Kyberturvallisuuskeskus

Kyberturvallisuutta arkeen!

Digi arkeen – neuvottelukunta 28.8.2019

Yksikön päällikkö Jarna Hartikainen

@JarnaHnen

Kyberturvallisuuskeskus

Kansallinen tietoturvaviranomainen, jonka tehtävinä mm.

- **Kerätä tietoa** tietoturvaloukkauksista ja niiden uhkista
- **Tiedottaa** tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta;
- **Selvittää** verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.
- Teleyritysten **tietoturvallisuuden ja varautumisen** valvonta ja ohjaus
- **Järjestelmien ja verkkojen tarkastus ja hyväksyntä**
- **Sähköisen viestinnän yksityisyydensuojaan** liittyvien velvoitteiden valvominen

Tietoturvatehtävien ohjaus ja vastuut yhteiskunnassa

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Viestintäpalvelujen tietoturvallisuus ja varautuminen

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon tietohallinnon varautumisen, valmiuden ja turvallisuuden yleinen ohjaus

Ulkoministeriö Utrikesministeriet

Kansainvälisistä tietoturvavelvoitteista huolehtiminen

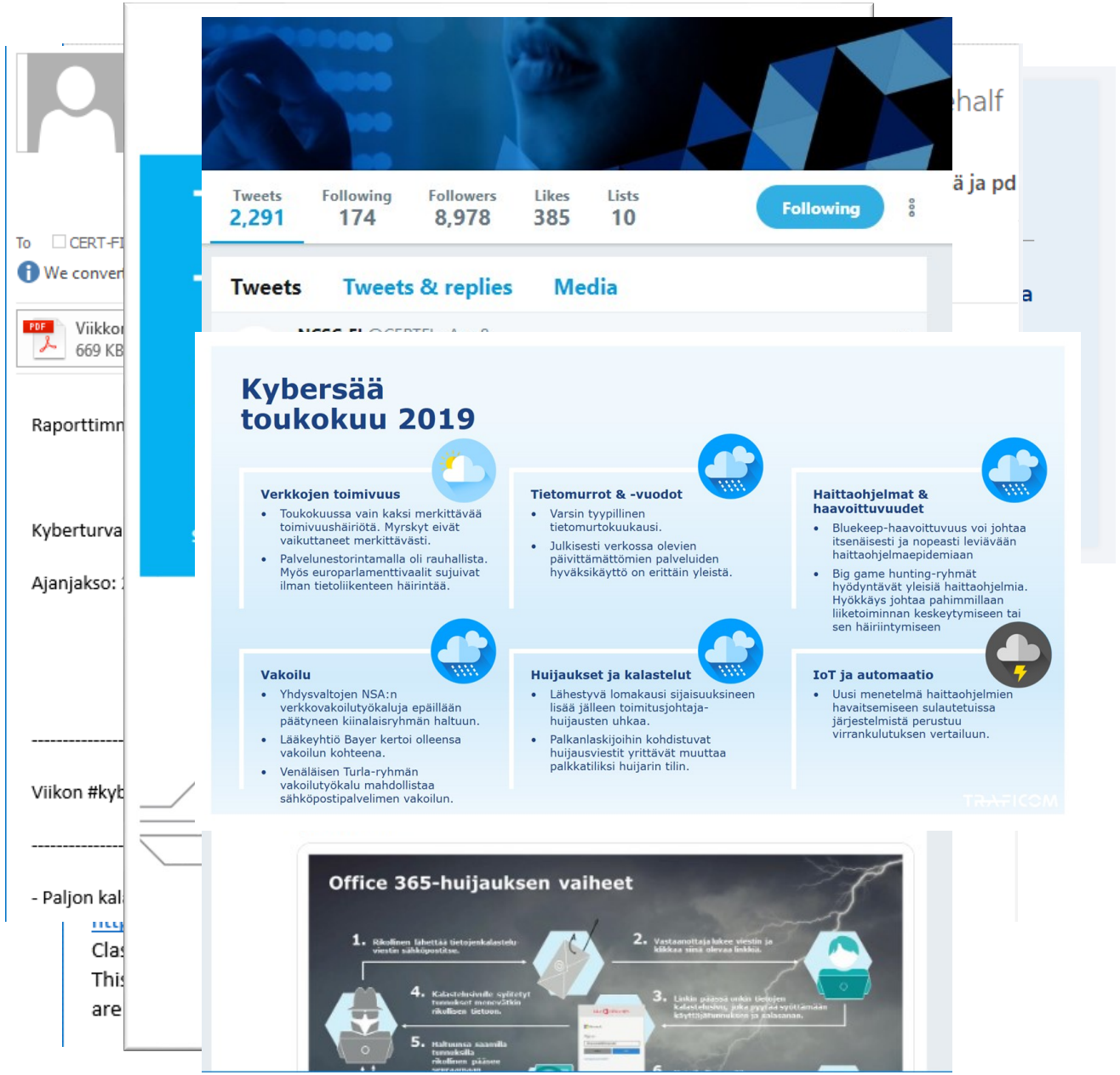
HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

Huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta

Kansallinen kyberturvallisuuden tilannekuva

Tilannekuvatuotteita

- Varoitukset
- Tietoturva nyt! –tiedotteet
- Haavoittuvuustiedotteet
- Uutis- ja haavoittuvuuskooste
- CIP-tiedotteet
- Ohjeet
- SOME: FB, Twitter @certfi
- Kybersää



Koordinointi ja avunanto tietoturvaloukkauksissa

Tarjoamme tarvittaessa **luottamuksellista** apua tietoturvaloukkauksen selvittämiseksi sekä koordinoimme tarvittavia toimenpiteitä.

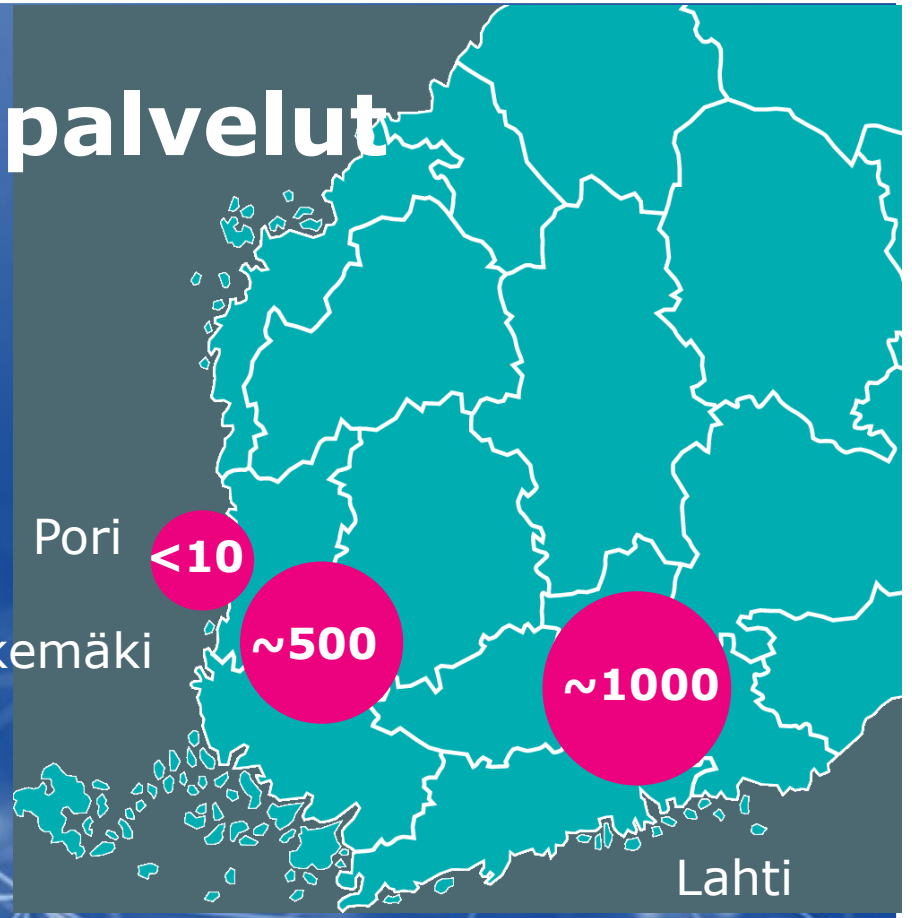
- **Toimenpiteet voivat pitää sisällään muun muassa:**
  - Tiedon jakamista
  - Yhteistyökumppanien ja -verkostojen kontaktointia
  - Teknistä analyysiä
  - Lainopillista neuvontaa

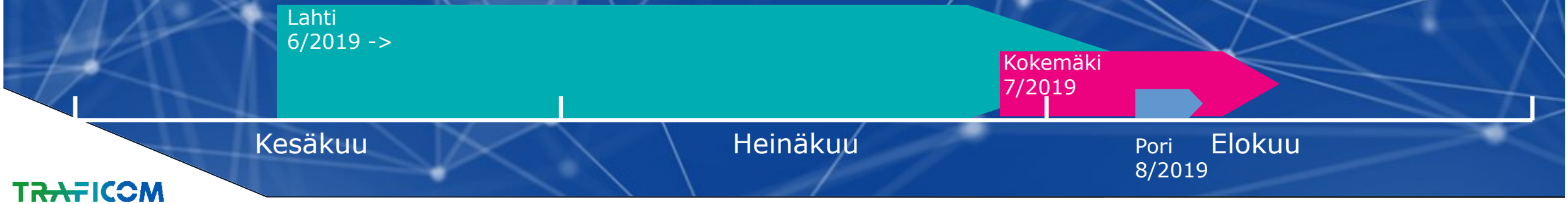
Kyberhyökkäys vaarantaa kuntapalvelut

Lahti - kaupungin koko tietoverkko - vaikutukset
- Terveyden- ja sosiaalihuollon pääsy potilas- ja ajanvaraustietoon
- Laajat vaikutukset kriittisiin palveluihin onnistuttiin estämään
- Korjauskustannukset elokuussa 690 000 €

Kokemäki - kaupungin hallinnon tietoverkko - vaikutukset
- Tietoverkon käyttökelvottomuus esti kunnan päätöksenteon
- Sosiaalihuollon käyttämät sähköiset palvelut pois käytöstä
- Kaupungin maksuliikenne pois käytöstä

Pori - koulujen tietoverkko - vaikutukset
- Käyttäjätilien kautta pääsy oppilaiden tietoihin ja tiedostoihin
- Laajentumisen riski kriittisempiin verkkopalveluihin, identiteettivarkaudet





TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää heinäkuu 2019

Verkkojen toimivuus

- Kolme merkittävää toimivuushäiriötä, mikä on keskimääräistä vähemmän
- Palvelunestohyökkäyksien vaikutukset onnistutaan torjumaan aiempaa paremmin

Vakoilu

- Pohjois-Korean väitetään anastaneen 2 miljardia US dollaria rahoittaakseen kyberhyökkäyksin ydinaseohjelman
- Kiinalaisryhmittymä Winnti on vakoillut vuosien ajan useita saksalaisia korkean teknologian yrityksiä

Haittaohjelmat ja haavoittuvuudet

- Applen iMessage-sovelluksessa useita vakavia haavoituvuuksia
- Mikrosoftin etähallinnan vakava haava (BlueKeep) voi johtaa haittaohjelmaepidemiaan

Tietomurrot ja -vuodot

- Kokemäen kaupungin järjestelmiin kohdistui tietomurto ja kiristyshaittaohjelma
- Tietomurtojen kohteeksi joutuneet organisaatiot määrättiin maksamaan satoja miljoonia euroja uhreille

Huijaukset ja kalastelut

- Lomakausi sijaisuuksineen on näkynyt jälleen lisääntyneinä toimitusjohtajahuijauksina.
- O365-aiheinen kalastelu jatkuu edelleen runsaana ja johtaa onnistuneisiin tietomurtoihin

IoT ja automaatio

- Sääntelyyn herätty Euroopan tasolla
- IoT-laitteiden hyväksikäyttö kohdentuu organisaatioihin, hyödyntäen organisaatioiden kasvaa varjo-IT:tä

Tietoturvailmiöiden riskiarviot, yksityishenkilöt

Huijaukset ja kalastelut

- Pankkitunnuksia ja luottokorttitietoja kalastellaan paljon.
- Huijaukset ja kiristykset hyvin yleisiä.

Palvelunestohyökkäykset

- Murrettuja kotireitittimiä ja muita IoT-laitteita käytetään mm. palvelunesto-hyökkäysten tekemiseen.

Haittaohjelmat & haavoittuvuudet

- Haittaohjelmat tarttuvat nopeasti internetiin turvattomasti kytkettyihin IoT-laitteisiin.

Vakoilu

- Poliittisesti arkaluontoisia aiheita käsittelevät SOME-aktiivit voivat joutua kybervakoilun kohteeksi.

Esineiden internet, IoT

- Yksityisiä tietoja paljastuu verkkoon kytkettyjen, mutta suojaamattomien laitteiden kautta.
- Laitteita hyödynnetään myös bottiverkoissa.

Viestintäverkot

- Digitaalisten palveluiden käyttö kasvaa, silti niiden toimivuudesta ei olla täysin riippuvaisia.
- Lyhyiden häiriöiden sietokyky on hyvä.

= Riski on pysynyt samana vuonna 2018 ▲ Riski on kohonnut vuonna 2018

TRAFICOM

Huijausviesti → kalastelusivu → tietovuoto

From: Apple
To: [redacted]
Sent: Monday, January 02, 2017 4:33 PM
Subject: Apple ID:n salasanan nollaaminen

Hyvä asiakas

Pyysit äskettäin Apple ID:si salasanan nollausta. Suorita prosessi loppuun klikkaamalla alla olevaa linkkiä.

Nollaa nyt >

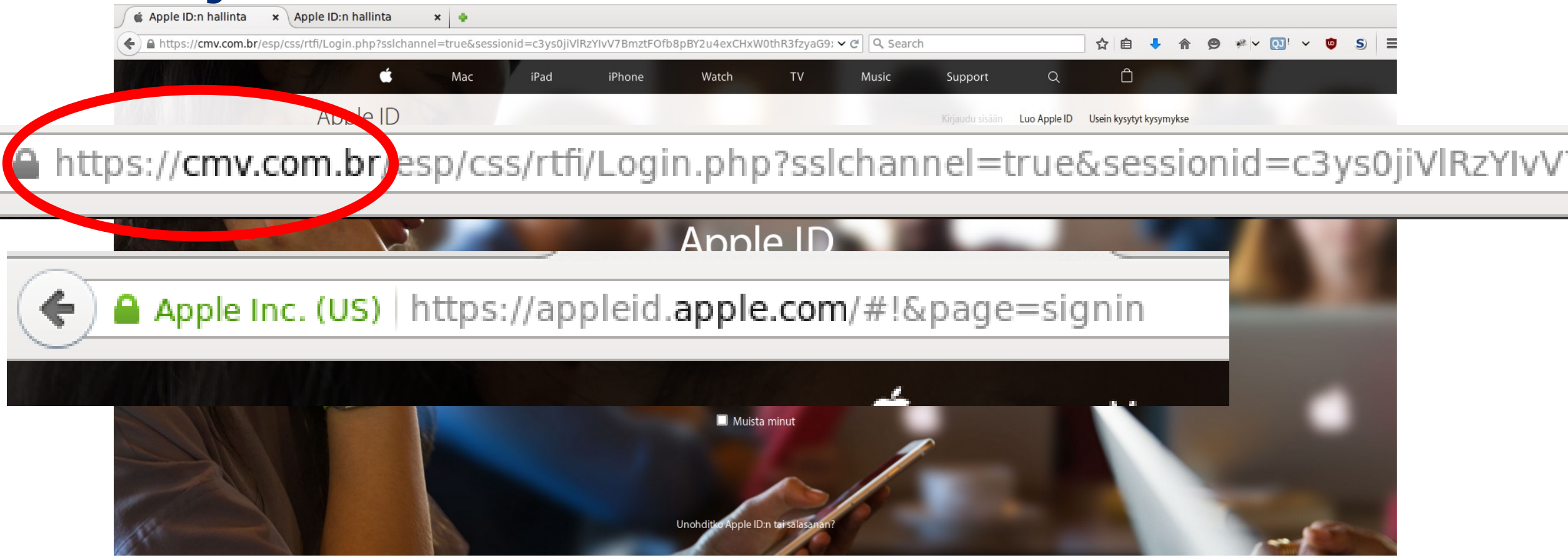
Jos et tehnyt tätä muutosta tai uskot valtuuttamattoman henkilön käyttäneen tiliäsi, click välittömästi osoitteessa appleid.apple.com. Tarkista ja päivitä tilisi turvallisuustiedot kirjautumalla sisään Apple ID.

Ystävällisin terveisin

Apple-tuki

Apple ID | Tuki | Tietosuojakäytäntö
Copyright © 2017

Huijausviesti → kalastelusivu → tietovuoto



Tilisi kaikkia Applen palveluja varten

Yksi Apple ID ja salasana antaa sinulle käyttöoikeuden kaikkiin Applen palveluihin.

Lisätietoja Apple ID:stä ›

Miten tietoturvan tulisi näkyä jokaisen arjessa?

- Mobiililaitteet
- Sovellukset
- IoT-laitteet

Mobiililaitteiden yleisiä turvallisuusohjeita

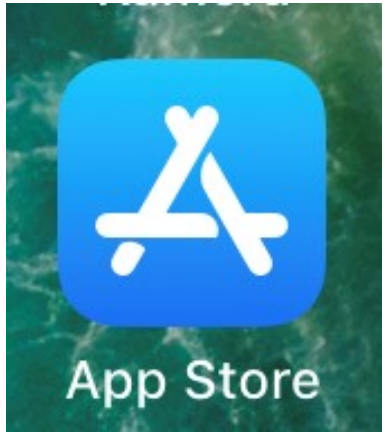
1. Käytä laitteessa suojakoodia
2. Käytä automaattista lukitusta
3. Asenna päivitykset
4. Lataa luotetuista sovelluskaupoista
5. Käytä pilvipalveluita harkiten

+ laitteen asianmukainen poisto ja tietojen hävitys

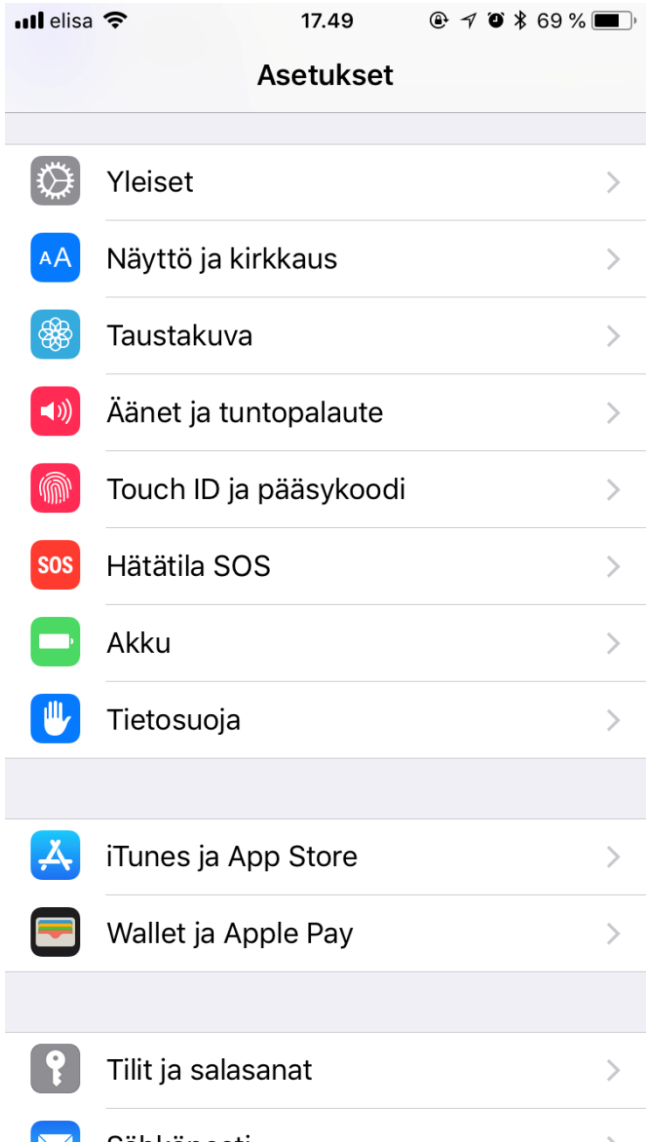
TRAFICOM
Kyberturvallisuuskeskus

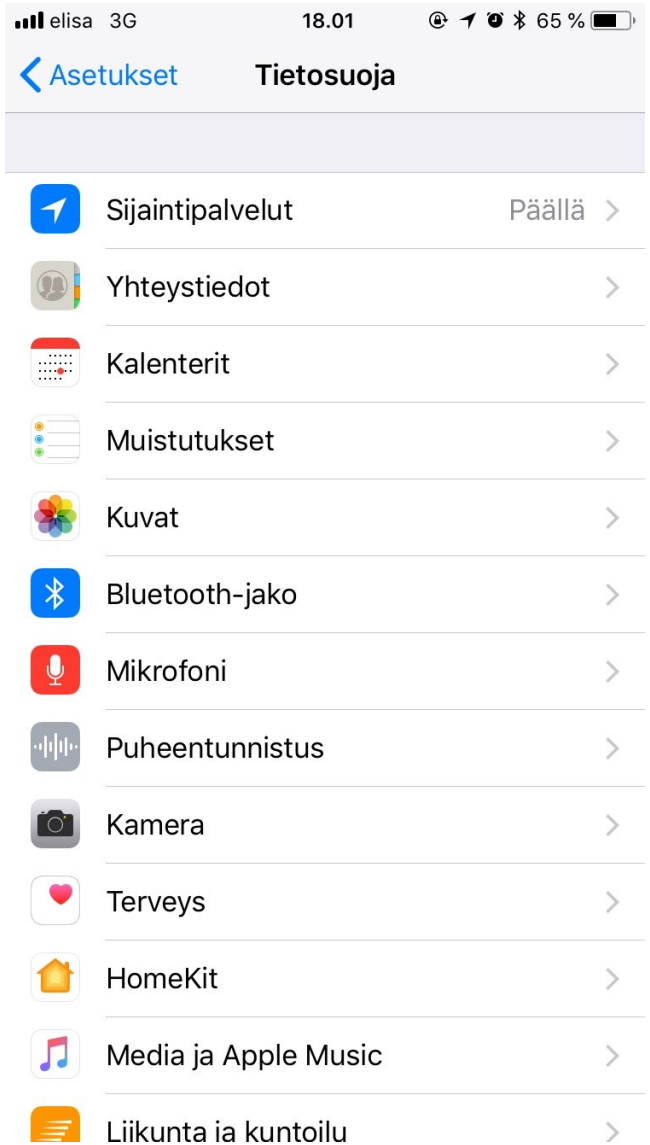
1. Turvallisia käytäntöjä sovellusten käyttöön

1. Lataa vain virallisista sovelluskaupoista
2. Tarkista sovellukset tekijä ja sovelluksen saama palaute
3. Vertaa sovelluksen pyytämiä käyttöoikeuksia sovelluksen toimintaan
4. Tarkista aika ajoin, oikeudet voivat muuttua
5. Ilmaiset sovellukset usein keräävät mainontaan käyttäjätietoja

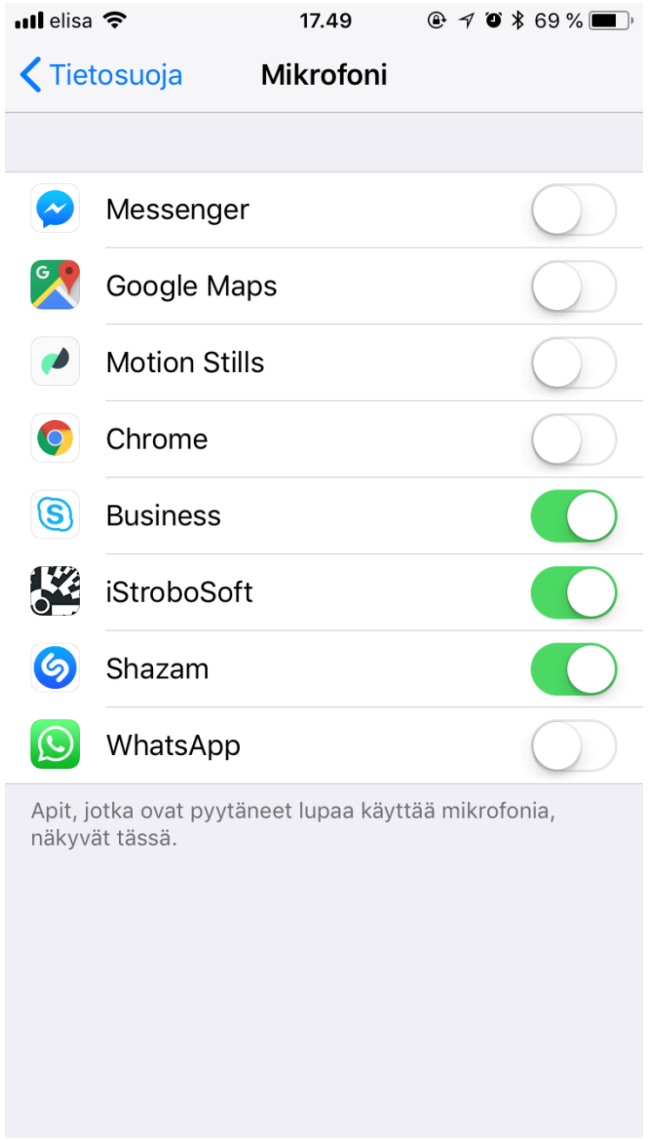


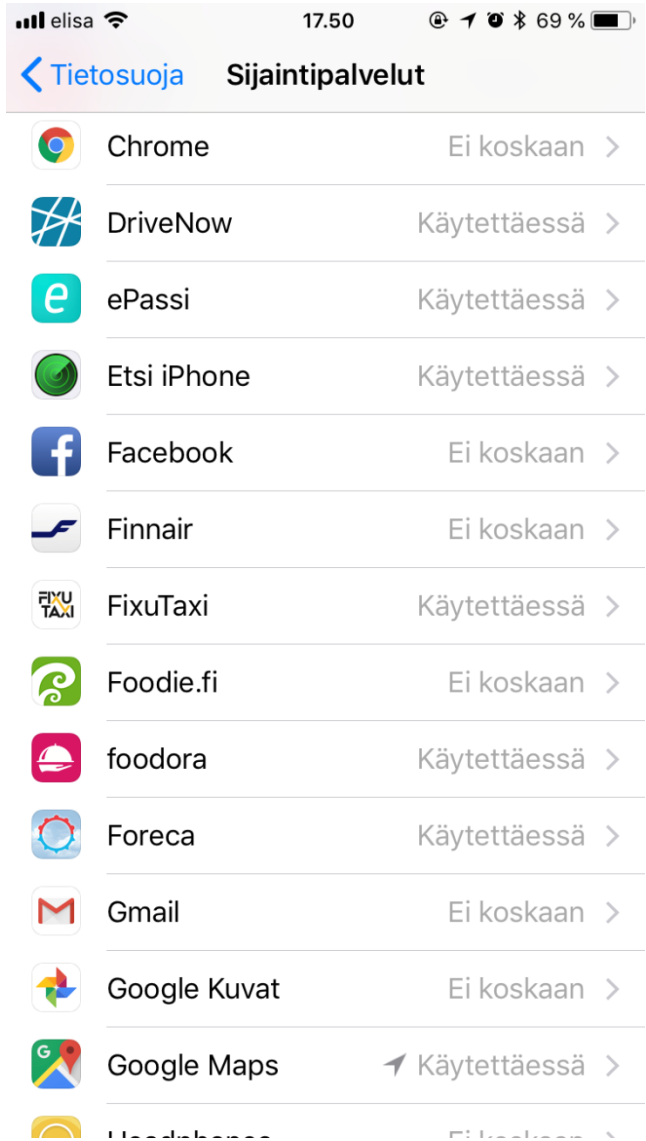
Esimerkki Apple

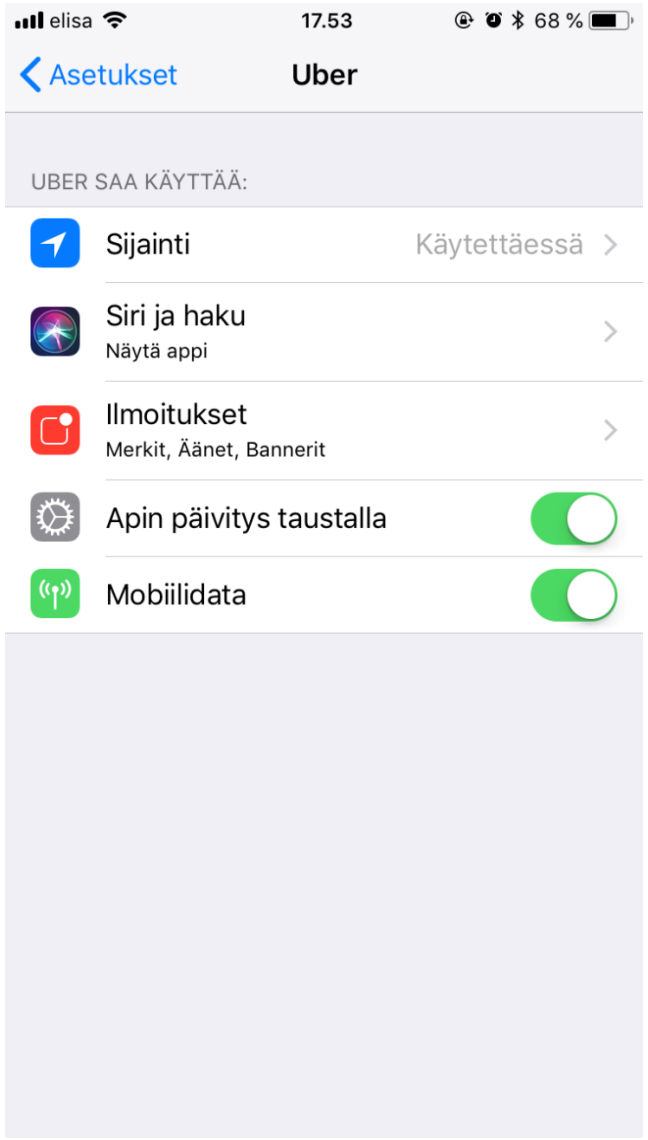




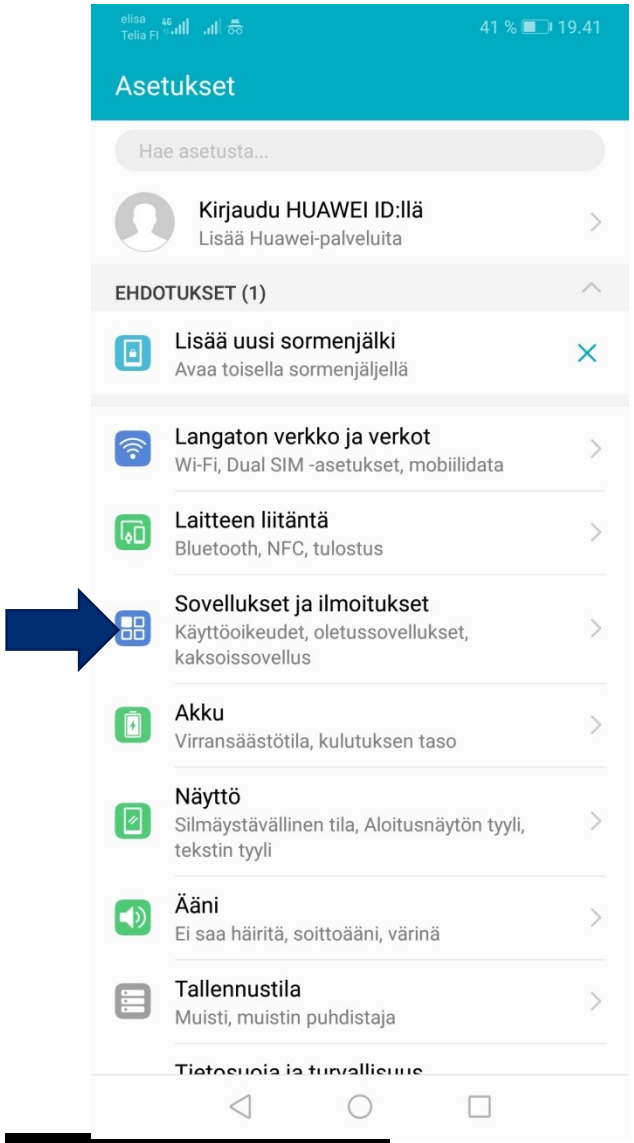
TRAFICOM
Kyberturvallisuuskeskus

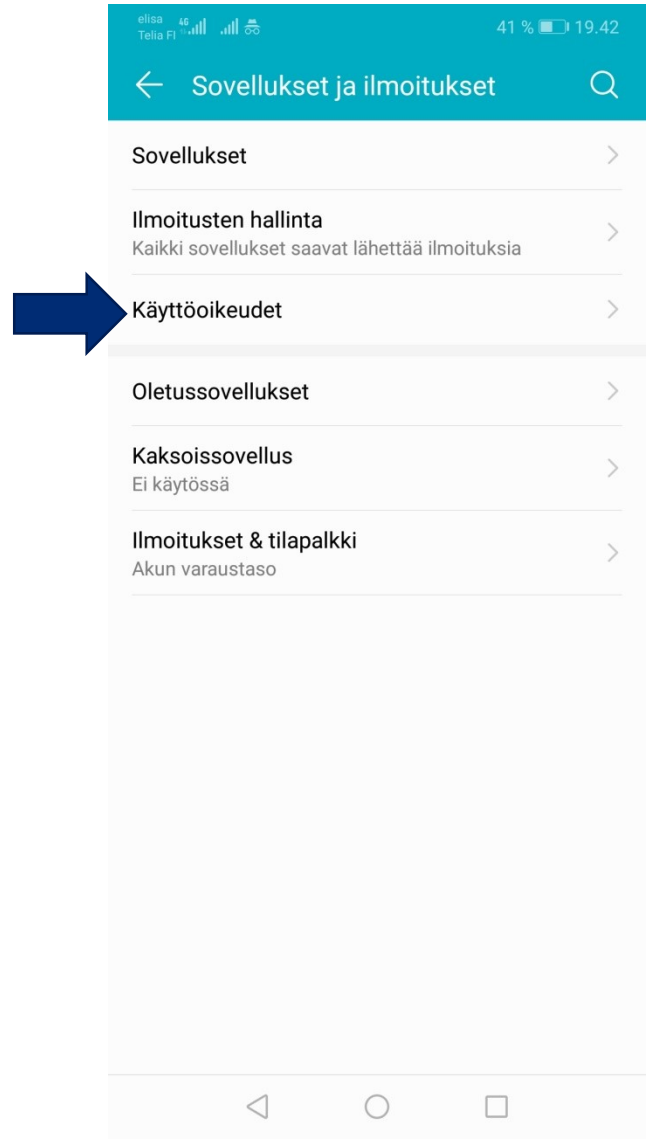

elisa
17.49
69 %
Tietosuoja
Mikrofoni
Messenger
Google Maps
Motion Stills
Chrome
Business
iStroboSoft
Shazam
WhatsApp
Apit, jotka ovat pyytäneet lupaa käyttää mikrofonia, näkyvät tässä.

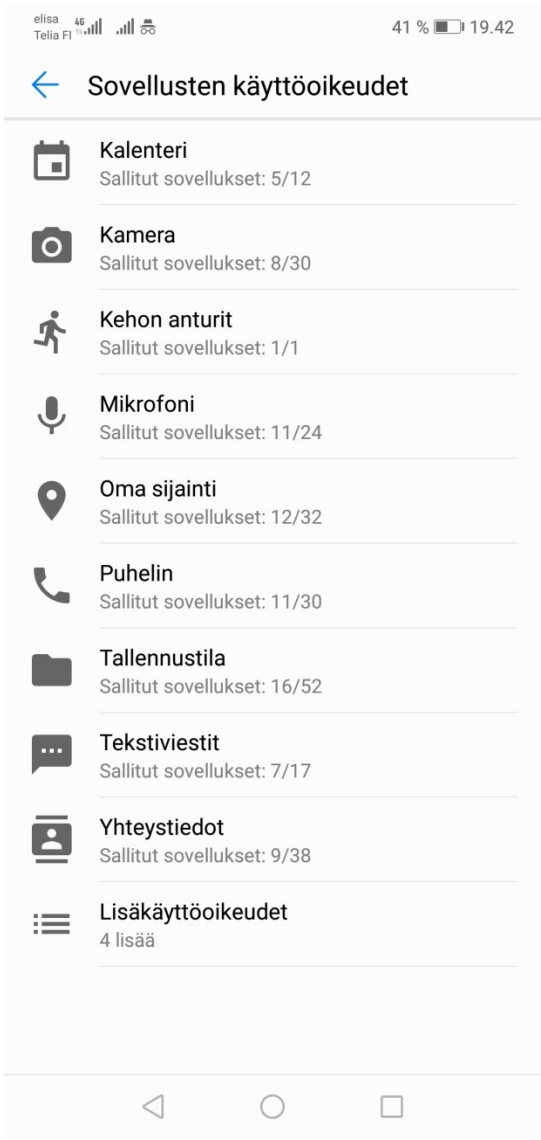

elisa
17.50
69 %
Tietosuoja
Sijaintipalvelut
Chrome
Ei koskaan
DriveNow
Käytettäessä
ePassi
Käytettäessä
Etsi iPhone
Käytettäessä
Facebook
Ei koskaan
Finnair
Ei koskaan
FixuTaxi
Käytettäessä
Foodie.fi
Ei koskaan
foodora
Käytettäessä
Foreca
Käytettäessä
Gmail
Ei koskaan
Google Kuvat
Ei koskaan
Google Maps
Käytettäessä


elisa
17.53
68 %
Asetukset
Uber
UBER SAA KÄYTTÄÄ:
Sijainti
Käytettäessä
Siri ja haku
Näytä appi
Ilmoitukset
Merkit, Äänet, Bannerit
Apin päivitys taustalla
Mobiilidata

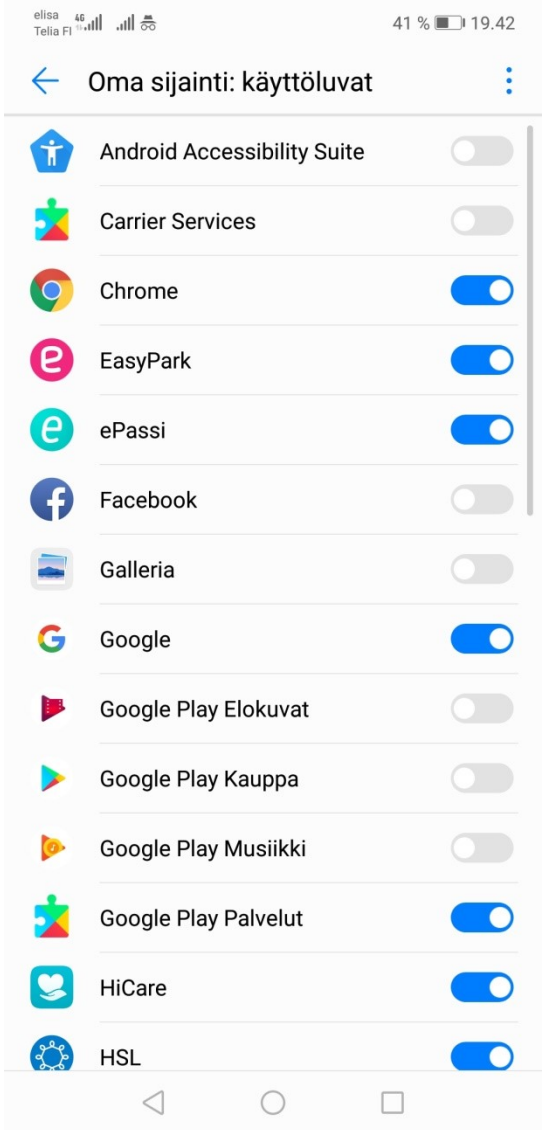
Esimerkki Android

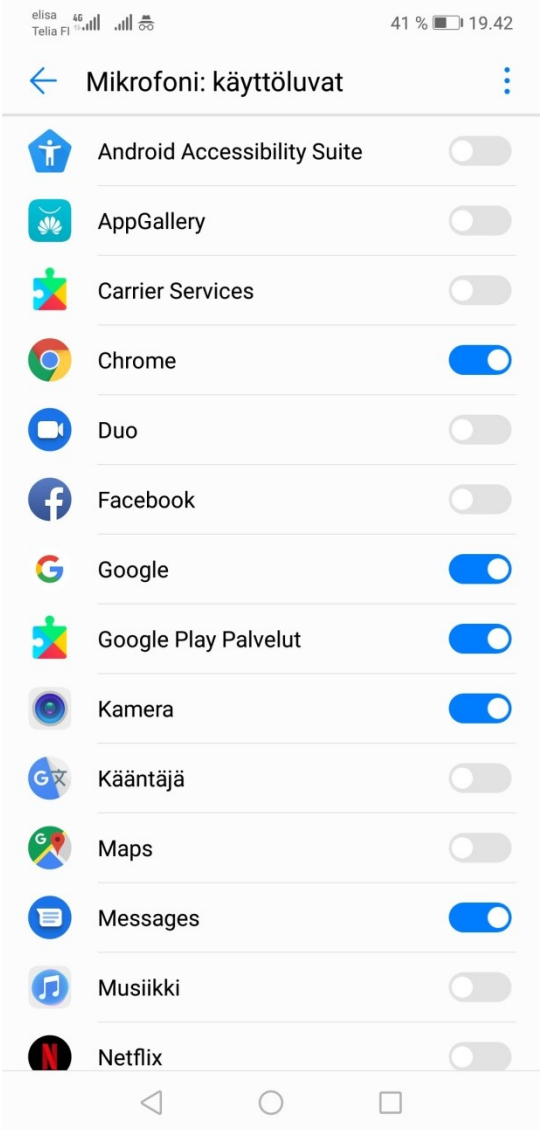






TRAFICOM Kyberturvallisuuskeskus





TRAFICOM
Kyberturvallisuuskeskus

TRAFICOM
Kyberturvallisuuskeskus

Nykykotien IoT-laitemäärät kasvavat räjähdysmäisesti

Kuluttajan huomioitava turvallisuudessa

1. Pääsyoikeudet hallittavissa, eli vaihdettava salasana

2. Tietoturvan elinkaarihallinnassa, eli päivitykset saatavilla

3. Laitteen yhteydet tarkistettavissa, eli mihin laite lähettää tietoja

Lapsille ja vanhemmille puuhatehtävien kera turvallisia vinkkejä nettiarkeen

www.kyberturvallisuuskeskus.fi/fi/ohjeet

Turvalismit tuovat tietoturvan osaksi arkea

Varmuuskopiot ovat kuin suojakerroin. Mitä enemmän, sen parempi.
#turvalismi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

www.turvalistit.fi

TOP 5 uhat ja ratkaisut yksityishenkilölle

UHAT

Rikolliset yrittävät varastaa käyttäjätunnuksesi

Huijaukset ovat internetin arkea

Huonosti suojatut laitteet

Valesovellukset virallisissa sovelluskaupoissa

Verkkopalveluista vuotaa arvokkaita tietoja

RATKAISUT

Älä anna sovelluksille tarpeettomia oikeuksia

Tarkista, onko saamasi viesti liitteineen aito

Salasanaohjelmat ja 2-vaiheinen tunnistautuminen

Suojaudu tietoturva-ohjelmistojen avulla

Tarkista luottokorttilaskusi säännöllisesti

TRAFICOM

Kiitos!

Jarna.hartikainen@traficom.fi

@JarnaHnen

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus