



Yksinyrittäjän ja mikroyrityksen KYBER- JA TIETOTURVA PIKAOPAS

Kyberturvan abc yrittäjille -hanke



Euroopan unioni
Euroopan sosiaalirahasto

Vipuvoimaa
EU:lta
2014–2020



Elinkeino-, liikenne- ja
ympäristökeskus



Kaakkois-Suomen
ammattikorkeakoulu

Sisällys

Internet ja kyberuhat.....	3
Mikä on haittaohjelma?	3
Miltä näyttää turvallinen nettisivun osoite?	4
Kuinka tunnistan väärennetyt nettisivun osoitteet?.....	4
Työasemat eli pöytätietokoneet ja kannettavat tietokoneet.....	5
Miten haittaohjelmilta voi suojautua?	5
Salasanahallintaohjelma.....	5
Yleisimmät käytetyt salasanat Suomessa	6
Sähköpostin käyttö / kaksivaiheinen tunnistautuminen	6
Miten voin turvata sähköpostini?	6
Kaksivaiheinen tunnistautuminen	8
Salasanahallintaohjelmien käyttöönotto	10
Sosiaalinen media ja verkkokauppa	11
Sosiaalinen media	11
Verkkokauppa	12
Mobiililaitteet ja internetiin kytketyt laitteet osana yrityksen kyberturvallisuutta	13
Kuinka suojata mobiililaitteet:	13
SIM-kortin lukitus Android puhelimessa:.....	14
SIM-kortin lukitus Apple puhelimessa	14
Verkkolevyt / palvelimilla olevat tiedostokansiot	14
Mitä on pilvi?.....	14
Miten minä valitsen minulle sopiva pilvipalvelun?	14
Varmuuskopiointi.....	18
Varmuuskopion toimivuus	21
EU:n yleinen tietosuojasetus	21
Liiketoiminnan jatkuvuussuunnitelma	23
Toiminta ongelmatilanteessa	25

Mikä on haittaohjelma?

- **Virus** – Virus on haittaohjelma, joka on yleensä ohjelmoitu vahingoittamaan tietokoneita, järjestelmiä tai verkkoja. Samoin kuin oikea virus, tietokonevirus tarvitsee isännän (tiedoston) levitäkseen. Virus pitää yleensä aktivoida, esim. klikkaamalla vahingossa vaarallista linkkiä.
- **Mato** - Madon ja viruksen pääero on se, että mato voi levittää kopioita itsestään saastumattomiin tietokoneisiin. Mato on haittaohjelma, joka toimii itsenäisesti ja joka voi suorittaa ja levittää ilman käyttäjän toimenpiteitä.
- **Kiristysohjelma (Ransomware)** - ”Ransom” on englantia ja tarkoittaa lunnasrahaa. Se on kiristysohjelma, joka lukitsee tietokoneen ja vaatii rahaa tietojen palauttamisesta.
- **Vakoiluohjelma** - on haittaohjelma, jotka piiloutu ja yrittää kaapata tietoja sekä seurata tietokoneiden ja mobiililaitteiden toimintaa huomaamatta.
- **Trojialainen** - on haittaohjelma, joka teeskentelee olevansa vaaraton huijatakseen meidät lataamaan sen. Troijalaisia käytetään monenlaiseen toimintaa, esimerkiksi takaovien luomiseen muille haittaohjelmille, vakoiluun, kalliiden tekstiviestien lähettämiseen jne.
- **Kalastelusähköposti** - Kalastelu voi tapahtua sähköpostin, sosiaalisen median, tekstiviestin tai minkä tahansa kanavan kautta: kaikki kalasteluhyökkäykset noudattavat samaa kaavaa. Hyökkääjä lähettää viestin saadakseen uhrinsa klikkaamaan

linkkiä, lataamaan liitetiedoston, lähettämään tietoja tai jopa siirtämään rahaa.

Miltä näyttää turvallinen nettisivun osoite?

<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

Kuinka tunnistan väärennetyt nettisivun osoitteet?

- Fake buttons eli painonappi, joka ei ole sitä - 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 väärennetyjen verkkosivustojen tarkistus
<https://transparencyreport.google.com/safe-browsing/search>

Työasemat eli pöytätietokoneet ja kannettavat tietokoneet

Miten haittaohjelmilta voi suojautua?

Virustorjunta ohjelmat ovat jokaisen päätelaitteen turvallisuuden kulmakivi. Virustorjunta ohjelmat tarkastelevat tietokoneen tiedostoja ja käynnissä olevia ohjelmia löytääkseen jotain, mikä voisi olla haitallista. Monet eri yhtiöt tekevät omia virustorjuntaohjelmia, joista osa on ilmaisia ja osa maksullisia.

Salasanahallintaohjelma

Salasanahallintaohjelmalla voi luoda vahvoja ja uniikkeja salasanoja eri palveluihin. Näitä salasanoja ei tarvitse muistaa, koska ohjelma tallentaa ne ja syöttää automaattisesti salasanan kirjautumisen yhteydessä.

Vaikka salasanahallintaohjelman ehdottamia salasanoja, 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

Yleisimmät käytetyt salasanat Suomessa

Alla lista 40 yleisimmistä käytetyt salasanat Suomessa 2021:

1	123456	11	lol123	21	kikkeli	31	1234
2	12345	12	asdasd	22	kamari	32	111111
3	salasana	13	password	23	moimoi	33	akuankka
4	qwerty	14	asd123	24	1234567890	34	n-sana
5	perkele	15	moi123	25	saatana	35	qwe123
6	123456789	16	paska	26	123qwe	36	1q2w3e4r
7	salasana1	17	kakka	27	aurinko	37	mansikka
8	paska123	18	qwerty123	28	abc123	38	jeejee
9	12345678	19	1234567	29	lollero	39	moikka
10	kakka123	20	123123	30	asdasd123	40	qwerty1

Sähköpostin käyttö / kaksivaiheinen tunnistautuminen

Miten voin turvata sähköpostini?

Gmail:

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

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.

Kaksivaiheinen tunnistautuminen

Google:

1. Omalta gmail-tililtä voi avata asetus valikon painamalla oikealla yläkulmassa olevaa käyttäjäkuvaketta, josta valitsee **Hallinnoi 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 vahvistuskoodin.
5. Kun saat vahvistuskoodin puhelimeesi, syötä siinä näkyvä numerosarja kenttään. Älä koskaan jaa kyseistä vahvistuskoodia kenenkään kanssa, vaikka sitä pyydetäisiin.
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**

Outlook:

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 annetaan QR-koodi, joka sinun tulee kuvata kännykän kameralla.
4. Voit kuvata QR-koodin avaamalla **Microsoft Authenticator** sovelluksen puhelimesilläsi 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**.

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 salasanana 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**.
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 tehdä siitä vielä turvallisemman.
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.

Sosiaalinen media ja verkkokauppa

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.

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.

Verkkokauppa

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.

- 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.

Mobiililaitteet ja internetiin kytketyt laitteet osana yrityksen kyberturvallisuutta

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.

SIM-kortin lukitus 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.

SIM-kortin lukitus 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

Verkkolevyt / palvelimilla olevat tiedostokansiot

Mitä on pilvi?

Pilvi ei ole yksi paikka. Se koostuu palvelimista datakeskuksissa ympäri maailmaa. Pilvi on yksinkertaistetusti sanottuna jonkun muun iso tietokone, jossa tietosi ovat.

Miten minä valitsen minulle sopiva pilvipalvelun?

Kun valitset pilvipalvelun, on hyvää tarkistaa, mitä kuuluu palveluun. Pilvipalvelut toimivat siten, että maksamalla enemmän palveluun kuuluu

enemmän. Pitää miettiä, mitä kaikkea tarvitset yrityksesi. Kallein palvelu ei välttämättä ole aina paras vaihtoehto.

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

Alle oleva lomake auttaa tekemään päätöksen siitä minkälainen pilvipalvelu sopisi yrityksellesi.

Pilvipalvelun nimi			
Minun käyttäjärjestelmäni			
Minkälaisia käyttäjärjestelmävaatimuksia 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 mobiililaitteisiin?	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei
Kuuluuko varmuuskopiointi palveluun?	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei
Kuinka kauan tietoja säilytetään varmuuskopioinnissa (esim. 30 päivää)?			
Mitä sovelluksia kuuluu palveluun?	<input type="checkbox"/> Word / Excel <input type="checkbox"/> Sähköpostin sovellus (esim.	<input type="checkbox"/> Word / Excel <input type="checkbox"/> Sähköpostin sovellus (esim.	<input type="checkbox"/> Word / Excel <input type="checkbox"/> Sähköpostin sovellus (esim.

	Outlook, Thunderbird) <input type="checkbox"/> Muita sovelluksia (esim. palkkalaskel ma)	Outlook, Thunderbird) <input type="checkbox"/> Muita sovelluksia (esim. palkkalaskel ma)	Outlook, Thunderbird) <input type="checkbox"/> Muita sovelluksia (esim. palkkalaskel ma)
Missä maassa tiedot ovat tallennettu?	<input type="checkbox"/> Suomi <input type="checkbox"/> EU <input type="checkbox"/> Muualla maailmassa	<input type="checkbox"/> Suomi <input type="checkbox"/> EU <input type="checkbox"/> Muualla maailmassa	<input type="checkbox"/> Suomi <input type="checkbox"/> EU <input type="checkbox"/> Muualla maailmassa
Pystynkö määrittämään tiedostojen / kansioden käyttöoikeudet?	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei
Pystynkö suojaamaan jakamislinkit salasanalla?	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei	<input type="checkbox"/> Kyllä <input type="checkbox"/> Ei
Minkälainen tuki kuuluu palveluun?	<input type="checkbox"/> Tuki ei kuuluu palveluun. <input type="checkbox"/> Tuki sähköpostin kautta <input type="checkbox"/> Chat-tuki <input type="checkbox"/> Tuki puhelimessa	<input type="checkbox"/> Tuki ei kuuluu palveluun. <input type="checkbox"/> Tuki sähköpostin kautta <input type="checkbox"/> Chat-tuki <input type="checkbox"/> Tuki v Tuki puhelimessa	<input type="checkbox"/> Tuki ei kuuluu palveluun. <input type="checkbox"/> Tuki sähköpostin kautta <input type="checkbox"/> Chat-tuki <input type="checkbox"/> Tuki puhelimessa

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)

Varmuuskopio Windows-koneella:

1. Näytön vasemmassa alanurkassa löytyy kohta **"Type here to search/Kirjoita tähän hakeaksesi kohteista"**. Klikkaa palkkia, ja kirjoita **"Settings/Asetukset"** ja paina "Enter".
2. Skrollaa alas, kunnes löytyy **"Update and Security/Päivittäminen ja suojaus"** ja paina painiketta.
3. Klikkaa **"Backup/Varmuuskopioi"**.
4. Valitse oikealla puolella **"Back up using File History/Varmuuskopioi tiedostohistorian avulla"** alapuolella plussa ja valitse ulkoinen kiintolevy.

Varmuuskopio 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 Omena-avalikko (🍏) > 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.

Tietojen palauttaminen varmuuskopiolta (Windows 10):

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.

Tietojen palauttaminen varmuuskopiolta (Windows 11):

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.

Tietojen palauttaminen varmuuskopiolta ulkoiselta levytä (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 liitettyä 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.

Esim. 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.

Varmuuskopion toimivuus

Kopiot eivät auta, mikäli ne eivät jostain syystä toimi. Testaa esimerkiksi varmuuskopion tekemisen jälkeen muutamalla tiedostolla, että ne todella voidaan avata ja palauttaa. On mahdollista, että tiedostot vioittuvat eli korruptoituvat, kun niitä kopioidaan. Et varmasti halua huomata, että tiedot, joita yrität hätätilanteessa palauttaa, ovat käyttökelttomia. Varmuuskopioinnin jälkeen sinun tulee myös varmistaa, että kaikki tarvittavat tiedostot, kansiot ja tiedot on varmuuskopitu. Luo selkeä ja kattava luettelo vaiheista, joita on noudatettava palauttaaksesi varmuuskopiotiedostot ja jakaaksesi ne kaikille tarvittaville henkilöille.

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.

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.

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.

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.

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 sijaitisivat eri paikoissa (esim. sähköpostissa, kännykkäsi yhteystiedoissa ja yrityksen työntekijöiden käytössä olevassa jaetussa Google-taulukossa sekä kaapin perukoille unohdetussa asiakkailta kerätyssä käyntikorttisivaskassa).

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

Liiketoiminnan jatkuvuussuunnitelma

Liiketoiminnan jatkuvuussuunnitelman laatimiseen voit ladata meidän nettisivuiltamme [osoite] pohja yksinyrittäjille, sekä pohja mikroyrittäjille (1–9 henkilöitä).

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.

Liiketoiminnan jatkuvuussuunnitelman sisältö Enisan (Euroopan unionin kyberturvallisuusvirasto) mukaan:

- Asiakirjan soveltamisala ja tarkoitus
- Suhde muihin suunnitelmiin
- Liiketoimintayksikön tiimin roolit ja vastualueet (tarvittaessa)
- Tilanteen arviointimenettely
- Yhteystiedot
 - Hallintaryhmä
 - Tärkeimmät toimittajat
 - Henkilöstö
 - Sidosryhmät
- Eskalaatioperusteet
- Toimintatarkistuslista
- Laitteita ja varastointia koskevat tiedot
- Palauttamismenettely

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 salasana (suositeltavaa tehdä eri verkosta, jos siihen mahdollisuus esim. puhelimen kautta jaettu.)