Digihuijausten tunnistaminen ja niiltä suojautuminen

Opas yrityksille ja organisaatioille
sekä Maija ja Matti Meikäläisille

oletietoinen.fi

Opetus- ja kulttuuriministeriö

POLIISI
POLIISIAMMATTIKORKEAKOULU

JYVSECTEC
by jamk

Ole tietoinen – älä tule yllätetyksi!

Kyberturvallisuus eli digitaalisen maailman turvallisuus ei ole vain asiantuntijoiden asia. Sinä ja minä, me kaikki – voimme turvata digiarkeamme jo pienillä teoilla sekä tietoisemmalla tekemisellä.

Nyt luettavanasi oleva napakka opas sisältää hyödyllistä perustietämystä digihuijauksista. Oppaan avulla opit tunnusmerkkejä ja keinoja, joilla voit torpata jo alkuunsa monen huijarin aikomukset.

Kannattaa muistaa, että huolellisestikin turvatut ja suojatut systeemit ovat aina herkkiä ihmisen tekemille ratkaisuille ja toiminnalle. Siksi myös digimaailmassa kannattaa keskittyä tekemään yhtä asiaa kerrallaan ja antaa pieni ajatus seuraavalle toimenpiteelleen, jonka aikoo tehdä.

Kaikesta varovaisuudestakin huolimatta huijarit onnistuvat!

Vahingon tapahtuessa ei pidä hävetä tai nolostella, vaan tehdä ilmoitus viranomaiselle ja varoittaa liikkeellä olevista huijareista myös kanssaihmisiä. Vaikenemalla tarjoamme kyberrikollisille vapaan temmellyskentän ja monta uutta mahdollista uhria huijattavaksi.

Kyberturvallisia lukuhetkiä ja kerro opeistasi myös kavereillesi!

Sisältö

Miksi me ihmiset olemme alttiita kyberrikollisten ansoille?

Ihminen ei odota joutuvansa hyökkäyksen kohteeksi. Arjessa toimitaan rutiininomaisesti ja usein kiireessä. Multitaskataan eli tehdään useita asioita yhtä aikaa, eikä keskitytä meneillään olevaan tehtävään.

Näin huijarit meitä huijaavat

- Luodaan vaikutelmaa kiireestä

  “Toimimalla pikaisesti voit...”

- Pelotellaan ja/tai uhkaillaan ongelmilla

  “Jos et nyt heti toimi niin...”

- Uskotellaan, että kyseessä on ainutlaatuinen tilaisuus

  “Sinut on valittu, juuri sinä voit voittaa!”

- Vedotaan myötätuntoon tai auttamisen haluun

  “Vain sinä kykenet auttamaan...”

- Kehotetaan viesteissä reagoimaan erilaisissa palveluissa tapahtuviin muutoksiin

  “Päivitä tietosi linkin kautta mahdollisimman pian tai muuten palvelu lakkaa toimimasta...”

Huijaamiseen soveltuvia kanavia

Sähköpostit | Somepalvelut | Tekstiviestit | Puhelimet | Ovensuut

Inhimillisiä piirteitämme, jotka altistavat huijauksille

- Huolimattomuus ja välinpitämättömyys

  ”On minun asiani, jos salasanani joka palveluun on Peruna4”

- Uteliaisuus ja seikkailunhalu

  ”Jaa, mitäs täältä löytyy, mikäs linkki se tämä on? Klikataas tästä”

- Myötätuntoisuus ja auttavaisuus

  ”Voi että, tuokin parka on ihan orpo, ja matkarahat isän ja äidin luokse puuttuu”

- Velvollisuudentuntoisuus

  ”Onpa hieno homma, kun pomo pyytää juuri minulta näin iltasella apua ja kehottaa tekemään heti 50 000 euron tilisiirron ilmoittamalleen tilille”

- Luottavaisuus

  ”Kerrankos poliisi minulta pankkitunnuksia pyytää, kun epäilee tililläni tapahtuneen väärinkäytöksiä”

- Ahneus

  ”Ohhoh, nyt olisi tarjolla tuhannen euron puhelin vain yhdellä eurolla, tähän tarjoukseen on pakko tarttua heti”

Huijari onnistuu todennäköisemmin organisaatiossa, jossa työntuiskeessa...

- **Sovellus- ja järjestelmäpäivityksiä ei tule tehtyä**, sillä ne ilmaantuvat aina yllättäen ja väärään aikaan keskeyttämään työntekoa
- **Tietojenkalasteluviestit kulkeutuvat roskapostifiltttereiden läpi** ja pääsy organisaation kriittisiin tietoihin onnistuu sähköpostejaan operoivien ihmisten avustamina
- **Olemassa olevia tietoturvariskejä ei tiedosteta tai hahmoteta**, eikä työntekijä ymmärrä riittävän hyvin omaa rooliaan ja tekemistään osana koko organisaation tietoturvallisuuskäytäntöjä
- **Tietoturvallisen käyttäytymisen merkitystä ei tunnisteta** erilaisten toimintojen, eri laitteiden ja järjestelmien rajapinnoilla työtä tehdessä ja siirryttäessä tehtävästä toiseen
- **Tietoturvallisen käyttäytymisen säännöt periaatteessa tiedetään, mutta silti annettuja ohjeita rikotaan** ja sovittuja käytäntöjä ohitetaan, sillä ne saattavat hidastaa tai monimutkaistaa työskentelyä
- **Organisaatiokulttuuri on sellainen, ettei vahingoista uskalleta raportoida ajoissa**
- **Tietoturvallinen käyttäytyminen vaatii omaan tehtävään varsinaisesti liittymättömiä vaiheita** ja erilaisia toimintoja, jotka työntekijän pitää erikseen muistaa
- **Työssä multitaskataan**, eli ei keskitytä meneillään olevaan tehtävään ja siksi saatetaan olla huolimattomia ja tehdään harkitsemattomia, tietoturvan kannalta huonoja ratkaisuja

Tunnista huijaukset ja suojaudu

Sähköpostihuijaus

Sähköposti on töissä ja vapaa-ajalla tehokas ja halpa viestintäväline. Samalla se on rikollisille tehokas ja halpa työväline tärkeiden henkilökohtaisten tai organisaation tietojen kalastelussa ja taloudellisen hyödyn tavoittelussa.

Tunnusmerkkejä

- Viestin lähettäjä voi olla tuntematon tai osoite epäilyttävä
- Viesti on tutulta henkilöltä, mutta epätyypillinen aiheeltaan
- Viesti on yllättävä ja odottamaton sekä sisältää linkin tai liitteen
- Viestin vastaanottajajoukko on epämääräinen sekoitus eri henkilöitä
- Viestin lähetysajankohta on poikkeava (esim. yö)
- Viestin otsikko tai liite ei liity viestin muuhun sisältöön
- Lähettäjä painostaa tekemään jonkin toimenpiteen
- Viestin sisältämä teksti, linkki tai liite vaikuttaa epäilyttävältä ja viestissä on kirjoitusvirheitä
- Viestissä kehotetaan tarkistamaan omia tietoja linkin kautta tai liitteestä
- Viestin linkissä oikean palveluntarjoajan osoite on väärin kirjoitettu
- Kun viet hiiren viestissä olevan linkin päälle, näkyvillä olevat osoitteet poikkeavat toisistaan

Suojautumiskeinoja

- Älä levitä tai julkista esim. somessa organisaatiostasi, itsestäsi tai läheisistäsi sellaisia tietoja, joista rikolliset voivat hyötyä
- Älä tee kiireessä klikkauksia tai päätöksiä. Jos jokin tuntuu epäilyttävältä, luota sisäisten hälytyskellojen ääneen, kyseessä voi olla huijausyritys
- Tee uskottavilta vaikuttavien, mutta normaalista toiminnasta poikkeavien sähköpostipyyntöjen varmistus puhelimitse
- Tuntuuko, että jokin viestissä epäilyttää? Pysähdy hetkeksi pohtimaan, eikö jokin tekijä sovi normaaliin viestintäkuvioon

Toimitusjohtajahuijaus

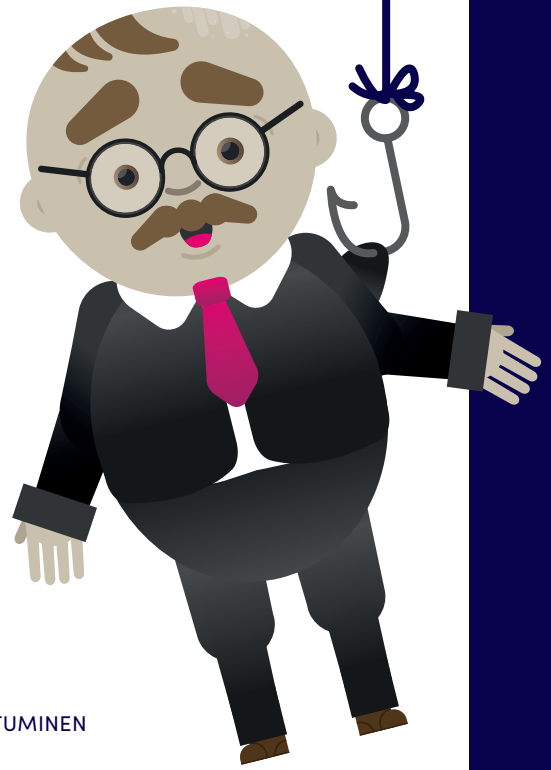
Toimitusjohtajahuijauksessa rikollinen tekeytyy johtajaksi ja pyrkii harhauttamaan organisaation työntekijää tekemään rahansiirron omalle huijaustililleen. Tavallisesti sähköpostitse lähetetystä viestistä saa vaikutelman, että viestin on lähettänyt oma johtaja, vaikka todellisuudessa huijari on ottanut tämän sähköpostitilin luvattomasti käyttöönsä.

Tunnusmerkkejä

- Saat rahansiirtopyynnön johtajalta hänen ollessaan lomalla tai matkoilla
- Rahansiirrolla on kiire ja se on toteutettava nopeasti jonkin tekosyyn varjolla
- Saatat saada vielä toisen viestin tutulta henkilöltä, jossa maksua kiirehditään
- Pyyntö voi vaikuttaa normaalikäytäntöihin verrattuna ristiriitaiselta
- Sinua pyydetään ohittamaan rahansiirtoja suojaavat valtuutuskäytännöt
- Varojen siirtotili on todennäköisesti Euroopan ulkopuolisessa pankissa

Suojautumiskeinoja

- Suhtaudu aina yllättäviin maksupyyntöihin varauksella, tee tarvittaessa tarkistuspuhelu
- Noudata sovittuja ja vakiintuneita laskutus- ja maksukäytäntöjä
- Noudata aina maksamiseen liittyviä ohjeita mahdollisesta painostuksesta huolimatta
- Tarkista sähköpostiosoite huolella, älä avaa epäilyttäviä linkkejä tai liitetiedostoja
- Älä levitä työnantajasi tietoja somessa ja vältä yksityisen sähköpostin käyttöä työkoneella
- Kerro epäilyttävistä rahansiirtopyynnöistä työtovereillesi



Tietojenkalastelu

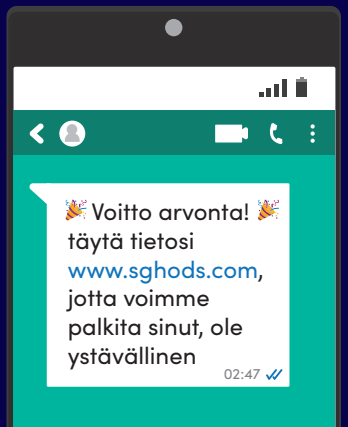
Tietojenkalastelussa huijari urkkii henkilökohtaisia tietoja kuten erilaisia tunnuksia ja salasanoja tai organisaation tärkeitä luottamuksellisia tietoja. Tietojenkalastelua tapahtuu esimerkiksi sähköpostitse ja tekstiviesteillä, mutta myös puhelimitse. Rikollinen esiintyy viranomaisen, pankin, kaupan tai muun palveluntarjoajan edustajan nimissä.

Tunnusmerkkejä

- Saat odottamattoman viestin tai puhelun yllättävältä osapuolelta ilman, että olet ensin itse ollut mitenkään asiassa aktiivinen
- Sähköposti-/tai tekstiviestissä sinua kehotetaan jostain syystä klikkaamaan ohessa olevaa linkkiä, jonka takana pyydetään tietojasi
- Saamasi viesti tai puhelun sisältö saattaa sisältää uhkauksen tai uskomattoman tarjouksen, tai jonkin muun toimenpidepyynnön, jota ilman et voi jatkaa tai selvitä jostain tietystä tilanteesta
- Vastauksellasi on kiire ja toimenpiteitä vaaditaan mahdollisimman pian

Suojautumiskeinoja

- Suhtaudu varauksella tuntemattomiin tai yllättäviin viesteihin tai puheluihin
- Suhtaudu varauksella tutulta saamaasi viestiin, jos sisältö poikkeaa tavanomaisesta
- Tarkista sähköpostilinkkien aitous, vastaako linkin nimi osoitetta, jonne linkki olisi ohjautumassa
- Pohdi viestin lähetysaikaa, lähettäjän nimeä, otsikkoa ja sisältöä - ovatko loogisia
- Tutki huolellisesti onko sähköposti- tai tekstiviestissä käytetty kieli hyvää suomen kieltä
- Havainnoi motivoidaanko sinua innostamalla tai uhaten tekemään jokin toimenpide
- Huijauspuhelua epäillessäsi voit soittaa tarkistuspuhelun väitetyn osapuolen organisaatioon



Kiristyshaittaohjelma

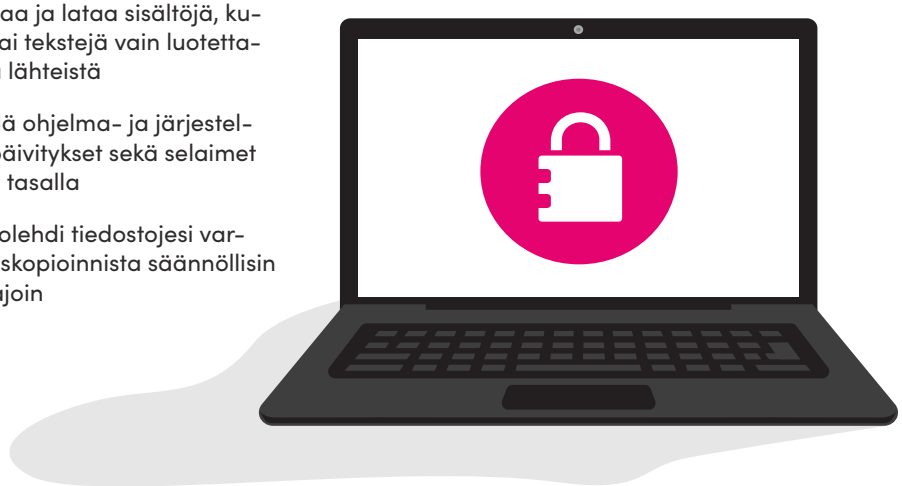
Tietokoneellesi iskeytynyt kiristyshaittaohjelma rajoittaa tai estää kokonaan pääsyn laitteellesi ja sen sisältämiin tiedostoihin. Kiristyshaittaohjelman tunnistat siitä, että näytölläsi on sävyltään uhkaava viesti, jossa väitetään, että saat tiedot haltuusi takaisin maksamalla lunnaita.

Tunnusmerkkejä

- Näytöllesi ilmestyvässä viestissä kerrotaan, että laite tai tiedostot on lukittu
- Uhkaviestin ulkoasu voi olla virallista muistuttava tai viranomaisteemainen
- Sinulta vaaditaan lunnasmaksua lukituksen poistamiseksi
- Sinua kehotetaan toimimaan tietyn ajan kuluessa tai pääsy tietoihin estyy pysyvästi

Suojautumiskeinoja

- Älä klikkaa sähköpostilinkkejä, jotka saat odottamatta ja epäilyttäviltä tahoilta
- Älä verkossa surffatessasi klikkaa epäilyttäviä linkkejä, pop up- tai viesti-ikkunoita
- Selaa ja lataa sisältöjä, kuvia tai tekstejä vain luotettavista lähteistä
- Pidä ohjelma- ja järjestelmäpäivitykset sekä selaimet ajan tasalla
- Huolehdi tiedostojesi varmuuskopioinnista säännöllisin väliajoin
- Käytä laajennettuja käyttäjäoikeuksia ainoastaan tilapäisissä ylläpitotehtävissä
- Suojaa laitteesi luotettavien valmistajien tietoturvaohjelmilla



Verkkosivuhuijaus

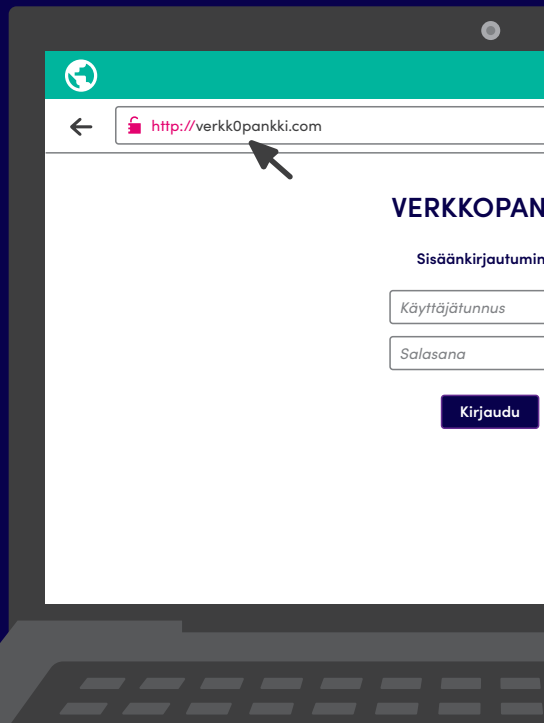
Verkkosivuhuijauksessa joudut ohjatuksi oikean sivuston sijaan todentuntuiselta vaikuttavalle ja näyttävälle huijaussivustolle. Väärennetyllä nettisivustolla huijarit pyrkivät kalastelemaan sinulta tärkeitä henkilökohtaisia tietoja omaan rikolliseen tarkoitukseensa.

Tunnusmerkkejä

- Nettiosoite tai hyperlinkki on julkaistu epäilyttävän lähteen yhteydessä
- Nettisivun osoitteessa on kirjoitusvirheitä tai se eroaa oikean palveluntarjoajan nettiosoitteen kirjoitusasusta
- Nettisivun osoitekenttä http-alkuinen, joka viittaa suojaamattomaan verkkoyhteyteen
- Nettisivun osoitteen loppuosaa täydentää epämääräinen merkkijono
- Nettisivun osoitteessa on kirjoitusvirheitä tai se eroaa oikean palveluntarjoajan nettiosoitteen kirjoitusasusta
- Nettisivun osoitteen loppuosaa täydentää epämääräinen merkkijono
- Käytössäsi olevan selaimen (esim. Firefox tai Chrome) osoitekentän pieni lukkokuvake huomauttaa nettisivuston turvallisuudesta

Suojautumiskeinoja

- Kirjoita nettisivun osoite selaimen osoitekenttään minkäänlaisten sähköposti tms. linkkien seuraamisen sijasta
- Suosi https-alkuisia suojattuja verkkoyhteyksiä sivuilla, joille vaaditaan henkilötietojen syöttämistä esim. tietolomakkeille
- Tarkista sivuston yhteyden turvallisuus osoitekentän tietoturvakuvakkeesta, joka on pieni lukonkuva osoitteen alussa
- Kiinnitä huomiota nettisivun osoitteen kirjoitusasun oikeellisuuteen ja virheettömyyteen



Haitallinen mainos

Haitalliseksi mainokseksi kutsutaan nettisivuilla olevaa mainosbanneria, joka saattaa klikkauksen seurauksena ladata koneellesi haittaohjelman tai ohjata pahaa-aavistamatta suoraan huijaussivustolle, jossa kalastellaan henkilökohtaisia tietojasi.

Tunnusmerkkejä

- Nettisivulla voi vilkkua ja välkkyä huomiota kerjääviä mainoksia
- Tietokoneesi alkaa toimia tavallista hitaammin
- Nettisivulla vieraillessasi näytöllesi avautuu uusi ponnahdus- tai selainikkuna
- Nettisivu ohjautuu yllättäen uudelle sivulle ilman selvää syytä tai erillisiä toimiasi
- Sinua kehotetaan tekemään ylimääräisiä toimenpiteitä ja asentamaan jotain koneellesi

Suojautumiskeinoja

- Ota automaattinen ponnahdusikkunoiden esto käyttöön selainasetuksissa
- Vältä klikkailemasta epäilyttävien ponnahdus- ja selainikkunoiden painikkeita
- Vieraile ainoastaan luotetuilla tai muutoin yleisesti tunnetuilla nettisivuilla
- Käytä laajennettuja käyttöoikeuksia ainoastaan tilapäisissä ylläpitotehtävissä
- Huolehdi järjestelmä- ja ohjelmistopäivitysten ajantasaisuudesta, sillä päivitykset korjaavat tietoturva-aukkoja
- Varmista pyydettyjen asennusten turvallisuudesta ennen niiden suorittamista

Tilausansahuijaus

Tilausansahuijaukseksi kutsutaan tilannetta, jolloin tietämättäsi sitoudut jonkin palvelun tai tuotteen pitkäkestoiseen tilaussopimukseen. Sinut siis erehdytetään sopimukseen, jota et oikeasti edes halua.

Tunnusmerkkejä

- Sinulle tarjotaan ilmaista tai erittäin halpaa kokeilueräätä
- Olet saamassa tuotteen pelkillä toimituskuluilla
- Olet yllättäen voittanut jotain osallistumatta kilpailuihin
- Saat tuotteesta tai palvelusta laskun, vaikka et ole mielestäsi tilannut mitään
- Saat kutsun tutkimukseen tai kyselyyn, ja osallistumisesta tarjotaan hintavaa palkkiota
- Viestin kieliasu voi olla ilmaisultaan kömpelö tai sisältää kirjoitusvirheitä

Suojautumiskeinoja

- Suhtaudu kriittisesti kohdallesi osuviin uskomattomiin tarjouksiin
- Harkitse ennen kuin klikkaat linkkiä - älä edes vieraile huijaussivustolle
- Tarkista asianomaisen yrityksen tiedot netistä
- Tarkista linkkien aitous, vastaako linkin nimi osoitetta, jonne linkki olisi ohjautumassa
- Älä vastaa epäilyttäviin sähköposteihin
- Älä tilaa mitään vain postilokeron kautta toimivilta yrityksiltä

WLAN*-huijaus

Tämän huijaustyypin mahdollistavat avoimet ja suojaamattomat langattomat lähiverkot, joita saattaa olla käytössä esimerkiksi yleisissä tiloissa ja kulkuneuvoissa. WLAN-huijauksessa joku ulkopuolinen taho seuraa tekemistäsi langattomassa verkossa ja urkkii salasanojasi ja muita tärkeitä tietojasi.

Tunnusmerkkejä

- Langattoman lähiverkon nimi ei ole entuudestaan tuttu tai yleisesti tiedossa oleva
- Samalla alueella on tarjolla useita saman nimisiä langattomia lähiverkkoja
- Yhteyden muodostamisessa käytettävä salasana on yleisesti tiedossa oleva
- Yhteyden muodostaminen langattomaan lähiverkkoon ei edellytä erillistä kirjautumista, vaan verkko on avoin
- Langattoman lähiverkon nimi poikkeaa tavanomaisesta tai oletetusta kirjoitusasustaan

Suojautumiskeinoja

- Muodosta yhteys ainoastaan tunnettuihin ja luotettaviin langattomiin lähiverkkoihin
- Vältä käyttämästä avoimia ja suojaamattomia langattomia lähiverkkoja
- Suosi tunnistautumista edellyttäviä suojattuja langattomia lähiverkkoja
- Ota pois käytöstä laitteen automaattinen yhdistäminen langattomiin lähiverkkoihin
- Edellytä käyttämiltäsi langattomilta lähiverkoilta riittävän vahvaa salausta
- Kytke langaton käyttö pois päältä laitteesta aina kun et aktiivisesti tarvitse sitä
- Hyödynnä VPN-palveluita muodostaaksesi suojatun yhteyden verkkojen välille
- Käytä mobiilidataa jos epäröit langattoman lähiverkon turvallisuutta

* Wifi | Avoin verkko | Langaton verkko

Hyviä neuvoja vapaa-aikaan ja työhön

1. Tarkista käyttämiesi palveluiden yksityisyysasetukset
2. Käytä vahvoja salasanoja tai kaksivaiheista tunnistautumista kirjautuessasi palveluihin
3. Säilytä salasanoja ja koodeja siten, etteivät ne voi päätyä vieraisiin käsiin
4. Aseta tilillesi ja maksukorteillesi nosto- ja maksuraja
5. Huolehdi, että laitteittesi järjestelmä- ja ohjelmistopäivitykset ovat aina ajan tasalla
6. Suojaa älylaitteesi lukitsemalla näytöt PIN-koodilla, salasanalla tai sormenjäljellä
7. Poista käytöstä sometilit ja palvelut joita et seuraa aktiivisesti tai et tarvitse
8. Ota tärkeistä tiedostoistasi ja kuvistasi säännöllisesti varmuuskopiot
9. Ole tarkkana kenelle annat tai mihin palveluun syötät henkilökohtaisia tietojasi
10. Tarkista omia tietojasi netistä hakemalla, minkälaisista asiayhteyksistä tietoja löytyy
11. Noudata etätyöskentelyssä työpaikalla yhteisesti sovittuja käytänteitä
12. Huolehdi työympäristön turvallisuudesta ja työvälineiden säilytyksestä
13. Käytä työskentelyyn lähtökohtaisesti vain työnantajan tarjoamia työvälineitä
14. Muodosta yhteys ainoastaan luotettuihin ja suojattuihin langattomiin verkkoihin
15. Turvaa verkossa työskentelyä käyttämällä VPN-etäyhteyttä
16. Hävitä aina henkilötietojasi sisältävät paperit huolellisesti, älä heitä niitä roskiin

Vältä digiansat ja paranna tietoturvaasi!

Katso YouTubesta

- **Älä joudu nettirikollisten kiristettäväksi**
- **Älä lankea tilausansaan**
- **Älä lankea tietojenkalasteluansaan**
- **Älä tule digihuijatuksi**

Kansallista kyberosaamista kasvattamassa,
CYBERDI-projekti 10/2018 – 12/2021

oletietoinen.fi

Opetus- ja kulttuuriministeriö

POLIISI
POLIISIAMMATTIKORKEAKOULU

JYVSECTEC
by jamk