Digimaailma – turvaton viidakko, mutta miten siellä voidaan toimia turvallisesti?

Suojelupoliisi ja Kyberturvallisuuskeskus ovat todenneet elokuun lopussa 2025, että kyberturvallisuuden uhkataso pysyy koholla. Myös Poliisi ja Finanssiala kertovat, että kansalaisiin kohdistuva verkkorikollisuus lisääntyy jatkuvasti.

TEKSTI: KIMMO ROUSKU

Suomi sijoittuu kansainvälisissä vertailuissa yleensä kymmenen kärkeen, kun mitataan digitalisaation tasoa ja kansalaisten aktiivisuutta digipalveluiden ja -laitteiden hyödyntämisessä. Samanaikaisesti digimaailmaan kohdistuvat globaalit uhat kasvavat.

Arvioni mukaan suomalaiset menettävät vuosittain 300–500 miljoonaa euroa verkkorikollisille. Koska kaikki rikokset eivät päädy viranomaisten tietoon, perustuu arvio muiden maiden lukuihin: esimerkiksi Saksassa ja Ranskassa summan arvioidaan olevan 6–7 miljardia euroa. Miten tähän tilanteeseen tulisi reagoida? Kuinka voimme varmistaa tietojemme ja palveluidemme turvallisuuden?

Ketkä meitä uhkaavat?

Digimaailmassa suurimmat uhat tulevat verkkorikollisilta ja harvemmin, mutta joissakin tapauksissa, valtiollisilta toimijoilta.

Rikolliset tavoittelevat taloudellista hyötyä, kun taas valtiolliset toimijat pyrkivät hankkimaan salassa pidettävää tietoa valtioidensa etujen ajamiseksi ja tiedusteluun.

Kansalaisia uhkaavat erityisesti verkkorikolliset, jotka yrittävät päästä pankkitileille, maksujärjestelmiin tai saada haltuunsa luottokorttitietoja. Heitä kiinnostaa myös muu taloudellisesti arvokas tieto tai aineisto, jota voidaan käyttää kiristykseen.

Lisäksi 2020-luvulla olemme kohdanneet uudenlaisia uhkia: informaatiovaikuttamista ja organisaatiotasoista häirintää. Niiden avulla ulkopuoliset toimijat, usein valtiolliset, pyrkivät vaikuttamaan yksilöiden kautta koko yhteiskuntaan, esimerkiksi horjuttamaan luottamusta, manipuloimaan tunteita ja ohjaamaan keskustelua tai jopa päätöksentekoa.

Nämä ilmiöt kuuluvat hybridivaikuttamisen pelikirjaan, jossa digitaalisten keinojen rinnalla hyödynnetään myös sotilaallisia, poliittisia ja taloudellisia vaikuttamismuotoja.

Me ihmiset olemme haavoittuvaisia

Edellä kuvatut uhat olisivat vähemmän vakavia, jos me ihmiset emme omalla toiminnallamme tekisi niitä mahdollisiksi.

Organisaatiotasolla ongelma voi syntyä siitä, että jokin laite jää päivittämättä tietoturvakorjauksella, jolloin hyökkääjä pääsee sisään. Käyttäjinä saatamme kiireessä klikata väärää linkkiä ja mahdollistaa sitä kautta esimerkiksi oman sähköpostitilin kaappauksen hyökkääjälle. Moni on myös vahingossa lähettänyt sähköpostilla luottamuksellista tietoa väärille vastaanottajille.

Yhä useamman vakavan tietomurron taustalta löytyy ohjelmistohaavoittuvuus: ohjelmoijan koodiin jäänyt virhe tai bugi mahdollistaa hyökkäyksen. Kaikissa näissä tapauksissa taustalla on ihminen – **inhimilliset erehdykset tekevät meistä haavoittuvia**.

Toistaiseksi emme voi vielä syyttää tekoälyä, koska sen toiminta pohjautuu meidän ihmisten toimintaan ja tuottamaan dataan. Mutta tulevaisuudessa tekoälypalveluiden kehittyessä, niistä alkaa kehittymään entistä itsenäisempiä, ihmisten toiminnasta riippumattomia kokonaisuuksia.

Miten hyökkäykset kohdistuvat meihin?

Verkkorikolliset ja muut vihamieliset toimijat käyttävät hyväkseen kaikkia laitteitamme ja palveluitamme. Hyökkäyksiä kohdistetaan muun muassa:

- sähköpostiin
- puheluihin
- tekstiviesteihin
- WhatsAppiin, Messengeriin ja muihin pikaviesteihin
- verkkosivuilta ponnahtaviin ilmoituksiin
- sosiaalisen median kanavien yhteydenottoihin

>>

Miten me käyttäjät voimme toimia turvallisemmin?

1. **Opettele tunnistamaan linkkiin liittyvä suomalainen nettiosoite.** Jos viranomaisen tai finanssialan toimijan nettiosoitteessa EI OLE **.fi** tai **.fi/osoitejatkuu**, se on erittäin todennäköisesti väärennetty. Älä klikkaa sellaisia linkkejä!
2. **Käytä laadukkaita, yksilöllisiä salasanoja ja salasananhallintaohjelmaa.** Salasanan hallintaohjelma poistaa kiusauksen kierrättää salasanoja ja katkaisee tietovuodon ketjun. Jokaisessa palvelussa pitää olla ainutkertainen salasana.
3. **Ota monivaiheinen todennus (MFA) kaikkiin tärkeisiin palveluihin.** MFA vaikeuttaa merkittävästi tilikaappausta, vaikka salasanasi vuotaisi.
4. **Pidä laitteet ja sovellukset automaattisesti ajan tasalla.** Päivitykset paikkaavat haavoittuvuuksia ennen kuin rikolliset ehtivät hyödyntää niitä.
5. **Pysähdy ennen klikkausta: arvioi viestit, linkit ja liitteet kriittisesti.** Suurin osa hyökkäyksistä alkaa sosiaalisella manipuloinnilla, ei tekniikalla.
6. **Maksa kaikki nettiostokset luottokortilla.** Tällöin digihuijauksissa ja muissa ongelmatapauksissa vastuu selvittämisestä on luottokorttiyhtiöllä.
7. **Asenna sovelluksia vain virallisista kaupoista ja tarkista pyydetyt oikeudet.** Luotetut lähteet ja rajatut oikeudet pienentävät haittaohjelmien ja tietovuotojen riskiä. Opettele tarkistamaan älylaitteesta, mitkä sovellukset saavat käyttää laitteen kameraa, mikrofonia, kuvia, tiedostoja ja yhteystietoja.
8. **Varmuuskopioi tärkeät tiedot 3–2–1-periaatteella (3 kopiota, 2 mediaa, 1 pilvessä).** Hyvä varmistus palauttaa arjen nopeasti myös laiterikon tai varastamisen jälkeen. Esimerkiksi älylaitteen tai tietokoneen ohella ulkoinen usb-kovalevy tai muistitikku ja pilvipalvelu.
9. **Opettele, miten voit etälukita tai paikantaa älylaitteeseesi toisella laitteella.** Jos laitteesi häviää tai varastetaan, voit yrittää paikantaa laitteen ja tarvittaessa tyhjentää sen sisällön etänä.
10. **Lukitse laitteesi PINillä/biometrialla ja käytä lyhyttä automaattilukitusta.** Nopea näyttölukko estää luvattoman käytön arjen tilanteissa, jos älylaite unohtuu tai se katoaa.
11. **Käytä suojattuja verkkoja; vältä avoimia Wi-Fi-verkkoja tai käytä VPN:ää.** Salaamaton verkko altistaa liikenteen urkinnalle ja istuntojen kaappaukselle.
12. **Jaa harkiten: säädä some- ja palveluiden yksityisyysasetukset minimiin.** Vähäisempi julkinen tieto heikentää huijausten kohdennusta ja identiteettivarkauksia.
13. **Keskustelkaa digimaailman ilmiöistä perhe-, suku- ja kaveripiirissä.** Mitä enemmän näistä ikävistä ilmiöistä avoimesti keskustellaan ja jaetaan tietoa, sitä helpommin niitä voidaan tunnistaa ja reagoida.
14. **Laadi oma ”mitä jos” -toimintasuunnitelma häiriötilanteille.** Tiedät heti, miten toimia (korttien sulku, salasanat, tuplavarmistukset, ilmoitukset), jolloin vahinko jää pieneksi. Muista Suomi.fi-ohje: https://www.suomi.fi/oppaat/tietovuoto
15. **Kuka tahansa voi joutua digihuijatuksi!** Itse olen menettänyt kolme kertaa rahaa digihuijauksen takia. Ja syynä ei ole se, että olisin tyhmä vaan se, että verkkorikolliset ovat niin hyviä! Vaikka olen puhunut ja kouluttanut näistä asioista 25 vuotta niin tiedän, että neljäs kerta on varmaan oven takana.

Olennaista on pysähtyä ja miettiä: kuka haluaa sinun klikkaavan linkkiä ja miksi? Jos itse käynnistät asioinnin esimerkiksi verkkokaupassa, maksaminen on luonnollista. Mutta jos saat yllättäen tekstiviestin ”maksa lasku”, on syytä olla poikkeuksellisen varovainen.

Organisaatioiden tietoturva ei ole ”rakettitiedettä”

Tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaamisen perusperiaatteet ovat pysyneet samoina koko 2000-luvun. Niiden merkitys on kuitenkin kasvanut: tänään palveluiden on oltava käytettävissä 24/7/365 ja niihin on voitava luottaa.

Suomessa astui voimaan 8.4.2025 kyberturvallisuuslaki ja NIS2-direktiivin mukaiset velvoitteet. Ne koskevat kriittisiä palveluntarjoajia, ja kyseessä on merkittävä EU-tason parannus, joka nostaa turvallisuuden tasoa myös Suomessa.

Vaikka organisaatio ei itse kuuluisi velvoitteen piiriin, sen käyttämät palveluntarjoajat ja alihankkijat todennäköisesti kuuluvat. Näin yhä useampi organisaatio hyötyy eräänlaisesta ”digiturvan laumasuojasta”. Suosittelen kaikkia tutustumaan Kyberturvallisuuskeskuksen erinomaiseen NIS2-sivustoon. ■

Kimmo Rouskulla on yli 40 vuoden kokemus digitalisaation hyödyntämisestä toiminnan uudistamisessa ja turvallisuuden kehittämisessä, ja hän on pitänyt urallaan yli 5000 koulutusta ja esitystä. Hänellä on ainutlaatuisen monipuolinen kokemus ICT-palvelutuotannon ja kyberturvallisuuden johtamis- ja asiantuntijatehtävistä, sekä operatiivisesta "kädet savessa", että hallinnollisesta työstä, joista viimeiset 30 vuotta hän on työskennellyt valtionhallinnon näköalapaikoilla.

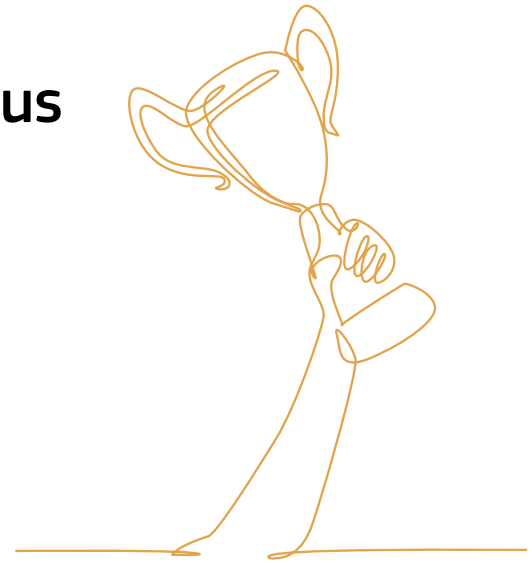
Kuva: Rousku/OpenAI ChatGPT.

Tällä hetkellä Kimmo toimii Digi- ja väestötietovirastossa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) pääsihteerinä sekä Tietoturva ry:n hallituksen varapuheenjohtajana. Lisäksi saatat törmätä hänen kirjoituksiinsa verkkorikollisuuden syövereistä IT-Kimmona, joissa hän pyrkii avaamaan, miten hän on tullut itse digihuijatuksi sekä miten verkkorikolliset toimivat käytännössä ja kuinka organisaatiosi tai sinä voit näiltä suojautua. Tämän ohella hän käyttää apunaan #Ai-Kimmoa, digitaalista tekoälykaksostaan.

Jos käytät LinkedIn-palvelua, liity hänen verkostoonsa: https://www.linkedin.com/in/kimmorousku/

https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi

Kimmo Rouskulle Tietoturvan suunnannäyttäjä 2025 -tunnustus



Traficomin Tietoturvan suunnannäyttäjä tunnustus myönnettiin keväällä 2025 Kimmo Rouskulle esimerkillisestä tietoturvaa edistävästä työstä. Tunnustus jaettiin nyt yhdeksättä kertaa.

Tieto on ainoa pääoma, joka kasvaa jaettuna

– Kimmo Rouskun laajat verkostot ja aktiivinen osallistuminen ovat tehneet hänestä alansa keskeisen vaikuttajan. Hänen työstään välittyy vilpitön halu suojella kansalaisten ja yhteiskuntamme digitaalista arkea. Tällä tunnustuksella osoitamme kiitoksemme hänen pitkäjänteisestä ja esimerkillisestä toiminnastaan kyber- ja digiturvallisuuden hyväksi Suomessa, Traficomin pääjohtaja **Jarkko Saarimäki** kertoi tunnustuksen perusteluista.

Tiedon jakaminen tukee yhteiskunnan eri sektorien kyberuhkiin varautumista ja vastaamista. Tämä varmistaa osaltaan sen, että Suomi on jatkossakin hyvin varautunut kyberuhkia vastaan.

– Kiitän Traficomia tästä merkittävästä tunnustuksesta, joka osuu erityisen sopivasti juuri nyt, kun juhlistan 40-vuotista uraani. Matkani on kulkenut ATK:n alkuvaiheista aina nykyiseen turvallisuus-, teknologia- ja tekoälytietoisuuden ja osaamisen kehittämiseen. Me suomalaiset saatamme toisinaan aliarvioida vahvuutemme, mutta yhteistyö ja verkostot ovat voimamme. Silti aina on varaa parantaa! Tervetuloa verkostoitumaan kanssani muistaen, että tieto on ainoa pääoma, joka kasvaa jaettuna – ja muuttuu samalla viisaudeksi. Eikä tähän tarvita tekoälyä, **Kimmo Rousku** muistuttaa.