

[äänite alkaa]

Tuija Kuusisto [00:00:00]: Hei! Olen Tuija Kuusisto. Toimin valtiovarainministeriössä tietohallintoneuvoksena.

Kimmo Rousku [00:00:06]: Minä olen vastaavasti Kimmo Rousku. Toimin digi- ja väestötietovirastossa eli DVV:ssä VAHTI-pääsihteerinä. Tuijan kanssa me molemmat tahdomme edistää julkisen hallinnon digiturvallisuutta ja sitä kautta luottamusta yhteiskunnassa ja Suomen kilpailukykyä.

Tuija Kuusisto [00:00:22]: Tässä Digiturvakompassi-sarjassa tapaamme julkisessa hallinnossa vaikuttavia henkilöitä. Mitä on turvallisuus digimaailmassa? Mihin suuntaan digiturvaa pitäisi kehittää. Tässä joitakin kysymyksiä yhdessä pohdittaviksi.

Kimmo Rousku [00:00:36]: Ja, ai että, siis mikä ihmeen digiturva? Digitaalisen turvallisuuden avulla huolehditaan riskinhallinnasta sekä toiminnan jatkuvuudesta, tietoturvasta ja tietosuojasta sekä edistetään samalla kyberturvallisuutta. Digiturva huolehtii meidän kaikkien tarvitsemien digipalveluiden toimivuudesta ja isona kokonaisuutena myös koko Suomen kyvystä selvittää erilaisista digimaailman häiriöistä ja hyökkäyksistä.

Tuija Kuusisto [00:01:04]: Tässä Digiturvakompassi-podcastin jaksossa meidän vieraamme tulevat työ- ja elinkeinoministeriöstä. He ovat johtaja Mika Nordman ja teollisuusneuvos Sirpa Alitalo. Meillä on nyt ensimmäinen podcast, jossa on kaksi vierasta. Katsotaan, miten keskustelu nelistään sujuu, mutta ainakin voi sanoa, että nyt sitten tämä sukupuolijaottelu on ihan tasapainossa. On kaksi miestä ja kaksi naista, niin siltä osin ainakin asia on hyvin kunnossa. Hyvää huomenta, Mika ja Sirpa, ja tervetuloa tähän meidän podcastiimme.

Puhuja 1 [00:01:42]: Oikein hyvää huomenta ja kiitos kutsusta. Tosi hieno päästä mukaan.

Sirpa Alitalo [00:01:47]: Huomenta myös minun puolestani ja kiitos kutsusta. Oli tosi mukavaa, että päästiin Mikan kanssa yhdessä tähän ohjelmaan.

Kimmo Rousku [00:01:57]: Huomenta kaikille vielä myös täältä Kimmonkin puolesta ja tervetuloa.

[00:02:13 taustamusiikki päättyy]

Tuija Kuusisto [00:02:13]: Digitaalinen turvallisuus tai usein sanotaan myös kyberturvallisuus, niin se hän nyt on tässä viime aikoina noussut myös kansainvälisen politiikan areenalle ja yritys- ja valtionjohtajienkin kansainvälisten huipputapaamisten agendalle. Kyberturvallisuudesta ja erityisesti tietenkin kyberhyökkäyksistä ja tietoturvaloukkauksista ja niiden vastatoimista ja vähän näistä hyökkääjistäkin keskustellaan aika vilkkaasti sekä täällä kyberalan asiantuntijoiden kesken että tietenkin mediassa, ja niin kuin mainittiin, myös poliittisessa ihan korkean tason päätöksenteossa täällä Euroopan unionin sisällä ja kaikessa kansainvälisessä yhteistyössä. Millä tavalla tämä kyberturvallisuuden, digitaalisen turvallisuuden, näiden hyökkäysten ja hyökkääjien, niistä käytävän keskustelun määrän kasvu, miten se mahdollisesti näkyy siellä teillä työ- ja elinkeinoministeriössä?

Sirpa Alitalo [00:03:11]: No kyllähän se näkyy. Kyberturvallisuushyökkäykset ja tämä varautumisteema ovat tosiaan laajasti esillä kansallisesti ja kansainvälisesti ja totta kai myös TEM on tässä hereillä. TEM:hän on tällainen kansalaisten ja yritysten toimintaympäristön rakentaja. Nykymaailmassa elinkeino- ja työelämä sekä yksittäisten kansalaisten ja yritysten elämä varsin vahvasti nojaa näihin digitaalisiin palveluihin ja sitä kautta kohdataan entistä enemmän näitä digitaaliseen toimintaympäristöön liittyviä riskejä. Kyber kulkee aina tässä digitalisaation vastinparina. Silloin kun pohditaan toimintamalleja, joilla pystytään selviytymään tässä uudistuvassa ympäristössä, niin kyllä siinä tarvitaan yritysten ja yhteiskunnan osalta panostamista osaamiseen, resursseihin, työkaluihin ja taas kansalaisten puolella huolellisuus ja tietoisuus tästä riskimaailmasta ovat keskeisiä pointteja. Niin kuin Tuija tuossa totesit, niin kyllähän esimerkiksi EU-tasolla aika vahvasti on viime vuosien aikana noussut keskusteluun tämä kyberteema, ja kyllä se näyttäytyy myös ministeriön osalta niin, että olemme mukana useissa kansain-

välisissä verkostoissa ja työryhmissä kyberteeman ympärillä. Myöskin näissä puheenjohtajuuskauden pääteemoissa kybe-asiat kyllä ovat ihan hyvässä asemassa. Esimerkiksi tällä hetkellä Slovenian puheenjohtajuuskauden yksi painopisteteema on kyberturvallisuuteen liittyvä eteneminen. Tokihan sitten tietysti TEM:in päässä se näyttäytyy myös tuossa meidän virastokentässämme, että isompia ulottuvuuksia on esimerkiksi huoltovarmuuskeskuksen digiturvallisuusohjelma, jossa visioidaan yhteiskuntaa, jonka kriittiset toiminnot kestävät kyberhäiriöitä ja siihen on budjetoitu myöskin rahoitusta niin, että pystyisimme käynnistämään projekteja, jotka edistävät yhteiskunnan digitaalista turvallisuutta. Samoin Business Finlandin puolella on tällainen Digital Trust -ohjelma, joka tarjoaa välineitä uudenlaisten uhkien ratkaisuihin. Mutta kyllä se on pikku hiljaa, ikään kuin, sitä mukaa kun palvelujen digitalisaatio edistyy, niin siinä rinnalla kyberteema nousee kyllä vahvasti sekä ministeriön sisällä että virastokentässä. Vähän jokaisen organisaation pöydältä löytyy ulottuvuuksia tähän kyberteemaan.

Kimmo Rousku [00:06:18]: Tässä hienosti nostitkin esille juuri sekä huoltovarmuuskeskuksen, Business Finlandin roolia ja kyllä täytyy olla todella tyytyväinen, että meillä on tällaiset toimijat, jotka pystyvät nimenomaan tukemaan ja rahoittamaan tätä meidän digitaalisen yhteiskuntamme turvallisuuden kehittymistä. Sitten, Mika, toimit digitaalisten palvelujen johtajana työ- ja elinkeinoministeriössä. Mitä digitaaliseen turvallisuuteen liittyviä asioita sinun työpöydälläsi liikkuu ja vastaavasti Sirpa, tahtoisitko tuoda vielä jotakin muuta esille digiturvatehtäviin liittyen?

Mika Nordman [00:06:54]: Joo, tässä digitaalisten palveluiden johtajan roolissa aika monipuolisesti on päässyt perehtymään näihin kyberturvallisuus-, tietoturvasasioihin. Ehkä akuutteja asioita, joita juuri esimerkiksi tällä viikolla, on kuultu muun muassa Supon kansallisen turvallisuuden katsauksen perusteella siitä, mikä meidän tilanteemme on tällä hetkellä ja kun katsomme siitä tulevaisuuteen päin. Ehkä tämä näkyy sillä tavalla, että mekin olemme ottaneet tietoturvapoliittikkamme- ja vastuamme pöydälle ja niistä on käyty keskustelua ihan viime päivinä ja haluamme tällä varmistaa olemme sitten TEM:issä oikeassa asennossa, jos jotain tapahtuisi. Tällaiset vastuasiat on yksi keskeinen elementti tällä hetkellä ja sitten tietenkin se, että TEM:issä ehkä aikasempiin vuosiin verrattuna meillä tulosohjaukseen liittyvät asiat, erityisesti digikulma on noussut esille. Digikulmaa kun edistetään, niin tieto- ja kyberturva on yksi keskeinen elementti näissä. Itse olen tulosohjaukseen liittyvissä asioissa hyvinkin mukana. Tulosohjaus tarkoittaa siis sitä, että meillä on TEM:in hallinnon alan toimijat, joita ministeriö tulosohjaa, mutta myös ministeriön sisällä käydään tietynlaisia tuloskeskusteluita osastojen kesken, ja näissä kaikissa kyberturva jollain tavalla näkyy. Ehkä yksi keskeinen vielä asia, mitä on pohdittu asiantuntijoiden kesken on se, että jos puhutaan kyber- ja tietoturvan tilannekuvasta, niin miten se muodostuu. Meikin ministeriössä nautimme valtioneuvoston kanslian tuottamia digipalveluita ja jos mieltii sitä

palveluketjua, että valtioneuvoston kanslia hankkii palvelut Valtorilta ja Valtori hankkii alihankkijalta ja ehkä alihankkijan alihankkijalta. Siitä muodostuu aika pitkä putki ja jos jotain poikkeamaa sattuu, niin miten tavallaan sitten tilannekuva muodostuu meille ministeriön johtoon päin ja minkä tyyppisissä tilanteissa sitten esimerkiksi digijohtajana vaikka kansliapäällikköä informoin asioista, että tämän tyyppisiä asioita. Ehkä yksi keskeinen asia on myös meidän isot hankkeemme. Kun rakennamme tällaisia turvallisia, luotettavia, digitaalisia palveluita kansalaisille ja viranomaisille ja muille sidosryhmille, että miten tietoturva-, kyberturva-asiat varmasti näkyvät näitten palveluitten rakentamisessa. Olen päässyt mukaan tällaisiin keskusteluihin, ja kuka hyväksyy tietoturva-vaatimukset ja mille tasolle ne asetetaan, ja tämän tyyppisiä asioita.

Sirpa Alitalo [00:09:43]: Minä voisin tuosta ehkä jatkaa oman tehtäväalueen näkökulmasta. Keskeisenä minulla ehkä näkyy hallinnon alan digitalisaation tilannekuvan hahmottaminen. Me olemme vuodesta 2018 lähtien ottaneet käyttöön mallin digikyvykkyyden mittaamiseen meidän virastokentässämme. Yhtenä osa-alueena siellä näkyy myös kyberin tilannekuva. Nyt tänäkin vuonna tehdyissä arvioinneissa näyttää siltä, että kyllä virastojen johto on varsin hyvin hereillä tämän kyberin edellyttämistä toimista. Näkymä siitä, että ollaan hereillä, tunnistetaan uhkat ja tiedetään, että virastoissa on paljon mielenkiintoista, kiinnostavaa sisältöä, että varmaankin tällaisiin mahdollisiin häiriöihin on tarpeen varautua. Ehkä toistaiseksi tulokset ovat osoittaneet varsin hyvää hereillä oloa kyberuhkien näkökulman osalta, mutta tilannehan muuttuu koko ajan ja uusia haasteita nousee esiin eli siinä mielessä tällainen jatkuva hereillä olo myöskin virastojen johdon työpöydällä on tarpeen.

Tuija Kuusisto [00:11:14]: Viime aikoina on havaittu, että erilaiset valeuutiset, disinformaatio siis ja muu tällainen tiedon tahallinen vääristely ja toisaalta sitten myös viranomaisten hyvin vahva pyrkimys fakta-perustaiseen viestintään nähdään ehkä osittain tällaisena vastakkainasetteluna ja se herättää aika voimakkaitakin näkemyksiä. Mitenkäs sitten työ- ja elinkeinoministeriön hallinnon alalla, voisitko, Sirpa, kertoa mahdollisesti jotakin käytännön esimerkkejä siitä, miten teillä mahdollisesti näkyy disinformaatio tai yritysten ja yhteisöjen tai viranomaisten tahalliseen vahingoittamiseen pyrkivä viestintä tai muu tällainen negatiivinen tietojen käyttö?

Sirpa Alitalo [00:11:58]: Joo, valitettavasti tällainen disinformaation jakaminen on lisääntynyt kyllä viime vuosina vähän samalla tavalla kuin muukin epäasiallinen puhe ja esiintyminen julkisuudessa. Yhtenä esimerkkinä viimeaikaisista huolista on ehkä virkamiehiin kohdistunut maalittaminen, että ministeriös-

sähän tehdään laaja-alaista lainvalmistelua ja jotkut erityisteemat tuntuvat herkkyytasoltaan olevan sellaisia, että ne ylittävät tämän disinformaation jakamisen kynnyksen ja kohdistuvat vaikka yksittäisiin virkamiehiin. Varmaan myös tänä aikana korona on ilmeisesti vähän lisännyt tällaista piirrettä, että myös muuhun kuin koronaan liittyvänä tällainen maalittaminen on lisääntynyt ja se on kyllä yksi esimerkki tästä disinformaatiosta. Toki on montaa muutakin, mutta tämä on ehkä sellainen, joka on näiden viimeisimpien aikojen esimerkki tästä disinformaatiosta.

Kimmo Rousku [00:13:05]: Eri puolella maailmaa, myös osin Suomessakin, valitettavasti, on tapahtunut selkeä muutos onnistuneiden kyberhyökkäysten määrässä ja vaikutuksessa. Viime aikoina pinnalla ovat olleet erityisesti kiristyshaittaohjelmat ja niiden kautta rikollisten saama taloudellinen hyöty. Osin Suojelupoliisi tuossa aikaisemmin mainitussa katsauksessaan myös toi näitäkin uhkia hyvin esille. Mitä vaikutuksia, Mika, kyberturvallisuus tilanteen globaalilla pahenemisella on ollut työ- ja elinkeinoministeriössä tai teidän hallinnon alallanne?

Mika Nordman [00:13:41]: Ihan selkeä kehitys on ollut siinä, että keskustelua käydään ihan joka tasolla, ja se on aktivoitunut. Lähes niin kuin kahvipöytäkeskusteluissa keskustellaan kyberturvallisuusasioista ja siinä mielessä tämä on tavallaan sitä yhteistä tietoisuutta ympäröivästä maailmasta, yhdessä ikään kuin pidetään sitä yllä. Sitten ehkä toinen merkittävä asia on se, että me haluamme TEM:issä ja hallinnon alalla, että meillä koko henkilöstö, meillähän on noin 8—9 000 henkilöä, että tietoisuus näistä kyberturva-asioista on kaikkien huulilla ja ei ikään kuin päästä yllättämään meidän virkahenkilöstöä ikävissä tilanteissa. Kouluttaminen ja osaamisen kasvattaminen, kannustamme osaamisen kasvattamiseen ja omaehtoiseen tiedonhankintaan, niin tämä on ehkä yksi merkittävä asia. Ehkä sitten, minkä olen kanssa havainnut, on se, että puhutaan paljon siitä, että onko meillä riittävästi osaamista ja mikä on riittävä määrä, minkä tyyppistä osaamista me tarvitsemme hallinnon alalla. Me turvaudumme tietenkin esimerkiksi valtioneuvoston kanslian tuottamiin palveluihin tietyissä tilanteissa, ja sitten meillä hallinnon alan toimijat, meillä on omia tietoturva-asiantuntijoita, mutta onko määrä riittävä ja onko laatu niin sanotusti kattava, niin siitä paljon puhutaan. Sitten mainitsi aikaisemmin tilannekuvan luomisen, niin se on kyllä ehdoton edellytys sille, että me pystymme elämään tässä nykypäivässä, että me saamme ajankohtaista ja ajantasaista tietoa näistä meitä uhkaavista riskeistä. Yksi elementti on sitten tietenkin riskien hallinta, että jos tuotamme digitaalisia palveluita ympäröivälle maailmalle tai yhteiskunnalle, niin meillä pitää olla tiedostettuna ne kaikki riskit tai ainakin pääosa niistä, joita voimme kohdata. Ehkä sitten vielä voisin mainita sen, että aika paljon puhutaan myös harjoittelusta ja harjoituksiin osallistumisista ja erilaisista toipumis-, varautumissuunnitelmista, toimintasuunnitelmista ylipäätään, että me tiedämme sitten, kun se poikkeama tilanne tulee, että miten me toimimme, ja kun meillä on aika verkottunut tapa

tehdä asioita, niin millä tavalla me näissä verkostoissa sitten toisaalta hallinnon alan sisäpuolella, mutta myös ulkopuolella, viestimme näistä asioista niin, että kaikki henkilöt, joille nämä asiat ovat tärkeitä ja ajankohtaisia, että he saavat kaiken sen tiedon. Sitten tietenkin yksi, kun puhutaan IT:stä ja tietojärjestelmistä, niin tietoturva-arkkitehtuuri kokonaisuudessaan on varmaan sellainen, jos katsoo vähän insinööriänsä päässä tilannetta, että miltä tämä nyt näyttää ja onko se nyt varmasti sellainen, mikä sopii tähän aikaan, miten sitä pitää kehittää ja kehittämisvastuu, tämän tyyppisiä asioita, on paljon keskustelussa. Ehkä tässä lyhyesti.

Tuija Kuusisto [00:17:00]: Tietotyöhön kuuluu nimenomaan tämä verkostoituminen ja se, että vuorovai-
kutetaan laajassa yhteistyössä eri tahojen kanssa. Sieltä sitten verkostosta ja sitä hyödyntäen voi näitä
ikäviä toimijoita myös ilmaantua sinne työpöydälle, esimerkiksi kiristyshaittaohjelmien muodossa tai
muunlaisen disinformaation hyödyntämisen kautta. Se herättää kysymyksen luottamuksesta ja kysy-
myksen siitä, että keneen voi oikeasti luottaa ja onko se luottamus täydellistä vai jollakin tavalla osittais-
ta. Tässä digi- ja väestötietoviraston digibarometrissä kysyitkin tätä luottamuksen tilannetta ja siellä
ovat vastaajat sanoneet, että noin [kahdeksankymmentä? 00:17:52] prosenttia luottaa siihen, että vi-
ranomaiset käsittelevät turvallisesti ihmisten henkilö- ja muita tietoja, mutta sitten yrityksiin ja juuri näi-
hin, kenen kanssa te työ- ja elinkeinoministeriössä toimitte, niin yrityksiin luottaisi vain noin 27 prosent-
tia henkilöistä. Mutta mitä, teollisuusneuvos Sirpa Alitalo, sinusta on luottamus?

Sirpa Alitalo [00:18:16]: Luottamus on kyllä varmaan turvallisuuden tunnetta. Julkisella sektorillahan
luottamus perustuu läpinäkyvyyteen, linjauksiin, periaatteisiin, auditointimenettelyihin ja julkisen sektorin
toimijoiden harjoituksiin, tällaiseen näkyvään toimintaan ja sitten taas yrityksiin liittyvä liiketoiminta, niin
sieltä se läpinäkyvyys asiakaspään asti jossain mielessä on vähäisempää. Se ehkä herättää kysy-
myksen siitä, että mitä se luottamus eri kohderyhmien kohdalla ja eri toimijoiden kohdalla pitää sisäl-
lään, mutta kyllä luottamus on seurausta siitä hyvästä kokemuksesta, hyvästä asiakkaan käyttökoke-
muksesta ja uskosta esimerkiksi siihen, että minua koskevia tietoja käsitellään turvallisesti. Useinhan
julkisen sektorin toimissa erityisesti lainsäädännön tarjoama viitekehys antaa uskoa ja luottamusta sii-
hen, että kansalaiset luottavat varsin vahvasti julkisen sektorin toimijoihin ja siinä mielessä yritysten ja
meidän viranomaisten lähestymistapa asiakasrajapintaan on erilainen ja varmaan tätä taustaa vasten
on ymmärrettävissä myöskin tuo, että julkisen sektorin osalta luottamus on vahvempaa. Siitä on kyllä
hyvä pitää kiinni. Luottamus on työlästä ansaita, mutta se voidaan menettää nopeasti ja helposti ja siinä
mielessä luottamukseen on hyvä panostaa ja varmistaa, että toimimme niillä läpinäkyvillä periaatteilla
niin, että kansalaiset ja yritykset ovat tietoisia siitä, millä lailla heitä koskevia tietoja esimerkiksi käsitel-

lään. Toki varmasti jatkossa myös yrityksillä on paljon tehtävää sen osalta, että tätä luottamusta saadaan vahvemmalle pohjalle.

Tuija Kuusisto [00:20:39]: Kiitos Sirpa. Miten, johtaja Nordman, miten sinä näet luottamuksen? Miten näet, kuka toimija on sinusta luotettava?

Mika Nordman [00:20:52]: Joo, kyllä Sirpa hyvin tätä asiaa kuvasi. Ehkä tähän voisi vielä täydentää sen, että jos miettii tällaisia julkisia digipalveluita, vähän rajaa tätä luottamusta siihen kohtaan, niin, kyllä minä kansalaisena, kun käytän palveluita, että jos niissä esimerkiksi on joku poikkeama tai häiriötilanne, niin niihin reagoidaan alta aikayksikön eli mahdollisimman nopeasti ja näistä viestitetään hyvin selkeästi ja avoimesti, eikä tavallaan pantata häiriötilanteiden tuomia vaikutuksia. Ehkä yleisesti voi todeta, että kun viranomaiset noudattavat hyvän hallinnon periaatteita ja hallintopäätöksistä voidaan valittaa ja niistä voidaan ikään kuin tehdä oikaisuvaatimuksia, kyllähän tämä isossa kuvassa luottamusta tuottaa. Ehkä yksi nosto, kun pohdin tätä kysymystä myös toiselta kantilta, että miten me voimme yhteiskuntana ulospäin luoda luotettavaa kuvaa Suomesta ja suomalaisista, niin kyllähän esimerkiksi vakaat olosuhteet yritystoiminnalle, jos miettii tällaisia konesalikeisesejä, mitä on nyt viime aikoina ollut, niin kyllähän tämä minusta kertoo sen, että myös Suomen rajojen ulkopuolella meihin luotetaan ja meillä on yhteiskunta sellaiseen asentoon rakennettu, että me itse luotamme itseemme ja toisaalta muut luottavat meihin. Se on tosi hieno tilanne. Ehkä tässä lyhyesti.

Kimmo Rousku [00:22:33]: Digi- ja väestötietovirasto tuottaa lokakuun viimeisellä viikolla jo toisen järjestyksessä olevan Digiturvaviikon, jossa me nostamme keskiöön, voisi sanoa, että henkilöstö, miksei kansalaisetkin voivat tulla opiskelemaan näitä tärkeitä, digiturvaan liittyviä taitoja ja osaamisia. Olenkin kaikkien verkostojeni kautta jo haastanut ja nyt haastan myös kaikki meidän podcastimme kuulijat, että osallistuthan itse henkilökohtaisesti Digiturvaviikolle, haastat oman organisaatiosi osallistumaan, verkostosi ja kollegasi osallistumaan. Tässä nyt tietysti haaste menee samalla myös Mikalle ja Sirpalle. Miten, ensinnäkin Mika, miten sinä huomioit digitaalisen turvallisuuden omassa elämässäsi?

Mika Nordman [00:23:21]: Ehkä kaikki lähtee terveestä skeptisyydestä. Aina pikkuinen varovainen minä on mukana, kun digipalveluita hyödyntää ja käyttää eli asenne pitää olla kohdillaan ja tietoisuus siitä,

että millä tahansa hetkellä voit joutua jonkun vihamielisen toimijan hampaisiin. Sitten ehkä tietenkin, jos mennään vähän enemmän tekniikkaan ja näihin laitteisiin ja sovelluksiin, niin tietenkin tällaiset peruseräkkeet, mitä myös työelämässä pitää noudattaa eli salasanoja pitää vaihtaa, niiden pitää olla turvallisia, sitten tietenkin kotona, kun on kaikenlaisia vempaimia, verkkolaitteita, niin pitää aina muistaa se, että niissäkin toimitaan parhaiden käytäntöjen mukaisesti. Ehkä sitten omaan elämään kuuluu myös se, että kun on lapsia ja lähipiiriä, niin jonkunlaisena tietoturvallisuuden soihdunkantajana tässä lähipiirissä toimii ja muistaa muistuttaa, että jos tulee vaikka uutisointia jostain haavoittuvuudesta, vaikka Applen puhelimiin tai jotain muuta, niin tekee tästä sellaisen asian, jota ei panttaa vaan nostaa sen pöytään. Vaikka ruokapöydässä keskustellaan sitten, että olettehan huomanneet, että tällainen päivitys on tulos ja muistakaahan päivittää. Vanhempia sitten tietenkin digipalveluiden käyttäjänä ja kuluttajana pitää aina silloin tällöin ohjata ja opastaa. Kyllä se on aika lailla arkipäivää, kun töistä pääsee, niin kyllä digitaaliset asiat pyöriivät myös vapailla mielessä ja tämä turvallisuus on sellainen, joka ehkä on, voisiko sanoa, kannattava teema tai kantava teema näissä asioissa.

Kimmo Rousku [00:25:19]: No, miten tämä näkyy, Sirpa, sinun elämässäsi eli miten huolehdit digiturvasta arjessa?

Sirpa Alitalo [00:25:26]: Ihan niillä arjen asioilla kyllä, että huolellisuutta sekä paperimaailmassa että digitaalisessa toimintaympäristössä. Mika tuossa hyvin kirjailikin noita jo, että salasanapolitiikka pitää pitää mielessä ohjeistuksen mukaisena ja huolehtia tietokoneen tai puhelimen päivityksistä ajallaan, käyttää näyttösuojaa, kun liikkuu eri ympäristöissä tietokoneen kanssa ja käsittelee työhön liittyviä tehtäviä erityisesti ja varmaan juuri tuollainen skeptisyys. Joku on joskus todennut, että jos joku juttu tai uutinen tuntuu liian onnekaalta, niin silloin voin jo ajatella, että se ei ole totta, se ei oikeasti tarkoita sitä, mitä sinulle viesteissä välitetään. Skeptisellä asenteella ehkä pystyy taklaamaan monta sellaista tilannetta, joissa tietoturva tai turvallisuus voi olla uhattuna, mutta normaali arki yhteisten pelisääntöjen pohjalta vie kyllä pitkälle.

Tuija Kuusisto [00:26:43]: Kiitos, tässä oli oikein hyviä näkemyksiä. Niinhän se on, että jos sähköpostissa luvataan, että tällä keinolla rikastut, niin pitäisi kysyä itseltään, että miten se on mahdollista, mikseivät sitten kaikki maapallon ihmiset käytä tätä samaa keinoa. Näinhän se menee. Kiitos kovasti teidän ajatuksistanne tässä meidän digiturva-podcastissa ja oikein rentoa ja mukavaa syksyn jatkoa. Kiitos!

Sirpa Alitalo [00:27:16]: Kiitos samoin.

Mika Nordman [00:27:17]: Kiitos samoin.

Kimmo Rousku [00:27:19]: Kiitos.

[äänite päättyy]