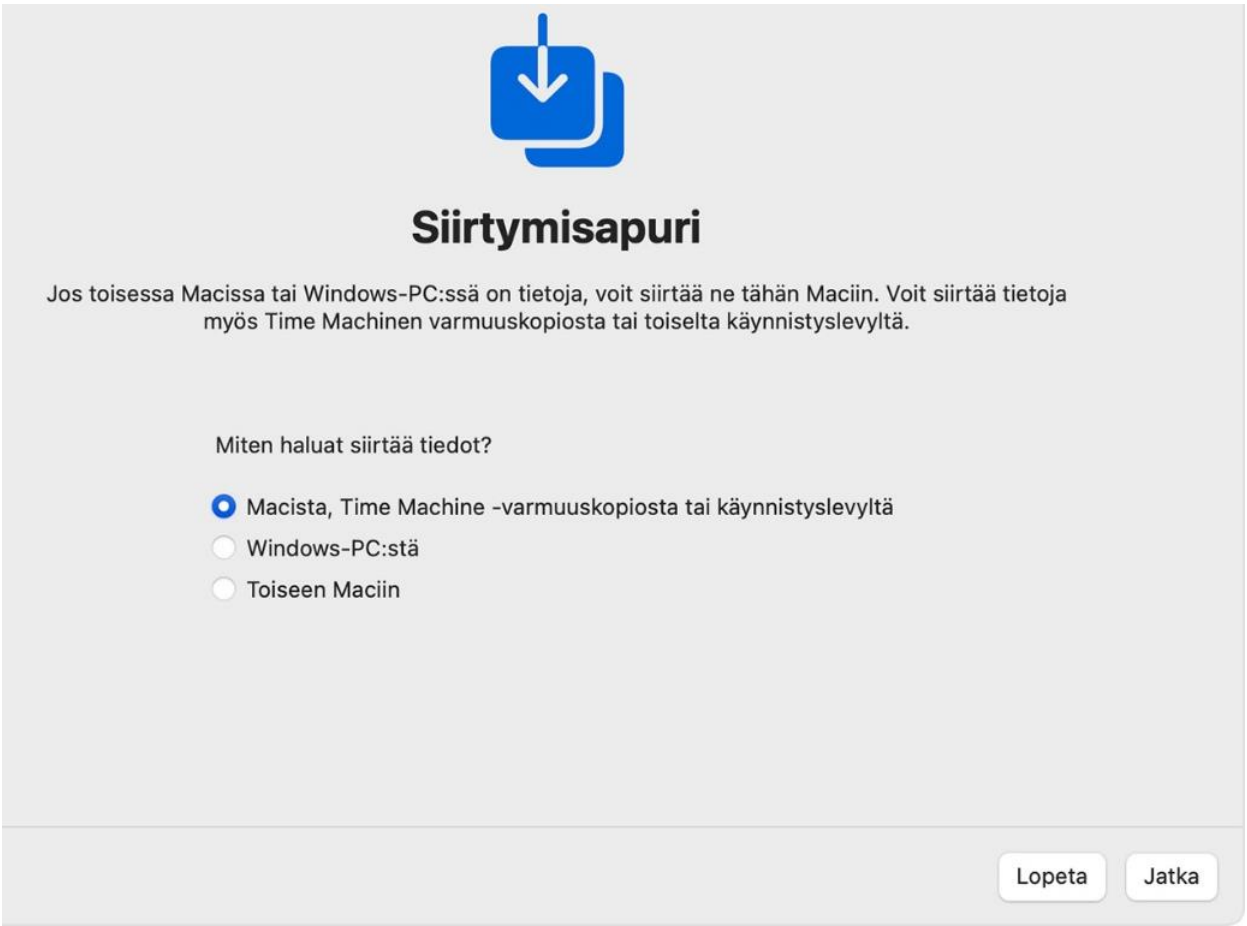
9.9 Kuinka palautan varmuuskopiot ulkoiselta levyltä (Mac)?

1. Jos sinun on asennettava macOS uudelleen, tee tämä ennen jatkamista. Jos esimerkiksi Macin käynnistyessä näkyy vilkkuva kysymysmerkki, sinun on ensin asennettava macOS uudelleen.
2. Varmista, että Time Machine -varmuuskopiolevy on liitettynä Maciin ja päällä.
3. Avaa Siirtymisapuri Macissa. Löydät sen Apit-kansion Lisäapit-kansiosta.

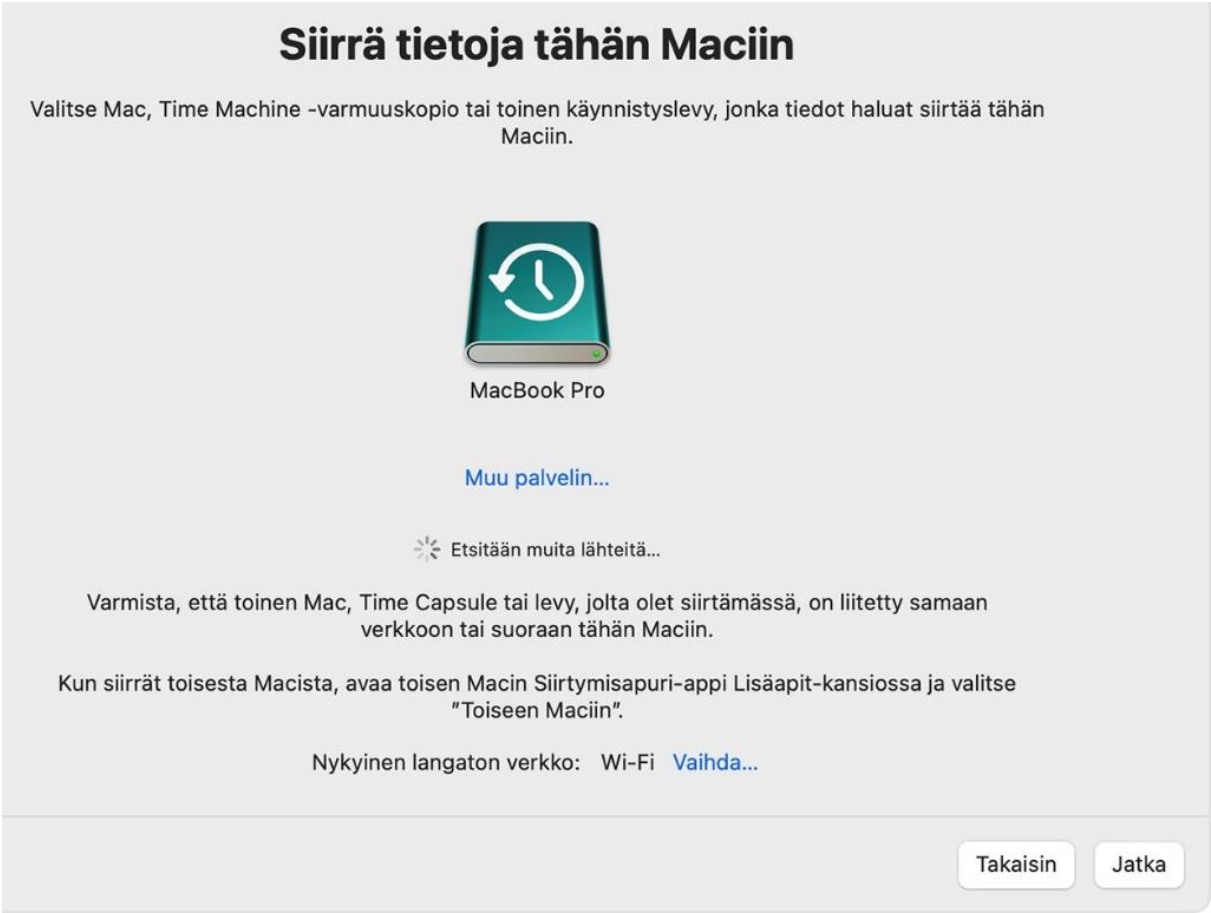
   Jos Mac avaa käynnistyksen yhteydessä käyttöönottoapurin, joka

kysyy esimerkiksi maan ja verkon tietoja, jatka seuraavaan vaiheeseen, sillä käyttöönottoapuri sisältää siirtymisapurin.

4. Kun järjestelmä kysyy, miten haluat siirtää tietosi, valitse siirtäminen Macilta, Time Machine -varmuuskopiosta tai käynnistyslevyltä. Klikkaa sitten Jatka.



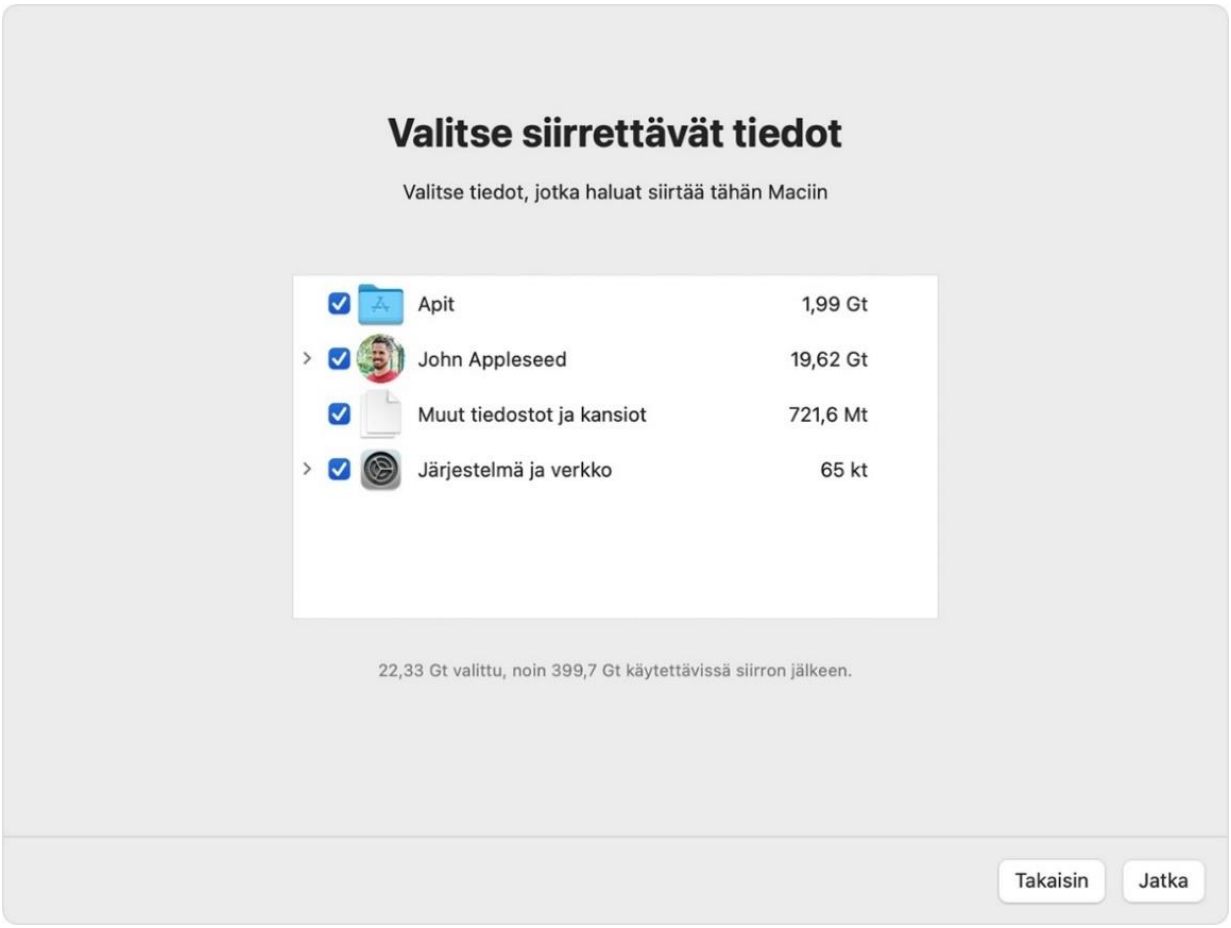
5. Valitse Time Machine -varmuuskopiosi ja klikkaa Jatka.



6. Valitse varmuuskopio ja klikkaa Jatka.

7. Valitse siirrettävät tiedot.

Tässä esimerkissä John Appleseed on macOS-käyttäjätili. Jos tilillä on sama nimi kuin Macissa jo ennestään olevalla tilillä, sinua pyydetään nimeämään vanha tili uudelleen tai korvaamaan Macissa oleva tili. Jos nimeät vanhan tilin uudelleen, se näkyy Macissa erillisenä käyttäjänä, ja sillä on erillinen kotikansio ja käyttäjätunnus. Jos korvaat Macissa olevan tilin, vanha tili poistaa ja sitten korvaa sen, mukaan lukien sen kotikansion sisällön.



8. Aloita siirto klikkaamalla Jatka. Suurten siirtojen suorittaminen voi kestää useita tunteja.

9.10 Kuinka varmistaa varmuuskopioiden toimivuus?

Tiettynä päivänä, esimeriksi 30 päivän välein, varmuuskopioiden tietoja tulee testata palauttamalla vain pieni määrällä tiedostoja tai kansioita tietokoneella sen varmistamiseksi, että varmuuskopio onnistui. Viimeinen asia, jonka tarvitset hätätilanteessa, on havaita, että tiedot, joita yrität palauttaa, ovat käyttökelvottomia tai jopa vioittuneet.

Varmuuskopioinnin jälkeen sinun tulee varmistaa, että kaikki tallennettavat tiedostot, kansiot ja tiedot ovat varmuuskopiossa. Luo selkeä ja kattava luettelo vaiheista, joita on noudatettava palauttaaksesi varmuuskopiotiedostot ja jakaaksesi ne kaikille, jotka ovat mukana

tietojen katoamisen sattuessa. Lista kannattaa lähettää sähköisesti, tulostaa ja jakaa asianosaisille. Joka tapauksessa tulostettu versio tulee olla helposti saatavilla.

9.11 Neljä keskeistä aluetta, joilla varmuuskopiointi menee pieleen

- **Laitteiston vika**
  Laitteisto vanhenee ja jossain vaiheessa menee rikki. Hajoaminen tulee kuitenkin usein täysin odottamatta, jonka takia varmuuskopiointien testaaminen on tärkeää. Ulkoiset kiintolevyt, levyryhmät ja muut varmuuskopiointilaitteet voivat epäonnistua. Suurin osa varmuuskopiolaitteiston syistä ja vikatilanteista ovat samat kuin muidenkin laitteistojen.

- **Ohjelmisto-ongelmia**
  Yksi yleisimmistä varmuuskopiointivirheiden lähteistä on, kun päivitysten aiheuttamat muutokset aiheuttavat ongelmia seuraavan varmuuskopion suorittamisessa. Tämä voi johtua siitä, että päivitykset tai korjaukset voivat olla yhteensopimattomia varmuuskopiokokoonpanon kanssa.
  Tärkein riskien hallinnassa on siitä, että päivitykset tehdään säännöllisesti ja varmistetaan, että yrityksessä on toinen toimiva varmuuskopio tallessa.

- **Inhimillinen virhe**
  Useasti ihminen on heikoin lenkki ATK-maailmassa. Paras suoja inhimillisiltä virheiltä varmuuskopioinnissa on kouluttaa

henkilökunta noudattamaan parhaita käytäntöjä ja seurata, että koulutus siirtyy ja pysyy työntekijöiden arkikäytäntönä. Varmista, että varmuuskopioita ja palautuksia suorittavat henkilöt ymmärtävät tarkalleen, mikä heidän tehtävänsä on.

- **Vika infrastruktuurissa**
  Varmuuskopiointi verkon kautta lisää tehokkuutta vähentämällä varmuuskopiointilaitteiden määrää. Se tuo kuitenkin myös toisen epäonnistumiskohdan varmuuskopiointiprosessiin.

9.12 Linkit

YouTubessa ohjeita miten varmuuskopioidaan:

Windows 10 Backup Free, Fast Easy with built in Windows 10 backup https://www.youtube.com/watch?v=jRs24C60q6g

(FN) iPhonen varmuuskopiointi – Miten varmuuskopioida iPhone https://www.youtube.com/watch?v=1xsPtkaL2xc

Windows 11: Create full backup to external USB drive and restore (Official) https://www.youtube.com/watch?v=3mUnKQ7ff0Y

How to back up your Mac with Time Machine – Apple Support https://www.youtube.com/watch?v=geJiTXOb37w

How to restore files from a Time Machine backup | Apple Support https://www.youtube.com/watch?v=CSwy_thSXow&list=PLIl2EzNYri0emtB96zErQCSnoNf_VOdLd&index=2

10 EU:n yleinen tietosuoja-asetus

Suomen yrittäjät ovat kirjoittaneet hyvän oppaan tietosuojasta. Tältä sivulta voit tilata Yrittäjän tietosuojaopas: https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

GDPR:n on oman yrityksen etu pitää asiakkaiden tiedot turvassa ja sen perusteella saada luottamusta asiakkailta sekä säästä rahaa.

10.1 Mitä GDPR tarkoittaa?

GDPR on lyhenne sanoista **G**eneral **D**ata **P**rotection **R**egulations. Suomeksi se tarkoittaa EU:n yleistä tietosuoja-asetusta. GDPR on voimassa kaikissa EU-maissa ja sen tarkoitus on säädellä henkilötietojen käsittelyä. GDPR:n avulla EU on halunnut parantaa henkilötietojen suojaa ja tietosuojaoikeuksia. Laki kehitettiin vastaamaan uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin. Suomessa Tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädäntöä.

10.2 Mikä on henkilötieto

Tiettyyn henkilöön (asiakkaaseen/työntekijään/yhteistyökumppaniin) liitettävissä oleva mikä tahansa tieto, kuten yhteystiedot. Ajattele henkilötietoja kuin palapeliä. Yksi pala ei välttämättä kerro paljon, mutta yhdistettynä ne paljastavat elävän kuvan elämästäsi.

Esimerkkejä henkilötiedoista:

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.fi
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot (esim. matkapuhelimen paikannustiedot)

Suorat tunnisteet sisältävät:

- henkilön koko nimi
- henkilötunnus
- henkilönimen mukainen sähköpostiosoite
- biometriset tunnisteet

Epäsuorat tunnisteet sisältävät:

- Sukupuoli
- Ikä
- Ammatti

10.3 GDPR:n keskeiset säännöt

GDPR:n siirtymäaika loppui 25. toukokuuta 2018. GDPR käsittelee tietosuojaperiaatteita, vastuullisuutta, tietosuojaa, sitä milloin sinulla on lupa käsitellä tietoja, suostumusta, tietosuojavastaavia ja ihmisten yksityisyysoikeuksia.

Vaikka GDPR on EU direktiivi, se velvoittaa organisaatioita ja yrityksiä missä tahansa, kun ne keräävät tietoja EU:n alueella asuvista ihmisistä.

Kun käsittelet tietoja, sinun on tehtävä se GDPR:n seitsemän periaatteen mukaan.

1. Lainmukaisuus, asianmukaisuus ja läpinäkyvyys.
2. Käyttötarkoituksen vastattava rekisterissä ilmoitettua tarkoitusta.
3. Tietojen olennaisuus ja tarpeellisuus.
4. Tietojen käsittelyn oltava turvallista ja luottamuksellista.
5. Tietojen oltava täsmällisiä ja tarvittaessa päivitettyjä.
6. Tietojen säilytys ja käsittely vain niin kauan kuin on tarpeellista.
7. Näiden periaatteiden noudattaminen on voitava osoittaa dokumentaation avulla. Yleensä keskeinen henkilötietojen käsittelyä kuvaava dokumentti on tietosuojaseloste.

10.4 Milloin minulla on lupa käsitellä tietoja?

Artikkelissa 6 löytyy tiedot, siitä milloin saat käsitellä tietoja. Alla olevassa listassa löytyy 6 esimerkkiä tietojen käsittelyyn liittyen.

1. Tietty henkilö on antanut sinulle nimenomaisen, yksiselitteisen suostumuksensa tietojen käsittelyyn (esim. markkinointisähköpostitilaus).

2. Käsittely on tarpeen sopimuksen toteuttamiseksi / valmistautumiseksi tietyn henkilön kanssa. (esim. vuokrasopimus).
3. Sinun on käsiteltävä tietoja noudattaaksesi lakisääteisiä velvoitteitasi (esim. tuomioistuimen määräys tai osakeyhtiölain edellyttämä osakasluettelo).
4. Sinun on käsiteltävä tietoja pelastaaksesi jonkun hengen. (esim. ensihoitajat)
5. Käsittely on tarpeen yleisen edun tai julkisen vallan edellyttämän tehtävän suorittamiseksi (esim. olet yksityinen jätehuoltoyritys).
6. Sinulla on oikeutettu etu käsitellä jonkun henkilötietoja. Esimerkiksi asiakas on halunnut tilata sinulta jotakin verkkokaupastasi tai työnantajavelvoitteista huolehtiminen.

Kun olet määrittänyt tietojenkäsittelysi laillisen perustan, sinun on laadittava yrityksellesi tietosuojaseloste, joka sinun tulee saattaa niiden henkilöiden tietoon ja hyväksyttäväksi, joiden tietoja käsittelet.

Jos päätät muuttaa perustelujasi ja tietosuojaselostettasi myöhemmin, sinulla on oltava hyvä syy. Dokumentoi tämä syy ja ilmoita siitä henkilöille, joita muutos koske. Näitä ilmoituksia ovat ne ilmoitukset, joita esimerkiksi ajoittain saat some-tileiltäsi (Voidaksesi jatkaa palvelun käyttämistä, sinun tulee hyväksyä uudet ehtomme tms.).

10.5 Suostumus

Suostumuksen suhteen on laadittu tiukat säännöt.

- Suostumuksen on oltava ”vapaasti annettu, täsmällinen, tietoinen ja yksiselitteinen”.
- Suostumuspyyntöjen on oltava selvästi erotettavissa muista asioista.
- Suostumuspyyntöjä on esiteltävä selkeällä muodolla ja selkeällä kielellä.
- Asiakkaat voivat peruuttaa antamansa suostumuksen, mikäli tietojen käsittelyyn ei ole perusteltua syytä.
- Sinun on kunnioitettava heidän päätöstään peruuttaa suostumuksensa. Et voi muuttaa käsittelyn oikeudellista perustetta johonkin muuhun perusteeseen.
- Alle 13-vuotiaat voivat antaa suostumuksen vain vanhemman luvalla.
- Sinun on säilytettävä suostumuksesta asiakirjatodiste.

10.5.1 Rekisteri, rekisterinpitäjä, henkilötietojen käsittelijä

Jokainen yritys, joka säilyttää henkilötietoja, on rekisterinpitäjä. Tämä tarkoittaa käytännössä jokaista yritystä, josta löytyy edes puhelin, jossa on asiakkaiden tietoja.

Rekisteri on mikä tahansa kokoelma henkilötietoja, vaikka ne sijaitsisivat eri paikoissa (esim. sähköpostissa, kännykkäsi yhteystiedoissa ja yrityksen työntekijöiden käytössä olevassa jaetussa Google-taulukossa sekä kaapin perukoille unohdetussa asiakkailta kerätyssä käyntikorttinivaskassa).

Henkilötietojen käsittelijä on yrityksen alihankkija/palveluntoimittaja, joka käsittelee yrityksen puolesta henkilötietoja (esim. työterveys ja tilitoimisto).

10.5.2 Ihmisten yksityisyysoikeudet

Ihmiset lainaavat tietojaan yrityksille. Organisaation on tärkeää ymmärtää heidän oikeutensa.

Asiakkaan (rekisteröidyn) oikeudet

- Saada läpinäkyvästi tietoa henkilötietojensa käsittelystä rekisterinpitäjän toimesta.
- Saada pääsy omiin henkilötietoihinsa. Varmista, että työntekijät ymmärtävät, että esimerkiksi haasteellista asiakasta ei voi kuvata värikkäästi asiakasrekisterissä.
- Oikeus saada virheelliset/puutteelliset korjattua.
- Oikeus tulla unohdetuksi. Tämä tarkoittaa, että organisaatio tai yritys poistaa heidän tietonsa kokonaan tietojärjestelmistä, niiltä osin kuin se on mahdollista (esimerkiksi lakisääteinen velvoite voi estää tämän joiltakin osin).
- Oikeus rajoittaa omien tietojensa käsittelyä.
- Oikeus saada omat tietojen siirretyksi järjestelmästä toiseen.
- Asiakkaalla on oikeus vastustaa henkilötietojensa käsittelyä.
- Asiakkaalla on oikeus olla joutamatta perusteetta automaattisen päätöksenteon kohteeksi.

10.5.3 Arkaluonteiset tiedot eli arkaluonteiset tiedot

Arkaluonteisia tietoja saa kerätä vain, mikäli

- rekisteröity on nimenomaisesti suostunut tähän;
- rekisterinpitäjän tulee tehdä näin lain vaatimuksesta (esim. sosiaalisen suojelun ala);
- se on tarpeen rekisteröidyn elintärkeiden etujen suojelemiseksi (esim. tiedottomuuden vuoksi);
- henkilö on itse tehnyt tiedoista nimenomaisesti julkisia;
- Käsittely tapahtuu asianmukaisin suojatoimin ammattiliiton tai poliittisen, filosofisen, uskonnollisen säätiön tai voittoa tavoittelemattoman yhteisön toimesta.

Arkaluonteisia tietoja ovat

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettiset / biometriset tiedot, jotka on kerätty henkilön tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

10.6 Mitä minun pitää huomioida omassa yrityksessäni?

GDPR:n mukaan sinun tulee toimia seuraavasti:

- Henkilötietojen käsittelyn minimoiminen. Käsittelee juuri niitä tietoja kun tarvitset, älä kerää liika tietoja.

- Henkilötietojen pseudonymisointi (tarkoittaa henkilötietojen käsittelyä siten, että niitä ei voi enää yhdistää tiettyyn henkilöön ilman lisätietoja) mahdollisimman pian.
- Läpinäkyvyys henkilötietojen käyttöön liittyen. Kerro asiakkaille, mihin tarkoitukseen keräät heidän tietojansa.
- Tietojenkäsittelyn seuranta.
- Antaa henkilötietojen käsittelijälle mahdollisuuden luoda ja parantaa suojausominaisuuksia.
- Tuotetta kehitettäessä on otettava huomioon tietosuojalait.
- Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olisi otettava huomioon myös julkisessa tarjouskilpailussa.
- Ylläpidä yksityiskohtaista dokumentaatiota keräämistäsi tiedoista. Mihin tarvitset niitä tietoja? Missä niitä säilytetään? Kuka on niistä vastuussa?
- Kouluttaa työntekijäsi siten, että he käyttävät hyvää kyberhygieniaa työskennelleessä.
- Tee tietojenkäsittelysopimuksia kolmansien osapuolten kanssa, jotka käsittelevät sinun kerättyjä asiakastietojasi.
- Jos laki vaati, esim. SOTE-ala, nimitä tietosuojavastaava.
- Käytä hyvää suojausta (esim. ota kaksivaiheinen tunnistautuminen eli autentikointi käyttöön.)
- Seuraa säännöllisesti, onko kaikki tietosuojaan liittyvä toiminta ja dokumentaatio ajan tasalla.

10.7 Mitä rangaistuksia GDPR:n rikkomisestä määrätään?

Jos yritys tai organisaatio ei noudata yleistä tietosuoja-asetusta, voidaan rangaistuksesi antaa sakkoja, joiden suuruus voi olla jopa **20 miljoona euroa tai 4 % vuosittaisesta liikevaihdosta.**

Esimerkkiä rangaistuksen saaneista yrityksistä Suomessa:

- Yksityishenkilö – 500 euroa
  Yksityishenkilö oli asentanut kiinteistölleen valvontakamerat, jotka tallensivat myös naapurikiinteistöt.
- Matkatoimisto – 6 500 €
  Asiakkaiden täyttämät viisumihakemuslomakkeet olivat julkisesti saatavilla matkatoimiston verkkopalvelimella. Tämä lomake sisälsi muun muassa rekisteröityjen nimet, passin numerot ja yhteystiedot.
- Vastaamo – 608 000 €
  Yritys rikkoi yleistä tietosuoja-asetusta laimin lyömällä henkilötietojen turvalliseen käsittelyyn sekä tietoturvaloukkauksesta ilmoittamiseen liittyviä velvollisuuksiaan. Rekisterinpitäjä ei ollut myöskään toteuttanut asianmukaisia toimenpiteitä henkilötietojen käsittelyn turvaamiseksi.

10.8 Linkit

GDPR-tarkistuslista: https://gdpr.eu/checklist/ (englanniksi)

EU:n tietosuojaverkkosivu: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi

Finlex Tietosuojalaki - https://www.finlex.fi/fi/laki/alkup/2018/20181050

Yrittäjän tietosuojaopas - https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

11 Liiketoiminnan jatkuvuussuunnitelma

Liiketoiminnan jatkuvuudella tarkoitetaan sitä, kuinka yritys jatkaa toimintaansa häiriön sattuessa. Tehokkainta on kehittää tietotekniikan palautussuunnitelma yhdessä liiketoiminnan jatkuvuussuunnitelman kanssa.

Liiketoiminnan jatkuvuussuunnitelman keskeiset ominaisuudet ovat toimiala-/liiketoimintakohtaisia, mutta useimmissa suunnitelmassa on yhteisiä komponentteja. Suunnitelma määrittelee selkeästi roolit ja vastuut. Lähes kaikissa nykyaikaisissa liiketoiminnan jatkuvuussuunnitelmissa hahmotellaan myös selkeästi tietotekniikan roolit kriittisten tietojen, sovellusten ja palveluiden säilymisen tai nopean palautumisen varmistamisessa keskeytyksen jälkeen. Nämä sisältävät:

- Tietojen varmuuskopiointi- ja palautustyökalut
- Pilvipalveluiden infrastruktuuri ja palvelut

Jatkuvuussuunnitelmassa tulee myös kuvata, mitkä palvelut ovat kriittisimpiä ja kuinka ne jatkossakin toimitetaan asiakkaille, työntekijöille, kumppaneille ja muille sidosryhmille.

Lopuksi vahva toiminnan jatkuvuussuunnitelma sisältää kriteerit ja ohjeet kaikkien mukana olevien ihmisten – työntekijöiden, asiakkaiden, kumppaneiden – terveyden ja turvallisuuden varmistamiseksi suunnitelmaa toteutettaessa ja hallittaessa.

11.1 Miten rakennan liiketoiminnan jatkuvuussuunnitelma?

Tämä on suuntaa antava, muokkaa palautussuunnitelma yrityksen tarpeiden mukaan.

Johdanto

Johdanto sisältä yrityksen tiedot, suunnitelman versio ja muutoksia, sekä avainhenkilöstön yhteystiedot.

Suunnitelman tavoitteet ja laajuus

Jatkuvuussuunnitelman tavoite on tarjota väline hätätilanteeseen / poikkeamaan, joka uhkaa häiritä normaalia liiketoimintaa.

Hätätilanne on todellinen tai uhkaava tilanne, joka voi aiheuttaa häiriöitä tai menetyksiä organisaation tavanomaisessa liiketoiminnassa siinä määrin, että se muodostaa sille uhan. Poikkeama on mikä tahansa tapahtuma, joka voi johtaa liiketoiminnan häiriöön tai rahallisia menetyksiä.

Jatkuvuussuunnitelman avulla voidaan varmistaa liiketoiminnan kannalta kriittisten palvelujen jatkuminen minimoimalla henkilöstölle, tiloille, laitteille tai arkistoille mahdollisesti aiheutuvien vahinkojen vaikutukset. Suunnitelma auttaa pienentämään poikkeamien riskit.

Liiketoiminnan jatkuvuussuunnitelmasta käy ilmi, miten yritys voi vähentää poikkeamaan mahdollisissa vaikutuksia valmistautumalla säilyttämään palvelut seuraavissa tilanteissa:

- Keskeisten tilojen menetys
- Tietotekniikan / tietojen menetys

- Televiestinnän menetys
- Kovalevyjen / paperitietojen katoaminen
- Sähkö- ja/tai vesikatkos
- Keskeisen yhteistyökumppanin / toimittajan menettäminen
- Sääolojen aiheuttamat häiriöt

Liiketoiminnan tärkeimmät prosessit ovat ne toiminnot, joita ilman liiketoiminta ei pysty jatkumaan.

Riskianalyysi

Tässä osiossa selvitetään erilaiset poikkeamat, jotka johtavat liiketoiminnan keskeytyksiin, sekä kuvataan poikkeamia, jotka voivat johtaa vakaviin seurauksiin liiketoiminnallesi.

- Tärkeät järjestelmät, kuten [esimerkki], eivät toimi [ajanjakson] aikana
- Toimistolle tai liiketiloille pääsy on fyysisesti estynyt, mutta järjestelmät toimivat.
- Toimistolle tai liiketiloille pääsy on fyysisesti estynyt ja järjestelmät ovat poissa käytössä.
- Tietoteknisten tietojen häviäminen tai vahingoittuminen (virustorjuntaohjelman tilauksen uudistaminen unohtuu tai tilauksen vanhenemista ei huomata)
- Laitteiston virhetoiminta
- Varkaus tai ilkivalta, yrityksen sisäinen ilkivalta (esim. tyytymättömän työntekijän aiheuttamat ongelmat)
- Vesivahinko
- Tiloihin pääsyn estävä ulkoinen tekijä (Toimistoavaimen hukkaaminen)

- Tärkeän kumppanin tai toimittajan menetys
- Liikenneverkon häiriöt
- Kyberhyökkäys
- Tulva, tulipalo tai muu luonnonkatastrofi

Hätätilanteen yhteydenottolomake

Hätätilanteen yhteydenottolomakkeen avulla työntekijöillä on helppo pitää yhteyttä sopiviin henkilöihin, jotta järjestelmäsi saadaan taas toimimaan.

Sisällytä tärkeitä yksityiskohtia, kuten:

- Koko nimi
- Tehtävännimike
- Yhteystiedot (työpuhelinnumero, sähköposti, jne.)

Kenen yhteystiedot tarvitset?

- Isännöitsijä
- Sähköyhtiön yhteyshenkilö
- Vakuutus yhteyshenkilö
- Laitetoimittajat
- IT-tuki

Liiketoiminnan jatkuvuussuunnitelman päivitys ja muita tietoja

Harjoittele säännöllisesti hätätilanteita. Harjoituksen aikana jatkuvuussuunnitelmastasi saattaa löytyä heikkouksia. Näitä heikkouksia

kannattaa käyttää suunnitelman parantamiseen. Tämä varmistaa, että suunnitelma on ajan tasalla.

Sisällytä seuraavat tiedot tähän osioon:

- Liiketoiminnan jatkuvuussuunnitelman vastaava
- Tehtävännimike
- Palautussuunnitelman luonti- ja päivitys päivämäärä
- Päivityksen kuvaus

Jatkuvuussuunnitelman tiimi

Liikennetoiminnan jatkuvuussuunnitelman tiimin jäsenten nimeäminen takaa, että toiminta on poikkeamatilanteissa suunnitelmallista. Kun roolit ja tehtävät on määritelty ennakkoon, kykenee yritys toimimaan suunnitelmallisesti eikä sijaa hämmennykselle jää. Liiketoiminta pääsee palautumaan normaalin nopeammin. On myös hyvä miettiä, kuka rooleista vastaa loma-aikoina ja pyhäpäivinä. Onko työntekijöillä myös henkilökohtainen puhelinnumerosi, jotta he saavat sinut kiinni tarvittaessa?

Sisällytä tärkeitä yksityiskohtia, kuten:

- Nimi
- Tehtävänimike
- Rooli jatkuvuussuunnitelmassa
- Yhteystiedot (työpuhelinnumero, sähköposti, jne.)
- Työntekijöiden roolit ja vastuut.

Mitä on palautumissuunnitelma ja mitä sisältää?

Palautussuunnitelma on asiakirja, joka auttaa yritystäsi käsittelemään odottamattomia tapauksia, kuten esimerkiksi kyberhyökkäyksiä tai sähkökatkoksia. Nämä tapahtumat voivat sulkea yrityksen IT-järjestelmät ja haitata yrityksen toimintaa. Palautussuunnitelman tavoitteena on saada yrityksesi toimimaan mahdollisimman nopeasti katastrofin tai tietomurron aikana. Tehokkaan palautussuunnitelman avulla pienennät riskiä menettää rahaa. Varmuuskopiot ovat tässä avainasemassa. Erityisen tärkeää on turvata luottamukselliset tiedot (esim. henkilötunnukset, luottokorttitiedot).

Palautussuunnitelma sisältää tietopalvelujen varmuuskopiointimenettelyt, palautusmenettelyt, internet sivun palauttaminen, palautumisprosessi ja ohje tietojen palauttaminen varmuuskopiolta.

Tietolaitteiden, ohjelmistojen ja palveluiden inventaari

Luetteloi laitteet yksityiskohtaisesti, kuten esimerkiksi:

- Malli, tuotenumero
- Laitetoimittaja
- Lyhyt kuvaus tuotteesta (esim. pieni musta laatikko, harmaa tulostin)
- Muut tiedot (kaistanleveys, liitteet, lisävarusteet, jne.)

Asetellee tavoitteet:

- Tarvittaessa palautusajan tavoite (esimerkiksi tietokone saatu toimimaan X päivässä)
- Tarvittaessa palautumispisteen tavoite (tavoitteena palauttaa 80 % tiedoista)

11.1.1 Liiketoiminnan jatkuvuussuunnitelman pohja

Liiketoiminnan jatkuvuussuunnitelman **yksinyrittäjille** - pohja voit ladata

https://www.xamk.fi/wp-content/uploads/2022/07/liiketoiminnan-jatkuvuussuunnitelma-yksinyrittajille.docx

Liiketoiminnan jatkuvuussuunnitelman **mikroyrittäjille** - pohja voit ladata

https://www.xamk.fi/wp-content/uploads/2022/07/liiketoiminnan-jatkuvuussuunnitelma-mikroyrittajille.docx

Liiketoiminnan jatkuvuussuunnitelman pohjat ovat suuntaa antava. Muokkaa sen yrityksen tarpeiden mukaan.

Ensimmäisessä esimerkissä on Essi. Essillä on pieni siivousyritys ja hän on yksinyrittäjä. Hän siivo pientiloja. Essillä ei ole oma toimisto.

Liiketoiminnan jatkuvuussuunnitelma

Essin siivouspalvelu Versio 1

Kirkkokatu 12.7.2022

48100 Kotka

Essinsiivouspalvelu.fi

Version historia				
Versio	Hyväksymä	Tarkistus-päivämäärä	Muutoksen kuvaus	Kirjoittaja

Avainhenkilöstö ja yhteystiedot

Nimi	Nimike	Puhelin	Sähköposti
Jere Mattila	IT-tuki	040-111 1111	jere@essille-tuki.fi

Mitkä ovat minun tärkeimmät sovellukseni?

• Outlook	• Isolta.fi • WordPress

Mitkä ovat minun tärkeimmät työvälineeni?

• Tulostin • Kannettava tietokone • Puhelin	• Internet-yhteys • Siivousvälineet • Siivousaineet

Tavoite

Jatkuvuussuunnitelman tavoite on tarjota väline hätätilanteeseen / poikkeamaan, joka uhkaa häiritä normaalia liiketoimintaa.

Hätätilanne on todellinen tai uhkaava tilanne, joka voi aiheuttaa häiriöitä tai menetyksiä organisaation tavanomaisessa liiketoiminnassa siinä määrin, että se muodostaa sille uhan. Poikkeama on mikä tahansa tapahtuma, joka voi johtaa liiketoiminnan häiriöön tai rahallisia menetyksiä.

Jatkuvuussuunnitelman avulla voidaan varmistaa liiketoiminnan kannalta kriittisten palvelujen jatkuminen minimoimalla henkilöstölle, tiloille, laitteille tai arkistoille mahdollisesti aiheutuvien vahinkojen vaikutukset. Suunnitelma auttaa pienentämään poikkeamien riskit.

Liiketoiminnan kannalta tärkeimmät prosessit

Liiketoiminnan tärkeimmät prosessit ovat ne toiminnot, joita ilman liiketoiminta ei pysty jatkumaan.

Suunnitelman laajuus

Liiketoiminnan jatkuvuussuunnitelmasta käy ilmi, miten yritys voi vähentää poikkeamaan mahdollisissa vaikutuksia valmistautumalla säilyttämään palvelut seuraavissa tilanteissa:

- Keskeisten tilojen menetys
- Tietotekniikan / tietojen menetys
- Televiestinnän menetys
- Kovalevyjen / paperitietojen katoaminen
- Sähkö- ja/tai vesikatkos
- Keskeisen yhteistyökumppanin / toimittajan menettäminen
- Sääolojen aiheuttamat häiriöt

Riskien arviointi

Riski	Todennäköisyys	Vaikutus	Yleiset valvontatoimenpiteet	Mahdolliset jatkotoimet
Tulipalo, joka tuhoaa tilat kokonaan tai osittain.	matala	korkea	Sähkölaitteiden säännöllinen huoltaminen	Sähkölaitteen vaihtaminen
Tietokone- tai toimistolaitteiden varastaminen	matala	keskitasoinen	Tee säännöllisisä varmuuskopiot ja säilyttää niitä eri paikassa kuin muut koneet.	Tarkista
Laitteiston virhetoiminta	keksitasoinen	korkea	Laitteiden säännöllinen tarkistaminen	Laitteiden huolto
Tietoteknisten tietojen häviäminen tai vahingoittuminen	matala	matala	Varmuuskopion tekeminen	Tarkista, pystytkö palauttaa tiedostoja varmuuskopiolta.
Tietoliikenneyhteyksien menetys	matala	matala	Pidä kalenteri ja	

			tärkeimmät yhteystiedot paperiversionakin	
Sähkökatko (enintään 3 pv)	matala	keskitasoinen	Pidä ladattu virtapankki puhelimen lataamiseen varten	
Yrittäjän vakava loukkaantuminen/kuoleminen	matala	korkea	Nimitä henkilö, joka voi asioida sinun puolestasi siinä tapauksessa.	Kirjoitta tärkeimmät salasanat ja käyttäjätunnukset paperiin.
Vesivahinko	matala	keskitasoinen	Varmista, että astianpesukoneen ja pesukoneen vesiliittymät ovat kiinni, kun et käytät koneita.	Vakuutus
Ilkivalta	matala	matala	Laitta ovet lukkoon, kun et ole kotona.	
Tiloihin pääsyn estävä ulkoinen tekijä (esim.	matala	matala	Vara-avain naapurilla.	Lukojen vaihtaminen.

toimistoavaimen hukkaaminen)				
Tärkeän yhteistyökumppanin tai toimittajan menetys	matala	matala		Etsi uuttaa toimittaja.
Kyberhyökkäys	matala	keksitasoinen	• Nouda kyberhygieniaa. • Tee varmuuskopiot. • Turva omat ja asiakkaan tiedot	• Vakuutus • Tietojen palauttaminen • Tee rikosilmoitus • Informoi tarvittaessa asiakkaita ja muita henkilöitä / yrityksiä, joita datavuoto koskee.

Todennäköisyys	matala	keskitasoinen	korkea
Vaikutus	matala	keksitasoinen	korkea

Tarkistuslista

Pidä muistipanot kaikista toteutetuista toimenpiteistä hätätilanteesta/poikkeamasta.

Arvioi tilanne ja tarvittava reagointitaso:	☐ Heti	☐ Viikon sisällä	☐ 2 viikon sisällä

Avainhenkilöstö ja yhteystiedot

Nimi	Nimike	Puhelin	Sähköposti
Netvisor	Asiakaspalvelu	010 505 8490	tuki.netvisor@visma.fi
Jere Pasuri	IT-tuki	040 111 1111	jere@essille-tuki.fi
Kiilto	Asiakaspalvelu	0207 710 100	asiakaspalvelu@kiilto.com
Eeva Korhonen	Isännöinti	050 222 2222	eeva@minun-talo.fi
Heli Kiviranta	Vakuutus	020 333 3333	Heli@minunvakuutus.fi

Yrityksen resurssit, varusteet, järjestelmät ja tallenteet

Prosessit/Tarvikkeet	**Heti**	**Viikon sisällä**	**2 viikon sisällä**
Siivousvälineet			
Siivousaineet	x		
Imuri	x		
Pesulaput	x		

Moppi	x		
Laitteet			
Puhelin	x		
Kannettava tietokone		x	
Tulostin			x
USB-tikku		x	
Asiakirjat			
Varmuuskopiot		x	
Paperiasiakirjat		x	
Sovellukset			
Microsoft Office		x	
Muita			

Hätätapauksen tarkistuslista:

Toiminta	Muistinpanot	Tehty
Oletko soittanut yhteistyökumppaneille?	Kuka: • IT-tuki • Vakuutusyhtiö • Isännöinti	☐ ☐ ☐
Onko puhelin ja tietokoneen laturit saatavilla?	• Tietokone • Puhelin	☐ ☐
Kenelle sinun on ilmoitettava mahdollisista muutoksista?	• Siirrä tämän päivän tapaamisia tarvittaessa	☐
Väliaikainen työpiste: • Riittäväkö käytettävissä oleva tila kaikkiin yritysten tarpeisiin tai tarvitsetko lisätilaa?	☐ Kyllä ☐ Ei	☐
• Onko sinun vaihdettava laitteita?	☐ Kyllä ☐ Ei	☐
	☐ Kyllä ☐ Ei	☐
• Onko sinulla pääsy kaikkiin olennaisiin järjestelmiin ja tietoihin? • Pitääkö postisi ohjata väliaikaiseen työpisteeseen?	☐ Kyllä ☐ Ei	☐
Tarvitsetko muita toimintamenettelyjä ja/tai ohjeita. Mitä?	**Toimintamenettely:** • **Ohjeet:**	☐

	• Tietojen palauttaminen varmuuskopiolta	☐
Ilmoita muille yhteistyökumppaneille, tavarantoimittajille jne. normaalien palvelujen / yhteistietojen palauttamisesta, kun kaikki on palautunut normaaliin.	Yhteistyökumppanit Tavaratoimittajat	☐ ☐
Taloudelliset menettelyt: • Kenellä on lupa hyväksyä lisämenot? • Pidä kirjaa kaikista menoista.	Kuka: •	☐ ☐
Tietojen säilyttäminen • Yritä palauttaa mahdollisimman paljon asiakirjaa ja säilytä ne jossakin, josta ne ovat helposti saatavissa.	Onko varmuuskopio?	☐
	Onko palautumisohje?	☐
	Onko kopiot paperillisista asiakirjoista?	☐
Kun poikkeama on ohi ja normaali tila on saavutettu, kerro asiasta asiakkaille.		☐
Tarkastelee toiminnan jatkuvuussuunnitelmaa ja arvioi tehty päätökset.		☐

Palautumissuunnitelma

Tietopalvelujen Varmuuskopiointimenettelyt

Tee näin suurten häiriöiden sattuessa:

- Pysy rauhassa.
- Hae liiketoiminnan jatkuvuussuunnitelman tarkistuslista
- Hae hätätapauksen tarkistuslista
- Toimii ohjeiden mukaan

Palautumismenettelyt

Nämä laitteet, henkilöt ja palvelut tarvitset välittömästi voidaksesi jatkaa liiketoimintaasi:

- Puhelin
- Varmuuskopio
- Tietokone

Internet sivun palauttaminen

Tiedot, jotka tarvitset verkkosivustosi palauttamiseen_

- Pilvipalvelun yhteystiedot: puhelinnumero, sähköposti
- Telia asiakaspalvelu: puhelinnumero, sähköposti

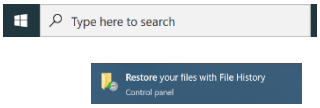
Palautumisprosessi

Nämä ovat vaiheet ja resurssit, joita tarvitaan häiriöiden tai liiketoiminnan palauttamiseksi.

- Varmuuskopio
- Tietokone
- Internet-yhteys
- Palautumisohje

Ohje tietojen palauttaminen varmuuskopiolta

1. Kirjoittaa hakukenttään ”**Restore Files / Varmuuskopioi ja palauta**”



2. Valitse ”**Restore your Files with File History/Palauta tiedostot Tiedostohistoria-toiminnon avulla**”
3. Etsi tarvitsemasi tiedosto ja käytä sitten nuolia nähdäksesi kaikki sen versiot.
4. Tallenna se alkuperäiseen sijaintiinsa valitsemalla Palauta.
5. Jos haluat tallentaa sen toiseen paikkaan, napsauta hiiren kakkospainikkeella Palauta, valitse Palauta kohteeseen ja valitse sitten uusi sijainti.

Liiketoiminnan jatkuvuussuunnitelman testit ja harjoitukset

Tämä on suunnitelma, joka tehdään hätätilanteen harjoittelua ja varautumista varten.

Testattu	Päivämäärä:		Seuraava testaus	*vuosi myöhemmin*
Harjoitus	Päivämäärä:		Seuraava harjoitus	*vuosi myöhemmin*

Tietolaitteiden, ohjelmistojen ja palveluiden inventaari

Laite	Malli	Tuotenumero	Laitetoimittaja	Lyhyt kuvaus	Muut tiedot	Hinta €
Kannattava tietokone	Lenovo IdeaPad 1	82LX0048MX	Verkkokauppa.com	Kannattava tietokone, harma	Windows 11 Home S	399,90 €
Tulostin	Epson Expression Home XP-2155	C11CH02408	Verkkokauppa.com	Mustesuihkumonitoimitulostin, musta	Mustepatruunat: Epson 603	57,99 €
Puhelin	Samsung Galaxy A22 5G	SM-A226B/DSN	Telia	Älypuhelin, vihreä		199 €
USB-tikku	Transcend JetFlash 350	TS4GJF350	Verkkokauppa.com	USB-muistitikku, musta	4 Gt	9,99 €

Microsoft Office	Microsoft 365 Family		microsoft.com	Word, Excel, Outlook	6 käyttäjää	10 €/kk
Laskutusohjelma	Isolta		isolta.com	Laskut ja palkanmaksut		10,90 €/kk
Nettisivu	Wordpress		Essinsiivouspalvelu.fi	WordPress-nettisivu		5 €/kk
Puhelinliittymä	5G-liittymä		Telia	Puhelinliittymä	5G, Rajaton netti, puhelut ja viestit rajaton	31,99 €/kk

Toisessa esimerkissä on Jussi. Jussilla on perheyritys. Hänen yrityksessänsä työskentelevät perheen lisäksi 3 vakituisia työntekijä. Jussilla on kalayritys.

Liiketoiminnan jatkuvuussuunnitelma

Paras Kala Kymenlaaksossa Versio 1

Virojoentie 23.6.2022

49900 Virolahti

paras-kala.fi

Version historia				
Versio	Hyväksymä	Tarkistus-päivämäärä	Muutoksen kuvaus	Kirjoittaja

Avainhenkilöstö ja yhteystiedot

Nimi	Nimike	Puhelin	Sähköposti
Jussi Alismäki	Johtaja	040 444 4444	jussi@paras-kala.fi
Anneli Alismäki	Lähiesihenkilö	040 444 4444	anneli@paras-kala.fi
Jyrki Ahven	Työntekijä	050 555 5555	jyrki@paras-kala.fi

Mitkä ovat minun tärkeimmät sovellukseni?

• Microsoft Office 365 • Isolta.fi	• Netvisor.fi • Vilkas.fi

Mitkä ovat minun tärkeimmät työvälineeni?

• Tulostin • Pöytäkone • Puhelin	• Internet-yhteys • Kassa • Maksupääte

Tavoite

Jatkuvuussuunnitelman tavoite on tarjota väline hätätilanteeseen / poikkeamaan, joka uhkaa häiritä normaalia liiketoimintaa.

Hätätilanne on todellinen tai uhkaava tilanne, joka voi aiheuttaa häiriöitä tai menetyksiä organisaation tavanomaisessa liiketoiminnassa siinä määrin, että se muodostaa sille uhan. Poikkeama on mikä tahansa tapahtuma, joka voi johtaa liiketoiminnan häiriöön tai rahallisia menetyksiä.

Jatkuvuussuunnitelman avulla voidaan varmistaa liiketoiminnan kannalta kriittisten palvelujen jatkuminen minimoimalla henkilöstölle, tiloille, laitteille tai arkistoille mahdollisesti aiheutuvien vahinkojen vaikutukset. Suunnitelma auttaa pienentämään poikkeamien riskit.

Liiketoiminnan kannalta tärkeimmät prosessit

Liiketoiminnan tärkeimmät prosessit ovat ne toiminnot, joita ilman liiketoiminta ei pysty jatkumaan.

Suunnitelman laajuus

Liiketoiminnan jatkuvuussuunnitelmasta käy ilmi, miten yritys voi vähentää poikkeamaan mahdollisissa vaikutuksia valmistautumalla säilyttämään palvelut seuraavissa tilanteissa:

- Keskeisten tilojen menetys
- Tietotekniikan / tietojen menetys
- Televiestinnän menetys
- Kovalevyjen / paperitietojen katoaminen
- Sähkö- ja/tai vesikatkos
- Keskeisen yhteistyökumppanin / toimittajan menettäminen
- Sääolojen aiheuttamat häiriöt

Riskien arviointi

Riski	Todennäköisyys	Vaikutus	Yleiset valvontatoimenpiteet	Mahdolliset jatkotoimet
Tulipalo, joka tuhoaa tilat kokonaan tai osittain.	matala	korkea	Sähkölaitteiden säännöllinen huoltaminen	Sähkölaitteiden vaihtaminen
Tietokone- tai toimistolaitteiden varastaminen	matala	korkea	Tee säännöllisisä varmuuskopiot ja säilyttää niitä eri paikassa kuin muut koneet.	Tarkista
Laitteiston virhetoiminta	keskitasoinen	korkea	Laitteiden säännöllinen tarkistaminen	Laitteiden huolto
Tietoteknisten tietojen häviäminen tai vahingoittuminen	matala	keksitasoinen	Varmuuskopion tekeminen	Tarkista, pystytkö palauttamaan tiedostoja varmuuskopiolta.
Tietoliikenneyhteyksien menetys	matala	keksitasoinen	Pidä kalenteri ja	

			tärkeimmät yhteystiedot paperiversionakin	
Sähkökatko (enintään 3 pv)	matala	korkea	Pidä ladattu virtapankki puhelimen lataamiseen varten, varmista generaattorin toiminta aika ajoin	
Yrittäjän vakava loukkaantuminen/kuoleminen	keskitasoinen	korkea	Nimitä henkilö, joka voi asioida sinun puolestasi siinä tapauksessa.	Kirjoitta tärkeimmät salasanat ja käyttäjätunnukset paperiin.
Vesivahinko	matala	korkea	Varmista, että astianpesukoneen ja pesukoneen vesiliittymät ovat kiinni, kun et käytät koneita.	Vakuutus

Ilkivalta	matala	keskitasoinen	Laitta ovet lukkoon, kun et ole yrityksen tiloissa.	Kameravalvonnan asennus/parantaminen
Tiloihin pääsyn estävä ulkoinen tekijä (Toimistoavaimen hukkaaminen)	matala	keskitasoinen	Vara-avain naapurilla.	Lukojen vaihtaminen.
Tärkeän kumppanin tai toimittajan menetys	matala	keskitasoinen		Etsi uuttaa toimittaja.
Liikenneverkon häiriöt	matala	matala	Varmista useampia maksuvaihtoehtoja	
Kyberhyökkäys	matala	korkea	• Noudata kyberhygieniaa. • Tee varmuuskopiot. Turva omat ja asiakkaan tiedot	• Vakuutus • Tietojen palauttaminen • Tee rikosilmoitus Informoi tarvittaessa asiakkaita ja muita henkilöitä / yrityksiä, joita datavuoto koskee.

Todennäköisyys	matala	keskitasoinen	korkea
Vaikutus	matala	keksitasoinen	korkea

Tarkistuslista

Pidä muistipanot kaikista toteutetuista toimenpiteistä hätätilanteesta/poikkeamasta.

Arvioi tilanne ja tarvittava reagointitaso:	☐ Heti	☐ Viikon sisällä	☐ 2 viikon sisällä

Avainhenkilöstö ja yhteystiedot

Nimi	Nimike	Puhelin	Sähköposti
Netvisor	Asiakaspalvelu	010 505 8490	tuki.netvisor@visma.fi
Jere Pasuri	IT-tuki	040 111 1111	jere@jussille-tuki.fi
Kiilto	Asiakaspalvelu	0207 710 100	asiakaspalvelu@kiilto.com
Eeva Tuk	Isännöinti	050 222 2222	eeva@minun-talo.fi
Heli Kiviranta	Vakuutus	020 333 3333	Heli@minunvakuutus.fi

Yrityksen resurssit, varusteet, järjestelmät ja tallenteet

Prosessit/Tarvikkeet	**Heti**	**Viikon sisällä**	**2 viikon sisällä**
Huonekalut			
Työpöytä		x	
Tuoli		x	
Arkistointikaappi			x

Kylmälaitteet	x		
Laitteet			
Puhelin		x	
Kannettava tietokone		x	
Tulostin		x	
Ulkoinen kiintolevy			x
Maksupääte	x		
Valvontakamera		x	
Reititin	x		
Asiakirjat			
Varmuuskopiot			x
Paperiasiakirjat		x	
Sovellukset			
Microsoft Office			
Sähköposti	x		
Internet-yhteys	x		
Laskutusohjelma		x	
Valvontakameroiden hallinta		x	
Muita			
Ilmastointi	x		
Varasto	x		
Kalan käsittely alue	x		
Generaattori		x	

Hätätapauksen tarkistuslista:

Toiminta	Muistinpanot	Tehty
Oletko soittanut yhteistyökumppaneille?	Kuka: • IT-tuki • Vakuutusyhtiö • Isännöinti	☐ ☐ ☐
Oletko ilmoittautunut työntekijöille?	Työntekijät: • Essi • Jussi • Katariina	☐ ☐ ☐
Onko puhelin ja tietokoneen laturit saatavilla?	• Tietokone • Puhelin	☐ ☐
Kenelle sinun on ilmoitettava mahdollisista muutoksista?	• Siirrä tämän päivän tapaamisia tarvittaessa	☐
Väliaikainen työpiste: • Riittäväkö käytettävissä oleva tila kaikkiin yritysten tarpeisiin tai tarvitsetko lisätilaa?	☐ Kyllä ☐ Ei	☐
• Onko sinun vaihdettava laitteita?	☐ Kyllä ☐ Ei	☐
	☐ Kyllä ☐ Ei	☐
• Onko sinulla pääsy kaikkiin olennaisiin järjestelmiin ja tietoihin? • Pitääkö postisi ohjata väliaikaiseen työpisteeseen?	☐ Kyllä ☐ Ei	☐

Tarvitsetko muita toimintamenettelyjä ja/tai ohjeita. Mitä?	**Toimintamenettely:** • **Ohjeet:** • Tietojen palauttaminen varmuuskopiolta	☐ ☐
Ilmoita muille yhteistyökumppaneille, tavarantoimittajille jne. normaalien palvelujen / yhteistietojen palauttamisesta, kun kaikki on palautunut normaaliin.	Yhteistyökumppanit Tavaratoimittajat	☐ ☐
Taloudelliset menettelyt: • Kenellä on lupa hyväksyä lisämenot? • Pidä kirjaa kaikista menoista.	Kuka: •	☐ ☐
Tietojen säilyttäminen • Yritä palauttaa mahdollisimman paljon asiakirjaa ja säilytä ne jossakin, josta ne ovat helposti saatavissa.	Onko varmuuskopio?	☐
	Onko palautumisohje?	☐
	Onko kopiot paperillisista asiakirjoista?	☐
Kun poikkeama on ohi ja normaali tila on saavutettu, kerro asiasta asiakkaille.		☐

Tarkastelee toiminnan jatkuvuussuunnitelmaa ja arvioi tehty päätökset.		☐

Palautumissuunnitelma

Tietopalvelujen Varmuuskopiointimenettelyt

Tee näin suurten häiriöiden sattuessa:

- Pysy rauhassa.
- Hae liiketoiminnan jatkuvuussuunnitelman tarkistuslista
- Hae hätätapauksen tarkistuslista
- Toimii ohjeiden mukaan

Palautumismenettelyt

Nämä laitteet, henkilöt ja palvelut tarvitset välittömästi voidaksesi jatkaa liiketoimintaasi:

- Maksupääte
- Internetyhteys
- Reititin
- Varmuuskopio
- Tietokone

Internet sivun palauttaminen

Tiedot, jotka tarvitset verkkosivustosi palauttamiseen_

- Pilvipalvelun yhteystiedot: puhelinnumero, sähköposti
- Telian asiakaspalvelu: puhelinnumero, sähköposti

Palautumisprosessi

Nämä ovat vaiheet ja resurssit, joita tarvitaan häiriöiden tai liiketoiminnan palauttamiseksi.

- Varmuuskopio
- Tietokone
- Internet-yhteys
- Palautumisohje

Tietojen palauttaminen varmuuskopiolta

6. Kirjoittaa hakukenttään ”**Restore Files / Varmuuskopioi ja palauta**”
7. Valitse ”**Restore your Files with File History/Palauta tiedostot Tiedostohistoria-toiminnon avulla**”
8. Etsi tarvitsemasi tiedosto ja käytä sitten nuolia nähdäksesi kaikki sen versiot.
9. Tallenna se alkuperäiseen sijaintiinsa valitsemalla Palauta.
10. Jos haluat tallentaa sen toiseen paikkaan, napsauta hiiren kakkospainikkeella Palauta, valitse Palauta kohteeseen ja valitse sitten uusi sijainti.

Liiketoiminnan jatkuvuussuunnitelman testit ja harjoitukset

Tämä on suunnitelma, joka tehdään hätätilanteen harjoittelua ja varautumista varten.

Testattu	Päivämäärä:		Seuraava testaus	*vuosi myöhemmin*
Harjoitus	Päivämäärä:		Seuraava harjoitus	*vuosi myöhemmin*

Tietolaitteiden, ohjelmistojen ja palveluiden inventaari

Laite	Malli	Tuotenumero	Laitetoimittaja	Lyhyt kuvaus	Muut tiedot	
Kannattava tietokone	Lenovo IdeaPad 1	82LX0048MX	Verkkokauppa.com	Kannattava tietokone, harma	Windows 11 Home S	399,90 €
Tulostin	Epson Expression Home XP-2155	C11CH02408	Verkkokauppa.com	Mustesuihkumonitoimitulostin, musta	Mustepatruunat: Epson 603	57,99 €
Puhelin	Samsung Galaxy A22 5G	SM-A226B/DSN	Telia	Älypuhelin, vihreä		199 €
Ulkoinen kiintolevy	LaCie Rugged USB-C		Gigantti	Ulkoinen kiintolevy	2 TB	89,99 €

Microsoft Office	Microsoft 365 Family		microsoft.com	Word, Excel, Outlook	6 käyttäjää	10 €/kk
Laskutusohjelma	Isolta		isolta.com	Laskut ja palkanmaksut		10,90 €/kk
Nettisivu	Vilkas		Paras-Kala.fi	Vilkas-verkkokauppa		23 €/kk
Puhelinliittymä	5G-liittymä		Telia	Puhelinliittymä	5G, Rajaton netti, puhelut ja viestit rajaton	31,99 €/kk
Reititin	DIR-X1860	D-LINK4320016	Gigantti	WiFi-boksi		99 €
Internetliittymä	Internet-yhteys		Telia	XL-paketti		29,90 €

Valvontajärjestelmä	Arlo Ultra 4K	Arlo VMS5240-100EUS	Gigantti	2x HDR-kamera 1x SmartHub-tukiasema		449 €
Kassajärjestelmä	Jeemly			Kokonainen kassajärjestelmä		89 €/kk

11.2 Kuinka varmistan liiketoiminnan jatkuvuussuunnitelman toimivuuden?

11.2.1 Pidä liiketoiminnan jatkuvuussuunnitelma ajan tasalla

Liiketoiminnan jatkuvuussuunnitelman pitäminen ajan tasalla on välttämätöntä. Kun aikaa kuluu ja yrityksesi kasvaa, myös riskit kasvavat ja muuttuvat. Uudet järjestelmät, laitteet ja IT-palvelut on sisällytettävä suunnitelmaasi ja vanhat poistettava.

11.2.2 Alustavat aiheet liiketoiminnan jatkuvuussuunnitelman testauksessa

Ensisijainen syy suunnitelman testaamiseen on saada selvää, toimisiko se hätätilanteessa. Koska tietoliikennejärjestelmät ovat harvoin staattisia, ne on testattava aina, suurten muutosten jälkeen (esim. uuden tietokoneen hankinta.)

Liiketoiminnan jatkuvuussuunnitelman testausprosessin tarkat yksityiskohdat voivat vaihdella yrityksen vaatimusten mukaan.

11.2.3 Liiketoiminnan jatkuvuussuunnitelman tarkistaminen

Ensimmäisessä askeleessa, käydään työntekijöiden kanssa suunnitelman läpi askel askeleesta ja selitetään jokaiselle työntekijälle heidän omat tehtävänsä ja toimintansa hätätilanteessa.

Toisen askeleen tarkoitus on testata jatkuvuussuunnitelma, matkien mahdollisimman tarkasti todellista hätätilannetta. Tämä auttaa yritystäsi selvittämään sen, tietävätkö kaikki työntekijät mitä heidän pitää tehdä

hätätilanteessa ja onko suunnitelmassa ristiriitoja, puutuvia tietoja tai virheitä.

Simulaatiossa suoritetaan useita skenaarioita sen arvioimiseksi, pystyvätkö työntekijät seuraamaan ohjeistusta ja saamaan liiketoiminta käynnistettyä nopeasti ja onnistuneesti.

11.2.4 Liiketoiminnan jatkuvuussuunnitelma testauksen tarkistuslista

- Tunnista ja mainitse testauksen tavoitteet ja strategiat, joita testausprosessissa käytetään
- Määrittele testin tarkoitus ja arvioi yksityiskohdat
- Muodosta kehitystiimi, johon kuuluu asiantuntijoita useilta aloilta (yrityksen koon mukaan)
- Suunnittele testausprosessille aikataulu testausprosessiin
- Dokumentoi palautussuunnitelman prosessit huolellisesti
- Mainitse testiin tarvittava tekniikka, koulutus ja menettelyt
- Varmista, että testiympäristö on valmis eikä häiritse tuotantojärjestelmiä tai muita toimintoja
- Tee harjoitus mahdollisten ongelmien tunnistamiseksi ja ratkaisemiseksi ennen kuin palautusuunnitelman testi alkaa
- Pysäytä, tarkista ja ratkaise ongelmat aina kun ne ilmestyvät
- Kirjaa raporttiin alkamisaika, päättymisaika, ongelmat, tulokset ja mikä toimi
- Päivitä palautussuunnitelma testin tulosten perusteella

11.3 Vuosikello

Vuosikello on vuosisuunnitelma, jonka avulla organisaatio tai tiimi voi suunnitella ja aikatauluttaa vuoden tekemiset ja prosessit. Sen avulla nähdään pitemmän aikajakson tapahtumat kokonaisuutena, ja sitä voidaan vuoden aikana jatkuvasti tarkentaa.

Vuosikellon pohjat voi ladata meidän verkkosivussamme [verkkosivu].

Hyödyt:

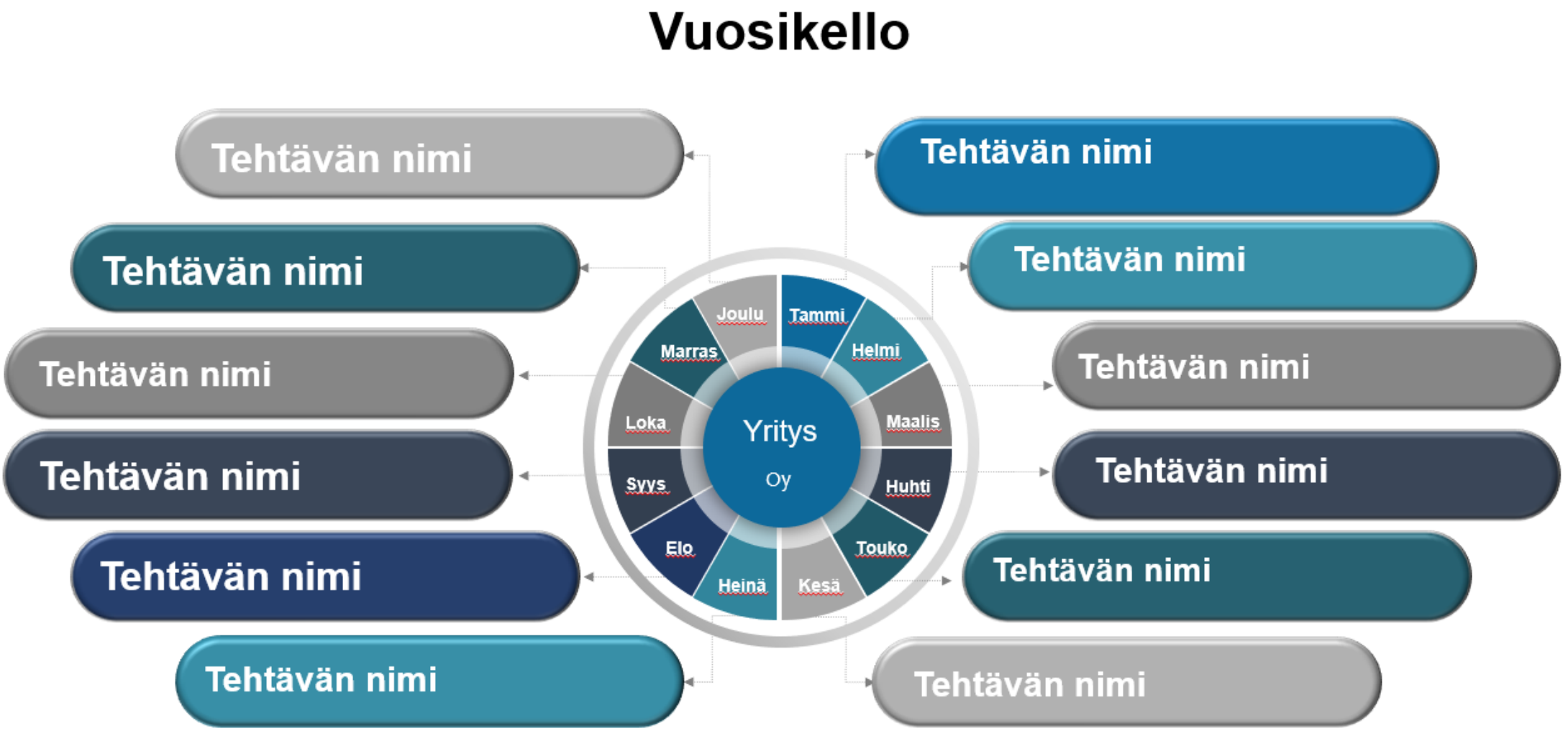
- Ajanhallinta
- Tekemisten ja prosessien läpinäkyvyys
- Tekemisten ennakointi
- Tekemisten ja prosessien kommunikointi
- Systemaattinen & looginen tekeminen
- Päällekkäisten tekemisten ja työkuormien visualisointi

11.3.1 Mitä vuosikelloon kannattaa laittaa?

Esimerkkejä asioista, joita vuosikelloon kannatta ottaa mukaan:

- Kokoukset
- Tiimipalaverit
- Henkilöstöasiat
    - Lomat
- Talouden prosessit
    - Budjetointi
- Koko yrityksen kattavat prosessit
    - Strategiaprosessi
    - Liiketoimintasuunnitelmien tekeminen

Seuraavissa sivuissa löydät kaksi esimerkkejä vuosikellosta/-taulukosta.



Vuosisuunnitelma

YRITYS OY

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan sosiaalirahasto

Elinkeino-, liikenne- ja ympäristökeskus

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Vuosikellopohjat voit ladata meidän verkkosivultamme

https://www.xamk.fi/wp-content/uploads/2022/07/tietoturvan-vuosikello-ja-taulukko.pptx

11.4 Linkit – Palautussuunnitelman pohja

(englanniksi)

- IT Disaster Recovery Planning: A Template https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf
- Smartsheet – Disaster Recovery Plan Templates - https://www.smartsheet.com/disaster-recovery-templates

12 Toiminta ongelmatilanteessa

- Irrota **heti** modeemin virtapiuha seinästä (varmista että verkkolaitteesta sammuu virta, eli valot eivät pala enää)
- Sammuta kannettava / pöytä tietokone (varmista kannettavan tietokoneen sammuminen pitämällä virtanäppäintä pohjassa)
- Hengitä, ota palautussuunnitelma esiin.
- Arvioi vahingot (tarkasta muut laitteet, jotka olivat yhdistettynä samaan verkkoon. Katso näistä laitteista merkkejä haittaohjelmasta. Jos laitteessa ei näy kiristysviestiä, älä siltikään yhdistä sitä verkkoon.)
- Palauta modeemi tehdasasetuksille (useissa modeemeissa on tehdasasetus painike sisäänrakennettu, jota pohjassa painamalla laite käynnistyy tehdasasetuksille.)
- Käynnistä saastunut tietokone siten että se ei ole yhteydessä verkkoon. Asenna käyttöjärjestelmä ja virustorjuntaohjelmisto uudelleen.

- Yhdistä yksi kone kerrallaan modeemiin, odota 10 minuuttia per yhdistetty tietokone/laite. Jos laite ei näytä kiristysviestiä, sammuta laite ja merkitse laite turvalliseksi, jotta et sekoita sitä toisiin. Tee sama kaikille tietokoneille/laitteille, jotka olivat yhdistettynä verkkoon. (Yhdistä laitteet aina siihen modeemiin, joka on laitettu tehdasasetuksille)
- Tarkista ulkoisen varmuuskopion ajantasaisuus ja käy tiedostot ja koko kone varmuuden vuoksi läpi virustorjuntaohjelmistolla.
- Vaihda kaikki verkkopalvelujen salasanat (suositeltavaa tehdä eri verkosta, jos siihen mahdollisuus esim. puhelimen kautta jaettu.)

Lähdeluettelo

Apple – iCloud: https://www.apple.com/fi/icloud/

Digituen tapahtumat - https://dvv.fi/digituen-tapahtumat?fbclid=IwAR1BwsVGn7kMOmzv4EXgGsxLgTG6Ub3JOwERjWrRIlFgmbgNpHRnsjK4z0Q

Dropbox: https://www.dropbox.com

Enisa - Euroopan Unionin kyberturvallisuusvirasto - https://www.enisa.europa.eu

EU:n tietosuojaverkkosivu: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi

Finlex Tietosuojalaki - https://www.finlex.fi/fi/laki/alkup/2018/20181050

GDPR Fines Tracker & Statistics - https://www.privacyaffairs.com/gdpr-fines/

GDPR-tarkistuslista: https://gdpr.eu/checklist/ (englanniksi)

General Data Protection Regulation GDPR - https://gdpr-info.eu

Google – Google Drive: https://www.google.com/intl/fi/drive/

How to back up your Mac with Time Machine – Apple Support https://www.youtube.com/watch?v=geJiTXOb37w

How to Test a Disaster Recovery Plan - https://goabacus.com/how-to-test-a-disaster-recovery-plan/

Kyberturvallisuuskeskus - https://www.kyberturvallisuuskeskus.fi/fi/

Microsoft - Henkilökohtainen OneDrive-pilvitallennus: https://www.microsoft.com/fi-fi/microsoft-365/onedrive/online-cloud-storage

Pieni yhteenveto parhaista ilmaisistä pilvipalveluista: https://www.internetopas.com/parhaat-ilmaiset-pilvipalvelut/

Resources and Information for GDPR - https://www.gdpr.org

The price of stolen info: Everything on sale on the dark web - https://www.helpnetsecurity.com/2022/06/22/stolen-info-sale-dark-web/

Tietosuojavaltuutetun Toimisto - https://tietosuoja.fi/tietosuojavaltuutetun-toimisto

Turvatieto - https://turvatieto.wordpress.com/2013/05/12/esimerkki/

Vale virustorjunta ohjelma, joka on troijalainen: Fake antivirus site promises coronavirus protection, delivers trojan (computerweekly.com)

Valtti Tietopankissa on hyvä opas ”Miten valitset yrityksellesi parhaat pilvipalvelut?”.

Tältä sivustosta voit ladata: https://tietopankki.valtti.com/pilvipalvelut

Varmuuskopioi palauta Winduwos - https://support.microsoft.com/fi-fi/windows/varmuuskopioi-ja-palauta-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef#WindowsVersion=Windows_10

Windows 11: Create full backup to external USB drive and restore (Official) https://www.youtube.com/watch?v=3mUnKQ7ff0Y

Writing a disaster recovery plan for your small business [free template] - https://www.ontrack.com/en-gb/blog/writing-a-disaster-recovery-plan-for-your-small-business-free-template

Yrittäjän tietosuojaopas - https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/