
TURVALLISESTI SOMESSA - SENIORIN OPAS SOSIAALISEN MEDIAN TIETOTURVAAN



Tekijä: Lotta Manninen – Informaatiotutkimuksen
opiskelija

Toukokuu 2025

SISÄLLYSLUETTELO

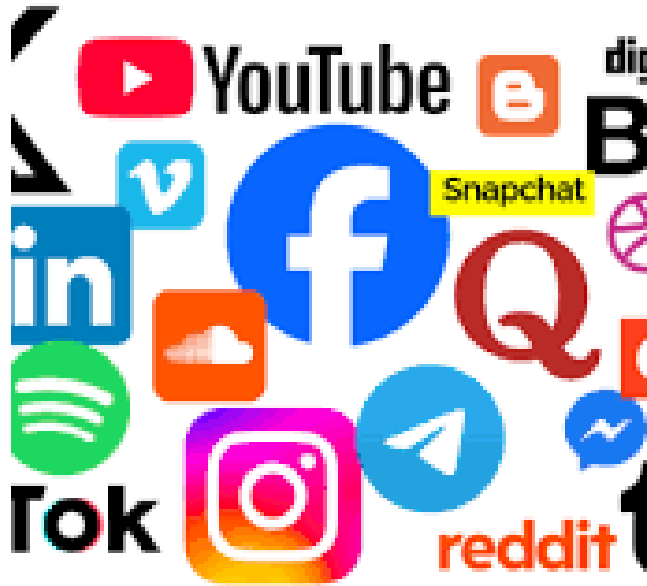
1. Oppaan sisältö.....	3	• 11. Häirinnän tunnistaminen ja estäminen.....	13
2. Mikä on sosiaalinen media?.....	4	• 12. Mainosten sekä piilomainonnan tunnistaminen.....	14
3. Miksi tietoturva on tärkeää?.....	5	• 13. Evästeet ja tietojen kerääminen.....	15
4. Vahvat ja turvalliset salasana.....	6	• 14. Laitteen tietoturva.....	16
5. Kakisvaiheinen tunnistautuminen.....	7	• 15. Turvallisen verkkosivun tunnistaminen.....	17
6. Yksityisyysasetukset.....	8	• 16. Vastuullisuus somessa.....	18
7. Huijausten tunnistaminen.....	9	• 17. Identiteettivarkauksilta suojautuminen.....	19
8. Valetilien tunnistaminen.....	10	• 18. Sosiaalisen median tilin jäädyttäminen tai poistaminen.....	20
9. Mitä tietoja jättää jakamatta?.....	11	• 19. Yhteenveto ja lisäresurssit.....	21
10. Tekijänoikeudet ja kuvien jakaminen.....	12		

1. OPPAAN SISÄLTÖ - TERVETULOA OPPIMAAN SOSIAALISEN MEDIAN TIETOTURVASTA!

- Tämän oppaan avulla voit oppia, kuinka sosiaalisen median käyttö onnistuu luottavaisesti, itsenäisesti ja turvallisesti.
- Sosiaalinen media tarjoaa mahdollisuuden pitää yhteyttä läheisiin, osallistua yhteisöihin, sekä jakaa kuulumisia, mutta on tärkeää ymmärtää miten oman yksityisyyden voi suojata ja tunnistaa mahdolliset riskit.
- Tässä oppaassa käsittelemme tietoturvaa, joka tarkoittaa käytännön keinoja, joilla voi hallita omaa verkkoelämääsi.



2. MIKÄ ON SOSIAALINEN MEDIA?



- Sosiaalisella mediallyä tarkoitetaan erilaisia verkkopalveluja, joissa voit olla yhteydessä muihin ihmisiin, lukea ja katsella muiden julkaisuja, tai jakaa itse kuvia, videoita, sekä viestejä.
- Tunnetuimpia sosiaalisen median palveluja ovat Facebook, Instagram, WhatsApp, Youtube, TikTok ja X. Kaikki nämä palvelut eroavat toisistaan, mutta kaikkia niitä yhdistää vuorovaikutus ihmisten välillä.
- Sosiaalinen media voi tarjota yhteisöllisyyttä, sekä rikastuttaa arkea. Sosiaalisessa mediassa pystyy usein myös seuraamaan ajankohtaisia uutisia ja tapahtumia.
- Palvelut ovat useimmiten ilmaisia, mutta ne keräävät käyttäjistään tietoa. Siksi olisi tärkeää ymmärtää, kuinka sosiaalisen median palveluita voidaan käyttää turvallisesti.



3. MIKSI TIETOTURVA ON TÄRKEÄÄ?

- Tietoturvalla tarkoitetaan yksityisyyden ja omien tietojen suojaamista internetissä.
- Sosiaalisen median palveluissa saatetaan monesti jakaa henkilökohtaisia asioita, kuten nimi, syntymäpäivä, kuvia ja videoita, sekä joskus jopa osoitetiedot. Jos henkilökohtaisia tietoja ei suojata, voivat ne joutua väärin käsiin.
- Tietoturva on erityisen tärkeää, sillä tietoturvauhkien määrä on kasvussa. Tietoturvauhkia ovat esimerkiksi huijaukset, identiteettivarkaudet ja haittaohjelmat. Näitä voit kuitenkin ehkäistä pienillä muutoksilla, jotka tässä oppaassa esittelemme.
- Tietoturvasta huolta pitäminen on kuin lukon laittaminen kotioveen – se suojelee sinua ja omaa hyvinvointiasi digitaalisessakin maailmassa.

4. VAHVAT JA TURVALLISET SALASANAT



- Ensimmäinen ja tärkein suoja tilillesi sosiaalisessa mediassa on salasana.
- Vahvan ja turvallisen salasanan tulisi olla pitkä (vähintään 12 merkkiä), sisältää pieniä ja isoja kirjaimia, numeroita, sekä erikoismerkkejä. Esimerkkinä: !bKAbcd0123.
- Salasanan tulisi olla sellainen, mitä kukaan ei voi arvata. Älä siis käytä nimeäsi, syntymäpäivääsi, tai muuta helposti arvattavaa tai tiedossa olevaa asiaa salasanassasi.
- On tärkeää, että salasana olisi eri jokaisessa palvelussa, älä siis käytä samaa salasanaa useammassa sosiaalisen median palvelussa.
- Salasanat voit kirjoittaa itsellesi ylös turvalliseen paikkaan tai käyttää salasanojen hallintaohjelmaa. Älä missään tilanteessa jaa salasanaasi muille, etenekään internetissä tai sosiaalisessa mediassa.

5. KAKSIVAIHEINEN TUNNISTAUTUMINEN



- Kaksivaiheinen tunnistautuminen, eli 2FA, antaa lisäsuojan tilillesi ja sen käyttö on erittäin suositeltavaa.
- Kaksivaiheisen tunnistautumisen avulla käyttäjälle kirjautuessa tarvitaan salasan lisäksi toinen tunnistus, kuten puhelimeen tuleva koodi. Tämä estää muiden ihmisten pääsyn käyttäjätilillesi, vaikka heillä olisi salasanasi.
- Useimmat sosiaalisen median palvelut tarjoavat mahdollisuuden kaksivaiheiseen tunnistautumiseen. Useimmiten kaksivaiheisen tunnistautumisen voi laittaa päälle sosiaalisen median palvelun profiiliasetuksista.

6. YKSITYISYYSASETUKSET



- Useimmissa sosiaalisen median palveluissa voit itse päättää, kuka näkee profiilisi, kuvasi ja julkaisusi. Yksityisyysasetukset määrittävät, kuka näkee julkaisemasi sisällön ja kuinka helposti sinut löytää.
- Yksityisyysasetukset tulisi tarkistaa säännöllisesti. Jos asetuksia ei säädä, kuka tahansa pystyy näkemään profiilisi, kuvasi, sekä julkaisusi. Yksityisyysasetusten hallinta on yksi tärkeimmistä tietoturvakeinoista, voit hallinnan avulla ehkäistä väärinkäytöksiä ja huijauksia.
- Esimerkkinä: voit rajoittaa näkyvyyden Facebookissa niin, että vain hyväksytyt ystäväsi näkevät julkaisusi.

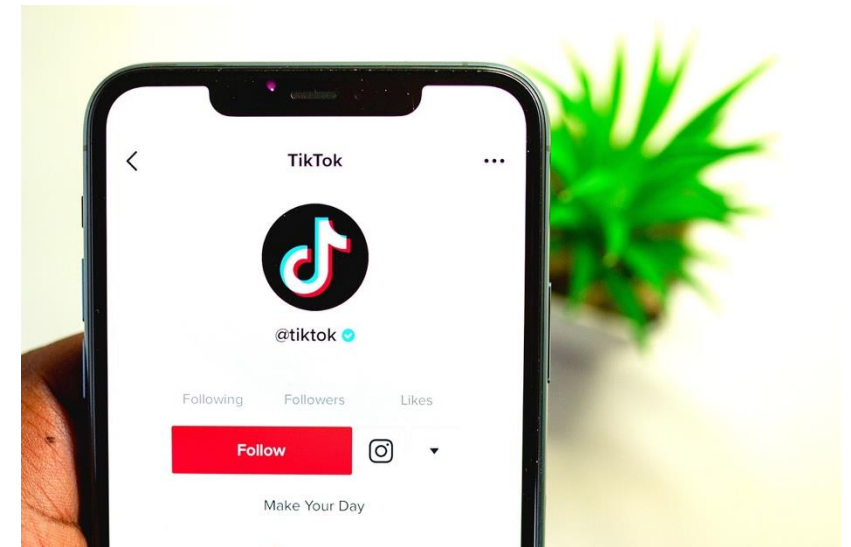
7. HUIJAUSTEN TUNNISTAMINEN



- Sosiaalisen median palveluissa liikkuu monenlaisia huijauksia ja ne voivat usein kohdistua iäkkäimpiin ihmisiin.
- Sosiaalisessa mediassa huijarit yrittävät usein saada sinut paljastamaan henkilökohtaisia tietoja, kuten henkilötunnusta, pankkitunnuksia, tai salasanoja. Yleisimpiä huijauksia ovat tekaistut kilpailut, rahankeruu pyynnöt tutun nimissä, valeprofiilit, sekä linkit, jotka ohjaavat väärennetyille verkkosivuille.
- Älä missään tapauksessa siis anna mitään henkilökohtaisia tietojasi, klikkaa epäilyttäviä linkkejä tai avaa tuntemattomien liitteitä. Aina viestin tullessa, tarkista viestin lähettäjä ja mieti, vaikuttaako viesti uskottavalta. Kun jokin kuulostaa liian hyvältä ollakseen totta, se todennäköisesti ei ole totta.
- Jos epäilet saaneesi huijausviestejä, älä toimi viestissä annettujen ohjeiden mukaisesti, vaan kysy neuvoa. Neuvoa voit kysyä esimerkiksi Enteriltä, ystäviltä, tai sukulaisilta. Voit myös ilmiantaatai estää käyttäjän, jolloin sama lähettäjä ei voi enää lähettää sinulle viestejä.

8. VALETILIEN TUNNISTAMINEN

- Valetili tarkoittaa väärennettyä käyttäjäprofiilia. Valetili voi esiintyä esimerkiksi viranomaisena, ystävänäsi tai julkisuuden henkilönä.
- Valetilit saattavat yrittää pyytää sinulta rahaa, tai saada henkilökohtaisia tietojasi. Tarkista siis aina, onko tili oikea. Voit tarkistaa tämän katsomalla onko tilillä paljon kavereita, oikeaa profiilikuvaa tai vanhoja julkaisuja.
- Jos epäilet valetiliä, ilmoita siitä sosiaalisen median palvelulle, voit tehdä näin ilmiantamalla käyttäjän. Älä myöskään hyväksy valetilin kaveripyyntöä.





9. MITÄ TIETOJA JÄTTÄÄ JAKAMATTA?

- Sosiaalisessa mediassa ei kannata jakaa ihan kaikkea. Sinun olisi hyvä aina miettiä tarkkaan, mitä jakaa itsestään julkisesti. Henkilökohtaiset tiedot voivat jossain tapauksissa päätyä väärin käsiin ja altistaa väärinkäytölle.
- Esimerkiksi syntymäaika, puhelinnumero, henkilötunnus, osoite ja pankkitiedot eivät kuulu julkiseen profiiliin, eikä edes yksityiskeskusteluihin sosiaalisen median palveluissa.
- Myös huomioitavaa on tarkka sijainnin jakaminen, tai läheisten kuvien jakaminen voi heikentää yksityisyyttäsi ja turvallisuuttasi.
- Aina julkaistaessasi jotakin sosiaaliseen mediaan, mieti, voiko joku käyttää jakamaasi tietoa sinua vastaan. Jos vastaus on edes ehkä, jätä tieto jakamatta.

10. TEKIJÄNOIKEUDET JA KUVIEN JAKAMINEN

- Kuvien jakaminen sosiaalisessa mediassa on hyvin yleistä, mutta siihen liittyy tekijänoikeus- ja tietoturvavastuu.
- Aina kun julkaiset sosiaalisessa mediassa kuvia, tarkista aina näkyykö kuvissa muita ihmisiä. Etenekin jos kuvan julkaisuun ei ole annettu lupaa kuvassa näkyvältä henkilöltä, kuvaa ei tulisi julkaista. Toisten yksityisyyttä on aina suojattava, sillä julkisilla alustoilla jaetut kuvat voivat levitä nopeasti, eikä niiden poistaminen ole aina helppoa.
- Tekijänoikeudet ovat tärkeä asia muistaa. Et saa käyttää toisten ottamia kuvia, piirroksia, tai mitään materiaalia ilman lupaa, ellein kuvaa ole selkeästi merkitty vapaasti käytettäväksi. Kuvan kopioiminen netistä ei tee siitä vapaata käyttöä.
- Suosi siis aina omia kuvia tai laillisesti jaettavaksi tarkoitettua sisältöä.



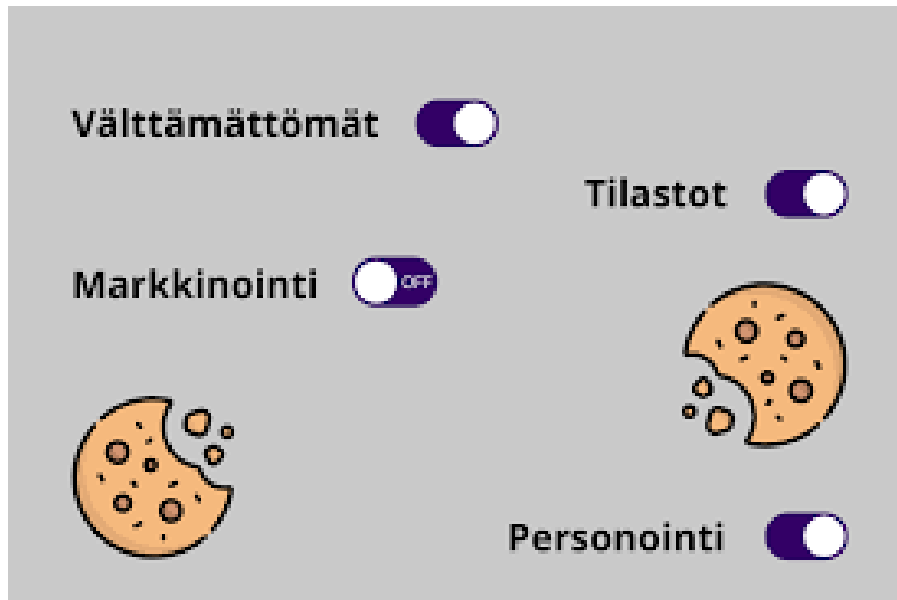
11. HÄIRINNÄN TUNNISTAMINEN JA ESTÄMINEN

- Myös sosiaalisessa mediassa voi altistua häirinnälle. Häirintä sosiaalisessa mediassa voi olla esimerkiksi loukkaavia kommentteja, toistuvaa ei-toivottua yhteydenottoa, uhkauksia tai yksityisten tietojen levittämistä.
- Kaikenlainen viestintä, joka saa sinut tuntemaan olosi epämukavaksi, olisi tärkeää ottaa vakavasti.
- Jos joudut sosiaalisessa mediassa häirinnän kohteeksi, älä vastaa viesteihin. Tallenna todisteet häirinnästä, esimerkiksi ottamalla kuvakaappauksia. Ilmoita häirinnästä myös palvelun ylläpidolle. Voit myös estää käyttäjän, joka häirintää aiheuttaa.
- Jos tulet häirityksi, aseta tilisi yksityiseksi, sekä käy läpi muutkin yksityisyysasetukset, kuten kuka näkee julkaisusi tai kuka voi kommentoida.

12. MAINOSTEN SEKÄ PIILOMAINONNAN TUNNISTAMINEN

- Sosiaalisessa mediassa näkemäsi sisältö ei ole aina välttämättä puolueetonta.
- Mainokset voivat esiintyä selkeästi merkittyinä, mutta joskus mainoksia on piilotettu esimerkiksi tunnettujen ihmisten julkaisuihin. Piilomainonnalla tarkoitetaan sitä, että palvelua tai tuotetta mainostetaan ilman, että kyseessä olisi selkeästi merkitty mainos.
- Sosiaalisessa mediassa yleisimpiä mainosmuotoja ovat sponsoroidut julkaisut, yhteistyöjulkaisut, sekä mainosvideot. Luotettavat sosiaalisen median vaikuttajat ja yritykset merkitsevät kaupallisen yhteistyön esimerkiksi tunnisteilla #kaupallinenyhteistyö tai #mainos. Jos julkaisussa ei ole selkeää merkintää mainoksesta, mutta julkaisu esittelee tuotetta tai palvelua hyvin ylistävään sävyyn, voi kyseessä olla piilomainonta.
- Olisi siis tärkeää suhtautua kriittisesti kaikkeen sosiaalisen median sisältöön. Taitavat käyttäjät osaavat tunnistaa mainokset myös silloin, kun ne ovat naamioitu aivan tavalliseksi sisällöksi.

13. EVÄSTEET JA TIETOJEN KERÄÄMINEN



- Aina kun käytät sosiaalista mediaa tai vieraillet jollakin verkkosivulla, sinusta kerätään monenlaisia tietoja.
- Evästeet (cookies) ovat tiedostoja, jotka tallentuvat laitteellesi ja joiden avulla sivustot voivat seurata käyttäytymistäsi verkossa tai muistaa käyttäjän asetuksia. Sosiaalisen median palveluissa evästeitä hyödynnetään esimerkiksi kohdennetussa mainonnassa.
- Useimmat sivustot ja alustat pyytävät suostumuksesi evästeiden käyttöön. Voit itse rajoittaa, kuinka paljon tietoa sinusta kerätään. Voit esimerkiksi valita vain välttämättömät evästeet, jolloin sinusta kerätään vähemmän tietoa,
- Tietoja, joita kerätään, voivat olla esimerkiksi sijainti, käyttämäsi laitteet, kiinnostuksen kohteet, tai selaushistoria. Tietoja käytetään usein palvelujen parantamiseen tai kaupallisiin tarkoituksiin.
- On tärkeää tarkistaa omat yksityisyyasetukset, sekä tutustua siihen, kuinka alustat käsittelevät tietojasi. Voit myös tyhjentää evästeet selaimen asetuksista säännöllisesti.

14. LAITTEEN TIETOTURVA



- Laitteesta riippumatta (tabletti, älypuhelin, tietokone) laitteen tietoturvasta huolehtiminen ehkäisee monia riskejä.
- Ensimmäisenä olisi tärkeää asentaa laitteeseen virustorjuntaohjelma, sekä pitää se ajan tasalla. Tämä suojaa haittaohjelmilta, jotka voivat esimerkiksi päättää laitteesi hallinnan tai varastaa salasanoja.
- Toisena kannattaa varmistaa, että laitteen käyttöjärjestelmä ja sovellukset päivittyvät automaattisesti. Tämä on tärkeää, sillä päivitykset usein sisältävät tietoturvaparannuksia, jotka suojaavat uusilta uhkilta.
- Kun lataat uusia sovelluksia, lataa ne ainoastaan virallisten sovelluskauppojen kautta, kuten Google Play:n tai App Store:n kautta. Älä lataa tuntemattomia sovelluksia tai anna sovelluksille turhaan lupia esimerkiksi sijainnin, yhteystietojen tai kameran käyttöön.

15. TURVALLISEN VERKKOSIVUN TUNNISTAMINEN



- Siirtyessäsi sosiaalisen median palvelun kautta jollekin verkkosivulle, esimerkiksi lukemaan artikkelia tai kirjautumaan palveluun, on tärkeää tunnistaa turvallinen verkkosivu.
- Turvallinen verkkosivu alkaa aina ” <https://> ” eikä pelkästään ” <http://> “. S-kirjain tarkoittaa sitä, että sivuston ja käyttäjän välinen yhteys on salattu.
- Tarkista aina myös verkkosivun osoite huolellisesti. Huijarit voivat tehdä osoitteita, jotka kovin muistuttavat oikeita sivustoja, mutta sisältävät pieniä eroja, kuten ylimääräisiä kirjaimia tai outoja sanoja. Esimerkiksi osoite “facebook.com” (oikea sivusto) voidaan muokata hieman eroavaksi “faceb00k.com”.
- Turvalliset sivustot eivät koskaan painosta sinua antamaan mitään henkilökohtaisia tietojasi ilman selvää tarkoitusta. Jos verkkosivu vaikuttaa epäilyttävältä, kannattaa poistua siltä heti.

16. VASTUULLISUUS SOMESSA

- Sosiaalisessa mediassa tulee käyttäytyä vastuullisesti, sillä se vaikuttaa niin omaan, kuin muidenkin ihmisten turvallisuuteen ja hyvinvointiin.
- Vastuullinen sosiaalisen median käyttäjä kunnioittaa toisten käyttäjien yksityisyyttä ja oikeutta olla rauhassa. On tärkeää aina muista, että sosiaalisessa mediassa jaettu sisältö voi jäädä pysyvästi näkyviin, jonka takia on kannattavaa miettiä, voisiko julkaistu sisältö loukata jotakuta tai johtaa väärinkäsityksiin.
- Vastuullisella käyttäytymisellä somessa tarkoitetaan myös sitä, että ei jaa valheellista tietoa, eikä osallistu kiusaamiseen tai vihapuheeseen. Aina kun tällaista käytöstä kohtaa sosiaalisessa mediassa, on siitä hyvä ilmoittaa palvelun ylläpidolle.
- Hyvät käytöstavat verkossa tuovat positiivista ja turvallista ilmapiiriä.



17. IDENTITEETTIVARKAUKSILTA SUOJAUTUMINEN

- Identiteettivarkaudella tarkoitetaan tilannetta, jossa joku käyttää luvattomasti toisen henkilötietoja, kuten kuvia, nimeä tai henkilötunnusta, huijatakseen tai hankkiakseen hyötyä. Sosiaalisessa mediassa on tärkeää suojata omia tietoja, sillä se ehkää tällaisia rikoksia.
- Voit suojata itseäsi identiteettivarkauksilta usein eri keinoin. Älä jaa henkilökohtaisia tietojasi, käytä vahvaa salasanaa, sekä hyödynnä kaksivaiheista tunnistautumista jos se on mahdollista.
- Pidä yksityisyysasetuksesi kunnossa ja tarkista ne säännöllisesti. Hyväksy ystäviksi tai seuraajiksi vain henkilöt, jotka tunnet tai jotka vaikuttavat luotettavilta. Älä klikkaa epäilyttäviä linkkejä tai lataa outoja liitteitä.
- Jos kuitenkin huomaat, että tietojasi on päästy käyttämään väärin, tee asiasta välittömästi rikosilmoitus, sekä ilmoita asiasta myös palveluntarjoajalle.

18. SOSIAALISEN MEDIAN TILIN JÄÄDYTTÄMINEN TAI POISTAMINEN



- Jos haluat lopettaa sosiaalisen median käytön joko pysyvästi tai tilapäisesti, voit joko poistaa tilin kokonaan tai jäädättää sen.
- Jäädättämisellä tarkoitetaan sitä, että tilisi ei näy muille, mutta voit halutessasi aktivoida sen uudelleen myöhemmin.
- Poistamisella tarkoitetaan sitä, että kaikki tilin tiedot, julkaisut ja yhteydet poistuvat pysyvästi.
- Esimerkkinä: voit jäädättää tilisi Facebookissa tai Instagramissa asetuksista kohdasta “tilin hallinta” tai “tietosuoja ja turvallisuus”. Lähes kaikissa sosiaalisen median palveluissa tilin jäädättäminen tai poisto tapahtuu asetusten kautta.
- Ennen tilin poistamista, on tärkeää varmuuskopioida itsellesi tärkeät viestit ja kuvat. Varmista myös, että olet kirjautunut ulos kaikilta laitteilta, sekä perunut mahdolliset tilaukset.

19. YHTEENVETO JA LISÄRESURSSIT

- Muista oppaasta ainakin nämä perusasiat: käytä vahvoja salasanoja, tarkista yksityisyysasetukset, ole kriittinen linkeille ja viesteille, sekä älä jaa liikaa tietoa itsestäsi.
- Turvallinen sosiaalisen median käyttö on mahdollista, kun tunnet vaarat ja osaat suojautua riskeiltä.
- Muista, että olet aina oikeutettu kunnioittavaan ja turvalliseen verkkoympäristöön. Epäselvissä tilanteissa kysy aina apua.
- Jos kaipaat apua, voit kääntyä Enter ry:n puoleen.

