

Kuinka huijari lähestyy ja miten suojaudumme

VTKL SENIORSURF 2022-01-16

Sisältö

Mitä, miksi, kuka

Mikä on huijarin tavoite, tavanomainen ympäristön ja verkkoympäristö

Kanavat – puhelut-viestit, some ja sähköpostit

Tarkastellaan eri kanavien kautta tulevia huijausyrityksiä

Esimerkkejä viesteistä

Kuvallisia esimerkkejä havaituista viesteistä, Internet osoitteen rakenne

Avainkohdat – muista nämä

Muutammat tärkeät muistettavat kohdat

Verkossa

Linkkejä avustavan tiedon lähteelle



Lähtötilanne

- Kuvitellaan lähtötilanteeksi sellainen, että asut suuressa kerrostalossa.
- Kerrostalossa työskentelee myös talon kunnossapitovastaava, jonka yksi tehtävä on päästää vierailijat ja asukkaat kulkemaan ulko-ovesta.
- Kerrostalossa on myös kellarikomero ja sinulla on toisessa kaupungissa mökki ja siellä vene. Käytät näitä oman aikataulusi mukaan. Kätevyyden vuoksi kellarikomero, mökki ja vene on sarjoitettu samalle avaimelle.
- Kotisi ovesta on turvalukko.
- Sinulle on annettu myös turvalukon avain pankin asiakastilaan, jotta voit hoitaa siellä asioitasi. Sinut tunnistetaan avaimesta ja kaikki toimii sujuvasti.
- Antaisitko pankin turvalukon avaimen ovellesi tulevalle tuntemattomalle henkilölle ?

Ja sama verkottuneessa maailmassa

- Olet jonkin operaattorin asiakas. Operaattorin tehtäviä hoitaa kunnossapitovastaava ja kerrostalo kuvaa operaattorin verkkoa.
- Kerrostalon pihasta lähtevä tie kuvaa Internetiä. Kunnossapitovastaava pyrkii parhaan arvionsa mukaan tunnistamaan asiallisia kulkijoita, keitä ulko-ovesta taloon päästetään.
- Käytät erilaisia palveluita (kellarikomero, mökki ja vene), joihin olet jostain syystä valinnut saman salasanan (saman sarjan avain).
- Onneksi kuitenkin valitsit tietokoneeseesi ja kännykkääsi vahvan uniikin salasanan (asunnon ulko-ovi).
- Ja pankin asiakastilan turvalukon avain, josta sinut tunnistetaan, kuvaa saamiasi verkkopankkitunnuksia.
- **Annatko verkkopankkitunnukset Internetissä tuntemattomalle taholle?**

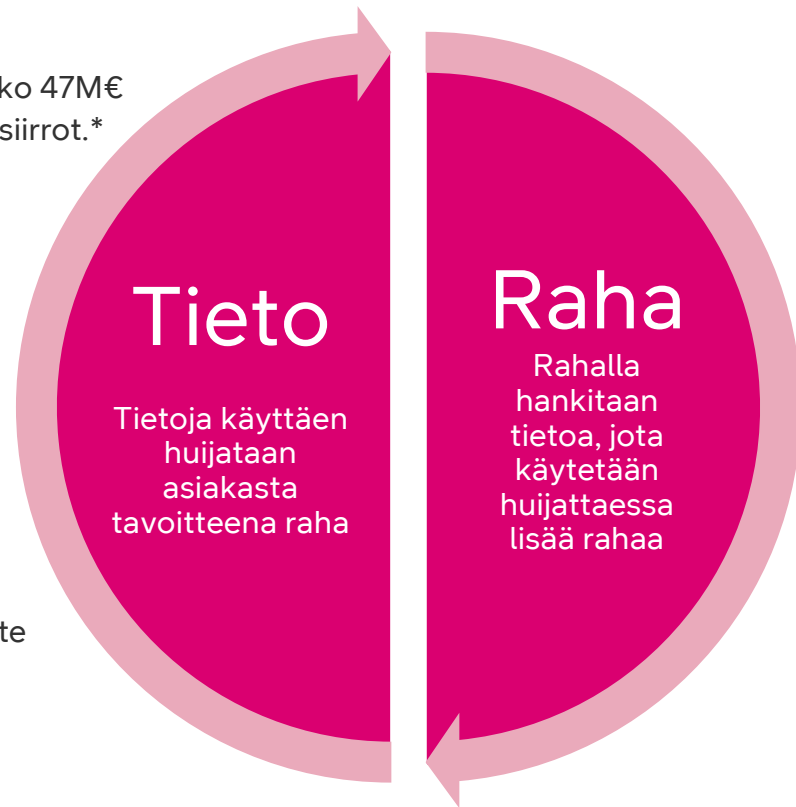


Miksi huijari lähestyy minua?

VTKL SENIORSURF 2022-01-16

Miksi juuri minut valittiin?

- Rahan vuoksi
 - Vuonna 2021 yli 2500 nettihuijaustapausta. Rikosvahinko 47M€ +pankit ja viranomaiset onnistuivat estämään yli 25M€ siirrot.*
- Tiedon vuoksi
 - Minulla voi olla tietoa, jolla saa rahaa kiertotien kautta
 - Huijarit ovat ammattilaisia, joiden tavoitteena on saada asiakas suostumaan heidän pyyntöihinsä (=rahaa)
 - Jotkut tekevät sitä näyttääkseen taitonsa
 - Joillakin on tavoitteena aiheuttaa tuhoa
 - Valinta saattoi olla satunnainen (puhelinnumero)
 - On mahdollista, että puhelinnumero tai sähköpostiosoite oli kerätty jollekin listalle
 - Tartuin tarjoukseen, joka oli liian houkutteleva



Huijauksissa tyypillistä

- Huijari tekee sinulle houkuttelevan tarjouksen, joka on vähän liian hyvä ollakseen totta
- Toisaalta saatat joutua tilanteeseen, joka on sinulle kiusallinen ja vaatii kiireellisiä toimenpiteitä
- Huijari voi myös kertoa, että sinua on huijattu ja nopeita toimenpiteitä tarvitaan
- ”Toimenpiteesi ovat tärkeitä juuri nyt”
- ”Tämä on elämäsi tilaisuus”
- ”Aikaa on rajoitetusti, joten älä kysele turhia vaan toimi.”
- Kun havaitset varoitusmerkkejä, ota aikalisä.
Voit kysyä tutulta kaverilta mielipidettä.
- Tarkasta tietoja yrityksen verkkosivu
- Mieti tunnetko toisen osapuolen, joka esittää vaatimuksen tai tarjouksen
- Mieti miksi juuri sinut valittiin ja onko tarina totta
- Mieti uskoisitko tarinan, jos sen kertoisi ovikelloa soittanut henkilö

Olemme havainneet
epätavallista toimintaa.
Tarkista maksu:
petos-op.fi

Huijaus



Eri kanavat

VTKL SENIORSURF 2022-01-16

Puhelut – puhelin on ovikellosi

- **Operaattorien toimenpiteistä huolimatta osa huijauspuheluista pääsee läpi**
- Puhelu tulee tyypillisesti ulkomaisesta numerosta tai numero ei näy. Se voi olla myös väärennetty näyttämään suomalaiselta mobiililiittymän numerolta.
- Puheluun vastaaminen ei vielä aiheuta mitään, mutta paljastaa mitä soittaja haluaa.
- Puheluun voi vastata. Se voi olla myös tärkeä puhelu.
Kun vastaat tuntemattomaan numeroon: puhelussa ei tarvitse kertoa nimeään ja sen voi myös lopettaa ilman muodollisuuksia, kun siltä tuntuu.
- Puhelun voi keskeyttää ja soiton voi varmistaa ao. pankista tai viranomaiselta ennen kuin antaa mitään tietojaan. **Oikea pankin työntekijä tai viranomainen ei koskaan pyydä pankkitunnuksia.**
- Huijarit voivat yrittää esittää sinulla olevan ongelman, joka vaatii välitöntä ratkaisua.

Ei tunnuksia puhelun soittajalle

- puhelinnumero = numerosarja, voidaan valita satunnaisesti, salainen numero ei estä soittoja
- Jos salaisen numeron käyttäjää puhutellaan nimellä, numero on todennäköisesti listoilla
- Kun tuntematon numero soittaa, useissa tapauksissa se on markkinointipuhelu
- Joissakin tapauksissa yritetty huijata esiintymällä IT-tukena tai myymällä sijoitustuotteita (esim. kryptovaluuttaa)
- Huijarit ovat soitelleet myös pankkihenkilönä tai viranomaisena esiintyen.
- Missään tilanteessa ei tule antaa pankkitunnuksia tai luottokortin tietoja niitä puhelimessa pyytävälle.

Internet-osoitteesta (esiintyy linkeissä)

Internet osoitteen rakenne. **Piste on osoitteen eri osien erotin.**

<http://omistaja/polku?toiminto>

aliverkkotunnus.maatunnus/

<https://www.s-pankki.fi/> ←oikea

<https://spannkioyj.com/> ←huijaus

<https://spankki-fioy.com/> ←huijaus

<https://spankki-oyfin.com/> ←huijaus

<https://spankkifioyj.com/> ←huijaus

<https://oyjspankki.com/> ←huijaus

<https://s-pankki-tukossa.info/> ←huijaus

<https://spankki-onlinefin.com/> ←huijaus

<https://spankkioyjfin.com/> ←huijaus

Esimerkkinä paljon julkisuudessa esiintynyt S-pankin aliverkkotunnus, joka on joutunut huijareiden kohteeksi

Sähköpostit

- Vakuuttavuutta tunnettujen brändien nimillä
- Viestii usein ongelmaa nettipalvelussa
- Huijausarvonnat, laskujen maksu
- Kiristyssähköpostit

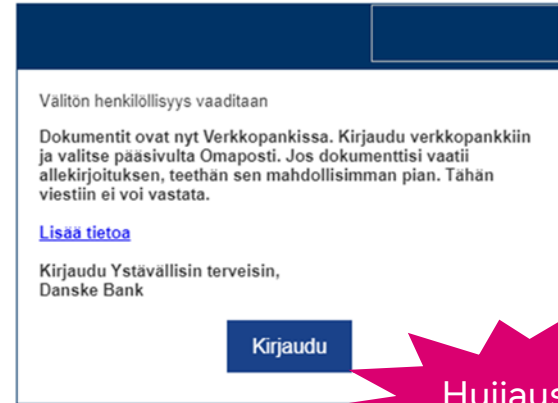
Vastausosoite: DNA <cc.fbi@gmail.com>
Otsikko: Vahvista
Päiväys: 20.09.2022

Hyvä DNA-internetin käyttäjä,

Haluamme ilmoittaa, että kahta samaasi viestiä ei ole lähetetty postilaatikkoosi uusimpien päivitystemme vuoksi. Postilaatikkosi on ylittänyt tallennusrajan 1 Gt. NAPSAUTA TÄTÄ <<https://survey.zoho.com>> päivittääksesi sähköpostisi, jotta et joutuisi lukittumaan tiliisi, ja odota sähköpostitiimimme vastausta. Pahoittelemme tästä mahdollisesti aiheutunutta vaivaa.

Toivottaen
DNAinternet

Huijaus



Ota meihin yhteyttä

Tähän sähköpostiin ei voi vastata, mutta voit ottaa meihin yhteyttä osoitteessa www.danskebank.fi

Danske Bank Group,
Danske Bank A/S, Parallvej 17, FI-2800, Tel. +45 33 44 00 00

[Peruuta tilaus/Vaihda sähköpostiosoite](#)

Huomaa, että tämä viesti saattaa sisältää luottamuksellisia tietoja. Jos olet saanut tämän viestin vahingossa, ilmoita virheestä lähettäjälle ja poista sitten viesti järjestelmästäsi tekemättä, jakamatta tai säilyttämättä siitä kopioita. Vaikka uskomme, että viesti ja sen liitteet ovat vapaita viruksista ja muista virheistä, jotka voivat vaikuttaa siihen tietokoneeseen tai IT-järjestelmään, jossa se vastaanotetaan ja luetaan, vastaanottaja avaa viestin omalla vastuullaan. Emme ota vastuuta mistään menetyksistä tai vahingoista, jotka johtuvat tämän viestin vastaanottamisesta tai käytöstä.

Huijausesimerkkejä

From: Prisma <mailmanager74@molami
Sent: perjantai 7. lokakuuta 2022 11.07
To: |
Subject: Arvomme 1000€:N Prisman Lahjakortti!

Arvomme 1000€:N Prisman Lahjakortti!

Sinut on valittu mukaan kuluttajatutkimukseen ja nyt sinulla on ainutlaatuinen mahdollisuus saada Prisman 1000€:n lahjakortti.

Vastaathan vain muutamaan kysymykseen ja tämän jälkeen täytät yhteystietosi. Kiitämme jo etukäteen.

Klikkaa tästä <linkki>



Huijaus

Laskusi on maksettu kahdesti

Source Plain text

.PALAUTUSNUMERO: 28HK9-€

Hei ,

Ilmoitamme kirjallisesti, että lokakuun 2022 viimeinen laskusi on maksettu kahdesti.

Pyydämme sinua pyytämään hyvitystä napsauttamalla alla olevaa linkkiä:

Voit muokata laskuasi osiassa:

[Hyvityspyyntö](#)

huomautus: Jos tätä ei ratkaista seuraavan 12 tunnin kuluessa, hyvitystä ei myönnetä.

Kiitos yhteistyöstäsi tässä asiassa.



Huijaus

Huijausesimerkkejä 2

Onnittelut

Huijaus

Saat täten ilmoituksen yhteensä 1 000 000 euron lahjoituksesta. Lahjoitettiin sinulle ja perheellesi myös eri yhteisöjen köyhien ja Ukrainan sodan uhrien auttamiseksi. Ota yhteyttä saadaksesi lisätietoja.

Kiitos paljon!

Sähköposti:

Luottamuksellinen
Allekirjoitettu asiakirja
[Pääsy allekirjoitettuihin asiakirjoihini](#)

Dan ja MacKenzie Scott

Hei,
Olemme OmaSp- lähettäneet Teille luottamuksellisen sähköpostiviestin. Sähköpostiviestin avaaminen ja lukeminen tapahtuu yläpuolella olevan suojatun linkin kautta. Turvallisuussyistä voitte lukea viestin vain yhdestä tietokoneesta/mobiililaitteesta korkeintaan 14 päivän ajan. Tallentakaa ja/tai tulostakaa viestin sisältö ja hävittäkää tämä ilmoitusviesti.
OmaSp- 24/7 asiakaspalvelu auttaa tarvittaessa numerossa 0200 3000 (pvm / mpm). Tähän viestiin ei voi vastata. Ystävällisin terveisin, OmaSp.

Subject

Sender

VOITA ITSELLESI 1000€:N LAHJAKORTTI K-MARKET!

hack@sk

Onnea! 1000€:N LAHJAKORTTI K-MARKET!

it@rome

VOITA ITSELLESI 1000€:N LAHJAKORTTI K-MARKET!

list@ant

Älä odota pidempään, saa rahat tilillesi nyt!

contact@

Voita 1000€ lahjakortti vapaavalintaiselle bensa-asemalle!

< >

Congratulation You May Win A Iphone 14 Pro

pushpat

Huijaus

Sosiaalinen media

- Facebook, FB Messenger, Instagram, Snapchat, WhatsApp ym
- Huijausmainokset
- Rakkaushuijaukset – tuntemattoman lähestyminen – rahan pyytäminen
- Sijoitushuijaukset, tällä hetkellä erityisesti kryptovaluuttaan sijoittaminen
- Huijauskilpailut
- Tunnusten kalastelu – **tiedot arvokkaita** - varmista yksityisyysasetuksesi
- ”Hukkasin/vaihdoin puhelimeni” – huijaus perheenjäsenen/tutun nimissä

- Millaista tietoa löytyy
 - tiedot kavereista, julkaistut kuvat (kuvien taka-alalla olevat asiat), mahdollisesti osoitteet,
 - palvelut, joita käyttää
 - harrastukset

Muista:

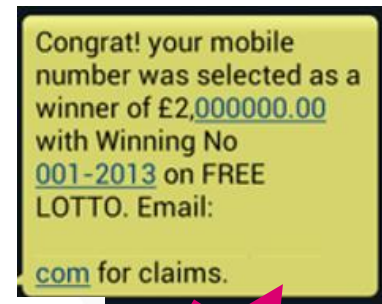
- **Kriittisyys tarjouksiin ja kilpailuihin – älä jaa kavereiden yhteystietoja luvatta, älä jaa tunnuksiasi, varmista tilanne omien yhteystietojesi kautta**

Viestit (SMS, MMS)

- Usein tunnettujen brändien nimissä (pankit, p...
- Kriittisyys viestien sisältöön – miksi minulle ?
- **Älä käytä viestissä olevaa linkkiä. Jos viesti vaatii pankkitunnuksia, lopeta.**
- Älä anna tuntemattoman viestin asentaa ohjelmia puhelimeesi
- **Epämääräinen viesti – älä yritä ymmärtää- suhtaudu kuten huijaukseen**
- Puhelinnumeroa ei käytetä arvontanumerona
- Käytä omia kirjanmerkkejä siirtymiseen



Huijaus



Huijauk
sia



Olet maksamassa palvelussamme: Tia Heinonen tilille FI21 1234 5 85. jos et ole tehnyt tällaista pyyntöä, ole hyvä ja kirjaudu sisään: S-Pankki.live

Hakukoneet

- Harvinaisina tapauksina myös hakukoneiden tuloksiin on onnistuttu saamaan huijareiden tuloksia. Eri hakukoneet antavat keskenään vähän erilaisia tuloksia.
- Yleisimmin hakutulosten vääristelyä esiintyy suurten internet brändien nimissä, jotka eivät palvele puhelimitse
- Toimijat esiintyvät puhelintukea tarjoavina yrityksinä
- Hakukonetoimijat pyrkivät karsimaan näitä jatkuvasti

Muistetaan jälleen

- Ei saa antaa omia pankkitunnuksia/luottokortin tietoja
- Ei saa antaa asentaa ohjelmistoja koneelle

Muistettavaksi

VTKL SENIORSURF 2022-01-16

Muistettavaksi muutamia

- Älä kirjaudu viestien linkeistä/älä soita viestien linkkien tarjoamiin numeroihin
 - Vastuulliset toimijat eivät liitä viesteihinsä linkkejä vaan pyytävät kirjautumaan palveluunsa tunnettujen yhteystietojen tai oman sovelluksen kautta. Jos epäilet, varmista lähipiiriltäsi mikä on oikea ja pyydä merkitsemään kirjanmerkiksi.
- Älä anna tunnuksiasi/salasanojasi
 - Palvelun tuottaja tuntee sinut ja hoitaa asiat omilla järjestelmillään. Tunnuksesi ja salasanasi ovat sinun. Käytä mobiilivarmennetta tai pankin omaa sovellusta tunnistautumiseen.
- Älä anna kenenkään tuntemattoman asentaa mitään koneellesi.
 - Käytä vain sellaisia tietokoneen tukipalveluita, joihin voit luottaa. Kysy rohkeasti osaavilta.
- **Jos vahingossa erehdyt tai epäilet erehtyneesi**
 - **Älä mieti mitä-jos vaan aloita korjaava toiminta heti.** Parempi varmistaa tilanne, kuin jäädä hautomaan asiaa. Pyydä apua osaavalta.
 - Jos edes epäilet pankkitunnustesi päätyneen ulkopuolisen tietoon, **ota AINA ENSIMMÄISEKSI yhteys PANKKIISI**, vasta sen jälkeen poliisiin. Nopealla toiminnalla pankki saattaa ehtiä estämään rahansiirrot.

Ennakkokysymyksiä

VTKL SENIORSURF 2022-01-16

Kysymyksiä 1

- Miten estää sähköpostiin tulevia toistuvia mainoksia (esim. kasinopelit ja lainatarjoukset)? Roskapostiksi merkitseminen ei auta.
 - Haasteena on se, että roskapostia lähettävät taho vaihtaa toistuvasti osoitetta, joista viestit näyttävät lähtevän. Käytettävä sähköpostiohjelma määrittelee miten se käsittelee spammiksi merkityt sähköpostit. Jotkut ohjelmat siirtävät hyvällä osumisprosentilla roskapostin omaan kansioon ja näin se ei ole ”oikean” postin joukossa.
- Miten ikäihminen, jolla ei ole pankkitunnuksia, saa mobiilivarmenteen käyttöönsä. Mobiilivarmementautuminen olisi paljon helpompi ja turvallisempi tapa tunnistautumiseen kaikkialle muualle paitsi pankkiasioihin.
 - Mobiilivarmenteen voi saada ilman pankkitunnuksia vielä yhden suomalaisen operaattorin liittymään tunnistautumalla poliisin myöntämän asiakirjan kanssa sen omassa myymälässä.

Kysymyksiä 2

- Mikä turvallisin keino hakeutua pankin sivulle tietokoneen nettislaimella, jos ei kirjanmerkkiä jo valmiiksi? Monesti neuvotaan ettei pankin osoitetta kannata etsiä hakukoneella. Joidenkin pankkien sivuilla neuvotaan että osoite pitää aina kirjoittaa osoitepalkkiin onko tämä kaikkein turvallisin keino verrattuna tuohon kirjainmerkkiin?
 - Oma kirjanmerkki on varmin tapa siirtyä esimerkiksi pankin sivulle. Kirjanmerkki on luotu yleensä rauhallisessa tilanteessa ja oikealle sivulle pääsy on varmistettu ennen kuin se on luotu.
 - Kirjoittamalla joka kerralla osoite uudelleen voi tehdä kirjoitusvirheen, joka johtaa ei-toivotulle sivulle.
 - Kännykässä ja tabletissa pankin oma sovellus on paras tapa käyttää verkkopankkia.
- Miten estää puhelinhuijaukset? Uskaltaako tuntemattomaan numeroon yleensäkin vastata?
 - Tuntemattomaan numeroon uskaltaa vastata. Näin saadaan varmuus siihen mitä asia koskee.
 - Vastaaminen ei itsessään aiheuta ongelmaa. Ongelma syntyy vasta, jos tekee vääriä toimenpiteitä puhelun aikana tai sen jälkeen. Mikäli puhelu vaikuttaa asiattomalta, luurin voi sulkea ilman muodollisuuksia.

Kysymyksiä 3

- Minulle on tullut parin kaverin Facebook-viesti, joissa on kyselty kuulumisia. Seuraavaksi on kysytty puhelinnumeroa tai pyydetty tutustumaan linkin mukaiseen sivustoon. Oletettavia kaappauksia? Miten näihin tulisi suhtautua?
 - Vaikuttaa siltä, että kaverien tilit on saatu huijareiden haltuun ja huijarit keräävät tarkempia tietoja kontaktilistan henkilöiltä. Pyynnöt kannattaa ohittaa ja myös kaverille voi yrittää välittää omien kontaktikanavien kautta tiedon siitä, että hänen tilinsä on todennäköisesti kaapattu. Facebookilla on ohjeet kaapatun tilin palauttamiseen <https://fi-fi.facebook.com/help/203305893040179>
- Ilmeisesti tämän tyyppiset nettiosoitteet ovat aitoja pääosoitteen alisivustoja? <https://digituki.hel.fi/> (Helsingin kaupungin alisivusto)
 - Kyllä. Tuon aliverkkotunnus on ”hel” ja maatunnus on ”fi”. Se joka hallitsee verkkoja voi tehdä haluamiaan alisivustoja joko noin, että palvelun nimi tulee eteen pisteellä erotettuna tai vaihtoehtoisesti niin, että maatunnuksen jälkeen tulee ”/” ja sen jälkeen palvelun tunnus. Osoitteessa ”hel.fi” on tärkeä osa ja se kertoo, että osoite on Helsingin kaupungin hallussa.

Kysymyksiä 4

- QR-kuva vastannee linkkiä?
 - Kyllä. QR-koodit voivat sisältää linkin Älypuhelimien kameran asetuksissa voi löytyä valinta ”Skannaa QR-koodit” ja sen voi asettaa haluamukseen.
- Miten saa puhelimen sähköpostiohjelmassa lähettäjän sähköpostiosoitteen näkyviin?
 - Klikkaamalla lähettäjän nimeä avatussa postissa paljastuu lähettäjän osoite ja vastaanottajat.
- Miten saa puhelimen sähköpostiohjelmassa näkyviin postissa olleen linkin?
 - Kun linkkiä painaa pitkään, tulee näkyviin sen sisältämä osoite.
- Facebookissa tulee vastaan toisinaan hassuja kyselyitä. Kannattaako niihin vastata?
 - Viestit näyttävät usein tulevan samalta toimijalta. Niiden tarkoituksena ei ole yksinomaan viihteen tarjoaminen, vaan taustalla voi olla myös järjestelmällistä tiedonkeruuta. Näihin kyselyihin voi liittyä yksinään viattoman oloisia kysymyksiä, mutta kun ne liitetään osaksi suurta tietomassaa, niistä tulee hyödyllisiä. Aihe on ollut esillä muutama vuosi sitten myös Helsingin Sanomissa <https://www.hs.fi/teknologia/art-2000006488268.html>
 - Jotain kertoo myös se, että Facebook on tällä hetkellä oikeudessa liiallisen tiedon keräämisestä Iso-Britannian kansalaisista. Vastaavaa on tapahtunut USA:ssa ja tapahtuneen muissakin maissa.

Kysymyksiä 5

- Keskustelussa tuli myös esiin laitteiden tarkastamisen tarve.
 - Suomalaisella F-Securella on osoitteessa <https://www.f-secure.com/fi/home/free-tools> tarpeellisia ilmaisia työkaluja.
 - Mikäli käytössäsi ei vielä ole virussuojausta, voit tehdä tarkastuksen ” F-Secure Online Scanner” työkalulla.
 - On tärkeää pitää tietokoneen virus- ja haittaohjelmasuojaus sekä varmuuskopiointi ajan tasalla.

Ohjeita ja neuvoja

Poliisin hyvät opastavat verkkosivut

- <https://poliisi.fi/tukea-ikaihmisille>
- <https://poliisi.fi/petosrikokset>

Kyberturvallisuuskeskuksen verkkosivut

<https://www.kyberturvallisuuskeskus.fi>

Kyberturvallisuuskeskuksen ajankohtaiset aiheet

<https://www.kyberturvallisuuskeskus.fi/fi/tietoturva-nyt>

Kuluttajaliiton ja muiden toimijoiden yhteinen VVV-kampanja

<https://www.kuluttajaliitto.fi/varo-varmista-varoita/>

DNA:n vinkkejä

<https://www.dna.fi/blogi/-/blogs/viisi-vinkkia-huijaussivustojen-valttamiseen>

Aiheeseen liittyviä linkkejä 2

Ohje rikosilmoituksen tekoon

<https://poliisi.fi/tee-rikosilmoitus>

Keskustelu ja tukipalveluiden numeroita (osa käytettävissä 24/7)

<https://tietovuotoapu.fi/fi/mista-apua>

Muita

Mobiilivarmenne <https://mobiilivarmenne.fi/>

Internet osoite <https://fi.wikipedia.org/wiki/URI>



Kiitos.

VTKL SENIORSURF 2022-01-16