Tietoa ja käytännön vinkkejä tietojen turvallisesta käytöstä

Jarkko Ilomäki 2022

Mtech
Digital Solutions

Esittely

Jarkko Ilomäki

Varatoimitusjohtaja ja teknologiajohtaja (Mtech)

DI (ICT), MBA

Kokemusta mm.

- Ohjelmistotuotannon eri tehtävistä
- Kansainvälisestä ohjelmistoliiketoiminnasta
- ProAgrian, Faban ja MTK:n asiakkuuksista

Mtech
Digital Solutions

Agenda

Tietoturva – mistä on kyse

Esimerkkejä

Suosituksia ja hyviä toimintatapoja

Yhteenveto

Mtech
Digital Solutions

Tietoturva – mistä on kyse?

Mtech Digital Solutions

Mitä tietoturva on?

Tietosuoja on **perusoikeus**, joka turvaa henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä

Tietoturva on **yksi tietosuojan toteuttamisen** keino

Tietoturvan tarkoituksena on **suojata** tietoja, tietoliikennettä ja näitä ylläpitäviä tietojärjestelmiä

Tietoturvaa vastaan tehtyjä toimia kutsutaan **tietoturva-** tai **kyberhyökkäyksiksi**

Yritysten osalta tietosuojaa ja tietoturvaa koskevat useat lait ja asetukset (esim. tietosuojalaki, GDPR, julkisuuslaki, laki yksityisyyden suojasta) ja niitä valvoo mm. tietosuojavaltuutettu ja poliisi

Mtech Digital Solutions

Miksi tietoa tulee turvata?

Tieto on omaisuutta, ja sillä on materiaan verrattava arvo

Tiedon arvo voi riippua siitä, moniko sen tietää

Tiedon vääristämisellä tai saavuttamisen estämisellä voidaan aiheuttaa haittaa

Tiedolla voidaan kiristää ja sitä voidaan varastaa

Nykytilanteessa maatalous ja siihen sisältyvät tietovarannot ovat yksi osa-alue, johon kohdistuvat hyökkäykset ovat kriittisiä ruoantuotannolle

Henkilökohtaiset tiedot, pienetkin, voivat avata reittejä muille hyökkäyksille

Mtech Digital Solutions

Tietoturvan ominaisuudet

Confidentiality
Luottamuksellisuus

Tietoja voi käyttää vain *ne*, joilla on siihen *oikeus*

Terveystietojasi voivat tarkastella vain sinun valtuuttamasi henkilöt

Terveystietoihisi pääsee käsiksi terveyskeskuksen siivooja

Integrity
Eheys

Tietoja voivat *muuttaa* vain siihen *oikeutetut*

Pankkitililtäsi lähtenyt maksu on sinun hyväksymäsi

Terveydenhuoltorekisteriin on ilmestynyt sinulle outoja merkintöjä

Availability
Saavutettavuus

Tietoon on *pääsy* ja *mahdollisuus* sitä *hyödyntää*

Pääset esimerkiksi pankin verkkopalveluun tunnistautumisen jälkeen

Verkkopankkiin ei pääse palvelunestohyökkäyksen johdosta

Non-Repudiation
Kiistämättömyys

Tekoa, kuten sopimusta, *ei voida kiistää* jälkikäteen

Allekirjoituksellasi vahvistat tehneesi sopimuksen asunnon ostamisesta

Sopimuksen allekirjoittikin henkilö, joka ei omistanut kyseistä asuntoa

Mtech Digital Solutions

Keitä ovat hyökkääjät?

”Script Kiddies”	Henkilöitä, joilla isoja puutteita tietoteknisessä osaamisessa, ja käyttävät valmiita ohjelmia ja skriptejä (”youtube-hakkerit”)
Mustahattuhakkerit	Henkilöitä, joilla merkittävää osaamista hyödyntää teknisten järjestelmien heikkouksia, tavoitteena yleensä raha.
Yritysvakoilu	Kilpailijoiden teknisen osaamisen anastaminen tai vahingoittaminen
Järjestäytynyt rikollisuus	Osaamista tietoteknisesti ja sosiaalisesti
Valtiollinen toimija	Kybertiedustelu ja –hyökkäykset ovat ulkopolitiikan jatke, ns. ”harmaan alueen operaatioita”
Lähipiiri	Syynä esimerkiksi henkilökohtainen kosto tai naiivius

Mtech Digital Solutions

Mitä ovat yleisimmät hyökkäystavat?

Adware	Laite alkaa näyttää mainoksia satunnaisesti ja lähettää käyttäjän tietoa mainostajille
Bots	Laitteille on asennettu salassa ohjelma, jo~~t~~ka voidaan herättää tietyn tilaisuuden tullen
DDoS	Distributed Denial of Service eli palvelunestohyökkäys
DNS Spoofing	Luodaan alkuperäisen sivuston näköinen verkkopalvelu, ja alkuperäisen palvelun osoite varastetaan
Doxxing	Henkilökohtaisten tietojen vuotaminen julkisuuteen (asuinpaikka, kalenteri, terveydentila, parisuhdeasiat)
Keyloggers	Ohjelma, joka kerää kaikki näppäimistön painallukset (esimerkiksi salasanat) ja lähettää ne hyökkääjälle
Man-in-the-Middle	Hyökkääjä tulee (yleensä verkkoliikenteessä) käyttäjän ja palvelun väliin ja esiintyy kummallekin osapuolelle toisena
Password Attack	Pyritään eri algoritmeilla murtamaan käyttäjän salasana~~n~~ (malleina esim. raaka voima (brute-force), sanakirja, tiedonetsintä)
Phishing	Tietojenkalastelu: hyökkääjä huijaa käyttäjän antamaan luottamuksellista tietoa suoraan tai esim. avaamalla haitallisen sähköpostin. Erityisversioita: whalephishing (kohteena omistajat ja johtoryhmätason henkilöt) ja spearfishing (kohdehenkilö, jota tutkittu etukäteen)
Ransomware	Kiristystoiminta, jolla esimerkiksi tietosisältö kryptataan ja avaamise~~e~~n tarvittava avain pitää ostaa
Social Attack	Suoraviivainen tiedustelu, esimerkiksi soitetaan henkilölle, esiinnytään tukihenkilönä ja pyydetään tunnuksia
Spyware	Vakoilee käyttäjän toimia ja kerää informaatiota, ei välttämättä aiheuta suoraan mitään negatiivisia vaikutuksia
Trojan	Normaaliin ohjelmaan kytkeytynyt toiminnallisuus, joka yleensä tekee yhden toimenpiteen (esim keylogger)
Viruses	Tarttuu suojaamattomalle koneelle ja leviää tiedostojen avulla – yleensä pohjustaa muita hyökkäyksiä
Worms	Kuten virus, mutta ei tarvitse käyttäjän toimintaa vaan hyödyntää esim. käyttöjärjestelmän aukkoja

Mtech
Digital Solutions

Esimerkkejä

Oysin psykoterapian palvelutoimittaja Vastaamo on joutunut tietomurron kohteeksi – Oysin potilastiedot ovat turvassa

21.10.2020 16:42

Tämän hetkisten tietojen mukaan tietovuoto ei koske Oysia.

Psykoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia

Potilastiedoissa kerrotaan henkilötietoja ja hyvin intiimejä tietoja asiakkaiden elämäntilanteista ja mielenterveyden ongelmista.

AGCO Announces Ransomware Attack

May 06, 2022

AGCO, Your Agriculture Company (NYSE:AGCO), a worldwide manufacturer and distributor of agricultural equipment, announced today that on May 5, 2022, it was subject to a ransomware attack that has impacted some of its production facilities. AGCO is still investigating the extent of the attack, but it is anticipated that its business operations will be adversely affected for several days and potentially longer to fully resume all services depending upon how quickly the Company is able to repair its systems. The Company will provide updates as the situation progresses.

Cautionary Statements Regarding Forward-Looking Information

Our expectations with regard to resolving the issues are forward-looking statements, and actual results could be materially different due to a number of factors, including our ability to successfully reinstall software and restore IT operations at the effected sites.

Mtech Digital Solutions

Ransomware-esimerkki

HP Hood

Type	Limited liability company
Industry	Food
Founded	1846; 176 years ago Charlestown, Massachusetts, United States
Founder	Harvey Perley Hood
Headquarters	Lynnfield, Massachusetts, United States
Area served	United States and International Locations
Key people	Gary Kaneb, President
Products	Dairy
Revenue	$2.7 billion
Owner	The Kaneb Family
Number of employees	More than 3,000
Subsidiaries	see list of brands below
Website	hphood.com

Hackers hit Hood. Dairy shut down milk production this week after 'cyber security event'

MARCH 18, 2022 DISSENT

Anissa Gardizy reports:

> It's not just passwords, credit card data, or personal records. Now, it appears the hackers have come for our milk and Hoodsies.
>
> H.P. Hood Dairy said Friday that it was the target of a "cyber security event," that forced it to temporarily shut its 13 dairy plants around the country this week. The closures meant Hood had to get rid of some dairy products, and the company warned there could be delivery delays for some customers as Hood's facilities get "back up and running."

Read more at Boston Globe.

Mtech
Digital Solutions

Phishing-esimerkki

Hei,

Olemme lähettäneet sinulle kirjeen (Ilmoitus tyypistä 3, ks. P-J).
jota ei ole seurattu. Voitteko vahvistaa tämän kirjeen vastaanottamisen?

Tämä sähköposti on viimeinen VAROITUS

Odotan vastausta 48 tunnin kuluessa.

Hallinto

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

POLIISI
POLICE OF FINLAND

KANSALLISEN POLIISIN PÄÄOSASTO

Internet-pedofiilien vastainen foorumi

SYYTTÄMISMÄÄRÄYS

AIHE : OIKEUDENKÄYNNIT
Native : PEDOPORNOGRAFIA
(Kyberavaruus) INTERNET
Menettelyn Viite 30090987/2022

Huomionne

Minä, allekirjoittanut Herra **Mikko Masalinin** Sisä-Suomen poliisilaitoksen poliisipäällikkö yhteistyössä Kansainvälisen rikospoliisijärjestön (**INTERPOL**) *kanssa ottaa huomioon rikoslain 20, 21-1, 21 artiklan 1 kohdan ja 75-78 artiklan*. Lähetämme sinulle tämän sähköpostiviestin pian tietoverkkoon tunkeutumisen tietokoneistetun takavarikon jälkeen ilmoittaaksemme sinulle, että sinuun kohdistuu useita voimassa olevia oikeudellisia menettelyjä, **Lapsipornografia – Pedofilia - Exhibitionismi - Kyberpornografia, Pornosivusto**

Tiedoksi 14. maaliskuuta 2016 annettu laki nro 2016-297 lisää rangaistuksia silloin, kun seksuaalinen ehdotus ja pahoinpitely tai raiskaus on voitu tehdä. olet syyllistynyt rikokseen sen jälkeen, kun sinut on otettu kohteeksi internetissä (mainossivusto), kun olet katsellut lapsipornografiaa sisältäviä sivustoja, ja verkkohyökkäysryhmämme on tallentanut todisteet.

Tuomioistuin, joka tuomitsee kaikki seksikauppaan liittyvät yritykset, ei voi jättää huomiotta mitään toimia tällaisten ilkivallan uhrien suhteen. Tilanteen korjaamiseksi ja sen välttämiseksi, että joudutte kansallisen syyttäjänviraston syyttäjän kuultavaksi ja että maineenne perheenne ja ystävienne keskuudessa saattaa vaarantua, ehdotamme, että teette yhteistyötä sovintoratkaisun aikaansaamiseksi. Sinun on maksettava **5 777 €** kiinteä rikossakko, jonka jälkeen Interpol peittää tapauksen, poistaa arkaluonteiset tietosi ja todisteesi tietokannoistamme ja keskeyttää kaikki sinua vastaan aloitetut menettelyt. Tämän jälkeen annamme ohjeet kansalliselle kyberturvallisuuskeskukselle (**NCSC**), jotta se voi auttaa sinua turvaamaan tietosi ja tietosi internetissä. Jos kuitenkin kieltäydyt yhteistyöstä tai jos kieltäydyt sanotusta, meidän on turvauduttava oikeudellisiin menettelyihin.

Ref.: 30090987/2022 PVP

Oikeuslaitos ryhtyy tarvittaviin toimenpiteisiin syytteen nostamiseksi sinua vastaan ja soveltaa rikoslakia, seksuaalirikoksiin sovellettavaa menettelyä ja alaikäisten suojelua, joten rikoslain **227-22 artiklan, 227-22-1 artiklan, 227-23 artiklan ja 227-24 artiklan mukaan sinua uhkaa 10 vuoden vankeusrangaistus ja 505 000 €** sakko.

Tämä tosiasia julkistetaan, jotta muut ihmiset, jotka haluavat harjoittaa tällaisia käytäntöjä, saadaan estettyä. Et ole tietämätön siitä, millaisia vaikutuksia, jälkiseurauksia tai vahinkoja tällä on elämääsi.

Jos kuitenkin päätät sopia asian tuomioistuimen ulkopuolella, sinun on vastattava tähän sähköpostiviestiin ja kirjoitettava kirje, jossa ilmoitat, että olet päättänyt sopia sakosta, mainitset summan ja allekirjoitat sen. Tämä on skannattava ja lähetettävä vastauksen liitteenä.

Ystävällisin terveisin,

Euroopan poliisin pääosasto, alaikäisten suojelusta vastaava prikaati.

National Cyber Security Centre

INTERPOL

MIKKO MASALININ KANSALLISPOLIISIN
PÄÄLUOTTAMUSMIES /HEAD OFFICE
POLIISITALO 1, PASILANRAITIO 13,00240
HELSINKI

Mtech
Digital Solutions

Phishing-esimerkki - Whalephishing

SERVICE

CJ

Christian Jurvanen <arelllreeazaz@gmail.com>
To Ilomäki Jarkko

Jarkko. I'm having a busy day and I believe I can count on you to keep this confidential. I will be surprising some of the staff with gift cards and I'm appointing you to handle this because it's meant to come as a surprise pending till they receive it, I need you to make an online purchase on my behalf or what local store do you think we have around to make this purchase? I'm considering Google play or Visa gift cards since they can be used anywhere and we can get them almost everywhere.

NOTE: I can't take calls at the moment so email will be fine.

Best Regards
Christian Jurvanen
Chief Executive Officer
Sent from my iPhone

Maksupyyntö

CJ

Christian Jurvanen <christian.jurvnen@mtech.fi>
To Laskutus

Mikä on tilimme saldo? Voimmeko maksaa 53,115 euroa?

Yli 200 000 suomalaisen Linkedin-tietoja vuosi hakkerifoorumille

31.10.2022

F-Secure varoittaa, että tietoja voidaan käyttää esimerkiksi tilitietojen kalasteluun.

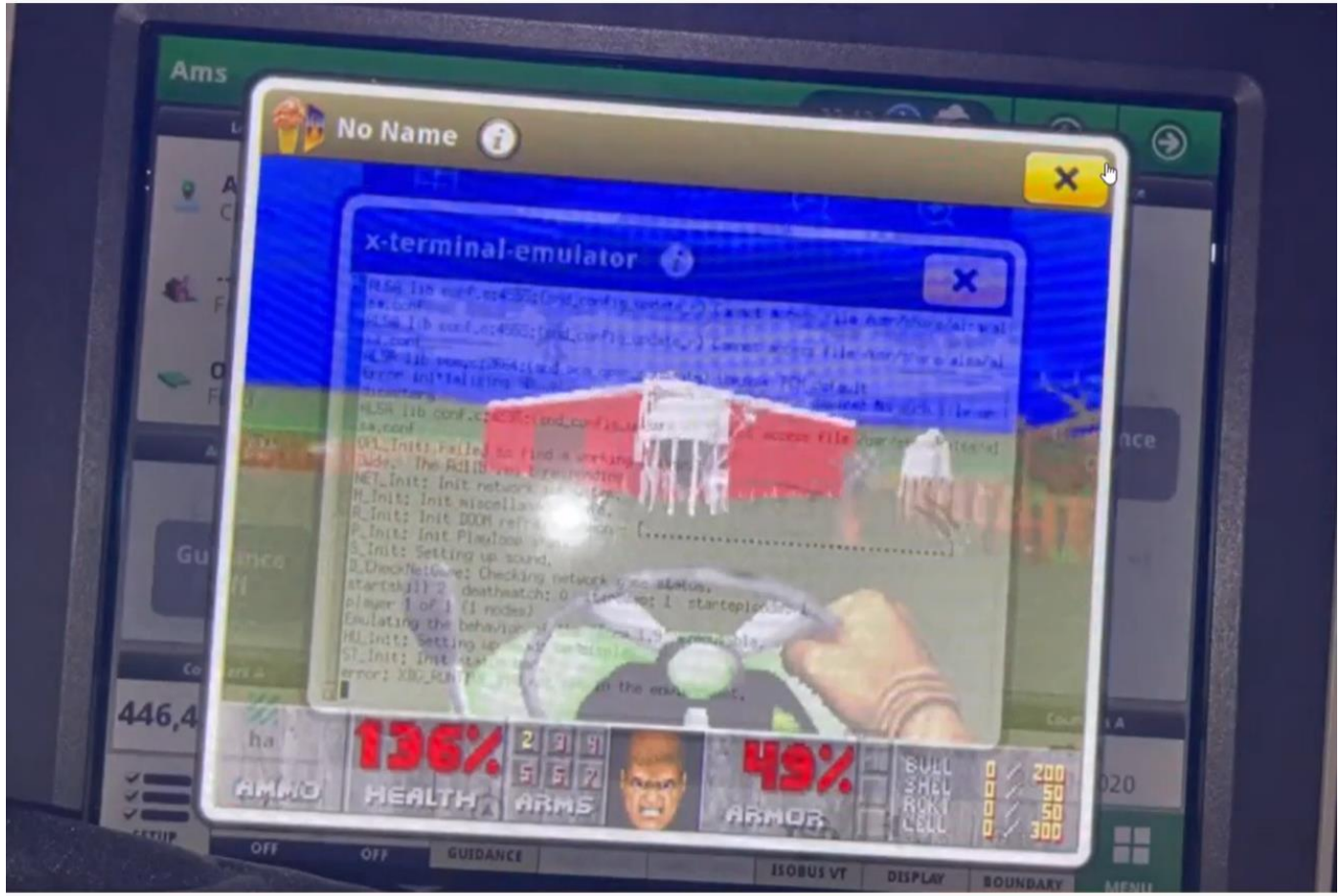
Yli 200 000 suomalaisen Linkedin-käyttäjän tietoja on vuotanut hakkerifoorumille, F-Secure kertoo Twitterissä. Tiedot sisältävät muun muassa nimiä, puhelinnumeroita ja sähköpostiosoitteita.

Tietoja voidaan F-Securen mukaan käyttää kohdennettuun tietojenkalasteluun, jolla hankitaan esimerkiksi tilitietoja tai muita arkaluonteisia tietoja.

Kohdennetussa tietojenkalastelussa rikolliset esiintyvät luotettavina henkilöinä ja huijaukset kohdistuvat tiettyihin henkilöihin tai organisaatioihin, kertoo F-Secure nettisivuillaan.

Linkedin on kiistänyt hakkeroinnin ja yksityisten tietojen vuotamisen, kertoo Cybernews.

Linkedin on sosiaalisen median palvelu, jota käytetään erityisesti työnhaussa ja ammatillisessa verkostoitumisessa.



Sick.Codes-niminen hakkeri esittelee, miten traktorien hallintajärjestelmät ovat haavoittuvia ajamalla JD4240-traktorin hallintakonsolissa Doomia

Lähde: https://www.youtube.com/watch?v=eX86doleFCk

Mtech
Digital Solutions

Suosituksia ja hyviä toimintatapoja

Merkittävin tunnistusmekanismi on edelleen käyttäjätunnus – salasana –pari

Heikkoutena ovat huonot salasanat ja niiden murtamisen helppous

Salasanan pituus	Vain numeroita	Vain pieniä kirjaimia	Isoja ja pieniä kirjaimia	Numeroita, Isoja ja pieniä kirjaimia	Erikoismerkkejä, numeroita ja isoja ja pieniä kirjaimia
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Lähde: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Käyttäjän tunnistus - salasanat

Salasanojen tulee olla riittävän pitkiä ja riittävän useasta komponentista (isot ja pienet kirjaimet, numerot, erikoismerkit) koostettuja

Eri palveluissa tulisi olla eri salasanat, erityisesti yhtään kriittisimmissä palveluissa

Mikäli mahdollista, käytä salasanaa tukemassa myös muita tapoja (Two-Factor Authentication, eli esimerkiksi SMS-viesti kirjautumisen vahvistamiseksi)

Yleisesti ottaen tunnistautuminen on sitä parempaa, mitä enemmän seuraavista asioista edellytetään käyttäjältä:

- Jotain mitä käyttäjä tietää (käyttäjätunnus, salasana)
- Jotain mitä käyttäjä on (sormenjälki, kasvojen tai silmän retinan tunnistus)
- Jotain mitä käyttäjällä on (puhelin - puhelinnumero, erillinen salasanalaite)
- Jotain missä käyttäjä on (erityisesti tarkemmissa järjestelmissä)

Varmuuskopiot

Tietoturvahyökkäysten yksi seuraus voi olla tietojen tuhoutuminen tai muuttuminen virheellisiksi tai käyttökelvottomiksi

Vaikka tiedoilla ei olisi liiketoiminnallista arvoa, niillä voi olla merkittävä tunnearvo (esimerkiksi valokuvat)

On myös ymmärrettävä, että tietokoneiden, puhelinten ja muiden laitteiden hajoamistodennäköisyys on 100%

Varmuuskopioiden avulla tietosi pysyvät tallessa, ja voit siirtää ne tarvittaessa uuteen laitteeseen.

Varmuuskopiot tulee ottaa erilliseen järjestelmään (eivät saa olla esimerkiksi samassa koneessa!) tai esimerkiksi pilvipalveluun

Voit mahdollisesti myös valita palveluntarjoajia, jotka hoitavat tiedon varmuuskopioinnin puolestasi ko. ohjelman osalta

Testaa että varmuuskopiosi toimivat!

Viruksilta, palomuuri, VPN (virtuaalinen yksityinen verkko) tarjoavat perussuojaa monta hyökkäystyyppiä vastaan

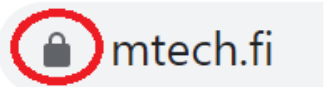
Virustorjuntaohjelma tutkii tietokoneessa olevia ja siinä käsiteltäviä tiedostoja sekä sähköpostiviestejä ja pyrkii poistamaan haitalliset tiedostot tai ilmoittamaan niistä.

Palomuurilla estetään luvaton pääsy juuri sinun verkkoosi ja suljetaan siten useita hyökkäysreittejä

VPN-yhteys piilottaa IP-osoitteesi, joka on yksi sinuun osoittava ”tienviitta” netissä

Näitä löytyy sekä valmisohjelmistoina (osa jopa ilmaisia, osa maksullisia) että laitteistoina (esimerkiksi WLAN-reititin voi sisältää nämä ominaisuudet)

Tietty suomalainen skeptisyys ja maalaisjärki vie pitkälle:

- Jos jokin kuulostaa ja tuntuu liian hyvältä, se on sitä
- Jos saat palkinnon arvonnassa, johon et osallistunut, olet vaarassa
- Yksikään oikea palveluntarjoaja ei kysy salasanaasi
- Vältä julkisten langattomien verkkojen käyttöä
- Älä jätä laitteitasi valvomatta
- Varmista saamasi viestit esimerkiksi nettihaun kautta – pitävätkö osoitteet paikkansa?
- Tarkasta että selaat nettisivuja suojatulla yhteydellä 

- Muista aina vaihtaa ostamiesi laitteiden oletussalasanat!
- Jos tuntematon henkilö aloittaa kanssasi ahkeran viestittelyn, kehuu sinua ja kyselee viattomalta tuntuvia asioita, olet vaarassa!

Yhteenveto

- Huolehdi tunnuksistasi, kenenkään toisen ei tarvitse salasanaasi tietää
- Jos jokin kuulostaa liian hyvältä, se on sitä
- Huolehdi varmuuskopioista ja riittävistä estotoimista
- Jos jokin alkaa mietityttämään, ota yhteyttä

Lisätietoja: jarkko.ilomaki@mtech.fi
https://www.linkedin.com/in/jarkkoilomaki/

Mtech Digital Solutions

Linkkejä lisätietoihin

Kyberopas maatiloille: https://www.minunmaatilani.fi/blogi/kybermaailman-haasteet-ja-mahdollisuudet-maatilan-arjessa-opas-julkaistu/

Liikenne- ja viestintäviraston kyberturvallisuuskeskus: https://www.kyberturvallisuuskeskus.fi/fi

Kodin Turvaopas – Kyberturvallisuus (Suomen Pelastusalan Keskusjärjestö SPEK): https://www.kodinturvaopas.fi/kyberturvallisuus/

SuomiDigi – Digiturvallinen etätyö: https://www.suomidigi.fi/artikkelit/kymmenen-suositusta-digiturvalliseen-etatyohon-ja-vapaa-aikaan

Open Web Application Security Project (OWASP): https://owasp.org/

USA:n kyberturvallisuuskeskuksen sivusto: https://www.cisa.gov/cybersecurity