

Älylaitteiden turvallinen käyttö

Jyväskylän seniorit ry
Senioritorstai 11
11.9. klo 14.00 – 15.00
Sepänkeskus
Reaktorisali

Laiteturvallisuus

Ohjelmien asennus

Päivitykset

Laitteiden suojaus

Toiminta internetissä

Reitittimen ja kotiverkon suojaus

Tekoälyhuijaukset

Ohjelmien asennus

- Asenna ohjelmat vain turvallisilta sivustoilta
 - Microsoft Store, Apple Store, Google Play, Laitevalmistaja (Esim. Samsung Store)
- Kun asennat ohjelman jostain muualta, niin tee se mieluiten ohjelmiston valmistajan omalta sivulta. Tai pyri varmistamaan sivun luotettavuus esim. kyselemällä hakukoneella (Google tms.) kokemuksia.
- Ole tarkkana, että asennusvaiheessa ei asenneta myös jotain muuta ylimääräistä. Usein sivuilla on ruksittu valmiiksi tämä ylimääräinen tai ainakin sitä tyrkytetään aktiivisesti.

Päivitykset

- Päivityksiä tulee yleensä vähintään kolmesta eri paikasta
 - Järjestelmäpäivitys laitteen valmistajalta (Microsoft, Apple, Samsung...)
 - Sovellukset l. Apit (Google Play, Apple Store, Samsung Store...)
 - Ohjelmistovalmistajalta (LibreOffice, Firefox...)
- Tarkista päivitykset säännöllisesti ja aseta ne tapahtumaan automaattisesti.
 - Wi-Fi:n kautta päivitys tapahtuu vain kun laite on käynnissä ja liitettyä Wi-Fi verkkoon.
 - Usein päivitykset tehdään kun laite ei ole aktiivisessa käytössä.
 - Jätä siis PC käyntiin silloin tällöin lopetettua työskentelyn koko yöksi.
 - Rajattomalla liittymällä päivitykset voi sallia huoletta mobiilidatalla
 - Ulkomailla, etenkin EU-alueen ulkopuolella, on syytä estää päivitykset mobiilidatalla, sillä se voi aiheuttaa kalliin laskun.

Virustorjunat

- Uusimmat puhelinmallit ja tietokoneet sisältävät nykyään useimmiten sisäänrakennetun virusohjelmiston, joten erillistä ei tarvitse välttämättä ostaa. (Windowsin Defender, Samsung Knox, jne)
- Turvaohjelmistot sisältävät usein jotain muuta, josta voi olla hyötyä. Esim. selaussuojaa pankkiyhteyksillä, salasanojen valvontaa, riskisivustojen valvontaa, jne.
- VPN on hyödyllinen jos käytät avoimia Wi-Fi verkkoja. Mutta kotiverkossa se voi haitata muiden ohjelmien toimintaa.

Puhelimen ja tabletin suojaus

- Lukitus
 - PIN-koodi, salasana, sormenjälki tai kasvojen tunnistus
- SIM-kortin PIN-koodi
 - Joku muu kuin ei mitään tai 0000 tai 1234.
- Varmuuskopio puhelin säännöllisesti
 - Ulkoinen kovalevy, muistitikku, PC tai ilvipalvelu
- Käyttöjärjestelmän versio
 - Jos käytät puhelinta muuhun kuin soittaminen ja tekstiviestit, niin uusi puhelin kun tietoturvapäivityksiä ei enää tehdä käyttöjärjestelmään tai tärkeisiin sovelluksiin (kuten pankki apit tai turvaohjelmistot).
 - Esim. Windows 10 tuki loppuu lokakuussa. Android 9:ssä kaikki apit ei toimi.

PC:n suojaus

- Pidä tietokone lukittuna (PIN, Salasana)
- Käytä palomuuria
- Käytä jotain virustorjuntaohjelmaa. Windows käyttöjärjestelmä sisältää oman hyvän ilmaisen virusotorjunnan (Defender)
- Suojaa käyttäjätili kaksivaiheisella tunnistautumisella
- Älä salli etäkäyttöä kuin omasta aloitteestasi
- Varmuuskopioi säännöllisesti
- Tee kullekin PC:n käyttäjälle oma käyttäjätili, myös vieraille.

Käyttäjätilien Suojaus

- Suojaa käyttäjätilesi (Apple, Google, Microsoft), Facebook, jne kaksivaiheisella tunnistautumisella. Niiden kautta voidaan identiteettitietojasi varastaa.
- Laita tileille palautuksen sähköpostiosoite (eri kuin tilin tunnuksena mahdollisesti käytetty sähköpostiosoite) ja puhelinnumero
- Aseta tileille vaihtoehtoiset sähköpostiosoitteet. Niitä voit tarvita jos varsinainen osoitteen käyttö estyy.
- Sääda tilin mainonta-, sijainninseuranta ja ilmoitusasetukset.
- Kun saat ilmoituksen siitä, että tilillesi on menty tuntemattomalta koneelta, niin käy vaihtamassa tilin salasana. Huomaa, että salasanan vaihtuessa k'joudut kirjautumaan myös muilla laitteillasi tilille (esim. GMAIL) uudella salasanalla.

Ohjelmien luvat

- Kaikki ohjelmat kysyvät lupaa laitteen eri resurssien (kamera, mikrofoni...) ja laitteen sisällön (tiedostot, kuvat, yhteystiedot ...) ja toimintojen (sijainti ...) käyttöön.
- Mieti huolella, mitä lupia sovellus tarvitsee sinun käytössäsi. Esim. navigaattori ei toimi, ellet anna sille lupaa sijainnin käyttöön, mutta ei tarvitse lupaa mikrofonin käyttöön, ellet käytä puheohjausta.

Ilmoitukset, mainokset

- Monet apit ja ohjelmat tunkevat näytölle koko ajan ilmoituksia. Tai sivustot lähettävät mainoksia.
- Ilmoitukset kannattaa asetuksissa sallia vain sinulle tärkeiltä sivustoilta (vero.fi,) apeista (112-appi) ja järjestelmän ilmoitukset.
- Tarjous ja mainosviestit vain niiltä sivuilta joista olet kiinnostunut.
- Spämmiviestien lähettäjiä on lähes mahdotonta estää jos sähköpostiosoitteesi on joutunut niiden lähettäjien listoille.

Oma toimintasi

- Ole huolellinen
- Älä mene tunnistautumista vaativiin palveluihin hakupalvelun tai jostain saamasi linkin kautta vaan kirjoita palvelun osoite itse.
- Älä tartu liian houkutteleviin tarjouksiin
- Käytä maksuissa luottokorttia tai maksupalvelua (Esim. Klarna) suoramaksun sijaan.
- Pyri varmistamaan verkkokauppojen ja palveluiden luotettavuus esim. kyselemällä muiden kokemuksia
- Älä suostu mihinkään yllättäviin pyyntöihin
 - Jos varoitellaan jostain uhasta esim. pankkitilien suhteen, ota yhteys pankkiin tai tutki verkkopankin ilmoitukset
- Älä hyväksy mitään tunnistautumispyyntöjä, ettet itse ole tunnistautumassa
- Älä hyväksy etäohjausohjelmien asennuspyyntöjä, ellet itse ole pyytänyt tukea.

Hakukone, Selain, Appi, Sovellus?

- Selaimen ja Hakukoneiden ero ei usein ole käyttäjille selvä.
 - Hakukone (Google, Bing, Baidu ...) on palvelu, joka hakee internetistä sinne talletettua tietoa ja antaa haun tuloksena linkit löytämiinsä lähteisiin.
 - Selain (Chrome, Safari, Edge, FireFox ...) on yleistyökalu jolla käsitellään internettiin tallennettua sivustoa. Sivusto avataan selaimessa saadun linkin (hakukone) kautta tai sinne mennään selaimen osoitekenttään kirjoitetulla osoitteella (Esim. suomi.fi).
 - Appi on täsmätyökalu jonkin tietyn tehtävän suorittamiseen (esim. pankki appi)
 - Sovellus on johonkin tiettyyn tehtävään suunniteltu ohjelma, yksinkertainen tai hyvinkin monimutkainen (Excel)

Miksi Hakukone on vaarallinen?

- Hakukone listaa löytämänsä tulokset tietyssä järjestyksessä.
- Rikolliset pystyvät ujuttamaan omat sivustonsa hakutuloksen kärkeen (Esim. väärennetyt pankkisivut)
- Ihminen avaa yleensä ensimmäisen tai jonkin heti seuraavista hakutuloksista ja joutuu rikollisen sivuille.
- Älä avaa tärkeitä sivustoja hakukoneen tai muualta saamasi linkin kautta vaan avaa selain ja kirjoita osoite itse.

Selaimen riskit

- Koska selain on yleistyökalu, joudut yleensä tekemään paljon asioita itse. Todennäköisesti teet virheitä (kirjoitat osoitteen väärin, asetukset tehty puutteellisesti...)
- Selain on monimutkainen. Siihen voi asentaa lisäosia. Se vaatii paljon säätöjä. Rikollisten on helpompi keksiä väärikäytön mahdollistavat viat ja heillä on aikaa hyödyntää niitä..
- Selain asennetaan milloin mistäkin. Haavoittuvuudet korjataan usein hitaasti. Korjauksen asennus omalle koneelle tapahtuu käyttäjän toimesta. Kukaan muu ei valvo sitä puolestasi.

Man-In-the-Middle hyökkäys (MITM)

- Yksi yleisimmistä tavoista kaapata luottamuksellisia tietoja tai ryöstää rahaa ihmisten pankkitileiltä
- Tapahtuu kun joudut vaikka Google-haun tai jostain saamasi linkin kautta huijaussivulle.
- Sinun ja pankin välissä toimii tietämättäsi huijari
- Pankkihyökkäyksessä huijari saa kirjautumistietosi ja kirjautuu itse niillä pankkiin
- Kun pankki kysyy vahvistuksia niin huijari välittää pyynnön sinulle
- Kun annat pyydetyn koodin tms. huijari vahvistaa sillä oman tapahtumansa.

Esim:

- Kaappaa tilisi vaikkapa kirjaamalla sinne oman mobiilipankin tai tunnistautumissovelluksen, jonka jälkeen hän voi jatkaa toimintaa tileilläsi ilman sinun mukanaoloa.
- Ohjaa yksittäisen maksun (ehkä suuremmaksi muokattuna) omalle tililleen
- Tunistautuu pankkitunnuksillasi johonkin toiseen palveluun

Miten suojautua MITM hyökkäykseltä

- Älä menee verkkopankkiin koskaan Google-haun perusteella
- Älä tunnistaudu verkkopankkitunnuksilla saamasi linkin takaiseen palveluun.
- Kirjoita verkkopankin osoite aina itse selaimen osoiteriville (tai kirjanmerkki)
- Käytä vain HTTPS-suojattuja verkkosivustoja (lukon kuva).
- Vältä yleensäkin verkkopalveluja, joiden yhteys on suojaamaton.
- Älä koskaan käytä verkkopankkia ilman VPN:ää julkisissa Wi-Fi-verkoissa
- Käytä VPN:ää tunnistautuessa ja etenkin julkisissa Wi-Fi verkoissa silloin kun jaat tärkeitä tietoja.
- Päivitä kaikki laitteet ja ohjelmistot (virusohjelmisto) säännöllisesti
- Käytä monivaiheista tunnistautumista
- Älä koskaan sivuuta selaimen varmennevirheitä
- Käytä muihin kuin pankkipalveluihin tunnistautuessa **Mobiilivarmennetta**. Se toimii myös selaimella operoitaessa.
- Vältä tuntemattomia sähköposteja, viestejä ja linkkejä.

Miksi Appi on turvallisempi

- Täsmätyökaluna Appi on yksinkertaisempi, siinä on vähemmän säätöjä ja sinun ei tarvitse tehdä kaikkea itse, esim. kirjoittaa pankin osoitteita.
- Yhteys pankkiin sisäänrakennettuna, väliin vaikeampi tunkea.
- Google ja Apple valvovat jatkuvasti jakelussa asennettuja Appeja.
- Virheelliseksi todetun Apin käyttöestetään
- Korjaus tulee nopeasti ja automaattisesti, jos laite oikein säädetty.
- Tukevat biometrista (sormenjälki ym.) tunnistautumista.

Tunnistautuminen

- Tunnistaudu pankkitunnuksilla vain pankkiin
- Käytä muualla tunnistautuessa mobiilivarmennetta
 - Häirinnänestokoodilla estät väärinkäytön
 - Älä hyväksy tuntemattomia vahvistuksia (Et ole itse juuri tunnistautumassa vaan puunto tulee yllättäen).
- Kansalaisvarmennetta voi käyttää tunnistautumiseen viranomaisasioinnissa. 2026 alkupuolella koko EU:n alueella
 - Sisätty henkilöllisyyskorttiin.
 - Digi- ja väestötietorekisterintä löytyy enemmän tietoa
 - Hightrust.id apilla kansalaisvarmennetta voi käyttää mobiililaitteissa kuten muita vahvoja tunnistautumisia..

Reititin ja Wi-Fi

- **Reititin (Router)**
 - Tietoverkkoja yhdistävä ja niiden välillä tietoa siirtävä ja reitittävä laite.
 - Reititin on osallisena aina vähintään kahdessa verkossa.
 - Kotona mobiili- ja/tai kiinteä laajakaistayhteys internetiin ja kodin johdotettu tai langaton verkko
- **WLAN** (wireless local area network l. langaton lähiverkko) eli **Wi-Fi**
 - Useimmiten internetiin kytketty reititin toimii tukiasemana eli muodostaa langattoman internet-yhteyden.
 - Lähiverkon alueella sijaitsevat laitteet kuten tietokoneet ja älytelevisiot saavat tällä tavalla internet-yhteyden, johon ne kytkeytyvät usein automaattisesti.
 - Lähiverkkoon kytkeytyneet päätelaitteet voivat olla yhteydessä myös toisiinsa, mikä mahdollistaa joissain tapauksissa tiedostojen salakatselun.
 - Älypuhelin voi toimia reitittimenä muille laitteille. Kun sen mobiiliyhteys jaetaan (hotspot) niin muodostetaan Wi-Fi muiden laitteiden käyttöön

Reitittimen asetukset

- Perusasetukset
 - Vaihda reitittimen oletuskäyttäjänimi ja -salasana.
 - Moni laite käyttää yhä admin/admin tai user/user yhdistelmää. Vaihda heti!
 - Päivitä reitittimen laiteohjelmisto (firmware). (asetta päivitykset tapahtumaan automaattisesti)
 - Käytä vähintään WPA2 (tai mieluiten WPA3) -salausta.
 - Usein yli viisi vuotta vanhoissa reititimissä ei ole tehokasta suojausta
 - Ota käyttöön palomuuuri (jos ei ole päällä oletuksena).
 - Estä etähallinta, ellei sitä oikeasti tarvita.
- Jos mahdollista, luo vieraille ja IoT-laitteille vierasverkko – näin ne eivät pääse samaan kotiverkkoon kuin omat tietokoneesi tai puhelimesi.
 - IoT (Internet of things, esineiden internet). Esim. älyvalaistus, jääkaapit, robotti-imurit.

Wi-Fi:n asetukset

- Vaihda SSID (verkon nimi) – älä käytä mallinimeä (esim. "TP-Link1234"), se voi antaa vihjeen hyökkääjälle.
- Vaihda oletussalasana vahvaksi salasanaksi: Ei "kotiverkko123", vaan esim. "Ruusu\$9!toffee".
- Piilota verkon nimi, jos et halua sen näkyvän kaikille (ei täysin turvaa, mutta hidastaa).
- Poista WPS (Wi-Fi Protected Setup) käytöstä – se on kätevä mutta turvaton oikotie yhdistämiseen.
- Rajaa laiteliikennettä: Joissain reitittimissä voi estää liikennettä MAC-osoitteiden mukaan.

Reitittimen hallinta

- Reitittimen pohjassa, kyljessä tai pakkauksessa on tarra, jossa on mm.
 - Kirjautumisosoite ip (esim: 192.168.8.1) tai http-osoite.
 - Hallintasivun (Website, Admin. User, tms) käyttäjätunnus ja salasana
 - WLAN SSID, joka on WiFi:n oletusnimi
 - WLAN/WiFi key, joka on WiFi:n oletussalasana
- Asetusten muuttaminen:
 - Tutustu laitteen käyttöohjeeseen (termistö ja hallintasivun siältö vaihtelee laitteittain.
 - Kirjaudu laitteella, jolla teet muutokset, oletus sanalla reitittimen WiFiin.
 - Kirjoita reitittimen ip osoite hallintalaitteen selaimen osoitekenttään ja mene hallintasivulle.
 - Anna tarvittavat tiedot (käyttäjätunnus ja salasana)
 - Avautuvalta sivustolta muuta reitittimen nimi, hallinnan ja WiFi:n salasanat. Voit piilottaa WiFi nimen.
 - Aseta salaukseksi WPA2 tai mieluiten WPA3, jos laitteesi tukevat sitä.
 - Estä etäohjaus ja UpnP (Universal Plug and Play, jos niitä ei tarvita) sekä WPS
 - Päivitä laitteen ohjelmisto ja aseta se tapahtumaan automaattisesti.
 - Varmista, että palomuuuri on käytössä.
 - Jos haluat, luo vierasverkko (Quest Network) vieraittesi ja mahdollisten IoT laitteiden käyttöön.
 - Sääda WiFi:n taajuus laitteittesi vaatimaksi (5GHz on nopeampi, mutta vanhemmat laitteet eivät tue sitä, 2.4GHz kantaa pidemmälle.
- HUOM! Kun vaihdat salasanat, yhteys todennäköisesti katkeaa ja joudut kirjautumaan sivulle uudelleen uusilla salasanoilla jatkaaksesi muiden asetusten muuttamista.
- Jos unohdat salasanat, niin reitittimen Reset-napista saat palautettua oletusasetukset ja pääset niillä tekemään asetukset uudelleen

IoT laitteista

- IoT (Internet of things, esineiden internet). Esim. älyvalaistus, jääkaapit, robotti-imurit jne.
 - Vaihda oletussalasanat heti. Etenkin IP-kameroissa ja älylukoissa!
 - Poista tarpeettomat palvelut laitteista (esim. etäyhteydet, jos et niitä käytä).
 - Pidä laiteohjelmistot ajan tasalla.
 - Yhdistä IoT-laitteet omaan aliverkkoon / vierasverkkoon.
 - Jos laite tarjoaa kaksivaiheista tunnistusta tai ilmoituksia kirjautumisista – ota ne käyttöön.
- Vältä halpoja tuntemattomia merkkejä, joista ei saa tietoa päivityksistä tai tietoturvasta.
- Vältä laitteita, jotka vaativat yhteyden epäilyttäviin ulkomaisiin palvelimiin ilman selitystä ja kuvausta toinnasta.
- Hankkiessasi laitteita mieti, että tarvitsetko todella sen internet ominaisuutta.

Tekoäly huijareiden työkaluna 1/3

- Väärennetyt viestit ja sähköpostit (phishing)
 - Tekoälyä käytetään luomaan erittäin uskottavia huijausviestejä:
 - Kielivirheettömät viestit: AI:lla voi tuottaa sujuvaa ja virheetöntä tekstiä, mikä tekee huijausviesteistä ja sivustoista uskottavampia.
 - Personointi: AI voi analysoida julkista dataa (esim. sosiaalisesta mediasta) ja personoida huijauksen uhrin mukaan.
- Deepfake-videoiden ja -äänen luonti
 - Tekoäly voi tuottaa väärennettyjä videoita tai ääntä, jotka jäljittelevät oikeita ihmisiä.
 - Äitihuijaus: Deepfake-ääntä käyttäen voidaan esittää lasta, joka on pulassa ja pyytää siirtämään rahaa.
 - Valehaastattelut tai valeuutiset: Deepfake-videoita voidaan käyttää levittämään väärää tietoa.

Tekoäly huijareiden työkaluna 2/3

- Chatbot-huijaukset
 - Tekoälypohjaisia chatbotteja voidaan käyttää huijaamaan ihmisiä verkossa:
 - Deittihuijaukset: AI voi pitää yllä uskottavaa keskustelua pitkään ja luoda tunnesiteen uhriin.
 - Asiakaspalvelun esittäminen: Väärä "tukibotti" voi pyytää maksutietoja tai kirjautumistunnuksia.
 - Esimerkki: "Olemme havainneet ongelman tililläsi – keskustele asiakaspalvelubottimme kanssa."
- Väärennetyt asiakirjat ja identiteetit
 - Tekoälyllä voidaan luoda realistisia:
 - Henkilöprofiileja, kuten LinkedIn-sivuja tai passeja
 - Tilitietoja ja dokumentteja, joita käytetään identiteettivarkauksissa

Tekoäly huijareiden työkaluna 3/3

- Automatisoitu huijauksen skaalaus
 - Tekoäly voi lähettää tuhansia yksilöityjä huijausviestejä automaattisesti:
 - Kielimallien käyttö massahuijauksissa
 - Tunteisiin vetoava sisältö: AI osaa valita sanat, jotka herättävät pelkoa tai kiireen tunnetta.
 - Esimerkki: "Tilisi suljetaan 24 tunnin sisällä – klikkaa tästä korjataksesi ongelma."
- **Yhteenvetona**
 - **Tekoäly tekee huijauksista:**
 - **Uskottavampia**
 - **Nopeampia tuottaa**
 - **Henkilökohtaisempia**
 - **Vaikeampia tunnistaa**

Miten suojautua tekoälyhuijauksilta 1/2

- Ole skeptinen. Liian hyvä tarjous on lähes varmasti huijausyritys
 - Pysähdy ennen kuin toimit
- Tarkista kieli ja tyyli
 - Tekoäly on nykyään hyvä suomen kielessä, mutta:
 - Huijauksissa voi olla oudon muodollinen tai epäsuomalainen kieli.
 - Nimissä tai allekirjoituksissa voi olla virheitä.
 - Virallinen taho ei käytä uhkailua tai painostusta.
- Älä luota ääneen tai kuvaan sokeasti
 - Nykyään voidaan jäljittää ihmisen ääni ja ulkonäkö todella tarkasti:
 - Jos "tuttu" soittaa ja kuulostaa oikealta mutta pyytää rahaa nopeasti – tarkista jollain toisella tavalla.
 - Älä luota pelkkään ääneen tai videopuheluun – voit kysyä jotain, mitä vain oikea henkilö tietäisi.
- Kaksivaiheinen tunnistautuminen
 - Ota käyttöön kaksivaiheinen tunnistautuminen (2FA) sähköposteihin, some-tileihin ja pankkipalveluihin. Jos joku saa salasanasasi tekoälyn avulla, 2FA estää silti pääsyn.

Miten suojautua tekoälyhuijauksilta 2/2

- Älä jaa liikaa tietoa netissä
 - Tekoäly voi kerätä tietoja eri lähteistä (Facebook, Instagram, TikTok, LinkedIn). Mitä vähemmän henkilökohtaista tietoa näkyy, sitä vaikeampi sinua on huijata uskottavasti.
- Vahvista asiat ennen kuin toimit
 - Jos saat vaikka viestin:
 - "Hei, voitko maksaa nopeasti tämän laskun puolestani?" – Soita ja varmista.
 - Älä klikkaa epäilyttäviä linkkejä tai anna tietojasi ilman tarkistusta.
- Hyödynnä virustorjunta ja selainlaajennukset
 - Hyvät virustorjuntaohjelmat ja selainlaajennukset (esim. tietojenkalastelun esto) voivat auttaa tunnistamaan väärennettyjä sivustoja ja haitallisia tiedostoja.
- Pysy ajan tasalla
 - Seuraa uutisia tai kyberturvallisuussivustoja, kuten:
 - Traficom Kyberturvallisuuskeskus: <https://www.kyberturvallisuuskeskus.fi>
 - Poliisi: <https://poliisi.fi/petosrikokset>
 - Tietotuvayhtiöiden artikkelit: [\\www.f-secure.com\\fi\\articles\\5-phishing-scams-to-avoid](https://www.f-secure.com/fi/articles/5-phishing-scams-to-avoid)

Pysy ajan tasalla digiasioissa

- Senioriapistä löytyy hyviä koulutusvideoita
 - Kirjaudu senioriappiin. Valitse etusivun oikean vasemman yläkulman valikosta (kolme alekkaista viivaa) **Viestintä** ja sen alta **Videot**.
 - Tai käytä linkkiä: <https://senioriappi.senioriliitto.fi/videot>
 - Aiheina mm. Huijaukset, Digiajan taidot ja Älypuhelin ja tabletti
 - **Huom!** Voit mennä senioriappiin myös tietokoneella tai vaikka älytelevisiolla sen internet selaimen kautta ja katsoa videot isommalta näytöltä.
- Verkosta löytyviä sivustoja
 - Seuraa uutisia tai kyberturvallisuussivustoja, kuten:
 - Traficom Kyberturvallisuuskeskus: <https://www.kyberturvallisuuskeskus.fi>
 - Poliisi: <https://poliisi.fi/petosrikokset>
 - Tietotuvayhtiöiden artikkelit: <https://www.f-secure.com/fi/articles>
- Näpäytä ylläolevia linkkejä niin pääset tutkimaan sivustojen sisältöä