DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvallisuuden käytännön vinkit

VAHTI-hyvät käytännöt tukimateriaali

1.12.2021

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

VAHTI / Kirves Juha (DVV)

1.12.2021

Sisällysluettelo

VAHTI / Kirves Juha (DVV)

1.12.2021

Digiturvallisuuden käytännön vinkit

Tässä VAHTI hyvät käytännöt tukimateriaalissa on koottu syksyllä 2021 muun muassa Digiturvaviikon verkkolähetysten chat-osioista ja muista usein kysytyistä kysymyksistä poimittuja käytännön digiturvallisuuden vinkkejä. Hyvät käytännöt ovat pääasiassa kirjoitettu koskemaan henkilökohtaisia ja henkilökohtaisessa omistuksessa olevia laitteita. Työnantajan laitteita käytettäessä on ensisijaisesti sovellettava työantajan tietoturva ja -suoja ohjeistusta.

1 Sovellusten turvallinen käyttö

1.1 Sovellusten ja päätelaitteen käyttöjärjestelmän päivitys

1.1.1 Miksi päätelaitteeni ei päivitä käyttöjärjestelmääni automaattisesti, vaikka automaattinen päivitys on päällä?

Joskus saattaa olla niin, että päätelaite ei aina päivitä itseään, vaikka automaattinen päivitys olisi käytössä. Siksi kannattaa välillä käydä itse tarkistamassa päivitykset. Esimerkiksi älylaitteiden osalta syynä saattaa olla liian vähäinen akun latauksen määrä tai se, että laitteen tallennustila on lähes täynnä. Kokeile päivittää itse ”manuaalisesti” automatiikan sijaan niin näet mahdollisen virheilmoituksen, joka estää päivityksen.

1.1.2 Miksi sovellukset, laitteen käyttöjärjestelmä tai laite tulee päivittää?

Sovelluksissa, laitteiden ohjelmistoissa ja käyttöjärjestelmissä saattaa olla haavoittuvuuksia eli virheitä ohjelmistoissa, joita verkkorikolliset voivat hyödyntää. Laitteiden ja ohjelmistojen valmistajat tekevät kuitenkin jatkuvasti päivityksiä, jotka korjaavat tunnistetutut haavoittuvuudet. Mitä pitempää laitteen uudet päivitykset jäävät suorittamatta, sitä enemmän laitteeseen jää haavoittuvuuksia, jotka altistavat sen verkkorikollisten hyökkäyksille.

1.2 Sovellusten keräämät tiedot

1.2.1 Minulla ei ole mitään salattavaa, joten miksi sillä on väliä, mitä tietoja palveluun itsestäni laitan?

"Ei mitään salattavaa" on usein virheellinen olettama. Nykypäivän uhka ei koske välttämättä itseä, vaan vaikutukset koskevat muita. Luovuttamiasi tietoja voidaan käyttää esimerkiksi työnantajaasi vastaan suuremman tietoverkkorikoksen toteuttamiseksi.
Kts. myös esim. https://tietosuoja.fi/-/minulla-ei-ole-mitaan-salattavaa-maailman-toiseksi-yleisin-valhe- ja https://kulma.kkv.fi/2016/09/14/minulla-ei-ole-mitaan-salattavaa/ sekä https://yle.fi/uutiset/3-7727020

Laitteeseen tallentunut salasana tai muun palvelun salasana saattaa olla mahdollista kaapata verkkorikollisen käyttöön. Sähköpostin salasanan avulla verkkorikollinen saattaa päästä kiinni sähköpostiisi ja hän voi vaihtaa kaikkien keskeisten käyttämiesi palveluiden salasanat ja saada siellä olevia tietoja haltuunsa. Tämän takia suosittelemme ottamaan monivaiheisen tunnistautumisen käyttöön, jolloin pelkällä käyttäjätunnuksen ja salasanan varastamisella tietosi eivät vaarannu.

Onko älylaitteellasi sellaisia valokuvia tai videoita, joiden et toivo päätyvän julkisuuteen?

1.4 Sovellusten oikeudet

1.4.1 Mitä oikeuksia sovelluksille kannattaa antaa?

Uutta sovellusta käyttöön otettaessa kysytään, mitä älylaitteen toiminnoista sovellus voi käyttää tai mihin tietosisältöihin sillä on käyttöoikeus. Tässä vaiheessa kannattaa olla tarkkana ja antaa sovellukselle ainoastaan ne oikeudet, jotka ovat välttämättömät niihin käyttötarkoituksiin, joihin sovellusta käytät.

Pelille ei välttämättä ole tarvetta antaa oikeuksia käyttää puhelimen kuvia ja puhelimen kuvankäsittelysovelluksen ei ole tarvetta käyttää puhelimen mikrofonia. Sovellusten oikeuksia on mahdollista määrittää puhelimen asetuksista käyttöönoton jälkeen. Suosittelemme, että käyt säännöllisesti, esimerkiksi kerran kuukaudessa katsomassa, millä sovelluksilla älylaitteellasi on oikeudet mikrofoniin, kameraan, valokuviin ja paikkatietoihin.

1.5 Sovellusten käyttöehdot

1.5.1 Sovellusten ja laitteiden käyttöehdot ovat pitkät. Kannattaako niitä lukea?

Käyttöehdoissa tai niiden lisäksi saatavilla olevassa tietosuojaselosteessa kerrotaan, mitä henkilötietoja sovellus käyttäjästään kerää, mihin tarkoitukseen niitä käytetään ja mille tahoille niitä välitetään. Lisäksi kerrotaan, miten kauan henkilötietoja säilytetään esimerkiksi sosiaalisen median tilin poistamisen jälkeen ja käyttäjän oikeuksista omiin henkilötietoihin.

Suosittelemme tutustumaan ainakin pintapuolisesti ehtoihin, jotta oikeasti tiedät, mihin kaikkeen sitoudut ottaessasi sovelluksen tai jonkin laitteen käyttöön. Käyttöehdot koskevat niin selaimella käytettäviä nettipalveluita, älylaitteiden sovelluksia kuin itse laitteita, esimerkiksi älytelkkaria. Oletko esimerkiksi selvittänyt, onko älytelevisiossasi kamera ja mikrofoni, mihin niitä käytetään ja kuinka ne saadaan otettua pois käytöstä?

1.6 Sijaintipalvelut

1.6.1 Kannattaako sovelluksen tai sivuston sallia sijainnin käyttö?

Hyvä perussääntö on, että kielletään sijainnin käytön aina, jos käytetty palvelu ei sitä välttämättä tarvitse. Jos käytetään esimerkiksi karttasovellusta tai karttapalvelua selaimen kautta, voidaan sijainnin käyttö sallia. Ostaessa verkkokaupasta pölynimuria, ei sitä välttämättä tarvitse antaa, vaan myymälä kannattaa valita itse listalta. Samoin kannattaa menetellä myös sovelluksien kanssa, esimerkiksi kuvankäsittelysovellukselle ei kannata antaa suostumusta.

Hyvä käytäntö on käyttää vaihtoehdon ”aina” sijaan ”käytettäessä”. Tällöin paikkatiedot annetaan sovellukselle vain silloin, kun sovellusta käytetään. Toimiessaan taustalla se ei niitä saa ja samalla myös paikallistamisen edellyttämä GPS/GNSS-tekniikka ei suotta kuluta laitteen akkua.

VAHTI / Kirves Juha (DVV)

1.12.2021

2 Huijaukset

2.1 Laskuhuijaukset

2.1.1 Sain omituiselta vaikuttavan laskun työantajani maksettavaksi. Sain perään vielä omituiselta kuulostavan puhelun henkilöltä, joka esittäytyi toimitusjohtajaksemme. Mistä on kyse?

Erityisesti kesälomakaudella yleistyvät laskuhuijaukset, joissa asian kiireellisyyteen ja kohdehenkilön korkeaan asemaan vedoten yritetään saada talousasioita lomakaudella hoitava henkilö maksamaan lasku sähköpostin lähettäjän osoittamalle tilille.

Näissä tapauksissa sähköpostin lähettäjän nimi on väärennetty tai sähköposti lähetetään kaapatusta sähköpostiosoitteesta. Huijausviesteissä usein vedotaan kiireeseen ja kerrotaan, että viestin vastaanottaja on ainoa, joka voi hoitaa tilanteen. Tilanne voidaan välttää varmistamalla laskun aitous luotettavalla tavalla eli henkilökohtaisella tapaamisella tai puhelinsoitolla tarkistettuun numeroon.

Huijausviestit noudattava usein samaa kaavaa. Aluksi tietoverkkorikolliset etsivät kohdeorganisaatiostaan taustatietoja esimerkiksi päätöksentekijöistä. Tämän jälkeen he lähettävät väärennetystä tai kaapatusta sähköpostiosoitteesta sähköpostin talousosastolle. Väärennetty sähköpostiosoite voi esimerkiksi poiketa oikeasta vain yhdellä kirjaimella tai merkillä. Viestien lähetys tapahtuu usein loma-aikaan. Viestit on kirjoitettu siten, että niissä vedotaan asian kiireellisyyteen ja kriittisyyteen organisaation toiminnalle. Lisäksi korostetaan sitä, että ainoastaan viestin vastaanottanut henkilö on kykenevä auttamaan tässä tilanteessa. Tätä viestiä saattaa seurata puhelinsoitto, jossa päätöksentekijäksi tekeytyvä rikollinen painostaa maksamaan kyseisen laskun. Viestin vastaanottanut henkilö saa ohjeistuksen, kuinka maksu tulee suorittaa. Maksu ohjataan tilille, joka on verkkorikollisten hallussa.

2.2 Verkkopankkitunnusten kalastelu

2.2.1 Minulle soitti pankkivirkailija, joka kysyi puhelimessa verkkopankkitunnuksiani, salasanaa ja avainlukulistan lukua. Mikä neuvoksi?

Pankit painottavat omassa viestinnässään, että eivät koskaan kysele asiakkaiden verkkopankkitunnuksia ja salasanoja sähköpostilla tai muulla viestinnällä. Älä koskaan luovuta tunnuksiasi näissä kyselyissä, koska kyseessä on varma huijaus. Myöskään viranomaiset eivät kysy pankkitunnuksiasi.

2.3 Tekstiviesti ja pikaviestin huijaukset

2.3.1 Minulle tuli viesti, jossa kerrotaan lähetyksen odottavan kuljettajalla palvelumaksua. En ole kuitenkaan tilannut mitään. Miten kannattaa toimia?

Erityisesti jos et ole tilannut mitään, kyseessä on todennäköisesti tietojen kalastelusta. Ilmiö tunnetaan myös nimellä Smishing. Huijauksissa yritetään saada käyttäjä luovuttamaan tietojaan esimerkiksi maksukortin numero tai pyydetään kirjautumaan sivustolle, missä kysytään pankkitunnuksia. Joissain tilanteessa voi olla tilanne, että oikealtakin taholta tulee viesti, jossa pyydetään esimerkiksi tullaamaan lähetys tai maksamaan käsittelymaksu. On hyvä aina tarkistaa sivuston linkki ja varmenne, kuten kohdassa **3.5 Varmenteen tarkistaminen** opastetaan. Vastaavia viestejä voi tulla myös pikaviestimien kautta.

2.4 Hakukonehuijaus

2.4.1 Kannattaako joka sivuille mennä ainoastaan hakukoneita käyttäen?

Ei kannata käyttää hakukonetta etenkään pankkien ja vastaavien palveluiden sivustoille, koska verkkorikolliset voivat ostaa tai muuten optimoida hakutulosten kärkeen omia huijaussivustoja. Käytä aina joko suoraan selaimen osoiteriville kirjoitettavaa osoitetta, joka kannattaa tallentaa kirjanmerkiksi tai jos palvelusta on saatavilla älylaitteelle oma sovellus (apps), hyödynnä sitä!

2.5 Huijauspuhelut

2.5.1 Miten voin vähentää huijauspuheluja?

Huijaus- ja muiden markkinointipuheluiden vähentämiseen voi auttaa oman numeron muuttaminen salaiseksi ja telemarkkinointieston aktivointi.

2.5.2 Sain puhelun oudosta ulkomaisesta numerosta, joka soi vain vähän aikaa. Kannattaako siihen soittaa?

Tällaisessa tilanteessa usein on kyseessä huijauksesta, joka toimii niin, että puhelinnumero on ohjattu maksulliseen numeroon. Näin numeroon soitettaessa tulee yllättävää lisäystä myös puhelinlaskulle. Tällainen huijaus toimii vain ulkomaisten numeroiden osalta, kotimaisiin numeroihin soitettaessa kerrotaan, millainen maksu siihen soitettaessa on odotettavissa.

2.5.3 Sain Microsoftin nimissä soitetun kuuluisan tukihuijauspuhelun – miten minun olisi pitänyt toimia?

Kun saat soiton ulkomailta, tuntemattomasta numerosta Suomesta, voi puhelun vastata. Jos puhelun taustalla kuuluu tyypillisiä call centerin eli puhelintukikeskuksen hälinäääniä ja esimerkiksi englannin kielistä puhetta taustalla, kannattaa olla erityisen varovainen. Voit sen jälkeen vastata puhelimeen pelkästään tervehtimällä ”Hei”, ”Haloo” ilman, että kertoo omaa edes etunimeä.

Jos vastaus tulee englanninkielellä ja normaalisti et koskaan hoida asioita puhelimessa englanniksi, suosittelemme lopettamaan puhelun ilman sen erikoisempia selityksiä tai anteeksipyyntöjä. Jos asia on aidosti tärkeä, henkilö ottaa yhteyttä uudelleen tai eri menetelmillä.

Jos kuitenkin alat kuuntelemaan puhelua ja siinä mainitaan ”Microsoft”, lopeta puhelu.

Näiden Microsoftin tukihuijauspuheluiden tarkoitukena on vakuuttaa uhri siitä, että hänen tietokoneessaan on ”hakkeri”, verkkorikollinen. Kun tämä on saatu aikaiseksi, soittaja – Microsoft – pystyy puhdistamaan tietokoneen. Tämä edellyttää etähallintaohjelman asentamista, esimerkiksi AnyDesk, TeamViewer tai RemoteDesk-nimisen ohjelman. Älä koskaan anna kenenkään asentaa omaan vapaa-ajan tai työkäyttöön tarkoitettuun tietokoneeseen etähallintaohjelmaa, ellet ole itse asiasta kyseisen IT-tuen kanssa sopinut ja tiedä sekä tunnista 100% yhteyttä muodostavan tahon ja henkilön.

Tällainen verkkorikollinen saatuaan tietokoneen haltuun, kaivaa tietokoneelta kaikki mahdolliset tiedot, joita he voivat väärinkäyttää. Lisäksi verkkorikollinen yrittää kalastella pankkikortti, luottokortti, pankkiyhteystietoja ja mikäli saa sellaisia haltuun, tyhjentää pankkitilit ja käyttää luottokorteissa käytettävissä olevan luottorajan sen maksimiin.

Eräs uudempi tapa saada nämä tiedot haltuun on pyytää muodollista, esimerkiksi 5 tai 10 euron palkkiota tietokoneen puhdistamisesta hakkereista. Jos tämän sallii, verkkorikollinen pystyy muuttamaan kyseisen summan 5 tai 10 euron sijaan esimerkiksi 500 tai 1000 euroksi.

2.6 Tietomurron tai identiteettivarkauden uhriksi joutuminen

2.6.1 Jäin identiteettivarkauden uhriksi. Mitä voin tehdä ja mistä voin saada apua?

Hengitä! Alla olevista linkeistä löytyy apua, jos tietosi ovat vuotaneet tai olet jäänyt identiteettivarkauden uhriksi tai muuten tarvitset lisätietoa.

https://www.riku.fi/toimi-nain-jos-tietojasi-on-vuodettu-verkkoon/

https://www.suomi.fi/oppaat/tietovuoto

3 Salasanat ja kirjautuminen

3.1 Salasanan hyvät ominaisuudet, esimerkiksi pituus

3.1.1 Miksi pitkä salasana on parempi, eikö tietokoneohjelma osaa yhtä lailla käydä kaikki sanat läpi, varsinkin, jos niissä on jokin logiikka. Onko esim. Kävelintänäänsenaatintorilla mitenkään vaikea tällaiselle ohjelmalle? Entä Kvelintnäänsnaatintrilla?

Pidemmän salasanan etu on se, että sen läpikäyminen vie tietokoneelta pidemmän aikaa. Jos salasanan murtaminen vie liikaa aikaa, niin sen purkamiseen ei verkkorikollisen kannata ryhtyä. Salasanoissa tosiaan pituus on suurin merkittävin tekijä ja toinen on se, että samaa salasanaa ei käytetä useammassa paikassa. Yksi tapa tehdä muistettavia ja pitkiä salasanoja on salalauseiden käyttö.

On myös totta, että saatetaan hyökätä niin, että kokeillaan eri sanoja peräkkäin. Tätä vastaan voidaan toimia niin, että käytetään kirjoitusvirheitä tai murresanoja, sopivassa määrin erikoismerkkejä.

On myös olemassa palveluja, joista voi tarkistaa, onko esimerkiksi vapaa-ajan palveluissa käyttämäsi sähköpostiosoitteen salasana ollut mukana jossain tietomurrossa vuotaneessa salasanalistassa. Tällainen palvelu on esimerkiksi https://haveibeenpwned.com. Voit palvelusta myös katsoa, onko jokin salasana vuotanut ylipäätään koskaan – esimerkiksi kun mietit uutta salasanaa käyttöönotettavaksi. Tämän voit testata osoitteessa https://haveibeenpwned.com/Passwords. Esimerkiksi salasana ”salasana saa ilmoituksen ”Oh no — pwned! This password has been seen 10 537 times before”. Ei todellakaan kannata käyttää.

Jos tunnuksesi löytyy palvelusta, kannattaa salasana käydä vaihtamassa, ellet sitä ole jo tehnyt mahdollisen tietovuodon jälkeen. Mikäli palvelu toimii eettisesti oikein ja avoimesti, se ilmoittaa käyttäjilleen tällaisista tilanteista ja pyytää vaihtamaan salasanat.

3.2 Salasananhallintaohjelma

3.2.1 Mikä on salasananhallinta ohjelma ja miksi sitä kannattaa käyttää?

Salasananhallintaohjelmaa voidaan käyttää salasanojen muodostamiseen ja säilyttämiseen, eräänlaisena salasanalompakkona. Salasananhallintaohjelmalle annetaan salasana, jota käytetään muihin salasanoihin pääsemiseen. Varjopuolena on se, että jos pääsalasana joutuu vääriin käsiin, joutuu myös kaikki muutkin salasanat. Salasananhallintaohjelma auttaa näin riittävän pitkien salasanojen muodostamisessa ja säilyttämisessä. Tämän ohella voit käyttää älylaitteesi tarjoamaa salasanojen tallennustoimintaa. Uusimmat laitteet pystyvät myös tarkistamaan, onko käyttämäsi salasana vuotanut tunnetuissa tietomurroissa ja varoittamaan niistä myös sinulle.

3.3 Kaksivaiheinen tunnistus

3.3.1 Mikä on kaksivaiheinen tunnistus?

Kaksi- tai muu monivaiheinen tunnistus tarkoittaa sitä, että käytetään jotain muuta vahvistamistapaa salasanan lisäksi. Esimerkiksi matkapuhelimeen voidaan lähettää tekstiviesti, joka sisältää esimerkiksi pin-koodin salasanan kirjoittamisen lisäksi, joka tulee myös syöttää palveluun kirjautuessa. Esimerkiksi pankit ottivat ensimmäisten toimialojen joukossa käyttöön kaksivaiheisen tunnistautumisen oman liiketoimintansa turvallisuuden varmistamisessa. Nyt kaikki vastuulliset toimijat tarjoavat sitä käyttäjilleen ja sinun tulisi sellainen ottaa käyttöön, jos tällainen on tarjolla.

3.4 Salasanan vaihtaminen

3.4.1 En pääse enää käyttämääni palveluun sisälle. Miten voin vaihtaa salasanani?

Useimmissa palveluissa on käytössä ”unohditko salasanasi” -toiminto. Käyttämällä sitä palvelu lähettää palveluun rekisteröimiseen käytettyyn sähköpostiosoitteeseen linkin, jonka kautta pääsee vaihtamaan salasanan.

Jos epäilet, että tilisi on joutunut vääriin käsiin, kannattaa salasanan vaihtaminen ehdottomasti tehdä mahdollisimman nopeasti, sillä esimerkiksi sosiaalisen median tiliä käyttämällä verkkorikollinen voi tehdä julkaisuja nimissäsi tai käyttää sähköpostia muiden palveluiden salasanojen vaihtamiseen.

Samalla kannattaa tarkastaa palvelusta, onko siellä tuntemattomia ”sessioita” eli avoimia yhteyksiä muilta laitteilta palveluun. Jos tuntemattomia yhteyksiä löytyy, ne kannattaa lopettaa ellei sitä tehdä automaattisesti salasananvaihdon yhteydestä.

3.5 Varmenteen tarkistaminen

3.5.1 Mistä tiedän, että sivusto, jolla vierailen ei ole todennäköisesti huijaussivusto ja tietoliikenne palveluun on salattu

Ennen kirjautumista kannattaa tarkistaa, että selaimen osoiterivissä on palvelun internet-osoitteen vieressä vasemmalla puolella lukon kuva ja osoitteessa https:// edessä, esimerkiksi https://dvv.fi/. Tosin esimerkiksi Google Chrome ei tuota etuliitettä nykyään näytä. HTTPS-

etuliite tarkoittaa sitä, että yhteys palveluun on selaimesta saakka suojattu. Suojan muodostamiseen tarvitaan varmenne, jota voi tarkastella lukon kuvaa klikkaamalla.

Varmenteen tiedot saa esille lukon kuvaa klikkaamalla. Asiallinen varmenne sisältää myös varmenteen kohteen tiedot ja varmenteen voimassaoloajan. Näin kannattaa varmistaa, että onko varmenne myönnetty sille palvelulle, jota oletat käyttäväsi. Huomaa, että osa myös verkkorikollisten palveluista on saattanut hankkia käyttöönsä toimivan varmenteen, mutta eri sivustolle!

4 Laitteiden turvallinen käyttö

4.1 Varmuuskopiointi

4.1.1 Miten kannattaa varmuuskopioida omien päätelaiteiden tiedot?

Varmuuskopiointia voi toteuttaa monella tapaa. Paras tapa riippuu teknisestä osaamisesta ja riskitasosta, jonka olet päättänyt hyväksyä. Useissa käyttöjärjestelmissä on nykyään ominaisuus, jolla voidaan varmuuskopioida päätelaitteen kaikki tiedot. Monet päätelaitteet voidaan varmuuskopioida esimerkiksi pilvipalveluihin. Pilvipalveluun tehtävässä varmuuskopiossa on se hyöty, että varmuuskopio on saatavilla kaikkiin laitteisiin. Lisäksi pilvipalvelu ei vaadi sen käyttäjältä laiteinvestointeja. Mahdolliset haitat ja epävarmuus liittyy siihen, milloin palvelun tiedot poistetaan ja miten. Etenkin työnantajan käyttöösi antamien laitteiden varmuuskopioinnissa tulee noudattaa varmuuskopioinnista annettuja ohjeita.

Tiedot voidaan myös varmuuskopioida ulkoiselle USB-levylle. Usein varjopuolena on se, että tiedot tallennetaan siltä laitteelta, johon levy on kiinnitetty. Toisaalta etuna on se, että varmuuskopioon on hankala kenenkään ulkopuolisen päästä käsiksi, ellei pääse käsiksi itse levyyn. Kannattaa myös huomioida, että työnantajan tiedot varmuuskopioidaan ainoastaan vain työnantajalta saatuun USB-levyyn. Tuntemattomat USB-laitteet voivat olla turvallisuusriski, sillä niihin voi olla asennettu haittaohjelmia. Tästä syystä yleensä kannattaa ainoastaan käyttää sellaisia USB-laitteita, joiden alkuperästä voit olla varma. Mikäli usb-laite tai laitteesi käyttöjärjestelmä mahdollistaa usb-levyn salauksen, se kannattaa ottaa käyttöön.

On myös olemassa verkkoon liitettäviä ulkoisia kiintolevyjä, joihin voi varmuuskopioida esimerkiksi samassa langattomassa verkossa olevia laitteita. Sellaisen käyttöönottaminen voi vaatia hieman harrastuneisuutta laitteen turvallisuuden varmistamiseksi.

4.2 Haittaohjelmien torjunta

4.2.1 Onko virustorjunta tarpeeton?

Virustorjunta – tai nykyään haittaohjelmien torjuntaohjelma ei ole menettänyt merkitystä, vaan se on muuttanut muotoaan. Sovelluksiin on tullut enemmän ominaisuuksia huijausten ja hyökkäysten tunnistamiseen. Osin haittaohjelmien torjuntaohjelmien kehittymisen vuoksi huijaukset ovatkin keskittyneet sosiaalisten keinojen hyväksikäyttämiseen suojauksien kiertämiseen. Osaatko itse tarkistaa, että haittaohjelmien tarkistusohjelma on asennettu ja ajan tasalla? Usein virustorjuntaohjelman lisenssi sallii ohjelmiston asennuksen useampaan laitteeseen, joten se kannattaa asentaa sekä työasemaan ja että mobiliilaitteeseen. Tai niin moneen laitteeseen, kuin lisenssit sallivat esimerkiksi perheen laitteisiin

4.3 Langattomien verkkojen käyttö

4.3.1 Mitä tulee tehdä ottaessa langatonta verkkoa käyttöön?

Kotona olevien langattoman reitittimen oletussalasanat ja langattoman verkon salasanat kannattaa vaihtaa. Langattoman verkon asetuksissa WPA2-PSK / AES on hyvä lähtökohta verkon salaukselle. Jos reititin ja kaikki siihen liitettävät langattoman verkon laitteet tukevat uudempaa WPA3-standardia, niin sitä kannattaa käyttää. Langattoman verkon suorituskykyä parantaa 5 GHz radiotaajuuden käyttö, jossa esim. naapureiden langattomien tukiasemien signaalit vähemmän häiritsevät oman verkon toimintaa verrattuna 2,4 GHz langattomaan verkkoon. Muista, että voit aina varalla käyttää oman älylaitteesi, esimerkiksi älypuhelimen tarjoamaa wifi-hotspot-toiminnallisuutta – siis jakaa vaikka älypuhelimesi internet wlan-tukiasemana.

5 Henkilökohtainen varautuminen

Kansalaisen tulisi varautua yhteiskunnan häiriötilanteeseen, kuten tietoliikenneyhteyksien, lämmön- tai sähkönjakelun katkokseen. Lisää tietoa löytyy täältä: https://72tuntia.fi/

5.1 Ruoka

5.1.1 Mitkä ovat hyväksi havaittuja varautumisruokia?

Liha- ja kalasäilykkeet, nötkötti, suklaa, näkkileipä, virvoitusjuomat.

Yleensäkin ruoka, joka ei vaadi kypsennystä. Varautumista voi tukea myös hankkimalla retki- tai risukeittimen, jonka avulla ruokaa voi valmistaa pihalla.

5.2 Lämpö

5.2.1 Jos lämmön jakelu katkeaa, mitkä ovat vinkkinne kerrostaloasujalle?

Lisää vaatteita kannattaa pukea ylle ja kerätä kaikki ihmiset samaan huoneeseen. Teltan pystyttämistä sisälle voi olla myös hyötyä ja ikkunoiden ja ovien tiivistämisestä matoilla. Voidaan myös hakeutua tilaan, jossa on lämmönlähde, kuten tulisija.

6 Sosiaalinen media

6.1.1 Millä keinoilla digijalanjälkeä voidaan hallita tai jopa vähentää?

Digijalanjäljen vähentämisen aloittamiseksi tulee määrittää oma riskitaso eli rooli, miten haluamme näkyä sosiaalisessa mediassa. Haluammeko jakaa kaiken elämästämme sosiaaliseen mediaan vai ylläpidämmekö siellä minkälaista kuvaa itsestämme. Internetiin laitettu tieto ei välttämättä koskaan sieltä poistu täysin. Sosiaalisen median palveluista voi kuitenkin poistaa vanhoja päivityksiä. Myös selaimen ja palvelujen hakuhistoriaa ja dataa voi aika ajoin poistaa.

Internetissä liikkuen omaa digijalanjälkeä voidaan pienentää myös käyttämällä VPN-yhteyttä, käyttäen esimerkiksi eri selainta tai jopa päätelaitetta sosiaalisen median palveluihin kuin laskujen maksamiseen. Myös sosiaalisessa mediassa on mahdollista tehdä eri profiilit työkäyttöön ja vapaa-ajalle. Samoin saattaa olla mielekästä luoda vapaa-ajalle useampi sähköpostiprofiili, jota käyttää eri palveluihin ja sovelluksiin kirjautumiseen.