Kyberin taskutieto

Digitaalista turvallisuutta jokaiselle

Panu Moilanen ja Irina Lönnqvist

Miksi tarvitset tämän oppaan?

Elämme maailmassa, joka on yhä digitaalisempi ja riippuvaisempi mm. tietojärjestelmistä, digitaalisista palveluista ja tietoliikenneyhteyksistä. Digitalisaatiosta on meille ennen kaikkea hyötyä: se tekee elämästä turvallisempaa, tehokkaampaa ja hauskempaa. Digitaalisuuteen liittyy kuitenkin myös turvallisuusriskejä.

Digitalisaatio muuttaa turvallisuutta kahdella tavalla. Kun digitaaliseen maailmaan tai sen kautta vaikutetaan

teknisesti, puhutaan yleensä kyberuhista, kyberturvallisuudesta ja jopa kybersodankäynnistä. Kun digitaalisessa maailmassa vaikutetaan informaatioon tai informaation kautta esimerkiksi ajatteluumme, puhutaan informaatiouhista, informaatioturvallisuudesta ja jopa informaatiosodankäynnistä.

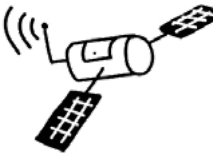
Digitaalisen maailman kautta voidaan vaikuttaa myös dataan – sitä voidaan esimerkiksi varastaa tai manipuloida. Yhteiskuntamme on yhä riippuvaisempi erilaisista suurista datavarannoista, joiden luottamuksellisuudesta, saavutettavuudesta ja eheydestä eli muuttumattomuudesta pitää varmistua. Esimerkki tällaisesta suuresta datavarannosta on terveystietoja sisältävä Kanta-palvelu. Lisäksi meillä kaikilla on omaa henkilökohtaista tärkeää dataa, jota pitää suojata.

Muutokset Suomen ja Euroopan turvallisuustilanteessa vaikuttavat myös digitaaliseen turvallisuuteen. Epävakaa turvallisuusympäristö näkyy myös digitaalisessa maailmassa konflikteina ja operaatioina, joista jotkut voivat olla kannaltamme haitallisia ja jopa vaarallisia.

Digitaalisessa maailmassa sanonta siitä, että ketju on juuri niin vahva kuin sen heikoin lenkki, pitää paikkansa. Me kaikki olemme lenkkejä erilaisissa digitaalisen turvallisuuden ketjuissa, jotka varmistavat paitsi omaamme, niin myös perheemme, lähiyhteisöjemme ja koko Suomen digitaalista turvallisuutta. Siksi meidän kaikkien tulee tuntea perusasiat digitaalisesta turvallisuudesta.

Digitaalinen maailma

Digitaalinen maailma saattaa kuulostaa ilmiöltä, josta vain asiantuntijoiden tulee ymmärtää jotain. Tämä ei pidä paikkaansa, vaan digitaalisuus koskee meitä kaikkia. Lähes kaikkiin arkemme asioiden hoitamiseen käytetään nykyisin tietojärjestelmiä, tietoverkkoja ja ohjelmistoja – eli digitaalista maailmaa. Digitalisaatio myös jatkaa etenemistään.



Digitaalisen maailman voidaan katsoa koostuvan teknisestä kybermaailmasta ja erilaisista digitaalisista informaatioympäristöistä. Kybermaailmassa kaikki koostuu biteistä, eli tiedon yksiköistä. Tätä voi verrata siihen, että fyysisessä maailmassa kaikki koostuu atomeista. Bittien ja atomien maailmat kietoutuvat yhä useammin toisiinsa. Televisio on fyysinen esine, mutta tarvitsee toimiakseen bittejä. Samalla tavoin atomien ja bittien yhteispeliä tarvitaan vaikkapa kaupankäynnissä, terveydenhoidossa ja liikenteessä.

Informaatioympäristö on käyttäjistä, tietoverkoista, palveluista ja informaatiosta koostuva ympäristö, jossa informaatiota kerätään, käsitellään, varastoidaan, välitetään, suojataan ja käytetään. Informaatiota on monenlaista. Se voi olla esimerkiksi eri tietojärjestelmien välillä liikkuvaa dataa tai ihmisten välistä viestintää ja vuorovaikutusta.

Olemme varmasti kaikki kuulleet uutisia siitä, kuinka erilaisten tietojärjestelmien toimintahäiriöt ovat vaikuttaneet tavallisten kansalaisten elämään. Ostoksien maksaminen kortilla lähikaupan kassal-

la ei ole onnistunut, verkkopankkiin kirjautuminen ei ole toiminut, tai kaupungin liikenne on ruuhkautunut liikennevalojen ohjausjärjestelmän seottua. Kaikissa näissä tilanteissa on kyse siitä, että digitaalisen maailman häiriöt ovat näkyneet myös reaalimaailmassa.

Kybersanasto

Digitaalinen maailma on digitaalisen informaation käsittelyyn tarkoitettu, toisiinsa yhteydessä olevista tietokoneista ja muista laitteista, tietoverkoista, palveluista ja käyttäjistä muodostunut ympäristö. Sen voidaan katsoa muodostuvan teknisestä kybermaailmasta ja erilaisista digitaalisista informaatioympäristöistä.

Digi- tai kyberuhka tarkoittaa mahdollisuutta sellaiseen tekoon tai tapahtumaan, joka toteutuessaan vaarantaa digitaalisen maailman oikean ja virheettömän toiminnan. Uhka voi olla esimerkiksi haittaohjelma, palvelunestohyökkäys tai tietomurto. Usein digitaalista maailmaa häiritsee myös täysin sattumanvarainen tapahtuma, esimerkiksi käyttövirhe, tietoliikennehäiriö tai sähkökatko.

Digitaalinen turvallisuus tarkoittaa sitä, että erilaiset digitaaliseen maailmaan kohdistuvat uhat ovat hallinnassa, ja digitaalinen maailma toimii oikein ja virheettömästi. Digitaalinen turvallisuus voidaan jakaa kyber- ja informaatioturvallisuuteen. Osa digitaalista turvallisuutta on kaikkien kansalaisten oikea ja vastuuntuntoinen toiminta digitaalisessa maailmassa.

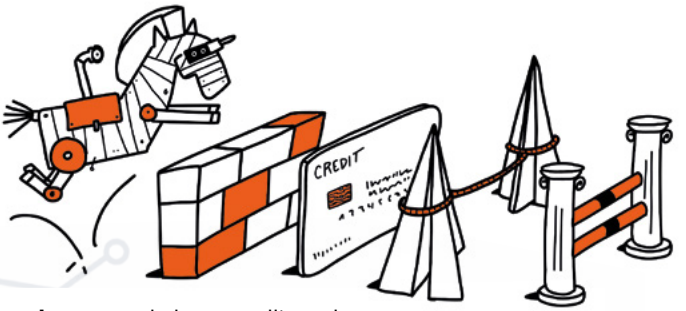
Haittaohjelmat ovat ohjelmia, joiden tarkoitus on aiheuttaa haittaa tai vahinkoa tietokoneelle, muulle älykkäälle laitteelle tai niiden kautta esimerkiksi käyttäjille tai muille kohteille. Haittaohjelmia ovat mm. virukset, kiristyshaittaohjelmat, vakoiluohjelmat ja takaovet. Haittaohjelmien pääsy laitteisiin pitäisi pystyä estämään.

Hybridivaikuttaminen on yleensä valtiollisen toimijan suoraan tai välitoimijoiden kautta toteuttamaa vihamielistä toimintaa, jossa esimerkiksi poliittisin, sotilaallisin, taloudellisin tai kyber- ja informaatiovaikuttamisen keinoin pyritään vaikuttamaan yhteiskuntaan sen horjuttamiseksi. Usein monia keinoja käytetään samanaikaisesti mm. pelon, epävarmuuden ja polarisaation luomiseksi. Digitaalinen maailma on yksi tärkeimmistä hybridivaikuttamisen ympäristöistä.

Informaatiovaikuttaminen on vaikuttamista saatavilla olevan informaation sisältöön ja kulkuun sekä sitä kautta eri vaiheissa olevan tapahtumasarjan lopputulokseen. Tavoitteena voi olla esimerkiksi kansalaisten mielipiteiden muokkaaminen. Informaatiovaikuttaminen voi olla myös vihamielistä. Silloin puhutaan mustasta informaatiovaikuttamisesta. Kun se liittyy meneillään olevaan konfliktiin tai kun sen taustalla on valtiollinen toimija, voidaan puhua myös informaatiosodankäynnistä.

Kiristyshaittaohjelma on haittaohjelma, joka tyypillisesti salaa tietokoneen tai muun älykkään laitteen sisällön. Sen jälkeen laitteen haltijaa kiristetään maksamaan lunnaita (yleensä rahaa kryptovaluuttana). Vastineeksi luvataan ohjeet salauksen purkamiseen. Lunnaita ei kannata maksaa. Kiristyshaittaohjelmilta voi suojautua tietoturvaohjelmistoilla ja varmuuskopioinnilla.

Kriittinen infrastruktuuri tarkoittaa kaikkia palveluita, järjestelmiä ja rakenteita, jotka ovat yhteiskuntamme toiminnalle elintärkeitä. Esimerkkejä kriittisestä infrastruktuurista ovat mm. energianjakelu, tietoliikenneverkot, terveydenhuolto ja sen tietojärjestelmät sekä maksujärjestelmät. Kriittinen infrastruktuuri ja digitaalinen maailma ovat kietoutuneita toisiinsa. Vihamielisen kybervaikuttamisen todennäköisin kohde on kriittinen infrastruktuuri.



Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen osa-alue. Siihen kuuluvat kybermaailmassa tapahtuva ja sitä koskeva tiedustelu, maanpuolustuksen kannalta merkityksellisten kyberympäristöjen suojaaminen ja tiettyihin kyberympäristöihin vaikuttaminen. Kyberpuolustuksesta vastaa Suomessa Puolustusvoimat.

Palvelunestohyökkäys (DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään tietyn verkkopalvelun normaali käyttö. Tavallisimmin hyökkäys toteutetaan kohdistamalla palveluun niin paljon palvelupyyntöjä ja verkkoliikennettä, että palvelu ei enää suoriudu tehtävistään. Palvelunestohyökkäykset ovat yleisimpiä teknisiä kyberhyökkäyksiä. Samalla ne ovat hyökkäyksiä myös informaatiotilassa, sillä usein ne estävät informaation saannin esimerkiksi medioiden tai viranomaisten verkkosivuilta.

Phishing eli tietojenkalastelu on toimintaa, jolla pyritään saamaan haltuun luottamuksellisia tietoja (esimerkiksi henkilö- tai tilitietoja) esiintyen tiedon saantiin oikeutettuna tahona. Näiden tietojen avulla voidaan sitten pyrkiä saavuttamaan esimerkiksi taloudellista hyötyä. Omien yksityisten tietojensa antamisessa tulee verkossa olla erittäin varovainen.

Pilvipalvelu on palvelu, joka tarjoaa tallennustilaa verkossa. Pilvipalveluun tallennettavat tiedot tallennetaan suuriin palvelinkeskuksiin, ja niitä käytetään verkon kautta. Pilvipalveluita voi käyttää esimerkiksi tietojen varmuuskopiointiin. Pilvipalveluihin ei kuitenkaan kannata tallentaa erittäin henkilökohtaisia tietoja, eikä niihin välttämättä saa tallentaa luottamuksellisia tai salaisia tietoja, esimerkiksi työhön liittyviä asiakirjoja.

Päivitys (ohjelmistopäivitys) tarkoittaa ohjelmiston muuttamista siten, että aiempi versio korvataan uudella ohjelmistoversiolla esim. virheiden ja tietoturva-aukkojen korjaamiseksi tai ominaisuuksien lisäämiseksi. Ohjelmistopäivityksiä tarvitaan yhä useampiin laitteisiin – tietokoneisiin, mobiililaitteisiin, verkkolaitteisiin ja esimerkiksi kodinkoneisiin. Huolehdithan, että tiedät, minkä kaikkien laitteidesi ohjelmistoja pitää päivittää.

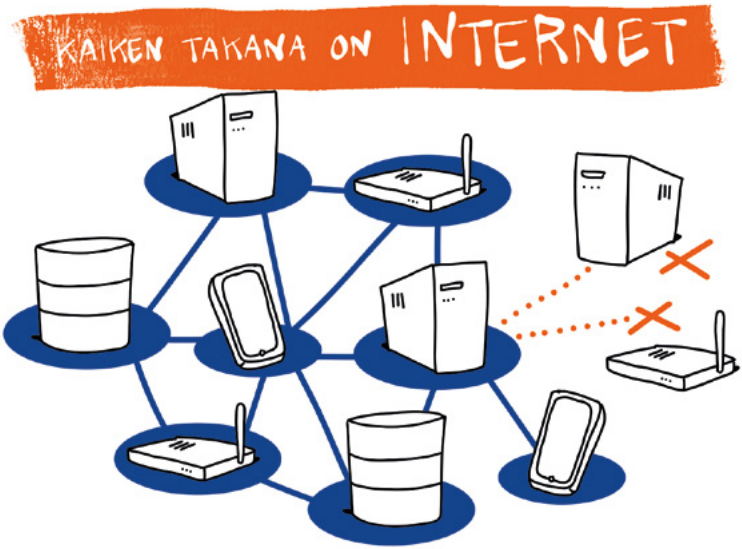
Syvävale eli deep fake on tekoälyllä luotu kuva-, ääni- tai videotiedosto, joka vaikuttaa oikealta mutta ei ole sitä. Esimerkiksi tasavallan presidentti voidaan saada sanomaan asioita, joita hän ei ole koskaan sanonut tai joita hän ei koskaan sanoisi. Olemassa olevista videoista voidaan myös vaihtaa ihmisten kasvoja tai henkilön ääni voidaan väärentää digitaalisesti.

Tekoäly on teknologiaa, joka kykenee tekemään ikään kuin älykkäitä toimintoja. Esimerkkejä näistä toiminnoista ovat mm. puheentunnistus, kielen kääntäminen ja erilaisten sisältöjen tuottaminen. Tekoälystä on paljon hyötyä, mutta sitä voidaan käyttää myös huijauksissa ja vihamielisessä informaatiovaikuttamisessa.

Tietoturva viittaa kaikkiin niihin järjestelyihin, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvaan kuuluvat muun muassa tiedon, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Yksilötasolla tietoturva tarkoittaa tärkeiden tietojen ja laitteiden suojaamista. Jokainen on vastuussa omasta tietoturvastaan.

Varmuuskopiointi tarkoittaa jonkin tärkeän tiedon kopiointia ja varastointia myös muualle kuin sen alkuperäiseen sijaintiin. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista. Esimerkiksi tietokoneiden ja mobiililaitteiden sisällöstä kannattaa tehdä varmuuskopioita. Varmuuskopioita kannattaa usein tehdä sekä ulkoiselle muistilaitteelle että johonkin pilvipalveluun.

Verkkolaite on laite, jonka kautta muut laitteet muodostavat yhteyden internetiin. Se voi olla esimerkiksi taloverkkoon kytkettävä reititin tai mobiiliverkkoon kytkettävä mobiilireititin. On erittäin tärkeää huolehtia verkkolaitteiden turvallisuudesta. Kun otat verkkolaitteen käyttöön, vaihda sen oletussalasana. Huolehdi myös verkkolaitteen päivityksistä säännöllisesti. Tarkista, tarvitsetko verkkolaitteen etähallintaa. Jos et, kytke se pois päältä.



Kirjautuminen on kuin avain

Me kaikki kirjaudumme päivittäin erilaisiin laitteisiin ja palveluihin. Kirjautuminen on kuin avain: se avaa pääsyn esimerkiksi yksityisiin tietoihimme, rahoihimme, muistoihimme ja moneen muuhun. Siksi kirjautumistiedoista kannattaa pitää huolta samalla tavalla kuin kotiavaimesta ja varmistaa, että käyttää riittävän varmoja ja turvallisia kirjautumismenetelmiä.

Yleisin tapa kirjautua on käyttäjätunnus ja salasana. On tärkeää käyttää riittävän hyviä salasanoja – sellaisia, joita ei voi murtaa arvaamalla tai laskemalla. Salasanassa pidempi on aina parempi. Pidemmänkin salasanan muistaa, kun se on salalause – siis esimerkiksi UlkonaOnKaunisAamu2024!!.

Lisäturvaa tuo se, että käyttää salalauseessa vaikkapa murresanoja tai muuten harvinaisempia sanoja ja lisää mukaan erikoismerkkejä ja numeroita.

Monet palvelut tarjoavat mahdollisuuden myös monivaiheiseen tunnistautumiseen (MFA). Se tarkoittaa

sitä, ettei kirjautumiseen riitä vain käyttäjätunnuksen ja salasanan antaminen, vaan kirjautuminen pitää vielä varmentaa esimerkiksi matkapuhelimen ja muuttuvan koodin avulla. Jos palvelussa on mahdollisuus monivaiheiseen tunnistautumiseen, sitä kannattaa aina käyttää.

Monesti on mahdollista käyttää myös biometristä kirjautumista, jossa kirjautuminen tapahtuu esimerkiksi sormenjäljellä tai kasvoilla. Tämä on useimmissa tapauksissa hyvä kompromissi turvallisuuden ja helppokäyttöisyyden välillä. Biometriseen tunnistautumiseen

liittyy myös ongelmia: biometristen tietojen omistajuus ja niihin liittyvät yksityisyydensuojakysymykset puhuttavat edelleen laajasti.

Informaatio on vallankäytön väline

Sanotaan, että tieto on valtaa. Siksi tietoon – eli informaatioon – pyritäänkin vaikuttamaan koko ajan. Arjessamme esimerkkejä vaikuttamisesta ovat mainonta tai valistuskampanjat, joilla meitä yritetään saada syömään terveellisemmin tai liikkumaan enemmän. Tämä on hyväksyttävää eli valkoista informaatiovaikuttamista. Jos vaikuttamisella on vihamielisiä ja pahantahtoisia tavoitteita, silloin ollaan tekemisissä mustan informaatiovaikuttamisen tai informaatiosodankäynnin kanssa.

Musta informaatiovaikuttaminen on vihamielistä vaikuttamista kansalaisiin, päätöksentekijöihin ja toimintakykyyn ohjailemalla saatavilla olevaa informaatiota Tavoitteena on tuottaa vahinkoa vaikuttamisen kohteena oleville ja heidän muodostamilleen yhteisöille.

Sosiaalinen media ja digitaalisuus ovat tehneet informaatiosta aiempaakin tärkeämmän vallankäytön välineen. Informaatiota on yhä enemmän ja se leviää nopeammin kuin aikaisemmin. Siksi informaatioympäristöistä on tullut oleellinen osa konflikteja ja sodankäyntiä.

Informaatiosodankäynti liittyy aina johonkin meneillään olevaan konfliktiin. Se on vihamielistä vaikuttamista valitun kohteen päätöksentekoon, toimintakykyyn ja mielipiteisiin informaatioympäristön kautta sekä suojautumista tällaisilta vaikuttamisyrityksiltä.

Keskeisimmät vihamieliset valtiolliset toimijat informaatiotilassa

ovat meidän suomalaisten näkökulmasta Venäjä ja Kiina, mutta myös monet muuta valtiot harjoittavat informaatiosodankäyntiä.

Venäläisessä sodankäynnissä informaatiosodankäynti on erittäin merkittävässä roolissa: sotaa käydään venäläisen ajattelun mukaan aina myös informaatiotilassa. Venäjän informaatiosodan kohteina ovat mm. Euroopan unioni ja Suomi, ja sen tavoitteita ovat esim. demokraattisten arvojen kyseenalaistaminen, unionin ja yhteiskuntien jakaminen ja hajottaminen sekä unionimaiden vakauden horjuttaminen.

Viime vuosina tekoälyn kehittyminen on muuttanut merkittävästi myös vihamielistä informaatiovaikuttamista. Tekoälyn avulla voidaan luoda erittäin uskottavia, mutta täysin keinotekoisia mediasisältöjä, joita kutsutaan syvävaleiksi. Tekoälybotit saattavat myös osallistua sosiaalisen median keskusteluihin ja levittää disinformaatiota eli paikkaansa pitämätöntä tietoa.

Maalais- tai kaupunkilaisjärjen käyttö on tehokkain tapa suojautua vihamieliseltä informaatiovaikuttamiselta. Mieti aina tarkasti, mitä informaatio tarkoittaa ja voiko se pitää paikkaansa. Kuka on viestin takana ja mikä voisi olla julkaisijan motiivi tai tavoite? Voitko varmistaa tiedon paikkansa pitävyyden muista lähteistä? Ja ennen kaikkea mieti, ennen kuin toimit: tykkäät, jaat, suutut tai teet jotain muuta. Pidä pää kylmänä ja ajatus kirkkaana! Tällä tavalla kehität myös media- ja monilukutaitoasi, jotka ovat oleellisia digitaalisen maailman kansalaistaitoja!

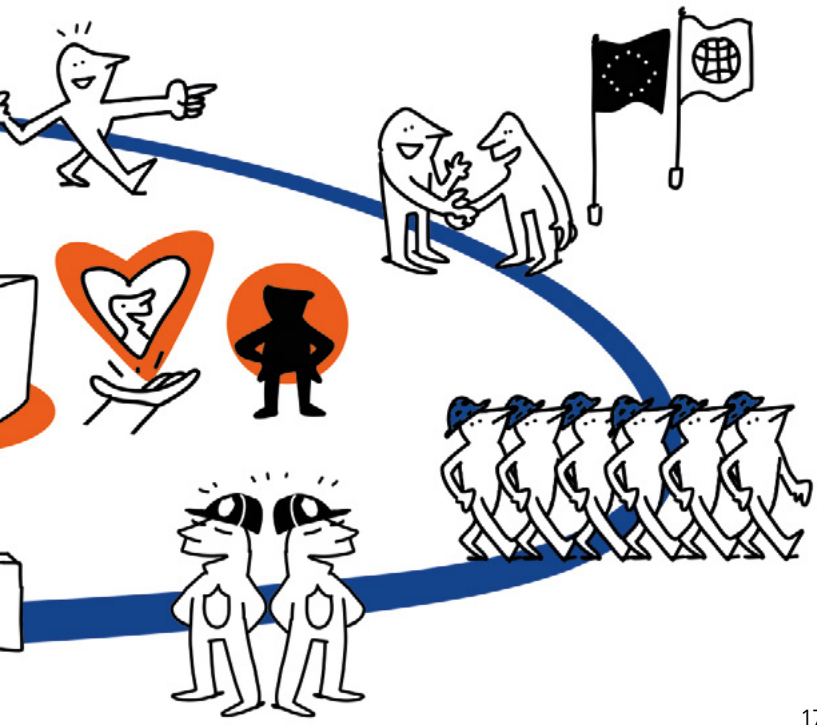
Varautuminen kannattaa

Vaikka moni asia onkin muuttunut digitalisaation myötä, niin silti ennalta varautuminen on edelleen oleellisin asia erilaisista häiriötilanteista selviämisen varmistamiseksi.

Arjen häiriöt ovat ikäviä, ja pahimmassa tapauksessa niistä voi aiheutua myös merkittävää haittaa ja jopa vaaraa. Ennen kaikkea ne rasittavat kuitenkin henkisesti: totuttujen toimintojen ja rutiinien

häiriintyminen saattaa horjuttaa turvallisuudentunnetta ja saada meidät epävarmoiksi. Tämä on normaalia, ja onkin hyvä jo etukäteen pohtia, kuinka selviämme, jos yhteiskuntamme perustoiminnot eivät joskus toimisikaan niin kuin tavallisesti esimerkiksi digitaalisen maailman ongelmien tai jonkin muun syyn vuoksi.

Oman selviytymisstrategian pohtimisen avuksi on tarjolla paljon tietoa. Helpoimmin löydät kattavat varautumisohjeet kriisi- ja häiriötilanteisiin suomi.fi -verkkosivustolta. Niihin kannattaa käydä tutustumassa heti: ohjeissa käydään läpi erilaisia häiriötilanteita tulvista säteilyonnettomuuksiin.



Digitaalisen turvallisuuden näkökulmasta kannattaa varautua ainakin seuraavilla tavoilla:

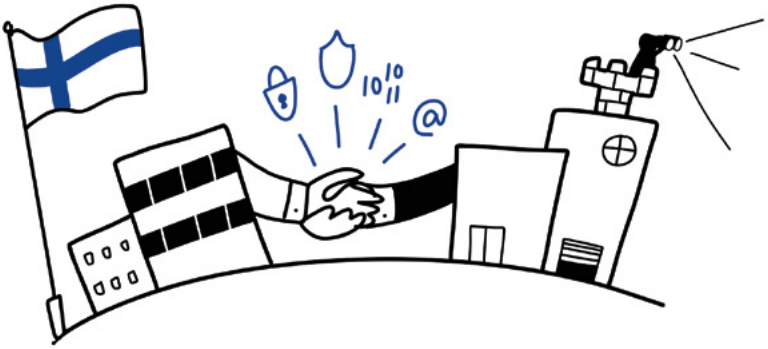
1. **Lue** tämän kirjasen takakannessa olevat kymmenen digitaalisen turvallisuuden käskyä ja noudata niitä.
2. **Varmista**, että sinulla on käytössäsi ainakin kaksi vahvan sähköisen tunnistautumisen menetelmää digitaalisten palveluiden käyttöä varten. Vahvan sähköisen tunnistautumisen menetelmiä ovat Suomessa esimerkiksi pankkitunnukset, mobiilivarmenne ja sähköinen henkilökortti. Kansainvälisesti käytössä on esimerkiksi eurooppalainen digitaalinen identiteettilompakko.
3. **Varaudu** siihen, etteivät maksujärjestelmät ja rahaliikenne aina toimi. Pidä ainakin kotona varalla myös käteistä ja harkitse myös maksamisen riskin hajauttamista esim. tileillä eri pankeissa tai eri tarjoajien maksukorteilla.
4. **Mieti**, miten saat tietoa ja pidät yhteyttä läheisiisi, jos tietoliikenteessä tai sähkönjakelussa on häiriöitä. Varaa kotiin paristokäyttöinen radio ja varavirtalähteitä. Pidä varavirtalähteet ladattuina.
5. **Seuraa** viranomaisten ja muiden luotettavien toimijoiden antamia ohjeita digitaaliseen turvallisuuteen liittyen. Ota tavaksesi esim. tarkistaa kuukausittain Kyberturvallisuuskeskuksen kybersäätiedote.
6. **Tärkeintä on säilyttää maltti** ja muistaa, että kyllä me pärjäämme! Jos emme yksin, niin ainakin yhdessä!

Ole mukana vahvassa ketjussa!

Niin kuin alussa totesimme, digitaalinen turvallisuus koskee meitä kaikkia ja digitaalisen turvallisuuden taidot ovat nykyisin kansalaistaitoja.

Digitaalisessa maailmassa kaikkien pitää tuntea perussäännöt sekä olla varovaisia ja valppaita – aivan kuten liikenteessäkin. Liikenteessä jo yksikin törttöilijä saattaa saada aikaan vakavaa vahinkoa. Tilanne on sama digitaalisessakin maailmassa. Helpoimmin löydät kattavat varautumisohjeet kriisi- ja häiriöitilanteisiin osoitteesta **www.suomi.fi/oppaat/varautuminen**. Siksi on tärkeää, että huolehdimme paitsi omastamme niin myös läheistemme osaamisesta. Näin toimien varmistumme siitä, ettemme ole digitaalisen turvallisuuden heikoimpia lenkkejä. Samalla varmistamme koko Suomen digitaalista turvallisuutta.

Tämän oppaan takakannessa on kymmenen kansalaisen digiturvakäskyä, joiden avulla parannat omaa ja myös muiden digitaalista turvallisuutta. Kun noudatat näitä käskyjä ja muita tämän kirjasen ohjeita, olet yksi lenkki vahvassa digiturvallisuuden ketjussa!



Haluatko tietää lisää?

Kiinnostuitko digitaalisesta turvallisuudesta ja haluaisitko tietää ja oppia sitä lisää? Tämän oppaan julkaisseet Maanpuolustuskoulutus MPK ja Jyväskylän yliopisto järjestävät molemmat kaikille avointa koulutusta digitaaliseen turvallisuuteen liittyen.

Saat tarjolla olevasta koulutuksesta tietoa verkosta osoitteista **mpk.fi/kyber** ja **r.jyu.fi/digiturva**.

Tervetuloa!

TEKSTI

Panu Moilanen
Irina Lönnqvist

KUVITUS

Linda Saukko-Rauta
Redanredan Oy, 2017-2022

TAITTO

Ossi Hietala ja Suvi Karjalainen

JULKAISIJAT

Jyväskylän yliopisto
Maanpuolustuskoulutus MPK

JULKAISUVUOSI

2025

PAINO

Jyväskylä/Rauma

ISBN

ISBN 978-952-86-0392-4 (painettu)
ISBN 978-952-86-0393-1 (pdf)

MPK
MAANPUOLUSTUSKOULUTUS
FÖRSVARSUTBILDNING

JYU. Since 1863.

ICT SUOMI

Kansalaisen kymmenen digiturvakäskyä

1. **Ole terveen epäluuloinen** ja kysy riittävän usein MIKSI.
2. **Mieti, mitä laitat verkkoon:** kaikkea ei tarvitse kertoa ja verkkoon laitettua ei saa sieltä enää pois.
3. **Älä klikkaa linkkejä** tai avaa liitetiedostoja, jos et ole varma niiden turvallisuudesta. Älä koskaan mene minkään palvelun kirjautumissivulle esim. tekstiviesti- tai sähköpostilinkin kautta.
4. **Huolehdi kaikkien laitteidesi** – myös esim. kodinkoneiden – päivityksistä ja tietoturvasta. Jos et itse osaa, kysy neuvoa! Tietoturva on väärä kohta säästää!
5. **Ole rahaan liittyvien** asioiden kanssa erityisen tarkka. Huolehdi pankkitunnuksistasi ja käytä yleiseen tunnistautumiseen esimerkiksi mobiilivarmennetta.
6. **Muista, että julkiset ja avoimet langattomat verkot** ovat turvattomia. Älä käytä julkisia laitteita mihinkään, mikä edellyttää kirjautumista. Älä lainaa mitään omia laitteitasi vieraille ihmisille.
7. **Muista varmuuskopiointi.** Tee varmuuskopioita niin ulkoisille muistilaitteille kuin pilvipalveluunkin. Jos mahdollista, kytke päälle automaattinen varmuuskopiointi.
8. **Käytä luotettavia ja turvallisia kirjautumistapoja.** Salasanan tulee olla riittävän pitkä. Käytä monivaiheista tunnistautumista aina kun mahdollista.
9. **Pohdi jo etukäteen**, miten tulisit arjessa toimeen myös ilman digitaalista maailmaa ja sen palveluita. Varaudu myös konkreettisesti!
10. **Ole varovainen, mutta älä pelkää** – digimaailmasta on selvästi enemmän hyötyä kuin haittaa. Opasta ja tue myös muita, jos siihen pystyt ja avulle on tarvetta.