OULUN AMMATTIKORKEAKOULU

# YRITYKSEN LYHYT OPAS KYBERTURVALLISUUTEEN

Käytännön tietoturvakäytännöt pienyrityksille

Henna Törmänen
Opinnäytetyö (AMK)
Syksy 2025
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

# TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma
Tradenomi (AMK)

Tekijä(t): Henna Törmänen
Opinnäytetyön otsikko: Yrityksen lyhyt opas kyberturvallisuuteen
Työn ohjaaja(t): Tanja Kangas
Työn valmistumislukukausi ja -vuosi: syksy 2025
Sivumäärä: 24 + 0

Tämän opinnäytetyön tavoitteensa oli laatia käytännönläheinen ja helposti omaksuttava opas pk-yrityksille kyberturvallisuuden parantamiseksi. Työn taustalla oli havainto, että pienillä yrityksillä on usein puutteelliset kyberturvallisuuskäytännöt ja rajalliset resurssit niiden kehittämiseen, mikä altistaa ne vakaville tieturvauhkille.

Työssä koottiin ja jäsenneltiin tietoa yleisimmistä pk-yrityksiin kohdistuvista kyberuhista, kuten haitta- ja kiristysohjelmista, tietojenkalastelusta, palvelunestohyökkäyksistä sekä sisäisistä uhista. Lisäksi esiteltiin perustason tietoturvakäytäntöjä, verkko- ja laiteturvallisuuden parantamiskeinoja, etätyöskentelyn turvallisuusohjeita sekä tietosuojaan liittyviä keskeisiä vaatimuksia, kuten GDPR:n noudattaminen.

Opinnäytetyön lähteinä käytettiin alan viranomaislähteitä, kuten Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen ohjeistuksia, sekä kansainvälisiä kyberturvallisuusjulkaisuja. Työn tuloksena syntyi selkeä ohjeistus, joka tarjoaa konkreettisia toimenpiteitä kyberuhkien tunnistamiseen ja riskien hallintaan pienyrityksissä.

# ABSTRACT

Oulu University of Applied Sciences
Degree Program in Business Information Systems
Option of Bachelor

Author(s): Henna Törmänen
Title of thesis: Short Guide To Cybersecurity For Businesses
Supervisor(s): Tanja Kangas
Term and year when the thesis was submitted: autumn 2025
Number of pages: 24 + 0

The aim of this thesis was to create a practical and easy-to-use guide to improve cybersecurity in small and medium-sized enterprises (SMEs). The work was motivated by the observation that many SMEs have insufficient cybersecurity practices and limited resources for developing them, making them vulnerable to serious security threats.

The thesis presents the most common cyber threats targeting SMEs, including malware and ransomware, phishing, denial-of-service attacks, and insider threats. It also introduces basic cybersecurity practices, measures to improve network and device security, guidelines for safe remote work, and essential data protection requirements such as compliance with the GDPR.

The study is based on authoritative sources, such as guidelines from the Finnish Transport and Communications Agency's National Cyber security Centre, as well as international cybersecurity publications. The result is a clear set of instructions providing concrete measures to identify cyber threats and manage risks in SMEs.

# SISÄLLYS

## SANASTO

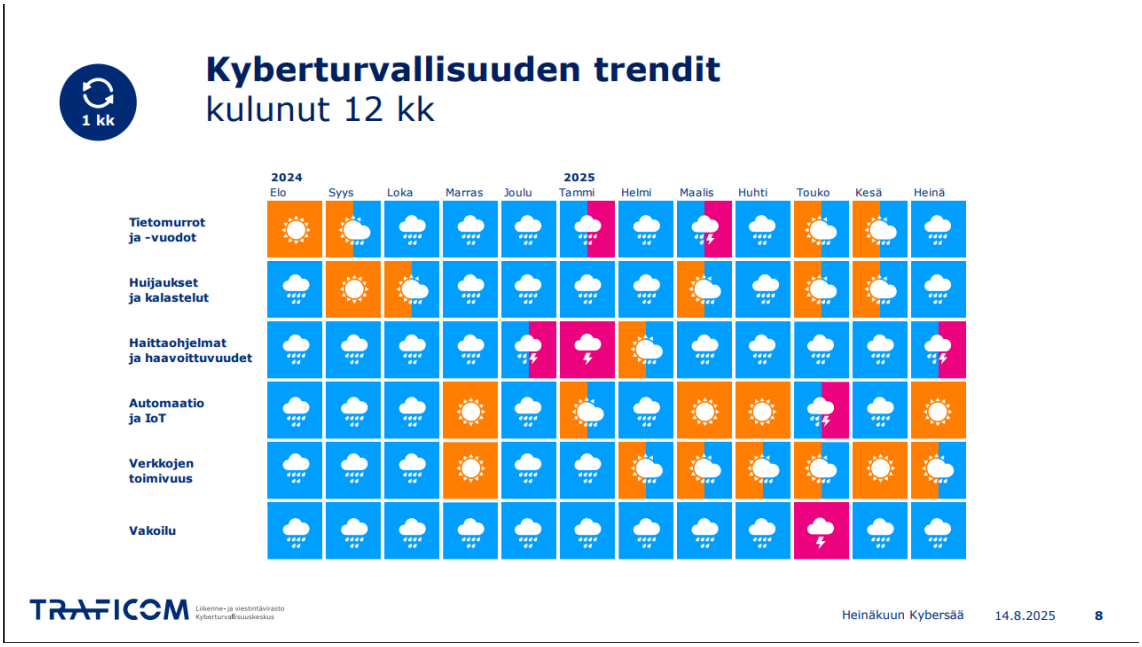
| | |
|---|---|
| BEC | Business Email Compromise. Yrityssähköpostin kaappaamiseen perustuva huijaus, jossa hyökkääjä esiintyy luotettavana liikekumppanina tai esimiehenä. |
| DDoS | Distributed Denial of Service. Hajautettu palvelunestohyökkäys, jonka tavoitteena on kuormittaa palvelu liikenteellä ja estää sen toiminta |
| Digitaalinen allekirjoitus | Kryptografinen menetelmä, jolla varmistetaan viestin tai asiakirjan aitous ja eheys. |
| GDPR | General Data Protection Regulation. Euroopan unionin yleinen tietosuoja-asetus, joka säätelee henkilötietojen käsittelyä. |
| Haittaohjelma | Ohjelma, joka aiheuttaa vahinkoa tietojärjestelmälle, esimerkiksi virus, mato tai troijalainen. |
| Insider threat | Sisäinen uhka. Yrityksen sisältä tuleva uhka, joka voi olla tahaton virhe, huolimattomuus tai tahallinen väärinkäyttö. |
| Kiristyshaittaohjelma | Haittaohjelma, joka salaa tiedostoja ja vaatii lunnaita salauksen purkamiseksi. |
| MFA | Multi-Factor Authentication, monivaiheinen tunnistautuminen. Kirjautumisen vahvistaminen useammalla kuin yhdellä tunnistautumistavalla. (Esimerkiksi salasana + sormenjälki). |
| Phishing | Tietojenkalastelu. Huijausmenetelmä, jossa käyttäjältä yritetään saada luottamuksellisia tietoja esiintymällä luotettavana tahona. |
| Pretexting | Sosiaalisen manipuloinnin muoto, jossa hyökkääjä luo tekaistun tilanteen saadakseen uhrilta luottamuksellisia tietoja. |
| RaaS | Ransonware-as-a-Service. Rikollisille tarjottava palvelumalli, jossa kiristyshaittaohjelma vuokrataan tai myydään. |
| Salasanan | |

| | |
|---|---|
| hallintaohjelma | Sovellus, johon käyttäjä voi tallentaa ja hallita salasanojaan turvallisesti. |
| SOC | Security Operations Center. Organisaation yksikkö, joka valvoo, analysoi ja reagoi kyberturvallisuusuhkiin. |
| VPN | Virtual Private Network, virtuaalinen yksityisverkko. Salaa verkkoliikenteen ja mahdollistaa suojatun yhteyden julkisessa verkossa. |
| WLAN | Wireless Local Area Network. Langaton lähiverkko, joka yhdistää laitteet toisiinsa ilman kaapelointia. |
| Zero Trust – arkkitehtuuri | Kyberturvallisuuden malli, jossa oletetaan, ettei mikään käyttäjä tai laite ole automaattisesti luotettava. |

# 1 JOHDANTO

Tässä opinnäytetyössä käydään käytännönläheisesti läpi pienyritysten suurimpia haasteita kyberturvallisuuden saralla. Tämän opinnäytetyön tarkoituksena on tuoda esille, kuinka käsittelet tietoja turvallisesti ja tiedostat mahdolliset uhat digitaalisessa ympäristössä. Pienyrityksillä on ollut haasteita kyberturvallisuuden kanssa, joka ilmenee Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen päivittäisistä ilmoituksista koskien kyberturvallisuuden vaarantumisesta. (Traficom 2020.)

Aihe on erityisen tärkeä varsinkin pk-yrityksille, koska heillä on alhaisempi kyberpuolustus. Erityisesti kiristyshaittaohjelma ryhmät ovat laajemmin alkaneet hyväksikäyttämään tätä ongelmaa. Useat organisaatiot Suomessa ovat joutuneet kiristyshaittaohjelmien uhriksi viimeisen vuoden aikana ja pahimmassa tapauksessa aiheuttanut tiedostojen katoamista ja lopettaa organisaation toiminnan kokonaan. (Europol 2024; Traficom 2025a.)




*Kuvio 1. Traficomin vuoden kybersää Suomesta: aurinko tarkoittaa rauhallista, sadepilvi huolestuttavaa ja ukkospilvi vakavaa tilannetta. (Traficom 2025b.)*

# 2 PIENYRITYSTEN YLEISIMMÄT UHAT

Digitaalisessa ympäristössä työskennellessä kyberturvallisuus on tärkeä osata ja tunnistaa. Kyberturvallisuus tarkoittaa tavoitetilaa, jossa voidaan luottaa kybertoimintaympäristöön ja jossa sen toimintaa turvataan. Mahdollisia kyberturvallisuus uhkia kutsutaan kyberuhkaksi. Seuraavaksi tarkastellaan yritysten yleisimpiä kyberuhkia. (Turvallisuuskomitea 2018.)

## 2.1 Haittaohjelmat ja kiristysohjelmat

Haittaohjelmilla tarkoitetaan ohjelmia, jotka on suunniteltu tuottamaan vahinkoa tietojärjestelmille tai sen käyttäjille. Ne voivat vaikuttaa koko järjestelmään tai sen yksittäisiin osiin. Esimerkkejä haittaohjelmista ovat muun muassa virukset, madot ja troijalaiset. (Turvallisuuskomitea 2018.)

Yleisimmät leviämistavat ovat sähköpostiin tuleva tietojenkalasteluviesti, tartunnan saanut tiedosto, järjestelmä tai ohjelmiston haavoittuvuus, tartunnan saanut USB-muistitikku tai haitallinen sivusto. (Microsoft 2025b.)

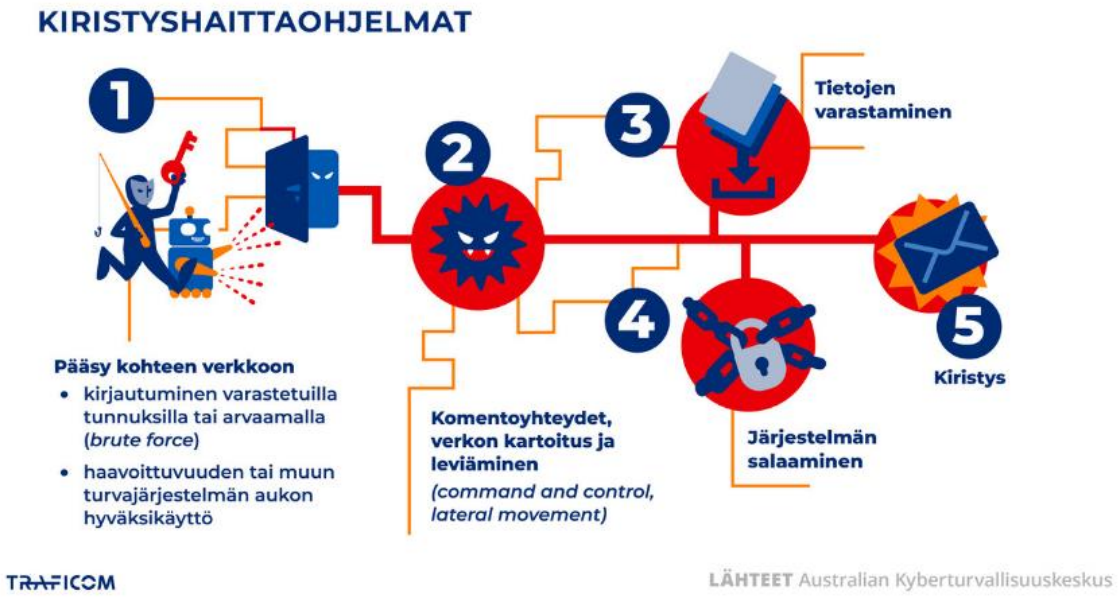
Haittaohjelmien päämääränä on usein taloudellisen hyödyn tavoittelu. Ne voivat esimerkiksi asentua järjestelmään varastaakseen arkaluonteisia tietoja, kuten pankkitunnuksia ja salasanoja, hyödyntääkseen laitteen resursseja kryptovaluutan louhintaan tai seuratakseen käyttäjän toimintoja. Haittaohjelmat voivat myös antaa rikollisille mahdollisuuden varastaa tiedostoja, salata niitä kiristystarkoituksessa tai harjoittaa vakoilua. (Traficom 2020.)

### Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat haittaohjelmien alalaji, jossa haittaohjelma voi tulla esimerkiksi sähköpostin liitetiedostona. Liitetiedoston avattua kiristysohjelma latautuu tietokoneelle, jonka jälkeen ohjelma esimerkiksi muuntaa joitakin tiedostoja salakirjoitettuun muotoon. Kiristyshaittaohjelma vaatii tämän jälkeen lunnaita, jotta se antaisi salauksen avauskoodin. (Turvallisuuskomitea 2018.)

### Miten suojaudut?

Tärkeintä on pitää käyttöjärjestelmät ja ohjelmistot päivitettyinä, varmuuskopioi tiedostot säännöllisesti, suhtaudu varauksella sähköpostissa ladattaviin liitteisiin ja linkkeihin. Muista luoda myös työkoneille omat käyttäjät, joilla ei ole pääkäyttäjän oikeuksia. Pääkäyttäjän oikeuksilla hakkerin on helpompi tehdä vahinkoa. (Traficom 2020a.)




*Kuvio 2. Traficom kiristyshaittaohjelmahyökkäyksen vaiheet. (Traficom 2024b.)*

## 2.2 Sisäiset uhat ja inhimilliset virheet

Sisäinen uhka tarkoittaa yrityksessä työntekijöitä, joilla on yrityksen sisällä pääsy tai käyttöoikeus yrityksen resursseihin, tietoihin tai järjestelmiin, jotka eivät ole yleisesti kaikkien saatavilla. Esimerkiksi henkilöllä voi olla kulkulupa, yrityksen tietokone, verkkoyhteys, pääsy pilviresursseihin, sovelluksiin, tietoihin ja muihin tärkeisiin yrityksen tietoihin. Sisäiset uhat voidaan jaotella neljään eri tyyppiin: Onnettomuus, ilkivaltainen, huolimattomuus ja vehkeily. Onnettomuudessa käyttäjä tekee virheen, joka johtaa mahdolliseen tietoturvahäiriöön. Ilkivaltaisessa tietoturvaloukkauksessa työntekijä tai luotettu henkilö tekee tahallaan jotain, jonka hän tietää vaikuttavan kielteisesti yritykseen. Huolimaton henkilö tietoisesti rikkoo suojauskäytäntöä, joka johtaa tietoturvaloukkaukseen. Vehkeilyssä henkilö tekee yhteistyötä kyberrikollisuusorganisaation kanssa vakoilu- tai varkaustarkoituksessa. (Microsoft 2025d.)

Verizonin Data Breach Investigations Report (DBIR) mukaan noin 60 % kaikista vahvistetuista tietomurroista sisältää inhimillisen komponentin, kuten huomaamattomuuden tai sosiaalisen manipuloinnin. Koulutus tehostaa raportointia, mutta ei poista inhimillistä haavoittuvuutta digitaalisissa tilanteissa. Sisäiset uhat ovat erityisen merkittäviä EMEA-alueella, missä jopa 29 % tietomurroista on peräisin organisaation sisältä- niin tahattomista virheistä kuin luvatusta väärinkäytöstä. Globaalisti virheiden osuus on suuri, mikä korostaa organisaatioiden sisäisten kontrollien merkitystä. (Verizon business 2025.)

## 2.3 Tietojen kalastelu ja sosiaalinen manipulointi

Sosiaalisessa manipuloinnissa käyttäjää pyritään manipuloimaan ja harhauttamaan paljastamaan luottamuksellista tietoa tai toteuttamaan, jotka

vaarantavat heidän turvallisuutensa. Manipuloinnissa hyökkääjä usein esittäytyy luotettavana henkilönä tai lähteenä saavuttaakseen uhrin luottamuksen. Keinoja on monia: hyökkääjä tekeytyy toiseksi henkilöksi, taivuttelee tai hämää saadakseen tärkeitä tietoja, kuten esimerkiksi salasanoja, taloudellisia tietoja ja pääsyn järjestelmiin ja verkkoihin. Loppujen lopuksi hyökkäysten tarkoitus on hyväksikäyttää ihmisen inhimillistä haavoittuvuutta datan tai rahan varastamiseksi. (Euroopan unionin neuvosto 2025.)

Tietojenkalastelu on yksi sosiaalisen manipuloinnin keino ja siinä hyökkääjä lähettää vilpillisiä sähköpostiviestejä tai linkkejä aidoilta näyttäville verkkosivustoille tarkoituksena huijata vastaanottajia klikkaamaan ja paljastamaan luottamuksellista tietoa, kuten esimerkiksi salasanoja, luottokorttinumeroita tai henkilötietoja. Kohdennetussa tietojenkalastelussa hyökkääjä naamioivat viestit vastaamaan tiettyjä kohteesta saatuja tietoja. Tietojenkalastelu sosiaalisen median kautta hyökkääjä käyttää usein hyväkseen suosittuja tai trendaavia aiheita, joiden avulla he luovat vilpillisiä viestejä, jotka vaikuttavat tärkeiltä ja luotettavilta. (Euroopan unionin neuvosto 2025.)

Sosiaalinen manipulointi oli mukana 17 %:ssa kaikista tietomurroista vuonna 2025, mikä nosti sen yhdeksi käytetyimmistä hyökkäysmenetelmistä. Tämän kategorian sisällä erityisesti säikyttely (prompt bombing) - hyökkääjän toistuvat MFA-pyyntöjen lähetykset, joiden tarkoituksena on saada käyttäjä vahvistamaan virheellisen kirjautumisen. (Verizon business 2025.)

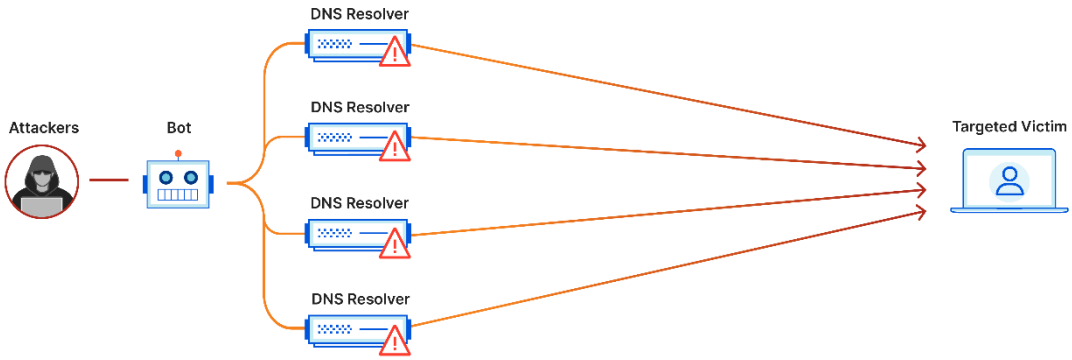
Myös pretexting eli harhautukseen pohjautuvay BEC- hyökkäykset (Business Email Compromise) ovat yleistyneet ja kehittyneet entistä taitavammiksi, minkä myötä tappioiden mediaanikustannus oli noin 50 000 USD tapausta kohden. Vaikka phishing ei ollut suurin suora hyökkäyskanava (ilmaantui noin 14 % tietomurroista), sen rooli on murtojen ketjussa huomattava. Kun mukaan lasketaan salattavien tunnusten väärinkäyttö ja phishing kautta toimitettu haittaohjelma, phishing oli mukana jopa 62 % inhimillisen toiminnan sisältävissä murroissa. Tämän perusteella voidaan arvioida, että yli yksi kolmasosa (37 %) kaikista tietomurroista alkuperäisenä syynä oli juuri phishing tai siihen liittyvä toimintaketju. (Verizon business 2025.)


*Kuvio 3. Traficom tietojenkalastelu Office 365-huijauksessa. (Traficom 2019.)*

## 2.4 Hajautettu palvelunestohyökkäys

Palvelunestohyökkäyksessä pyritään kuormittamaan ja lamaannuttamaan jokin palvelu tai tietojärjestelmä. Esimerkiksi hyökkäys voi lamaannuttaa sähköpostin suurella määrällä sähköpostiviestejä tai reitittimen liian suurella määrällä palvelupyyntöjä. (Turvallisuuskomitea 2018.)

Palvelunestohyökkäyksiä on haastavampi estää, mutta pitämällä palvelinten ohjelmisto ajan tasalla, hyökkäyksiä vaimentavat konfiguraatiot ja monitorointi ratkaisulla. Konfiguraatiot voivat helpottaa järjestelmää muun muassa yksittäisten yhteysten nopeusrajoituksilla, TCP-yhteyksien käsittelyjonon pidennyksillä, keskeneräisten TCP-yhteyksien kierrätystä ja SYN-evästeiden käyttöönotolla. (Traficom 2022b.)




*Kuvio 4. Cloudflare havaintokuva hajautetusta palvelunestohyökkäyksestä. (Cloudflare.)*

# 3 PERUSTASON TIETOTURVAKÄYTÄNNÖT PIENYRITYKSILLE

## 3.1 Laitteiden ja ohjelmistojen päivittäminen

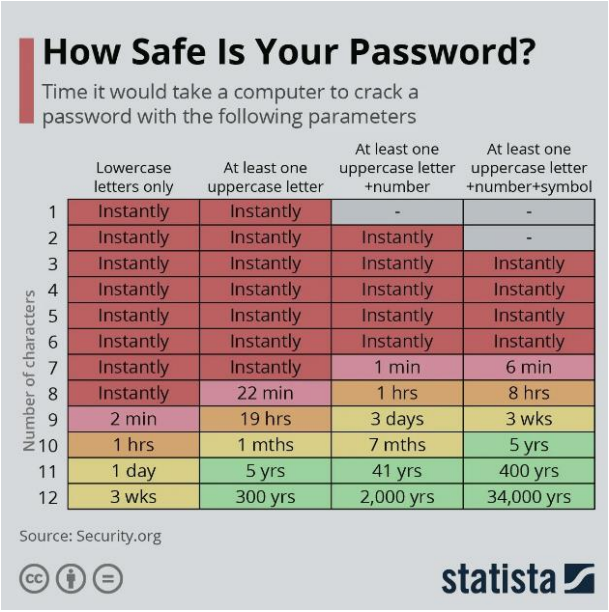
Nykyään laitteita on moneksi ja niiden käyttö on lisääntynyt kaikilla elämänosa-alueilla suuresti. Laitteiden haavoittuvuudet avaavat mahdollisuuden muun muassa hakkereille käyttää tilaisuutta hyväksi ja tehdä mahdollisimman paljon vahinkoa. Tämän takia on tärkeää pitää laitteiden ja niiden ohjelmistojen päivitykset ajan tasalla, jotta riskit ja mahdollisuudet saataisiin minimoitua. Muista pitää esimerkiksi nämä laitteet ajan tasalla: tietoturvaohjelmisto, internetselaimet, käyttöjärjestelmä, sovellukset, ohjelmistot, mobiililaitteet, modeemit, reitittimet ja kaikki muut kodin mahdolliset älylaitteet. (Traficom 2020b.)

Päivitykset ovat kriittinen osa kyberturvallisuutta, sillä haavoittuvuuksien hyväksikäytöt ovat nousseet merkittäväksi hyökkäyskanavaksi. DBIR 2025-raportin mukaan 20 % tietomurroista johtui haavoittuvuuksien hyväksikäytöstä. Osuus on kasvanut 34 % edellisvuoteen verrattuna, mikä kuvaa trendin vakavuutta. (Verizon business 2025.)

## 3.2 Salasanojen hallinta ja monivaiheinen tunnistautuminen

Salasanat suojaavat meidän tärkeitä tietojamme eri palveluissa. Näitä ovat esimerkiksi palvelut, tietosi, rahasi ja identiteettisi. Tämän takia vahva salasana on tärkeä pitääksesi tärkeimmät tiedostosi turvassa. Hyvän salasanan piirteitä ovat muun muassa pitkä ja yksilöllisyys, koska sen arvaaminen on haastavampaa. Vähimmäisvaatimus on ainakin 15 merkkiä ja mieluiten lausemuotoisena kuin yksittäisenä sanana. Tämä voi mahdollistaa käyttämällä erilaisia erikoismerkkejä täydentämään sitä. (Traficom 2023.)

Salasanojen muistamiseen on tehty muun muassa hallintaohjelmia, johon on mahdollista tallentaa eri palveluiden salasanat. Kirjautuesssasi verkkopalveluun ohjelma huolehtii automaattisesti salasanan syöttämisestä. Ennen mahdollisen ohjelman hankkimista kannattaa tarkistaa, että se on yleisesti tunnettu ja säännöllisesti päivittyvä tuote. (Digi- ja väestötietovirasto 2020.)




*Kuvio 5. Kuinka turvallinen on salsanasi? (World Economic Forum 2021.)*

Monivaiheisessa tunnistautumisessa käyttäjätunnuksen ja salasanan lisäksi käytetään yksilöivää tietoa, jotta pääsee kirjautumaan sisään. Se on yksi tehokkaimmista keinoista suojata käyttäjätunnuksia ja estää luvaton pääsy tileille. Muita tunnistautumistapoja voivat olla muun muassa puhelinsovellus tai biometrinen tunniste, kuten esimerkiksi sormenjälki. Tämä estää tehokkaasti tilikaappausta ja tietojenkalastelusta vähemmän hyödyllisiä menetelmiä. Pk-yritysten näkökulmasta monivaiheinen tunnistautuminen on suhteellisen helppo ja kustannustehokas parantaa yrityksen tietoturvaa. (Traficom 2024.)


*Kuvio 6. Monivaiheinen tunnistautuminen. (Traricom 2024a.)*

### 3.3 Tiedon varmuuskopiointi ja palautus

Yritykset säilövät monenlaista tietoa muun muassa laitteilla kuin fyysisesti kuten esimerkiksi paperilla. Tietojen varmuuskopiointi on viime vuosina helpottunut suuresti esimerkiksi muistitikuilla ja erilaisilla pilvipalveluilla. Tiedon varmuuskopioinnin helppouden myötä suositellaan 3-2-1 nyrkkisääntöä: tärkeimmistä tiedostoista pitää olla ainakin kolme kopiota, jotka on tallennettu kahdelle eri medialle, joista yksi on tallennettu fyysisesti eri paikkaan. (Järvinen P. 2022)

National Cyber Security Centre korostaa, että luottamuksellisen ja liiketoiminnalle kriittisen datan varmuuskopiointi on keskeinen osa tietoturvaa. Ajantasaiset ja testatut varmuuskopiot auttavat palauttamaan normaalityön nopeasti esimerkiksi onnettomuuden, teknisen vian tai kyberhyökkäyksen jälkeen, mikä mahdollistaa liiketoiminnan jatkuvuuden. Säännölliset varmuuskopiot kannattaa automatisoida ja suorittaa esimerkiksi viikottain tai kuukausittain datan määrän ja toiminnan kriittisyyden perusteella. Muista myös testata palautus, jotta tiedät miten käyttää häiriötilanteessa. Backup-laitteiden ei tulisi olla jatkuvasti verkkoyhteydessä, koska haittaohjelmat voivat hyödyntää niitä hyökkäyksen aikana. Offline- tai irrotettavat varmuuskopiot (esim. ulkoinen kovalevy) vähentävät riskiä huomattavasti. Pilvipalvelut antavat hyvän saatavuuden ja mahdollisuuden palauttaa aiempia versioita, jos nykyinen tiedosto on vahingoittunut. Huolimattoman pilvitallennuksen riski on se, että hyökkääjä voi tuhota myös

pilvikopiot. jos käyttöoikeudet eivät ole riittävän turvallisia. (National Cyber Security Centre 2017.)

### 3.4 Turvallinen internetin ja sähköpostinkäyttö

Turvallisen internetin käyttöä voidaan tarkastella monella tasolla. Tässä opinnäytetyössä tarkastellaan sitä kahdesta eri näkökulmasta, jotka ovat netin käyttö työpaikalla ja julkisella paikalla. Työpaikalla langaton lähiverkko eli wifi-verkko on tärkeä suojata, koska muulloin tunkeilijan on helppo päästä tunkeutumaan yrityksen eri laitteisiin ja asentamaan esimerkiksi haittaohjelmia.

Wifi-verkon tieturva jatkuu seuraavaksi reitittimeen. Reititin on yleisnimi laitteelle, joka ohjaa verkon ip-paketteja liitännästä tai verkosta toiseen. Käytännössä laite, joka ottaa vastaan internet-yhteyden ja jakaa sen käytettäväksi langattomasti työpaikalla.

Tämän takia on tärkeää ylläpitää reitittimen päivityksiä ja vaihtaa salasana parempaan. Toinen tärkeä asia muistaa on reitittimen uudelleenkäynnistys säännöllisesti, koska se tuhoaa reitittimen muistissa mahdollisesti olevan haittaohjelman. (Järvinen P. 2022)


*Kuvio 5. The University of Maine tietoturvakäytännöt. (The university of Maine 2023.)*

# 4 VERKKOTURVALLISUUS JA TIETOVERKOT

## 4.1 Palomuurit ja VPN

Palomuuri tarkoittaa tietokoneen verkkoturvallisuusjärjestelmää, joka rajoittaa internet-liikennettä, joka suuntautuu yksityiseen verkkoon, siitä ulos tai kulkee sen sisällä. Palomuurin tarkoitus on päättää, minkä verkkoliikenteen annetaan kulkea ja mitä liikennettä taas pidetään vaarallisena. Palomuurin suojaus suojaa sinua seuraavilta tekijöiltä: ei-toivotut yhteydet oudosti käyttäytyvästä lähteestä voidaan estää salakuuntelua sekä edistyneitä jatkuvia uhkia, työpaikan verkkoselausrajoitukset ja kansallisesti hallinnoitu intranet. Palomuurin käytön aikana on hyvä muistaa vielä seuraavat asiat: Päivitä palomuurisi aina niin pian kuin mahdollista ja käytä virustorjuntaa sen kanssa. (Kaspersky 2025a.)

VPN eli virtuaalinen yksityisverkko tarkoittaa valmiuksia muodostaa suojattu verkkoyhteys julkisessa verkossa. Virtuaalisen yksityisverkon on tarkoitus salata internet-liikenteesi ja kätkeä identiteetti verkossa. Tämä hankaloittaa kolmansien osapuolien seurantaa toimintaasi verkossa ja varastaa dataa. Riippuen VPN-palvelimestasi virtuaalinen yksityisverkko auttaa turvalliseen salaukseen, sijaintisi salaamiseen, aluerajatun sisällön käyttämiseen ja suojatun datan siirtoon. (Kaspersky 2025b.)

Palomuuri ja VPN eivät ole vastustajia, vaan eri kyberturvallisuuskerroksia. Yhdistelmä, joka tarjoaa sekä ulkoisen suojauksen että yksityisyyden ja etäyhteyden suojauksen. Palomuuri hillitsee pääsyn verkkoon ja estää haittaohjelmat, kun taas VPN suojaa datan liikkeen ja mahdollistaa turvallisen etäkäytön. (NordVPN 2023.)

## 4.2 Turvallinen WLAN ja langattomien verkkojen suojaukset

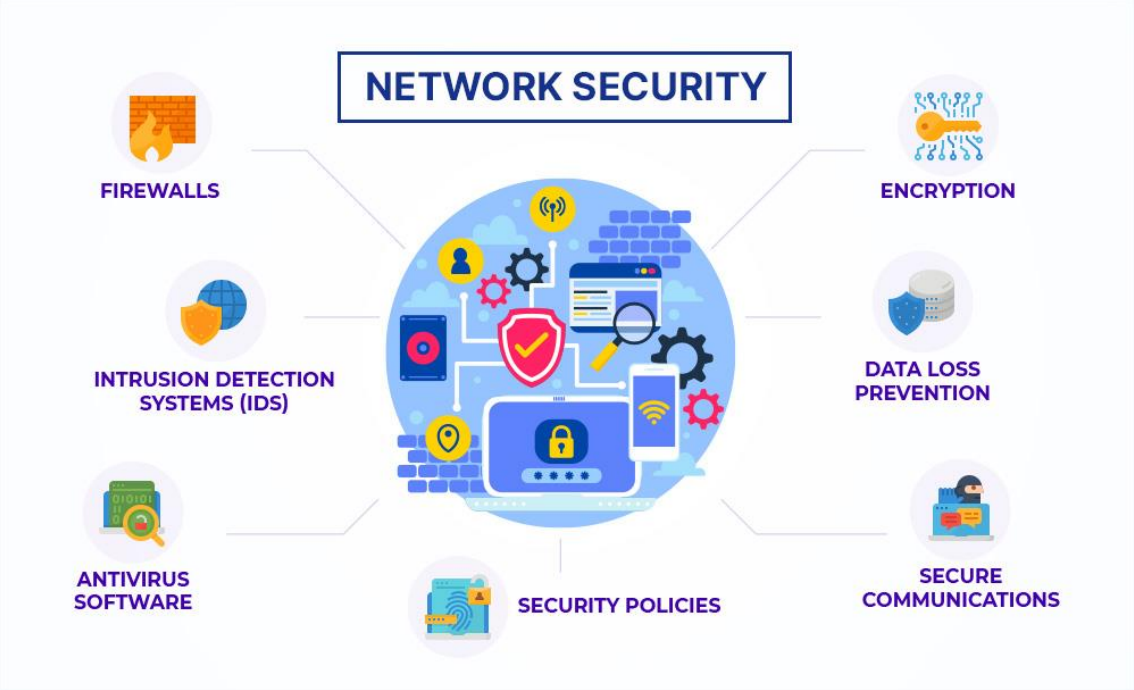
WLAN eli wireless local area network tarkoittaa langatonta lähiverkkoa. Ne ovat hyvin suosittuja niiden edullisuuden, käyttöönoton helppouden ja joustavuuden vuoksi. Valitettavasti helppous ei takaa turvallisuutta. Mahdollisia vaaranpaikkoja ovat esimerkiksi esteettömät tukiasemat ja samannimiset verkot. Vaarantekijän on helppo tunkeutua tukiasemaan, jos tukiasemaa ei ole estetty tai asetettu vahvaa salasanaa, jolloin he voivat lähettää muille verkon käyttäjille tai verkon laitteille haitallista liikennettä. (Viestintävirasto 2014.)

Suojaamattoman verkon käyttäminen kuten esimerkiksi naapurin avoimen verkon käyttäminen vaarantaa viestinnän luottamuksellisuutta. Loppujen lopuksi avoimissa ja suojaamattomissa langattomissa lähiverkoissa tietoturvasta huolehtiminen jää pääasiassa käyttäjän vastuulle. Jos haluat parantaa tätä turvausta, VPN on yksi hyvä vaihtoehto sitä varten. (Viestintävirasto 2014.)

### 4.3 Työntekijöiden turvallinen etätyöskentely

Tässä tiivistetään vielä tärkeimmät pointit, joita kannattaa muistaa tehdessäsi etätöitä. Tärkeintä on noudattaa työnantajan tai oppilaitoksen antamia ohjeistuksia etätyöskentelyssä. Muista käyttää tuttuja ja suojattuja verkkoja minimoidaksesi riskejä. Laitteiden sovellusten päivittäminen on myös tärkeää turvataksesi laitetta mahdollisilta tietoturvauhilta. Riippuen siitä, että käytätkö yrityksen omia laitteita etätyöskentelyssä vai omaa laitetta työskentelyyn, on hyvä muistaa olla sekoittamatta omia yksityisiä verkkopalvelutilejä yrityksen omien tietojen jakamiseen. (Traficom 2020c.)

Kotona työskennellessä on myös tärkeää vartioida työpaikan luottamuksellisia tietoja esimerkiksi myös omilta perheenjäseniltä. Tahattomasti vuodettu tieto voi olla väärissä käsissä erittäin suuri riski koko yritykselle. Muista myös keskustella työasioista vain paikoissa, joissa sivulliset eivät pääse kuulemaan keskustelua tai puhelua. Sama koskee myös tietokoneen tai älypuhelimen näyttöäsi, kun käsittelet luottamuksellista tietoa. (Traficom 2020c.)




*Kuvio 6. Externetworks verkkoturvallisuus perusteet. (Externetworks.)*

# 5 TIETOJEN SUOJAAMINEN

## 5.1 Digitaaliset allekirjoitukset

Digitaalisessa allekirjoituksessa luottamukselliset tiedot suojataan edistyneillä salausalgoritmeilla ja hash-funktioilla, jotka hyödyntävät monimutkaisia matemaattisia kaavoja varmistaakseen allekirjoitusten aitouden ja asiakirjojen eheyden. Salausalgoritmit huolehtivat siitä, että viestin tai asiakirjan sisältö voidaan lukea vain sille tarkoitetulla avaimilla, kun taas hash-funktio luo yksilöllisen ”sormenjäljen” asiakirjasta. Jos asiakirjaa muutetaan allekirjoittamisen jälkeen, hash-arvo muuttuu, mikä paljastaa heti luvattomat muutokset. (OneFlow 2024.)

Tämä tekninen ratkaisu mahdollistaa sen, että digitaalinen allekirjoitus ei ole pelkkä nimi tiedoston lopussa, vaan varma todiste allekirjoittajan henkilöllisyydestä ja asiakirjan muuttumattomuudesta. Verrattuna perinteisiin allekirjoitusmenetelmiin digitaalinen allekirjoitus nopeuttaa prosesseja, koska asiakirjat voidaan allekirjoittaa ja toimittaa välittömästi verkon kautta ilman fyysisiä toimituksia. Tämä säästää aikaa ja kustannuksia, vähentää paperin käyttöä ja tukee näin myös ympäristötavoitteita. (OneFlow 2024.)

Lisäksi digitaalinen allekirjoitus pienentää merkittävästi petos- ja virheriskejä, koska sen tekninen toteutus tekee väärentämisestä tai luvattomasta muokkaamisesta käytännössä mahdotonta. Sen vuoksi se on yhä useammin ensisijaisen vaihtoehto sopimusten, virallisten asiakirjojen ja muiden luottamuksellisten dokumenttien käsittelyssä niin yrityksissä kuin julkishallinnossa. (OneFlow 2024.)

## 5.2 GDPR ja tietosuojakäytännöt

Toukokuussa 2018 tuli voimaan yleinen tietosuoja-asetus (GDPR), joka on Euroopan unionin keskeinen tietosuojalaki. Tietosuojalaki koskee kaikkia EU:n jäsenvaltioita sekä organisaatioita, jotka käsittelevät EU:n kansalaisten henkilötietoja. Tietosuoja-asetuksen päätavoite on suojata yksilön yksityisyyttä antamalla heille kontrolli omiin henkilötietoihinsa ja asettamalla tiukat säännöt siitä, miten organisaatiot voivat kerätä, tallentaa, käsitellä ja jakaa näitä tietoja.

Asetus määrittelee, että henkilötietojen käsittelylle on oltava laillinen peruste, kuten rekisteröidyn suostumus, sopimus tai lakisääteine velvoite. Organisaatioiden tulee myös noudattaa tietojen minimoinnin, tarkkuuden ja säilytysajan rajoittamisen periaatteita, jotta tietojen käsittely olisi mahdollisimman turvallista ja läpinäkyvää.

Asetus edellyttää myös, että organisaatiot toteuttavat asianmukaisia teknisiä ja organisatorisia toimenpiteitä tietoturvan varmistamiseksi. Joissakin tapauksissa organisaation on nimettävätietosuojavastaava, joka valvoo GDPR:n

noudattamista ja toimii yhteyshenkilönä valvontaviranomaisille. GDPR:n rikkomisesta voi seurata merkittäviä seuraamuksia, mukaan lukien hallinnollisia sakkoja, jotka voivat olla jopa miljoonia euroja tai prosentuaalinen osuus organisaation vuotuisesta liikevaihdosta, riippuen rikkomuksen vakavuudesta. (Digiturvamalli 2025.)


*Kuvio 7. GDPR seitsemän periaatetta. (Usercentrics 2024.)*

# 6 POHDINTA

Opinnäytetyön tavoitteena oli kerätä kattavasti tietoa pk-yrityksille, joka helpottaisi tiedon saantia. Taustalla oli pk-yritysten tiedonpuute kyber- ja tietoturvasta, mikä altistaa ne merkittäville tietoturvariskeille. Työn aikana koottu tieto kattaa keskeiset uhat, perustason suojaustoimet sekä verkko- ja tietosuoja-asioiden käytännön toteutuksen. Tämä kokonaisuus muodostaa tiiviin lähtökohdan yritysten oman kyberturvallisuuden kehittämiselle.

Tulokset osoittavat, että suurin osa pienyritysten kohtaamista riskeistä liittyy joko inhimillisiin virheisiin, päivittämättömiin järjestelmiin tai puutteelliseen tietoisuuteen kyberuhkista. Erityisesti kiristyshaittaohjelmat ja tietojenkalastelu nousevat merkittäviksi uhkakuviksi. Lisäksi sisäiset uhat ja etätyöskentelyn tietoturvariskit osoittavat, että pelkkä tekninen suojaus ei riitä, vaan tarvitaan myös henkilöstön koulutusta ja tietoturvakulttuurin kehittämistä.

Työn vahvuutena on sen käytännönläheisyys ja helppolukuisuus, joka soveltuu eri tasoisille tietoturvaosaajille. Haasteena oli rajata sisältö, että se pysyy tiiviinä mutta silti kattavana. Tämän seurauksena joitakin erikoistuneempia aiheita, kuten syvälliset tekniset toteutusohjeet tai kansainvälisen tietoturvalainsäädännön vertailu, ei käsitelty tässä työssä.

Prosessin aikana kirjoittajan osaaminen kyberturvallisuuden eri osa-alueista syveni huomattavasti. Erityisesti kuinka tärkeää on sovittaa tietoturvasuosituksia kohderyhmän resursseihin ja toimintaympäristöön. Tietoisuuden lisääminen ja selkeiden ohjeiden tarjoaminen voivat olla ratkaisevia tekijöitä tietoturvatason parantamisessa.

# LÄHTEET


Cloudflare. What is a DDoS attack? Saatavissa: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ Viitattu: 20.8.2025.

Digi- ja Väestötietovirasto 2020. Digiturvavinkki: Salasanojen hallinta ja turvallinen kirjautuminen. Saatavissa: https://dvv.fi/blogi/-/blogs/digiturvavinkki-salasanojen-hallinta-ja-turvallinen-kirjautuminen Viitattu 16.8.2025.

Digiturvamalli 2025. Mikä on GDPR? Vaatimusten esittely. Saatavissa: https://www.digiturvamalli.fi/blogi/mika-on-gdpr Viitattu 10.8.2025.

Euroopan unionin neuvosto 2025. Eurooppa-neuvosto. Saatavissa: https://www.consilium.europa.eu/fi/policies/cybersecurity-social-engineering/ Viitattu 21.3.2025.

Europol 2024. Internet Organised Crime Threat Assessment (IOCTA). Pdf-tiedosto. Saatavissa: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 Viitattu 23.5.2025.

Externetworks. What is Network Security? Saatavissa: https://www.extnoc.com/learn/computer-security/network-security Viitattu 20.8.2025.

Hornetsecurity 2024. What is Data Backup and Recovery? Saatavissa: https://www.hornetsecurity.com/en/blog/what-is-data-backup-and-recovery/ Viitattu 6.4.2025.

Järvinen P. 2022. Yrityksen tietoturvaopas. Helsingin seudun kauppakamari. Helsinki.

Kaspersky 2025a. Mikä on palomuuri? Määritelmä ja selitys. Saatavissa: https://www.kaspersky.fi/resource-center/definitions/firewall Viitattu 20.4.2025.

Kaspersky 2025b. Mikä VPN on ja kuinka se toimii? Saatavissa: https://www.kaspersky.fi/resource-center/definitions/what-is-a-vpn Viitattu 27.4.2025.

Microsoft 2025a. Mikä on Kyberturvallisuus? Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-cybersecurity?#Typesofcybersecuritythreats Viitattu 27.4.2025.

Microsoft 2025b. Mitä haittaohjelmat ovat? Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-malware#malware-defined Viitattu 27.4.2025.

Microsoft 2025c. Mitä kiristysohjelmat ovat? Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-ransomware Viitattu 27.4.2025.

Microsoft 2025d. Mitä sisäiset uhat ovat? Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-insider-threat Viitattu 27.4.2025.

National Cyber Security Centre 2017. Small Business Guide: Cyber Security. Saatavissa: https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data Viitattu 15.8.2025.

NordVPN 2023. Firewall vs. VPN: Which one to use and when? Saatavissa: https://nordvpn.com/fi/blog/firewall-vs-vpn/?srsltid=AfmBOopscOT0tKMNK2ADAbFyzCggAwetVREYf5kM6gNcwr_EP4faaE78 Viitattu 18.8.2025.

OneFlow 2024. Miten tehdä digitaalinen allekirjoitus turvallisesti? Saatavissa: https://oneflow.com/fi/blogi/digitaalinen-allekirjoitus-turvallisesti/ Viitattu 26.5.2025.

The University of Maine 2023. Data security best practices. Saatavissa: https://umaine.edu/arcsim/2023/05/08/data-security-best-practices/ Viitattu 20.8.2025.

Tietosuojavaltuutetun toimisto s.a. Tietosuoja. Saatavissa: https://tietosuoja.fi/tietojenkalastelu Viitattu 21.3.2025.

Traficom 2019. Organisaatio! Torju Office 365-tunnusten kalastelu oppaamme avulla. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/organisaatio-torju-office-365-tunnusten-kalastelu-oppaamme-avulla Viitattu 20.8.2025.

Traficom 2020a. Kyberturvallisuuskeskus, Pienyritysten kyberturvallisuus. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pienyritysten-kyberturvallisuusopas Viitattu 7.3.2025.

Traficom 2020b. Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen! Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen Viitattu 28.3.2025.

Traficom 2020c. Kyberturvallisuuskeskus. Tee etätyöstä turvallista vinkkiemme avulla. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tee-etatyosta-turvallista-vinkkiemme-avulla Viitattu 7.5.2025.

Traficom 2022. Kyberturvallisuuskeskus, Toimintaohje- kiristyshaittaohjelma. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toimintaohje-kiristyshaittaohjelma Viitattu 13.3.2025.

Traficom 2022b. Kyberturvallisuuskeskus. Toimintaohje- palvelunestohyökkäys. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toimintaohje-palvelunestohyokkays Viitattu 24.3.2025.

Traficom 2023. Salasanat haltuun- kuka käyttää tiliäsi? Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun Viitattu 28.3.2025.

Traficom 2024a. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi Viitattu 14.8.2025.

Traficom 2024b. Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa Viitattu 20.8.2025.

Traficom 2025a. Kyberturvallisuuskeskus, Kybersää Tammikuu 2025. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202025 Viitattu 23.3.2025.

Traficom 2025b. Kyberturvallisuuskeskus, Kybersää Heinäkuu 2025. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202025 Viitattu 20.8.2025.

Turvallisuuskomitea 2018. Kyberturvallisuus sanasto. Saatavissa: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ Viitattu 11.3.2025.

Usercentrics 2024. What do you need to know about the 7 principles of GDPR. Saatavissa: https://usercentrics.com/knowledge-hub/principles-of-gdpr/ Viitattu 20.8.2025.

Verizon business 2025. Data Breach Investigations Report (DBIR). Saatavissa: https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf Viitattu 15.8.2025.

Viestintävirasto 2014. Kyberturvallisuuskeskus. Langattomasti, mutta turvallisesti. Pdf-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf Viitattu 7.5.2025.

World Economic Forum 2021. This chart shows how long it would take a computer to hack your exact password. Saatavissa: https://www.weforum.org/stories/2021/12/passwords-safety-cybercrime/ Viitattu 20.8.2025.