DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvan Usein Kysytyt Kysymykset (UKK) – Digiturvatunti henkilöstölle

VAHTI-hyvät käytännöt tukimateriaali

Versio: Digiturvatunti henkilöstölle – meille kaikille - 15.2.2024

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

Sisällysluettelo

Digiturvan Usein Kysytyt Kysymykset (UKK) – Digiturvatunti henkilöstölle

1 Johdanto

Tämä tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn ja toiminnan edistämisesi. Tukimateriaali pohjautuu julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) asettamien VAHTI-työryhmien asiantuntijoiden kokoamiin riskienhallinnan, toiminnan jatkuvuuden ja valmiuden, tietoturvallisuuden ja tietosuojan hyviin käytäntöihin. Hyvien käytäntöjen mukaisesti toimimalla edistämme samalla kyberturvallisuuden toteutumista. Tämä tukimateriaali koostuu meille esitetyistä kysymyksistä ja niiden vastauksista.

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme riittävästi parannus ja korjausehdotuksia, julkaisemme tästä päivitetyn version. Lähetä palautetta sähköpostitse digiturva@dvv.fi, kirjoita viestin otsikoksi Digiturva UKK. Käytämme tätä materiaalia apuna 15.2.2024 alkaen järjestettävissä ”Digiturvatunti henkilöstölle – meille kaikille” -webinaareissa. Kiitos kaikista kysymyksistä! Jos olet toimittanut meille kysymyksen, on myös mahdollista, että emme vastaa siihen sellaisenaan, vaan koostamme useista saman aiheisista kysymyksistä yhden kootun vastauksen. Digiturvatunti-webinaarin kysymykset ja vastaukset lisätään tämän materiaalin lopussa olevaan omaan osioon.

Voit lähettää kysymyksen myös tämän Menti-kyselyn avulla:
https://www.menti.com/alfspnxua3cu

Mikäli organisaatio käyttää tässä materiaalissa olevia kysymyksiä ja vastauksia omassa toiminnassaan, jokainen organisaatio ja asiantuntija vastaa itse siitä, että vastaus sovitetaan tarkemmin organisaation omaan toimialaan ja sitä koskevaan lainsäädäntöön sekä että se tukee organisaation omia linjauksia ja ohjeistuksia.

Kysymykset on jaoteltu digitaalisen turvallisuuden viitekehyksen viiden osa-alueen mukaisesti. Materiaalin loppuun kootaan erikseen Digiturvatunti-webinaarissa julkaistavat kysymykset ja vastaukset.

Tulemme lisäämään tähän materiaalin maaliskuun 2024 aikana aikaisemmin laaditun Usein Kysytyt Kysymykset-asiakirjan vastaukset, kun tarkistamme ja varmistamme niiden ajantasaisuuden. Pyrimme saamaan sen julkaistua maaliskuun Digiturvatunnin yhteydessä.

2 ”Digiturvatunti henkilöstölle – meille kaikille”-webinaarin yhteydessä esitettyjä kysymyksiä

Vastaamme tässä luvussa DVV:n yhteistyössä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen sekä muiden viranomaisten ja toimijiden kanssa tuotettussa Digiturvatunti henkilöstölle-webinaarissa esitettyihin kysymyksiin.

Näitä voi toimittaa meille
- lähettämällä oheisen Menti-kyselyn kautta
https://www.menti.com/aln7xp7fmsbk

- esittämällä kysymyksen https://live.mediaserver.fi/dvv/digiturva webinaarin lähetyssivuston Chat-toiminnon kautta

Emme voi valitettavasti luvata vastausta kaikkiin kysymyksiin, samoin osaan kysymyksistä saattaa olla jo vastaus tässä asiakirjassa sekä erityisesti lainsäädäntöön tai sen tulkintaan liittyviä kysymyksiä kannattaa esittää oman organisaation tukiorganisaatiolle.

2.1 Digiturvatunti – 15.2.2024

2.1.1 Onko tiktok niin vaarallinen, kuin siitä on kirjoitettu? Onko mitään keinoa käyttää sitä edes vähän turvallisemmin?

Tiivistys: käyttöön liittyy riskejä – jos on pakko käyttää, älä asenna apps-sovellusta vaan käytä nettiselainta ilman palveluun kirjatumista. Työtehtävissä usein suositellaan on tätä varten hankitun / dedikoidun laitteen hankintaa.

TikTok-palvelun turvallisuudesta on paljon käyty keskustelua – tämän osalta kannattaa noudattaa voimassa olevaa oman organisaation ohjeistusta.

Muun muassa Suomessa Suojelupoliisi on nostanut katsauksissaan esille sovellukseen liittyvät riskit – yksi heidän suositus on: ” – Jos Tiktokia haluaa käyttää tai tarvitsee työssään, sitä varten kannattaa hankkia erillinen laite.”

Vapaa-ajan osalta on myös suositeltavaa käyttää sen oman sovelluksen (Apps) sijaan **nettiselaimella**, joka parantaa jonkin verran sen turvallisuutta. Muista tällöin:

- Älä kirjaudu palveluun
- Tyhjennä selaimen eväste- ja muu syntyneet tiedot käytön jälkeen
- Älä hyväksy mitään sovelluksen suostumuksia, joita se pyytää sinulta
- Älä käytä tätä selainta myöskään kirjautuneena TikTokin-tilin käyttöön, koska tällöin TikTok pystyy hyödyntämään tietojasi evästeiden avulla sinun profilointiin.

- Tällöin voisi olla järkevää, että käytät tätä käyttöä varten erillistä sitä varten asentamaasi nettiselainta.

Suosittelemme tutustumaan myös tähän YLEn tekemään testiin ”Masentava sovellus”.

Loimme 13-vuotiaan Ellan – Tiktok tarjosi hänelle sisältöä itsemurhasta ja kalorien laskemisesta | MOT | Yle

2.1.2 Viime vuonna paljon varoiteltiin kotireitittimien turvattomuudesta. Onko tietoa, kuinka paljon kansalaiset ovat niitä uusineet?

Tiivistys: taustalla SUPOn suositus tarkistaa kotireitittimien turvallisuus ja asetukset ja tarvittaessa päivittää laite uudempaan. Käsittääksemme näitä on ahkerasti hankittu mm. Black Friday ja muista alennusmyynneistä. Valitettavasti näitä turvattomia laitteita vielä löytyy ja verkkorikolliset ja haktivistit käyttävät niitä mm. palvelunestohyökkäyksissä apunaan Suomesta.

Kodin digilaitteissa kannattaa varmistaa:

- laitteen kirjautumiseen liittyvän tunnuksen salasana on vaihdettu, mielellään salalauseeksi, joka kannattaa tallettaa kotiin vaikkka paperilla turvalliseen paikkaan talteen

- laitteen ohjelmisto on päivitetty tuoreimpaan saatavilla olevaan versioon. Jos uusia versioita ei ole saatavilla ja jos tiedetään, että laittessa on tietoturvahaavoittuvuuksia, suositellaan vahvasti uuden, turvallisemman laitteen hankkimista.

- jos laite mahdollistaa niin sanotun etähallinnan avoimesti kaikkialta internet-verkosta, kannattaa miettiä, onko se kriittinen ominaisuus, jonka voisi ottaa pois päältä. Tällöin kaikki laitteen hallinta pitäisi tehdä kotiverkosta.

Lue lisää näistä Kyberturvallisuuskeskuksen ohjeista:

Tietoturvaohjeita kotiin ja työpaikalle | Kyberturvallisuuskeskus

LAITTEIDEN SUOJAAMINEN
Turvaa tietosi: Vinkkejä puhelimen tietoturvalliseen käyttöön
Kotiverkon ja reitittimen tietoturva
Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen

2.1.3 Voiko nämä lunnasrikolliset iskeä kotiini ja kotikoneeseeni? En ole näistä juurikaan lukenut, koskeeko vain yrityksiä?

Tiivistys: alun perin ensimmäiset lunnashaittaohjelmahyökkäykset tehtiin kotikoneisiin, merkittävä kasvu tapahtui 2010-luvun alkupuolella. Koska tätä kautta rikolliset eivät saa kovinkaan merkittävää summaa rahaa verrattuna siihen käytettävä työmäärä, nämä ovat nykyisin erittäin harvinaisia. Rikolliset keskittyvät organisaatioihin, ja näiden vakavien hyökkäysten määrä on ollut myös Suomessa merkittävässä nousussa.

Organisaatioiden yksi keskeinen uhka vuonna 2024 on siihen kohdistuvat ammattimaisten rikollisjärjestöjen toimesta suoritetut lunnashaittaohjelmahyökkäykset.

Lue lisää näistä Kyberturvallisuuskeskuksen ohjeista:

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

OHJEITA ORGANISAATION JOHDOLLE

Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje
Kyberturvallisuus ja yrityksen hallituksen vastuu -opas
Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille

2.1.4 Miksi rikolliset saavat käyttöönsä näitä suomalaisia osoitteita eli .fi?

Tiivistys: Suomessa Liikenne- ja viestintävirasto Traficom vastaa suomalaisten .fi-domain-osoitteiden myöntämisestä ja hallinnasta. He eivät voi estää tällaisen osoitteen käyttöä, ennen kuin se syyllistyy esimerkiksi rikolliseen toimintaan.

Tämä on myös yksi keskeinen syy, miksi meidän jokaisen kansalaisen tulisi ilmoittaa kaikista digimaailmassa eteen tulevista uhista. Vaikka taloudellinen menetys voisi olla olematon tai et ole menettänt rahaa tai tietojasi lainkaan, valitettavasti joku toinen henkilö on voinut menettää merkittäviä summia rahaa ja/tai oman identiteettinsä.

Tämän takia kannattaa matalalla kynnyksellä ilmoittaa tietoturvaloukkauksesta tai sen epäilystä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukseen heidän nettilomakkeellansa:

https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

sekä tehdä rikosilmoitus – itse asiassa sinun ei tarvitse tietää tai arvioida, onko kyseessä millainen rikos, vaan viranomainen (Poliisi) tekee tämän arvioinnin:

https://poliisi.fi/tee-rikosilmoitus

Lisätietoa yleisimmistä verkkorikoksista Poliisin sivuilla:
https://poliisi.fi/petosrikokset

2.1.5 Milloin me päästään salasanoista eroon ja mikä tällainen tekniikka voisi olla? Voiko salasanojen hallintaohjelmiin luottaa, eikös niissä ole ollut murtoja??Kertaatteko viisi tärkeintä vinkkiä salasanoihin liittyen?

Tiivistys: Ei välttämättä vuosi(kymmeni)in, vaikka osa palveluista on mahdollistanut ns. salasanattoman palveluiden ja laitteiden käyttämisen. Yhä useampi kirjautuu älylaitteelle esimerkiksi kasvojen tunnistuksella tai visuaalisella koodilla.

2.1.6 Kertaatteko viisi tärkeintä vinkkiä salasanoihin liittyen?

Viiden sijaan nostamme esille seitsemän muistettavaa seikkaa salasanojen hallinnan suhteen ja yhden vinkin sähköpostiosoitteiden hallinnan osalta.

1. Jokainen salasana pitää olla ainutkertainen … eikä sellaista tehdä numeroimalla uusi lisäämällä olemassa olevan perään 1,2,3 jne.

2. Salasanan sijaan käytä >20 merkin mittaista salalausetta, esmerkiksi helmiKuukuukusista#kylminkö??

3. Älä luovuta salasanoja kenellekään. Organisaation IT-tuki ei koskaan tarvitse tai saa pyytää salasanaasi, kuten myöskään pankki tai viranomainen.

4. Ota käyttöön kaksivaiheinen tunnistus kaikissa niissä palveluissa, joissa sinulla on tärkeää tietoa ja joita käytät säännöllisesti. Koti- ja vapaa-ajan käytössä suosittelemme, että sinulla on ns. varalaite, älypuhelin tai tabletti. Jos ainoa käyttämäsi laite hajoaa, häviää tai varastetaan, esimerkiksi pankki- ja muiden tunnistautumisratkaisujen palauttaminen uudelle laitteelle voi olla työlästä.

5. Tärkeimpiä salasanoja kannattaisi vaihtaa, esimerkiksi vuosittain. Tällä estetään se, että jos joku on kaikista varotoimenpiteistä huolimatta saanut selville salasanasi ja käyttää palvelua, esimerkiksi sähköpostiasi, tällainen luvaton ja huomaamaton väärinkäyttö loppuu salasanan vaihtuessa.

6. Voit tallettaa salasanat kirjallisesti / sähköisestä talteen, mutta varmista niiden turvallinen säilyttäminen huolella. Mieti, jos tämä lappusi tai mikäli tallennat sen tiedostoon älylaitteelle, päätyisi julkisuuteen, saako joku ulkopuolinen selville, mikä salasana on tarkoitettu mihin palveluun ja onko niitä sekoitettu joillakin lisämerkeillä?

7. Ethän käytä työsähköpostia vapaa-ajan asioiden hoitamiseen? Oletko harkinnut useamman sähköpostiosoitteen käyttöä? Älä koskaan käytä työpaikan sähköpostiosoitetta minkään yksityisasian hoitamiseen. Muista, myös työpaikat ja työpaikan sähköpostiosoitteet vaihtuvat! Mieti, kannattaisiko sinulla olla esimerkiksi 2-3 eri sähköpostiosoitetta:

1. Kriittisiin palveluihin ja laitteisiin kirjautumiseen käytettävä sähköposti, myös viranomaisasiointiin. Kaikista tärkein sähköpostiosoite ja siihen liittyvä salasana.

2. Toinen sähköpostiosoite, esimerkiksi ei niin tärkeisiin palveluihin ja laitteisiin kirjautumiseen.

3. Kolmas sähköpostiosoite. Tätä voi käyttää kaikkiin muihin vapaa-ajan palveluihin kirjautumiseen, myös etukäteen hieman oudommilta tai turvattomammalta vaikuttaviin palveluihin.