PROJECART

Kuinka meitä huijataan verkossa

- Mitä se tarkoittaa?
- Miten ihmisiä huijataan?
- Miten se on mahdollista?
- Miten sitä vastaan voi toimia?

©Harri Lähdesmäki

Verkkorikollisuus on varastamista



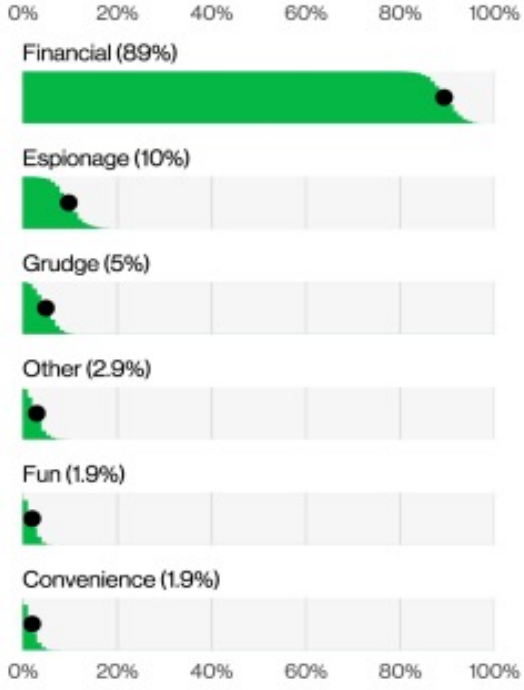
Suomalaisia yritettiin huijata 148,0 miljoonan euron edestä vuonna 2025. Vastaava luku vuonna 2024 oli 107,2 miljoonaa euroa. Oikeat luvut ovat todennäköisesti tätä suurempia*. Kumulatiivisesti 400 000 suomalaista menettänyt rahaa verkkorikollisille.

Taulukko: https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-huijata-148-miljoonaa-euroa-vuonna-2025/
Miksi verkkorikoksia jää pimentoon: * https://www.cybersecurityintelligence.com/blog/cybercrime-victims-rarely-report-incidents-8782.html
https://www.threatmark.com/why-underreporting-holds-back-fraud-prevention/
Suomalaisten digitaalinen luottamus: https://dvv.fi/-/tuore-tutkimus-digitaalinen-luottamus-vahvistuu-vaikka-suurin-osa-suomalaisista-kohtaa-digihuijauksia

©Harri Lähdesmäki

Verkkorikollisten kaikkein suurin motiivi on raha

Maailmanlaajuisesti kyberrikollisuuden on arvioitu olevan **1 200 miljardin euron** liiketoimintaa*
Arvon odotetaan nousevan 11 900 miljardiin euroon vuoteen 2028 mennessä**



Vertailuna: Suomen valtion budjetti vuodelle 2027 on 92,5 miljardia euroa

Verkkorikollisuus ei enää edellytä vahvaa tietoteknistä osaamista. Ohjelmia ja materiaaleja voi ostaa kuka tahansa ja kokeilla niiden käyttöä ilman kokemusta**.

Rikollisuus on nykyään entistä enemmän järjestäytynyttä. Myös valtiolliset toimijat*** ovat aktiivisia, erilaisin tarkoitusperin.

Mitä kyberrikollisuus on, katso esim:
https://www.youtube.com/watch?v=n4_tSbsl5DI

Lanteet:

- Taulukko: Verizon Data Breach investigations report 2023
- * ETN-lehti ja https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/
- ** https://www.bleepingcomputer.com/news/security/police-shut-down-reboot-of-crimenetwork-marketplace-arrest-admin
- ***esimerkki: How to Spot a Russian Deepfake | Bloomberg Investigates https://www.youtube.com/watch?v=X9GQiouEdJ8&t=97s
- **** https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

©Harri Lähdesmäki

Sosiaalinen media ja verkkorikollisuus

- Sosiaalinen media toimii nykyään **kyberrikollisuuden keskeisenä kiihdyttimenä, tiedonkeruualustana ja jakelukanavana**.
  - Alustojen suunnaton suosio, käyttäjien sinisilmäisyys ja verkostojen sisäänrakennettu luottamus tekevät niistä ihanteellisen maaperän digitaalisille rikollisille.
- **SUOMALAISET** kohtaavat paljon huijauksia sosiaalisessa mediassa.
  - Yleisin kokemus on epäilyttävän linkin klikkaaminen, mitä on tehnyt 28 prosenttia suomalaisista.
  - Toiseksi yleisin on keskustelu somessa mahdollisen huijarin kanssa, mitä on tehnyt 14 prosenttia vastaajista, kertoo OP Pohjolan kyselytutkimus.

- *“Huijarit saavuttavat somessa valtavan volyymin huijauksilleen. Somessa kannattaa muistaa olla riittävän epäilevä, jotta tunnistaa huijauksen. Epäilyttävä keskustelu kannattaa lopettaa eikä jatkaa eteenpäin linkistä”*, OP Pohjolan petostorjunnan asiantuntija **Adriana Jakimova** sanoo tiedotteessa.

Ilta-Sanomat 31.8.2026 Henrik Kärkkäinen

https://www.is.fi/digitoday/tietoturva/art-2000012242660.html

©Harri Lähdesmäki

Onko tekoäly todellinen uhka?

Lyhyt vastaus: on.

- Hyödynnetään jo nyt hyvin laajamittaisesti ja kehitys on erittäin nopeaa
- Käytössä sekä hyökkäyksissä että niiden torjunnassa
- Tehostaa perinteisiä huijauksia sekä suoria hyökkäyksiä
- Uhat kasvavat merkittävästi kun käytetään tekoälyagentteja*
- Agenttien kontrollointi nousee haasteeksi, esim. OpenAI ja Huggingface tapaus*

*https://www.redwoodresearch.org/research/hugging-face-incident?utm_source=chatgpt.com#core-takeaways-about-this-incident

©Harri Lähdesmäki

Tekoäly varastamisen välineenä

AI teknologiat parantavat olemassa olevien varastamisen keinoja, esim.

- **Login-murrot**, esim. BruteForceAI, agentti kirjautumistietojen etsintään
- **AI based ransomware**, käyttää kielimalleja löydetyn tiedon arkaluontoisuuden arvioimiseen -> tekee hyökkäyksen ja kiristyksen itsenäisesti
- **AI based phising**, yleisimmin sähköpostiviesti, AI tekee viesteistä nopeasti huomattavasti uskottavampia, personoituja esim. sosiaalisen median avulla,
- **AI based fraud,** useita tapoja, esim. mallintaen ihmisen deepfake videoon äänen kanssa, hyvin uskottavasti, mm. Deittihuijaukset tai julkisuuden henkilöiden* käyttö huijauksissa
- **AI base exploits**, hyödyntää julkisesti saatavia järjestelmien heikkoustietoja CVE, agentti hyödyntää itsenäisesti haavoittuvuuksia
- Kaikkien edellä mainittujen yhdistelmä; laajamittainen hyökkäys

Lähde: IBM Technology video: https://www.youtube.com/watch?v=0tHb6U2604g ja
X-Force Threat Intelligence Index 2026 (26.2.2026)
*https://www.mtvuutiset.fi/artikkeli/huolestuttava-huijausilmio-on-vienyt-monelta-vanhukselta-rahat-pahin-vasta-edessa/9319880
Katso myös: Hugging face: https://huggingface.co/ ja https://www.databreachtoday.com/

©Harri Lähdesmäki

Varastamisessa ei ole mitään uutta

Varastamista on ollut aina

- Korostui kun ihminen siirtyi metsästäjä-keräilijästä maanviljelijäksi
  - Sivilisaatiot syntyivät, varastaminen ja siitä saadut tuomiot kehittyivät *
- Historian aikana tekniset keinot sekä varastaa että puolustautua varkauksilta ovat kehittyneet
  - Aina on ollut haaste pysyä tekniikan kehityksessä mukana
- Ihminen on säilynyt hyvin samanlaisena,
  - Myöskään keinot vaikuttaa ihmiseen eivät ole oleellisesti muuttuneet**

Esimerkki Code of Hammurabi 1753BC: * https://en.wikipedia.org/wiki/Code_of_Hammurabi
Esimerkki: ** https://www.mariobekes.com.au/the-spanish-prisoner-the-timeless-anatomy-of-a-scam/

©Harri Lähdesmäki

Huijausviesteillä on pitkä historia, esimerkki 1800-luvulta



Eugène-François Vidocq

”*Herra, – Teitä epäilemättä hämmästyttää kirjeen saaminen teille tuntemattomalta henkilöltä*”, yksi tällainen kirje alkoi.

Kirjeen rakenne on taitava: ennen surutarinansa paljastamista kirjoittaja tarjoaa ensin porkkanan: arkun, joka sisältää 16 000 frangia kultaa sekä timantteja, jotka kirjoittajan mukaan hän ja hänen isäntänsä joutuivat jättämään taakseen sen jälkeen, kun heidät pidätettiin matkan aikana.

Aseteltuaan panokset hän jatkaa kirjoittaen mahdollisesta oletetusta vankeusrangaistuksestaan ennen lopullista pyyntöään, joka tässä tapauksessa on hyvin hienovarainen: ”*Pyydän tietää, voinko avullanne hankkia kyseistä arkkua ja osan sen sisältämistä rahoista. Voisin sitten hankkia välittömät tarpeeni ja maksaa asianajajalleni, joka sanelee tämän ja vakuuttaa minulle, että joillakin lahjoilla voisin vapauttaa itseni tästä asiasta*.”

Eugène-François Vidocq; Mémoires de Vidocq, chef de la police de Sûreté, jusqu'en 1827
https://www.atlasobscura.com/articles/the-9-lives-of-the-spanish-prisoner-the-treasure-dangling-scam-that-wont-die

©Harri Lähdesmäki

Erilaisia huijausviestejä

- ” letters from Jerusalem” tai ”Spanish prisoners”->Nigerialaiskirjeet*
- Bisnesviestit
- Konfliktiviestit
- Romantiikkaviestit (9/2026 mennessä n. 900 kpl, 6,2 miljoonaa € **)
- Lottoviestit
- Työpaikkaviestit
- Kaupankäyntiviestit
- Pankkiviestit
- Palkkatappajaviestit
- Toisen kierroksen huijaus

Huijattu voi päätyä myös itse rikolliseksi, vahingossa tai kiristyksen kautta***

Luettelo: https://fi.wikipedia.org/wiki/Nigerialaiskirjeet

- https://www.opit.com/magazine/cybersecurity/lessons-from-history-how-fraud-tactics-from-the-18th-century-still-impact-us-today-3/

**https://www.iltalehti.fi/suhteet/a/aca3e357-e466-4771-b281-a45c9acaf1e5/

*** Iltalehti 13.9.2026, Silja Säily: Suomalaisia rekrytoitu todella alhaiseen työhön Lontooseen

©Harri Lähdesmäki

PROJECART

Ihminen

Miksi ihminen on heikko lenkki turvallisuuden ketjussa?

©Harri Lähdesmäki

Kuka niihin huijauksiin oikein lankeaa?

NETTIPETOKSIA on monenlaisia. Paljon on myös ihmisiä, jotka taas ihmettelevät, kuinka joku voi langeta ilmiselvään – tai ”ilmiselvään” – huijaukseen.

Poliisilla on tähän vastaus. Kuka tahansa. Myös sinä.

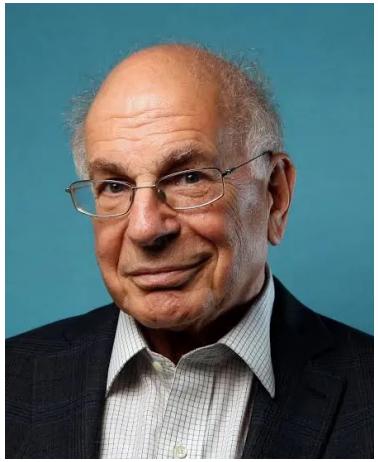
– Poliisilla ei ole stereotypiaa siitä, millaisen taustan omaavaan ihmiseen petos uppoaa. Poliisi ei enää näe asiaa näin, sanoo Keskusrikospoliisin rikosylikonstaapeli **Juha Springare** poliisin, Traficomin, DVV:n ja Aalto-yliopiston yhteisessä tiedotustilaisuudessa.

Ilta-Sanomat 4.12.2025 Henrik Kärkkäinen

©Harri Lähdesmäki

Thinking, Fast and Slow

- Daniel Kahneman*, 2011



Tunnepohjainen, nopea reagointi

- Automaattinen, emotionaalinen, intuitiivinen ja vaivaton

Ajatteleva, hidas reagointi

- Harkitseva, looginen, vaativa ja hidas

* Katso, erityisesti Notable contributions: https://en.wikipedia.org/wiki/Daniel_Kahneman

©Harri Lähdesmäki

Thinking, Fast and Slow

- Nopea ajattelu ja reagointi on ihmisen perimässä
- Aikoinaan auttoi selviytymään
- Edelleen ensisijainen tapamme kohdata meihin kohdistuvia signaaleja
- Heuristinen, intuitiivinen päätös eli kognitiivinen "nyrkkisääntö”

Erilaisia heuristiikkoja:

- Saatavuuden heuristiikka: Arvioimme asioiden todennäköisyyttä sen mukaan, kuinka helposti muistamme vastaavia tapauksia (esim. uutisoidut onnettomuudet tuntuvat yleisemmiltä).
- Edustavuuden heuristiikka: Luokittelemme asioita sen perusteella, kuinka hyvin ne vastaavat mielikuvaamme tyypillisestä edustajasta
- Ankkurointi: Päätöksenteko nojautuu liikaa ensimmäiseen saatavilla olevaan tietoon ("ankkuriin").

©Harri Lähdesmäki

Muita tieteen näkökulmia

Kognitiiviset vinoumat (bias) ja heuristiikat

- **Affect-heuristiikka**, henkinen oikotie, päätökset nopeasti, tunteet – vaikuttavat päätöksiin.
  - WNE Security
- **Trust in authority, Ihmisten taipumus luottaa auktoriteetteihin tai** viranomaisiin, helpommin aktivoituvat huijausviesteistä.
  - Ranktracker
- **Familiarity & mere exposure effect**, Viestin tai toimintatavan usein nähty toisto, nostaa reagoinnin todennäköisyyttä ilman kriittistä arviointia.
  - WNE Security

©Harri Lähdesmäki

Huijausten ja ihmisaivojen mekaniikkaa

Huijari toivoo onnistuvansa huijaamaan uhriltaan rahaa

- Uhri taas HAAVEILLEE luvatusta rahapalkinnosta

Sillä ei useinkaan ole väliä MILLAINEN VIESTI on kyseessä.

- Ihmisaivot reagoivat huomattavasti herkemmin MAHDOLLISESTI SAATAVILLA olevaan kuin siihen kuinka TODENNÄKÖISTÄ sen saaminen on

Tärkeää on myös huijauksen LUOTTAMUKSELLINEN luonne

- Vastaanottajia PUHUTELLAAN YSTÄVINÄ ja luottamussuhdetta rakennetaan pikkuhiljaa. Heiltä pyydetään todisteita, kuten kuvaa passista, jotta huijari ”voisi luottaa” auttajaansa. Vastavuoroisesti huijari TODISTELEE kuvilla jne. dokumenteilla omaa henkilöllisyyttään

Henkilö, jolla koetaan olevan AUKTORITEETTIA, olemme tottuneet vetoamaan auktoriteetteihin, PANKILTA tullut sähköposti logoineen on USKOTTAVA.

- KIIREELLÄ taas yritetään hoputtaa uhria TOIMIMAAN PIAN

Loppujen lopuksi hyvin YKSINKERTAISIA asioita, joita tehdään SUUNNITELMALLISESTI

©Harri Lähdesmäki

PROJECART

Verkkorikollisuuden torjunta
- Mitä jokainen meistä voi tehdä

©Harri Lähdesmäki

Tekniikkaa, lyhyesti

- Töissä: Noudata työnantajan tietoturvaohjeita koskien työpaikan laitteita ja käytäntöjä
- Poissa kotoa: vältä julkisia vierasverkkoja
- Kotona, muista kotiverkon suojaus:
    - *Reitittimen suojaus, ohjelmistojen päivitykset
    - Kaupallinen suojausohjelmisto suositeltava
    - Langattoman verkon suojaus, huom! vierasverkko
- Älypuhelinten ladattavien applikaatioiden riskiarvio
- IoT-laitteiden ja muiden verkkoa käyttävien riskit; TV:t, pesukoneet, valvontakamerat jne. - liitä vierasverkkoon
- Mieti mitä jaat sosiaalisessa mediassa

* Iltalehti 8.4.2026: FBI toteutti operaation Venäjää vastaan: Supo ja Traficom mukana, Supon tiedote
Tietoturvan viranomaisseuranta ja tietoturvan loukkaamisilmoitukset: https://www.kyberturvallisuuskeskus.fi/fi/
Uutiskirje: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

©Harri Lähdesmäki

Viisi yleistä vinkkiä joita kerrotaan yleisesti ja usein

- Kirjaudu pankkiin, viranomais- sekä muihin palveluihin aina itse – älä linkeistä.
- Älä koskaan kerro pankkitunnuksia tai PIN-koodejasi kenellekään.
- Älä asenna sovelluksia viestien linkeistä.
- Huijari pyrkii luomaan kiireen tuntua, että varovaisuus unohtuisi. Pysähdy miettimään, jos sinua hoputetaan.
- Lopeta puhelu heti, jos soittaja kysyy pankkitunnuksia tai haluaa siirtää varojasi ”turvatilille”.

Lähde: Taloustaito 24.11.2025

Jos olet joutunut verkkorikoksen uhriksi, katso toimintaohjeet esim. https://www.riku.fi/nettihuijaus/

Ohjeita väärän tiedon tunnistamiseen: https://thl.fi/ajankohtaista/tiedotteet-ja-uutiset/naista-merkeista-tunnistat-vaaran-tiedon-verkossa

©Harri Lähdesmäki

Voit myös kokeilla kolmen sanan mallia

Mielikuvaharjoittele 3-vaiheinen toimintamalli*

Yhteydenoton tai viestin varalle, joka:

- Herättää tunteita, postiivisia tai negatiivisia
- Pelkoa
- Toivoa
- Korostaa nopeaa toimintaa

Muista: Luottamus on aivoille säästömekanismi; jos pidämme lähdettä luotettavana, emme tutki viestiä tarkasti.

©Harri Lähdesmäki

*vaikutteet haettu Suomen koulujen mediakasvauksesta, https://kavi.fi/mediakasvatus/ ja https://youtu.be/Bgmjs6AcFjU

1. STOP

- Älä tee yhtään mitään
- Mikään taho ei voi vaatia sinulta välitöntä toimintaa
- Anna ajan kulua, tunnetason laskea
- Jos kyseessä on puhelu, joka nostaa sykettä, tuo kiireen tai vaaran tuntua - lopeta puhelu välittömästi

©Harri Lähdesmäki

PROJECART

2. AJATTELE

- Lue/perehdy viestiin huolella,
- Älä klikkaa mitään (linkki, kuva, tiedosto tms.)
- Arvioi saamasi viesti, keneltä se on, mitä se sisältää, mitä siinä kehotetaan tekemään
- Jos vastasit puheluun, mieti siitä samat asiat ja arvioi soittajan luotettavuus – pienikin epäilys on yleensä oikea

©Harri Lähdesmäki

PROJECART

3. TOIMI

- Todettuasi pienenkin epäilyn, hävitä viesti avaamatta sitä
- Vastuu viestin perillemenossa on aina lähettäjällä
- Tarvittaessa varmista oliko viesti aiheellinen, käyttämällä turvalliseksi tietämiäsi kanavia, esim. verkkopankkia, siten kun aina sitä käytät
- On suositeltavaa merkitä viesti kalasteluviestiksi tms. jos mahdollista, esim. Outlook: Report/Report Phishing

©Harri Lähdesmäki

Sama asia toisin esitettynä:

Keskusrikospoliisin kolmen kohdan sääntö huijauksien varalle:

1. Mieti hetki ja epäile kiireen tunnetta
2. Lue viesti vielä kertaalleen ja ymmärrä, mitä olet varmistamassa
3. Jos vahinko tapahtuu, ota ensin yhteys pankkiisi ja tee sitten rikosilmoitus poliisille

Katso myös: https://nytvalppaana.fi/fi

©Harri Lähdesmäki

Lähde: Tekniikka ja talous 12.12.2025

Finanssialan tilaisuus 4.2.2026, neuvoja:

”Pidä tietosi ja taitosi ajan tasalla, jaa tietoa ihan arkipäivän keskustelussa.”
Ylitarkastaja Nora Siera, Keskusrikospoliisi

”Minä en lähtisi tekemään mitään kenenkään toisen pyynnöstä tai aloitteesta.” ”Mikään pankkiasia ei ole niin kiireinen että se pitää hoitaa just nyt.”
Petostorjunnan asiantuntija Maija Ahonen, OP Pohjola

”Jos syke nousee pankin tai viranomaisen lähestymisen takia niin sitten pitää toiminta lopettaa hetkeksi ja miettiä.”
Johtaja Niko Saxholm, Finanssiala ry

https://www.youtube.com/live/GBmhSWgUyRg

©Harri Lähdesmäki

PROJECART

Kiitos ja turvallista toimintaa verkossa!

Kysymyksiä?
Kommentteja?

©Harri Lähdesmäki