

Nuoret verkossa

Kasvattajan opas kyberrikosten ehkäisyyn ja vastuulliseen verkkokäyttämiseen.



2026

Sisällys

1 Johdanto	3
2 Nuoret verkossa	5
3 Mitä ovat kyberrikokset	7
3.1 Kyberrikokset Suomen lainsäädännössä	8
3.2 Tietoverkkorikosten erityispiirteitä	9
4 Nuorten kyberrikollisuus Suomessa	10
4.1 Osaaminen	10
4.2 Motiivit	11
4.3 Vahingot	13
4.4 Seuraukset	13
4.5 Esimerkkejä nuorten tekemistä tietoverkkorikoksista	14
4.6 Laillisen ja laittoman toiminnan rajan hahmottaminen	15
5 Tuetaan yhdessä vastuullista verkkokäyttäytymistä	18
5.1 Kysy, kuuntele, ole läsnä	18
5.2 Onko lapsi kiinnostunut hakkeroinnista tai tietoturvatestaamisesta?	21
6 Usein kysyttyä tietoverkoissa toimimisesta	25
6.1 Mitä ihmettä on hakkerointi?	25
6.2 Voiko pimeää verkkoa käyttää laillisesti?	26
6.3 Ovatko videopelit haitallisia?	27
6.4 Miten suhtautua nuoren ihmissuhteisiin verkossa?	28
7 Mistä apua, jos...	29
7.1 Kohtasin verkossa tietoturvapoikkeaman, haitallista sisältöä, tai löysin haavoittuvuuden	29
7.2 Kohtasin verkossa epäilyttävää tai rikollista toimintaa	31
7.3 Lapsen tai nuoren verkkokäyttäytyminen huolestaa	32
Nuorten suusta	33
Mitä nuoret toivoisivat vanhempien ja kasvattajien tietävän kyberistä	33
Nuorten suosimia sosiaalisen median kanavia	34
Kyber-sanastoa	35



1 Johdanto

Teknologia kehittyy hurjaa vauhtia, ja etenkin nuorten elämässä erilaisilla verkkoalustoilla toimiminen on keskeinen osa arkea. Nuoret viettävät jopa yli puolet valveaikaajastaan erilaisilla verkkoalustoilla, ja käyttävät verkkoa niin koulutehtäviin, harrastuksiin, kuin yhteydenpitoon perheen ja kavereiden kanssa. Reaalimaailman keskustelut ja harrastukset jatkuvat verkossa ja päinvastoin, ja digitaalinen elämä on luonnollinen osa nuoren arkea.

Digitaalisuus on tuonut mukanaan paljon mahdollisuuksia, mutta myös haasteita. Digitalisaation myötä myös rikollisuus on siirtynyt enenevässä määrin verkkoon, ja verkkorikollisuus on kasvanut räjähdysmäisesti. Verkkovälitteisyyden myötä rikokset eivät enää ole sidottuja tiettyyn tapahtumapaikkaan, vaan rikos voi tapahtua missä vain, mukaan lukien kotona tietokoneen tai mobiililaitteen äärellä. Rikoksentekevälaineita ja -ohjeita on entistä helpommin saatavilla myös avoimessa verkossa, eikä verkkorikoksen tekeminen välttämättä vaadi merkittävää teknistä osaamista. Myös Suomessa, verkkorikollisiin tekoihin syylistyvät ensikeräiset ovat keskimäärin hyvin nuoria, jopa alakouluikäisiä.

Tämä opas tarjoaa huoltajille, kasvattajille ja muille nuorten parissa toimiville tietoa nuorten kyberrikollisuudesta, vastuullisen verkkokäyttäytymisen tukemisesta, sekä vinkkejä laillisista mahdollisuuksista tietotekniikan parissa. Oppaan tarkoituksena on toimia helppokäyttöisenä tiedonlähteenä nuorten kyberrikollisuuden ennaltaehkäisyyn sekä tarjota tukea kyberasioista keskustelemaan nuorten kanssa. Opas lähestyy kyberrikollisuutta nimenomaan tieto-verkkosidonnaisten rikosten näkökulmasta.

Keskusrikospoliisissa toteutetussa nuorten kyberrikollisuuden ehkäisyn toimenpideohjelmassa havaittiin tarve helppokäyttöiselle ja luotettavalle materiaalille kyberaiheista keskustelemisen tueksi. Lapsille ja nuorille verkossa toimiminen on arkipäivää, ja nuoret saattavat olla hyvinkin taitavia tietoverkon ja erilaisten sovellusten ja laitteiden käyttäjiä. Ymmärrys verkon pelisäännöistä ja laillisen ja laittoman toiminnan rajoista ei kuitenkaan aina kasva yhtä nopeasti kuin tekninen osaaminen. Nuoresta saattaa tuntua, ettei verkkoa valvo kukaan, eikä tekojen seurauksia välttämättä ymmärretä. Verkossa liikkuminen saattaa myös jäädä vähemmälle huomiolle arkisissa keskus-

teluissa aikuisten kanssa. Tietämättömyys voi johtaa huonoihin valintoihin, ja nuori voi jopa päätyä käyttämään taitojaan rikollisiin tarkoituksiin esimerkiksi rikollisten houkuttelemana. Siksi aikuisten rooli opastamassa lapsia ja nuoria turvalliseen ja lailliseen verkkokäyttöön korostuu.

Jos teknologia ja nuorten käyttämät sovellukset tuntuvat itselle vieraalta, saattaa myös aiheesta keskusteleminen tuntua haastavalta. Kyberaiheista keskustelemista ei kannata turhaan jännittää. Ei tarvitse olla teknisesti lahjakas voidakseen keskustella nuoren kanssa verkossa toimimisesta. Riittää, että aikuinen on läsnä, kuuntelee ja keskustelee, ja tätä kautta pyrkii ehkä lisäämään omaakin ymmärrystä tietoverkoista. Tästä oppaasta löydät tietoa nuorten kyberrikollisuudesta, tietoverkoissa toimimiseen liittyvästä lainsäädännöstä Suomessa, tukea kyberaiheista keskustelemiseen, sekä toimintaohjeita erilaisiin verkkoympäristössä vastaan tuleviin ongelmatilanteisiin. Lisäksi opas tarjoaa aiheesta kiinnostu-

neille hyödyllisiä vinkkejä materiaaleista, joiden kautta kybermaailmaan voi perehtyä syvällisemmin.

Opas on tuotettu osana Keskusrikospoliisin ja Euroopan unionin osarahoittamaa Cybercrime Exit -hanketta.



**CYBERCRIME
EXIT**



**Euroopan unionin
osarahoittama**



2 Nuoret verkossa

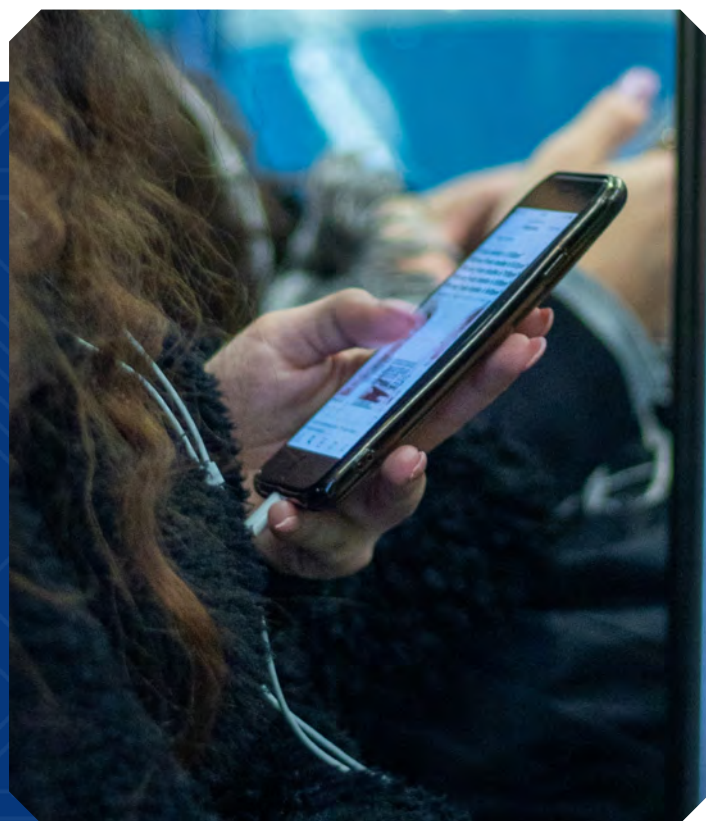
Digiympäristö on kiinteä osa nuorten arkea. Suurin osa lapsista ja nuorista liikkuu erilaisilla verkkoalustoilla, kuten sosiaalisessa mediassa, pelialustoilla, keskustelukanavilla ja verkkosivuilla. Verkkoympäristö tuo mukanaan paljon mahdollisuuksia, ja kyberosaamista tarvitaan yhä enemmän tulevaisuudessa. Aktiivinen verkkoalustojen käyttö kuitenkin altistaa nuoret myös erilaisille uhille. Suurin osa nuorista onkin kohdannut verkossa jonkinlaista haitantekoa, kuten tietojenkalasteluyrityksiä, häirintää, tai lapsille sopimatonta sisältöä. Erilaiset tietoturvaan ja nuorten turvallisuuteen liittyvät huolenaiheet näkyvät usein keskusteluissa, ja nuorta onkin tärkeää opastaa suojautumaan erilaisilta verkkouhilta. Tähän on tarjolla hyviä materiaaleja Poliisin verkkosivuilla ja sosiaalisen median kanavilla, sekä esimerkiksi [Kyberturvallisuuskeskuksen](#) ja useiden järjestöjen, kuten [Pelastakaa Lapset ry:n](#) ja [Mannerheimin Lastensuojeluliiton](#) sivuilla.

Lasta ja nuorta on yhtä tärkeää opastaa itse toimimaan verkossa vastuullisesti. Nuoren tekninen kiinnostus ja osaaminen saattaa olla hyvinkin vahvaa. Kyberaiheista kiinnostunut nuori saattaa olla utelias testaamaan

taitojaan, tutkimaan miten alustat ja laitteet toimivat, kokeilemaan verkosta löytämiään työkaluja ja tekniikoita, tai opettelemaan esimerkiksi omien sivustojen rakentelemista, koodaamista tai hakkerointia, eli luovaa ongelmanratkaisua tietoverkkojen parissa.

Tietotekninen kiinnostus on hieno juttu, ja kyberosaaminen taitona yhä tärkeämpää. Vaikka tekninen osaaminen olisi hyvinkin hallussa, laillisen ja laittoman verkkotoiminnan raja ei välttämättä kuitenkaan ole nuorelle yhtä selvää. **Verkkomaailmasta ei itsestään löydy viitoitusta siihen, mikä on oikein tai väärin, tai laillista tai laitonta.** Siinä missä nuorelle tavataan reaali maailmassa opettaa esimerkiksi liikennesäännöt, jotta nuori toimisi turvallisesti liikenteessä, täytyy myös verkon pelisäännöt opetella. Tässä nuori kuitenkin jää usein yksin. Nuoret ovatkin riskissä myös itse syyllistyä haitantekoon tai rikolliseen toimintaan verkossa, ja aikuisten opastusta tarvitaan myös verkkomaailmassa laillisen ja laittoman toiminnan rajojen ymmärtämiseksi.

Nuorelle opetetaan usein pienestä pitäen, että esimerkiksi kaupasta ei saa varastaa. Lisäksi reaali maailmassa valvonta ja kontrollimekanismit ovat vahvasti läsnä ohjaamassa toimintaa. Kaupassa on myyjä, valvontakameroita ja vartijat, jotka voivat puuttua tilanteeseen huomauttaen nuoren syyllistyneen näpistykseen. Tietoverkossa vastaava valvonta ja kontrolli on rajallisempaa eikä välttämättä näy nuorelle yhtä selkeästi. Nuoresta voikin tuntua, ettei toimintaa ohjaa kukaan, eikä rikoksesta jää kiinni.



Hyödyllisiä materiaaleja:

- **Kyberturvallisuuskeskus:** Turvallisesti netissä-oppaat lapsille ja vanhemmille
- **Pelastakaa Lapset:** Digitaalinen lapsuus
- **Suojellaan Lapsia:** Oppaat ja ohjeistukset
- **Mannerheimin Lastensuojeluliitto:** Turvallisesti digitaalisessa ympäristössä



3 Mitä ovat kyberrikokset

Kyberrikoksilla viitataan kohtalaisen laajasti erilaisiin tietoverkossa tapahtuviin tai tietoverkkoja hyödyntäviin rikoksiin. Tietoverkkorikokset voidaan karkeasti jaotella tietoverkkosidonnaisiin ja tietoverkkoavusteisiin rikoksiin. Tietoverkkosidonnaisilla rikoksilla tarkoitetaan rikoksia, jotka kohdistuvat tietoverkkoihin ja -järjestelmiin, ja tietoverkkoavusteisilla rikoksia, joiden tekemisessä hyödynnetään tietoverkkoja.

Tietoverkkoavusteiset rikokset ovat sinänsä perinteisiä rikoksia, joiden tekemiseen tietoverkot ovat mahdollistaneet uusia tekotapoja. Rikos ei siis varsinaisesti kohdistu tietoverkkoon, ja sen tekeminen olisi mahdollista myös ilman tietoverkkoja.

Esimerkiksi erilaiset nettipetokset, kuten niin sanotut romanssihuijaukset, verkossa tapahtuva huumausainekauppa tai seksuaalissävytteisten kuvien luvaton jakaminen tai niillä kiristäminen ovat tietoverkkoavusteisia rikoksia.

Tietoverkkosidonnaiset rikokset puolestaan ovat niin sanottuja puhtaita kyberrikoksia, jotka tapahtuvat tietoverkkoympäristössä, eikä niiden tekeminen ole mahdollista ilman tietoverkkoja. **Tällaisia rikoksia ovat esimerkiksi palvelunestohyökkäykset ja tietomurrot, kuten luvaton kirjautuminen toisen käyttäjätilelle.**

Kyberrikoksiin sisältyy usein sekä tietoverkkosidonnaisten että tietoverkkoavusteisten rikosten elementtejä, ja kyberrikokset toimivatkin monesti valmistelevina rikoksina muulle rikolliselle toiminnalle.

Rikoksentekijä voi esimerkiksi tietomurrolla pyrkiä saamaan selville henkilötietoja, joita tekijä voi myöhemmin hyödyntää identiteettivarkauden tai petoksien tekemisessä.

Tekijä voi myös esimerkiksi murtautua toisen henkilön digilaitteelle tai sosiaalisen median tilille saadakseen haltuunsa materiaalia, jolla tekijä voi kiristää uhria.

Tietoverkkosidonnainen rikos

- ▶ Rikos, joka kohdistuu ja tapahtuu tietoverkoissa tai tietojärjestelmissä.
- ▶ Tapahtuu aina tietoverkkoympäristössä, rikoksen tekeminen ei ole mahdollista ilman tietoverkkoja.
- ▶ Toimivat usein liitännäisrikoksina muille rikoksille.
- ▶ Esimerkiksi tietomurto, palvelunestohyökkäys.

Tietoverkkoavusteinen rikos

- ▶ Rikos, jonka tekemisessä hyödynnetään tietoverkkoja tai tietojärjestelmiä.
- ▶ Niin sanottuja perinteisiä rikoksia, jotka tapahtuvat verkkoympäristössä.
- ▶ Rikos ei varsinaisesti kohdistu tietoverkkoon, rikos voidaan tehdä myös tietoverkon ulkopuolella.
- ▶ Esimerkiksi nettipetos, huumausainekauppa verkossa.

Lue lisää:

- ▶ Rikoslaki 39/1889
- ▶ Poliisin verkkosivut poliisi.fi/kyberrikokset
- ▶ Ajantasaisen lainsäädännön löydät osoitteesta finlex.fi.

3.1 Kyberrikokset Suomen lainsäädännössä

Suomessa tietoverkkorikoksista on säädetty Rikoslaisissa. Rikoslain 34, 35 ja 38 -lukuista muun muassa löytyy tietoverkkorikoksille erityisiä säädöksiä. Lisäksi tietoverkkosidonnaisiin rikoksiin liittyviä säädöksiä löytyy myös muusta lainsäädännöstä, kuten tekijänoikeuslaista.

Laki ei suoraan erittele kyberrikoksia omana kokonaisuutenaan, vaan tietoverkkorikokset on pääasiassa sisällytetty osaksi nimikkeitä, jotka kattavat sekä tietoverkoissa että niiden ulkopuolella tapahtuvat tekotavat.

Esimerkiksi petoksen tai identiteettivarkauden tunnusmerkit ovat samat riippumatta siitä, tapahtuuko teko verkkoympäristössä vai reaali maailmassa.

Samoin tietoliikenteen häirintä voi tapahtua verkossa, mutta yhtä lailla tarkoittaa vaikkapa häiriösoittoja hätäkeskukseen tai postin työntekijän toiminnan estämistä.

3.2 Tietoverkkorikosten erityispiirteitä



Kyberrikokset eivät välitä valtioiden rajoista. Rikoksia voidaan tehdä Suomesta käsin minne päin maailmaa tahansa ja toisinpäin, ilman että rikoksentekijä on koskaan edes vieraillut kyseisessä maassa.



Kyberrikoksella aiheutettu taloudellinen vahinko on usein mittavampaa kuin muun tyyppisissä nuorten tekemissä rikoksissa. Yksittäisellä, harmittomaltakin vaikuttavalla kyberteolla voi saada aikaan laajaa vahinkoa.

Esimerkiksi palvelunestohyökkäykset (DDoS, distributed denial of service) usein kuvataan harmittomana digitaalisena liikenneuhkana. Pahimmillaan palvelunestohyökkäyksellä voidaan kuitenkin aiheuttaa vakavaa vahinkoa yksilölle tai yritykselle, ja jopa vaikuttaa yhteiskunnan kriittisen infrastruktuurin, kuten sähköverkon tai hätäkeskuslaitoksen toimintaan.



Palvelunestohyökkäykset ovat nuorten keskuudessa erittäin yleisiä etenkin peliympäristöissä, joissa niin sanottua dossamista hyödynnetään pelikokemuksen tehosteena pelien modifikaation ja huijauksien tapaan. Nuori voi esimerkiksi pyrkiä häiritsemään vastapelaajan toimintaa voittaakseen pelissä.



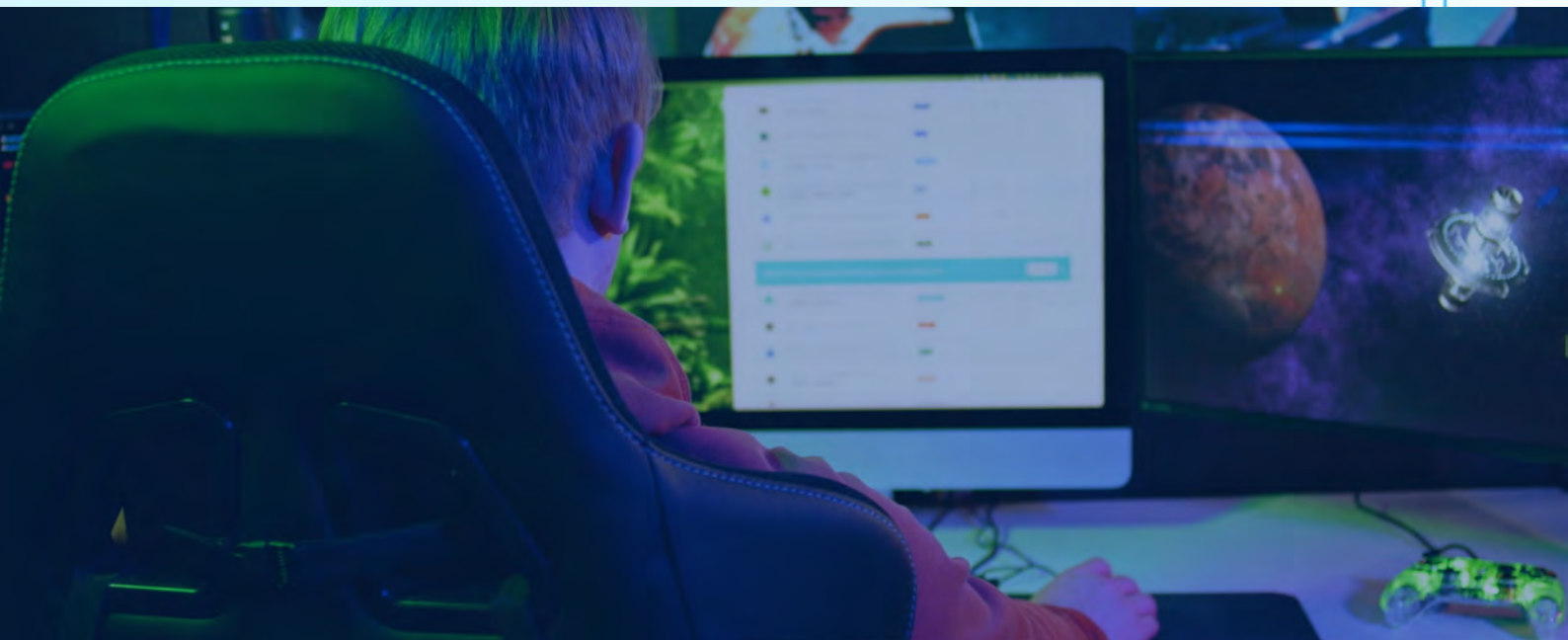
Yleisten hakukoneiden kautta on mahdollista kohtalaisen helposti löytää **verkkorikosten tekemiseen soveltuvia ohjeita ja työkaluja**. Lisäksi ohjeita ja vinkkejä on nuorten saatavilla erilaisilla keskustelufoorumeilla ja kanavilla, kuten keskustelusovellus Discordissa tai videopalvelu YouTubessa.



Verkkorikoksia on mahdollista tilata ostopalveluna (**Crime-as-a-Service, CaaS**). Kuka tahansa kykenee ostopalvelua käyttämällä kohtuullisen vaivattomasti tekemään kyberhyökkäyksen valitsemaansa kohteeseen, ilman, että käyttäjällä itsellään tarvitsee olla merkittävää tietoteknistä osaamista.

Myös automatisoiduilla työkaluilla tehty hyökkäys on rikos. Lisäksi automatisoituja työkaluja käyttäessään tekijä ei välttämättä itsekään pysty ennalta varmistumaan hyökkäyksen laajuudesta tai todellisesta kohteesta.

Ymmärtämättömyys toiminnan seurauksista ei poista rikosvastuuta.



4 Nuorten kyberrikollisuus Suomessa

4.1 Osaaminen

Uutisoinnissa järjestäytyneiden rikollisryhmien ja valtiollisten toimijoiden tekemät kyberhyökkäykset usein korostuvat. Monelle saattaakin tulla yllätyksenä, miten suuri osa tietoverkkorikoksista on todellisuudessa yksittäisten henkilöiden, kuten nuorten tekemiä. Myös kyberrikoksen kohde on rikostilastojen valossa yleisimmin yksittäinen henkilö ja hänen käyttäjätilinsä. Sekä Suomessa että kansainvälisesti, verkkorikosten tekijöiden keskimääräinen ikä on laskenut nopeasti, ja verkkorikoksiin syyllistyy vuosittain myös merkittävästi alle rikosvastuun olevia, jopa alakouluikäisiä lapsia. Myös Suomessa tietoverkkorikollisista teoista jää vuosittain kiinni alle 15-vuotiaita.

Kyberrikoksen tekemiseen ei välttämättä vaadita merkittävää teknistä osaamista, vaan tietoverkkorikoksessa voi yksinkertaisimmillaan olla kyse hyvinkin arkisesta teosta, kuten kaverin käyttäjätilin luvattomasta käytöstä. Tietoverkkorikosten tekemiseen käytettäviä välineitä ja ohjeita on nykyisin helposti nuorten saatavilla avoimessa verkossa. Tällaisia palveluja voi löytää jopa yksinkertaisella haulla yleisistä hakukonepalveluista. Palvelut ovat usein edullisia, tai niitä voi olla mahdollista kokeilla ilmaiseksi, mikä tuo palvelut helposti myös nuorten saataville. Yhä nuorempia lapsia myös rekrytoidaan rikolliseen toimintaan erilaisilla verkkofoorumilla.

Nuori voi esimerkiksi ostopalvelua käyttämällä käytännössä suorittaa paljonkin vahinkoa aiheuttavan palvelunestohyökkäyksen omalta tietokoneeltaan muutamaa nappia painamalla, ilman että nuori ehkä itse edes ymmärtää, miten hyökkäys tapahtuu ja millaista vahinkoa siitä aiheutuu.

Nuorten teknistä osaamista ei kuitenkaan tule vähätellä. Osa tietoverkkorikoksiin syyllistyvistä nuorista on tietoteknisesti erittäin lahjakkaita ja kykenee itsenäisesti toteuttamaan monimutkaisia verkkohyökkäyksiä. Vakavien kyberrikosten kohdalla tekijöillä onkin usein laajaa teknistä osaamista.

4.2 Motiivit

Arkiset motiivit

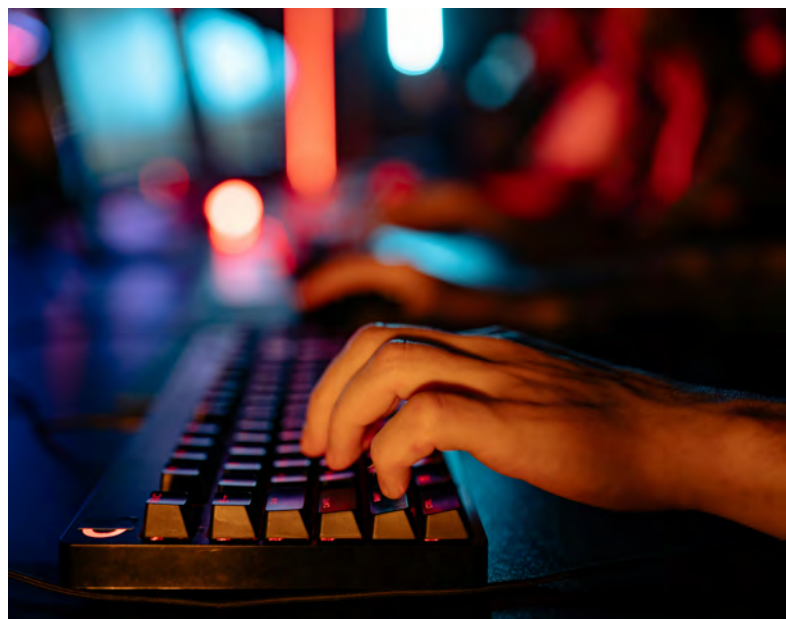
Etenkin rikospolun alkuvaiheessa nuoren tekemän kyberrikoksen motiivit ovat usein melko harmittomia ja arkipäiväisiä. Nuori ei aluksi useinkaan tavoittele taloudellista hyötyä tai pyri aiheuttamaan vahinkoa, vaan teon taustalla saattaa olla esimerkiksi jännityksen haku, uteliasuus, kiusanteko tai esimerkiksi mustasukkaisuus. Nuori saattaa haluta testata taitojaan ja kokeilla rajoja, eikä välttämässä ymmärrä tai välitä, missä vaiheessa toiminta muuttuu laittomaksi. Harmittomaksikin tarkoitettulla teolla voi kuitenkin aiheuttaa mittavaa vahinkoa. Myös taloudelliset motiivit yleensä tulevat jossain vaiheessa toimintaan mukaan, kun nuori huomaa, että toiminnalla voi ansaita rahaa.

Käyttäytymisen normalisoituminen verkkoalustoilla

Tietyn tyyppinen käyttäytyminen verkkoalustoilla saattaa olla niin normalisoitua, ettei nuori välttämättä miellä toimintaa häiritseväksi tai rikolliseksi. Esimerkiksi pelialustoilla dossaaminen, eli palvelunestohyökkäysten tekeminen on harmillisen yleistä. Dossaamisen taustalla on usein puhtaasti kiusanteko, eikä toimintaa ehkä mielletä rikolliseksi. Tutkimusten mukaan dossaaminen kuitenkin toimii usein nuoren ensimmäisenä kosketuksena kyberrikoksiin ja saattaa normalisoida rikollista toimintaa verkossa, luoden pohjaa vakavammalle rikoskierteelle.

Haktivismi

Nuoria voidaan houkutella tekemään kyberhyökkäyksiä myös kyberympäristössä tapahtuvan aktivismin varjolla. Haktivismissa kyberhyökkäyksiä hyödynnetään verkossa tapahtuvan aktivismin välineenä, pyrkimyksenä osoittaa tyytymättömyyttä tai saada muutosta johonkin asiaan. Haktivismin motiivit ovat yleensä poliittiset. Tyypillisiä haktivismin muotoja ovat esimerkiksi palvelunestohyökkäykset valtiollisia toimijoita kohtaan. Hyökkäykseen osallistuva nuori voi ajatella toimivansa hyvän asian puolesta. Todellisuudessa nuoren voi kuitenkin olla hankala varmistua siitä, mikä hyökkäyksen todellinen kohde on, ja millaisia seurauksia hyökkäyksestä aiheutuu.



Verkkoyhteisöt ja rikolliseen toimintaan houkuttelu

Nuori voi osallistua rikolliseen toimintaan myös osana isompaa paikallista tai kansainvälistä verkkoryhmää. Rikollisia ryhmittymiä voi verkossa muodostua erilaisilla foorumeilla tai esimerkiksi pelialustoilla. Rikollista toimintaa tapahtuu niin avoimessa verkossa kuin sen ulkopuolella, esimerkiksi TOR-verkossa. Ryhmittymiin liittyminen on kohtalaisen helppoa maantieteellisestä sijainnista riippumatta, ja nuori voi ajautua verkkoryhmiin muun muassa nuorten suosimien pelien tai muiden suosittujen alustojen kautta. Verkkoryhmän jäsenet voivat myös aktiivisesti lähestyä nuorta verkkoalustoilla ja houkutella mukaan rikolliseen toimintaan.

Nuorta voidaan houkutella taloudellisilla motiiveilla tai muun muassa **pelillistämällä** toimintaa, eli verhoamalla rikolliset teot teknisiksi haasteiksi tai peleiksi. Erilaiset näkyvästi toimivat rikolliset ryhmät, tai laittoman kaupan todistaminen verkossa voivat myös herättää nuoressa uteliaisuutta, ja vahvistaa kiinnostusta rikollisia verkkoryhmiä kohtaan.

Joillain verkkoalustoilla on käytössä niin kutsuttu **ranking -järjestelmä**, jossa kokeneemat käyttäjät ovat korkeammalla statuksella. Korkean statuksen omaava käyttäjä saattaa helpommin saada nuoren luottamuksen ja voi kutsua nuoren mukaan verkkoalustan ulkopuoliseen ryhmään, tarkoituksenaan esimerkiksi rekrytoida nuorta rikolliseen toimintaan.

Nuoret ovat usein otollisia kohteita rikoksiin houkuttelulle. Alle 15-vuotiaat nuoret eivät ole rikosoikeudellisessa vastuussa Suomessa. Lisäksi rikoksesta epäillyn ikä otetaan huomioon syyllisyyttä ja rikoksen seurauksia arvioitaessa, mikäli epäilty rikoksen tekijä on alle 21-vuotias. Nuoria saatetaankin houkutella rikolliseen toimintaan verkossa juuri heidän nuoren ikänsä vuoksi.

Nuoria voidaan verkkoalustoilla käyttää myös rikosten välikappaleena esimerkiksi rahanpesussa. Verkosta tuttu kaveri voi lähettää nuorelle rahaa esimerkiksi virtuaalivaluuttana, ja pyytää nuorta tekaistun syyn varjolla lähettämään rahat eteenpäin toiselle käyttäjälle tai takaisin henkilölle reaalivaluuttana. Pyytämä tarjoaa nuorelle pienen summan rahaa kiitoksena palveluksesta. Nuori voi ajatella tienäänsä helppoa rahaa, eikä välttämättä ymmärrä tilanteessa tapahtuneen mitään väärää tai ole tietoinen toiminnan todellisesta laajuudesta.

4.3 Vahingot

Tietoverkkorikoksella voidaan aiheuttaa tuntuva vahinkoa. Rikoksesta voi seurata uhrille paitsi taloudellista vahinkoa, myös pitkäaikais- ta inhimillistä kärsimystä. Rikoksella voidaan myös vaikeuttaa yritysten tai koko yhteiskunnan toimintaa, ja seuraukset saattavat pahimmillaan olla hyvinkin vakavia. Nuori ei välttämättä verkossa toimiessaan ymmärrä, miten laajaa vahinkoa toiminnalla voi aiheuttaa. Suomessakin on tullut esiin tapauksia, joissa kiusantekotarkoituksessa tehdystä teosta on aiheutunut satojen tuhansien eurojen vahingot. Toimiessaan osana verkkoryhmittymää, ei nuori ehkä edes tiedä toiminnan todellista laajuutta tai aiheutettua rikosvahinkoa. Myös alle 15-vuotias lapsi on velvollinen korvaamaan aiheuttamansa vahingon.

4.4 Seuraukset

Tietoverkkorikokset voivat olla erittäin vakavia ja laajamittaisia, uhaten jopa yhteiskunnan toimivuutta ja kriittistä infrastruktuuria. Rikoksynnyksen ylittyminen ei kuitenkaan vaadi laaja-alaista toimintaa, ja kiusanteoksi tai hauskaksi jekuksikin tarkoitettu teko voi täyttää rikoksen tunnusmerkistön. Myös kiusantekona tehdyllä rikoksella voi olla nuorelle pitkäkestoisia seurauksia.

Nuoret tekivät palvelunestohyökkäyksiä koulun palvelimelle, tarkoituksenaan kiusantekomielessä häiritä koulun Wilma-järjestelmää. Hyökkäykset kuitenkin lamauttivat myös useita muita kunnan järjestelmiä, vaikuttaen tuhansien kunnan työntekijöiden työskentelyyn. Korjaustyöt veivät useita päiviä, ja hyökkäyksestä aiheutui kunnalle mittavaa taloudellista vahinkoa.

Vahingonkorvausvastuu: Tietoverkkorikoksesta aiheutuneet vahingonkorvaukset voivat nousta mittaviksi ja vaikuttaa nuoren elämään pitkälle tulevaisuuteen. Myös alle 15-vuotias lapsi on velvollinen korvaamaan aiheuttamansa vahingon.

Rikosoikeudellinen vastuu: Yli 15-vuotias nuori on rikoksesta myös rikosoikeudellisessa vastuussa. Tietoverkkorikoksesta voi seurata sakko- tai vankeusrangaistus, sekä rikosrekisterimerkintä. Rikosrekisteri voi aiheuttaa nuorelle vaikeuksia hakiessa opiskelu-, harjoittelu-, tai työpaikkaa, sekä rajoittaa mahdollisuuksia matkustaa joihinkin maihin.

Laitteiden menetys: Rikoksen tekemisessä käytetyt laitteet, kuten nuoren puhelin, tabletti tai tietokone voidaan takavarikoida ja tuomita valtiolle menetetyksi.

Käyttöoikeuden menetys: Verkkoalustat voivat estää rikollisessa toiminnassa käytetyt tilit, kuten esimerkiksi nuoren pelitilin, jonka kasvattamiseen nuori on saattanut käyttää valtavasti aikaa ja mahdollisesti myös rahaa.

4.5 Esimerkkejä nuorten tekemistä tietoverkkorikoksista

Datavahingonteko RL 35:3 §

Tietovälineellä tai tietojärjestelmässä olevan datan oikeudeton hävittäminen, turmeleminen, kätkeminen, muuttaminen, vahingoittaminen tai salaaminen.

Pari koetta on mennyt penkin alle, ja nuorta harmittaa hänen saamansa huonot arvosanat. Nuori kirjautuu urkkimallaan salasanaa ilman lupaa opettajan Wilma -järjestelmään, ja käy muuttamassa saamansa huonot arvosanat paremmiksi.

Tietoliikenteen häirintä RL 38:5 §

Posti-, tele- tai radioliikenteen häiritseminen tai estäminen esimerkiksi puuttamalla laitteiden toimintaan tai lähettämällä häiritseviä viestejä.

Nuori haluaa tehdä koululleen kiusaa, ja lähettää verkosta löytämänsä ohjelman avulla valtavan määrän roskapostia koulun sähköpostilaatikkoon, häiriten koulun sähköpostiliikennettä.

Tietojärjestelmän häirintä RL 38:7 a §

Tietojärjestelmän toiminnan oikeudeton estäminen tai häiritseminen esimerkiksi syöttämällä, vahingoittamalla, muuttamalla tai poistamalla dataa.

Nuori pelaa verkossa joukkuepelejä, ja hänen joukkueensa hävittyä nuori joutuu pelistä ulos. Häviöstä harmistuneena nuori päättää netistä saatavan booter-palvelun avulla tehdä palvelunestohyökkäyksen pelipalvelimelle, kaataen hetkeksi pelipalvelimen toiminnan, jotta muutkaan eivät voi pelata pelejä.

Tietomurto RL 38:8 §

Oikeudeton tietojärjestelmään murtautuminen tai järjestelmässä olevien suojattujen tietojen selvittäminen esimerkiksi käyttämällä luvatta toisen salasanaa tai kiertämällä järjestelmän suojaus.

Nuoret ovat jakaneet toistensa käyttöön erään verkkopalvelun käyttäjätunnukset. Toisen nuorista keksii, että samoilla tunnuksilla pääsee kirjautumaan myös toisen nuoren sosiaalisen median tilille. Nuori kirjautuu luvatta some-tilille, ja lähettelee toisen nuoren nimissä herjaavia viestejä.

Viestintäsalaisuuden loukkaus RL 38:3 §

Toiselle osoitetun kirjeen tai viestin luvaton avaaminen, suojattuun sähköiseen viestiin murtautuminen tai viestien tai puheluiden salakuuntelu.

Nuori saa käsiinsä koulukaverinsa puhelimen ja lukee luvatta puhelimesta olevia tekstiviestejä ja sosiaalisen median yksityisviestejä. Nuori levittää viesteistä saamiaan henkilökohtaisia ja arkaluontoisia tietoja eteenpäin muille koulun oppilaille.



4.6 Laillisen ja laittoman toiminnan rajan hahmottaminen

Rajanveto laillisen ja laittoman toiminnan välillä voi joskus olla haasteellista, ja useat eri tekijät vaikuttavat toiminnan laillisuuden arviointiin. Myös toimintaympäristöllä, käytetyillä työkaluilla ja toiminnan tarkoituksella on merkitystä, ja toiminnan laillisuutta voidaan joutua arvioimaan tapauskohtaisesti. Nuoren kanssa kannattaakin yhdessä pohtia verkossa toimimisen rajoja erilaisissa arkisissa tilanteissa. Apuna voi käyttää esimerkiksi seuraavia tilanteita.



Käyttäjätunnukset

Nuoret saattavat joskus lainailla toistensa käyttäjätilejä erilaisiin tarkoituksiin, kuten pelata verkkossa tai katsoakseen sisältöä sosiaalisessa mediassa. Omia käyttäjätunnuksiaan ei koskaan kannata jakaa kenellekään, sillä tunnusten jakaminen voi johtaa väärinkäytöksiin. Toisen henkilön käyttäjätunnusten käyttö ei kuitenkaan lähtökohtaisesti ole laitonta, jos käyttöön on tunnusten omistajan lupa. Laki ei siis suoraan kiellä nuoria esimerkiksi käyttämästä toistensa sosiaalisen median tai pelitilin tunnuksia, jos tunnusten käyttöön on molemminpuolinen suostumus. Monet saattavat myös lainata toisilleen vaikkapa suoratoistopalvelujen tunnuksia.

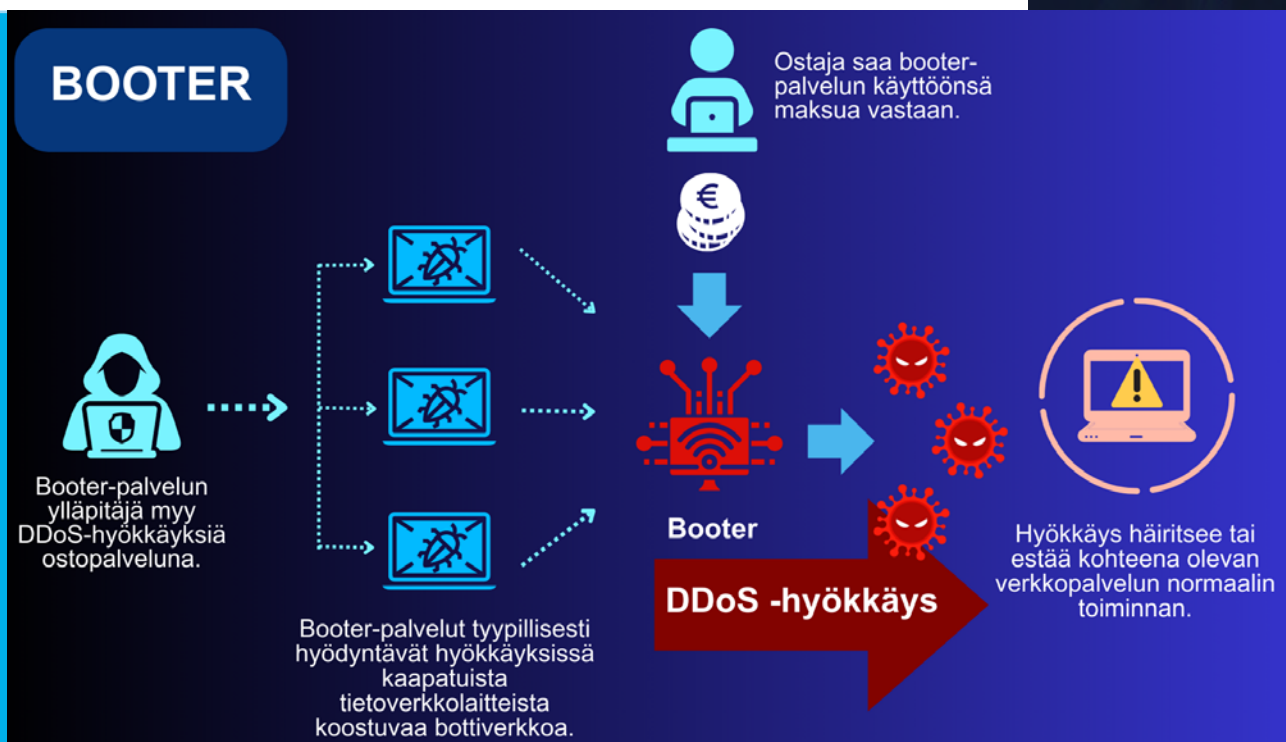
Käyttöoikeus kuitenkin rajoittuu yhdessä sovittuun käyttöön.

Mikäli tunnuksia käyttää laajemmin kuin on sovittu tai tunnuksilla yrittää kirjautua palveluihin, joiden käyttöön tunnusten omistaja ei ole antanut lupaa, voi syyllistyä rikokseen. Samoin vaikkapa maksullisen lisäosan ostaminen palvelussa toisen tunnuksilla saattaa olla laitonta, mikäli ostokseen ei ole tilin omistajan lupaa. On myös hyvä huomioida, että toiminta, joka ei suoraan riko lakia saattaa kuitenkin olla palvelun käyttöehtojen vastaista ja aiheuttaa ongelmia. Useat suoratoistopalvelut muun muassa kieltävät tunnusten jakamisen oman talouden ulkopuolelle.

Kuormitustestaaminen

Tietojärjestelmän niin sanottu **stressi- eli kuormitustestaaminen** on lähtökohtaisesti sallittua, kunhan testaus tehdään järjestelmän omistajan luvalla, laillisia välineitä käyttäen, eikä testaus vaikuta muihin verkossa oleviin palveluihin tai laitteisiin. Stressitestausta on tavanomainen osa yritysten tietoturvatestaamista, ja useat tietoturva-alan yritykset tarjoavat tähän liittyviä palveluja. Esimerkiksi oman verkkosivustonsa tai pelipalvelimensa toimivuutta voi siis lähtökohtaisesti kuormitustestata, kunhan testaaminen tehdään laillisilla työkaluilla, eikä testauksessa esimerkiksi hyödynnetä bottiverkkoa tai häiritä muita järjestelmiä. Ennen testaamista kannattaakin varmistua käyttämiensä työkalujen laillisuudesta ja toiminnasta. Epävarmoissa tilanteissa on turvallisempaa kääntyä testaamisessa virallisen tietoturva-alan yrityksen puoleen.

Palvelunestohyökkäyksen tekeminen ilman järjestelmän omistajan lupaa tai booter-palvelua käyttämällä sen sijaan on lähtökohtaisesti laitonta. Booter-palveluja myyvät sivustot saattavat väittää tarjoavansa tietoturvatestaamiseen soveltuvia työkaluja. Todellisuudessa booter-palvelut kuitenkin tyypillisesti hyödyntävät toimiakseen laitonta infraa, kuten tietomurroin kaapattuja bottiverkkoja, joiden avulla palvelunestohyökkäyksiä tehdään. Booter-palveluja käyttämällä on myös vaikea varmistua, mihin kaikkeen hyökkäys todellisuudessa vaikuttaa. Käyttämällä booter-palvelua vaikkapa oman pelipalvelimen testaamiseen voi siis tiedostamattaankin häiritä myös itselle kuulumattoman palvelimen tai muun järjestelmän toimintaa. Myös laillisten työkalujen, kuten massasähköpostityökalujen käyttäminen tietoliikenteen häiritsemiseen esimerkiksi roskapostia lähettämällä on lähtökohtaisesti laitonta.



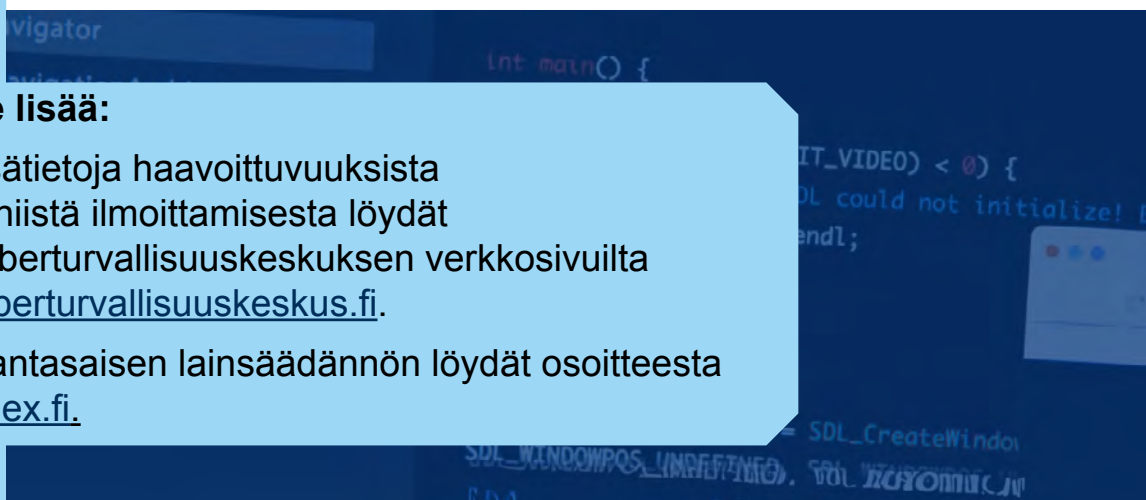


Oman toiminnan sallittavuutta arvioidessa on hyvä huomioida esimerkiksi seuraavat seikat:

- **Missä toimintaympäristössä liikon.** Yhä useammin toimitaan jonkinlaisessa verkotetussa ympäristössä, jolloin täytyy miettiä, mitä juuri kyseisessä verkkoympäristössä on sallittua tehdä. Esimerkiksi oman järjestelmän haavoittuvuuksien skannaaminen sisäisessä verkossa saattaa olla sallittua, mutta sama toiminta ulkoisessa verkossa tai virtuaalipalvelimen kautta voi jo olla laitonta.
- **Kuka testattavan järjestelmän omistaa,** ja onko toimintaan järjestelmän omistajan lupa. On eri asia tutkia omaa järjestelmäänsä, kuin esimerkiksi koulun järjestelmää.
- **Milloin toiminta menee liian pitkälle.** Haavoittuvuutta ei lähtökohtaisesti kannata lähteä tutkimaan pidemmälle luvatta, sillä haavoittuvuutta tutkiessaan saattaa päätyä laittoman toiminnan puolelle.
- **Ilmoittaminen kannattaa aina.** Joskus on mahdollista, että tietoturva-aukkoa epähuomiossa tai uteliaisuuttaan tutkii pidemmälle kuin ehkä olisi sallittua, ja haavoittuvuudesta ilmoittaminen saattaa tämän vuoksi mietityttää. Löytämästään tietoturva-aukosta kannattaa kuitenkin aina ilmoittaa, vaikka aukkoa olisikin jo ehtinyt tutkimaan. Ilmoittamalla aiheuttaa aina vähemmän vahinkoa kuin ilmoittamatta jättämällä.



- Lisätietoja haavoittuvuuksista ja niistä ilmoittamisesta löydät Kyberturvallisuuskeskuksen verkkosivuilta kyberturvallisuuskeskus.fi.
- Ajantasaisen lainsäädännön löydät osoitteesta finlex.fi.





5 Tuetaan yhdessä vastuullista verkkokäyttäytymistä

Lapset ovat usein hyvin taitavia teknologian käyttäjiä. On kuitenkin tärkeää, että lapselle on tarjolla tukea hänen harjoitellessaan digitaalisessa maailmassa toimimista. Siinä missä lapsen kanssa käydään läpi vaikkapa liikennesääntöjä, lapsi ja nuori tarvitsee aikuisten opastusta myös ymmärtääkseen verkon pelisäännöt ja pystyäkseen toimimaan vastuullisesti ja laillisesti verkossa.

5.1 Kysy, kuuntele, ole läsnä

Nuoren verkkoelämästä keskustelun ei tarvitse olla sen ihmeellisempää kuin mistään muustakaan nuoren elämän osa-alueesta puhuminen. Teknistä osaamista tärkeämpää on olla läsnä, osoittaa kiinnostusta nuoren asioita kohtaan, sekä halu oppia ja ymmärtää. Nuori usein itse mielellään avaa aihetta lisää, jos nuorelle tärkeää aihetta kohtaan osoittaa kiinnostusta.

Iso osa nuoren elämästä ja sosiaalisista suhteista voi tapahtua verkossa. Nuorelle erilaiset verkossa tapahtuvat harrastukset, kuten videopelit, sekä verkossa muodostetut kaverisuhteet ja yhteisöt ovat usein aivan yhtä tärkeitä kuin reaali maailmankin. Kyberympäristö ja reaali maailma eivät ole nuorelle erillisiä todellisuuksia, vaan toimivat toistensa jatkeina.

✓ **Ole kiinnostunut nuoren harrastuksista ja ihmissuhteista verkossa.**

Sisällytä nuoren digielämä osaksi arkisia keskusteluja siinä missä reaali maailman tapahtumatkin. Myös nuoren on helpompi kertoa verkossa kohtaamistaan ongelmista, jos kyberympäristöstä keskusteleminen on normaali osa arkea.

✓ **Tutustu alustoihin ja sovelluksiin, joita lapset ja nuoret käyttävät, ja keskustele säännöllisesti sovelluksista nuoren kanssa.** Sinun ei tarvitse tietää kaikkea voidaksesi keskustella sovellusten turvallisesta käytöstä nuoren kanssa.

✓ **Tutustu verkkomaailmaan liittyvään sanastoon.**

Kaikkea ei tarvitse tietää, mutta keskustelu on helpompi aloittaa, jos aikuisella on edes jonkinlainen käsitys tietoverkkoihin liittyvistä termeistä.

✓ **Ole utelias ja kysy kysymyksiä.**

Suurin osa meistä keskustelee mielellään omista kiinnostuksen kohteistaan, eivätkä nuoret ole poikkeus. Tietotekniikasta kiinnostunut nuori avaa usein mielellään aihetta enemmän, jos nuoren harrastusta kohtaan osoittaa kiinnostusta ja halua oppia.

Omaa tietämättömyyttään ei kannata arastella. On parempi kysyä kysymyksiä ja pyytää nuorta esimerkiksi avaamaan vieraita termejä tai alustojen toimintaa enemmän, kuin tehdä oletuksia ja mahdollisesti ymmärtää väärin mistä on kyse.

Keskustelujen kautta on mahdollista oppia enemmän nuoren harrastuksesta ja kiinnostuksen kohteista, ja mahdollisesti myös saada lisätietoa siitä, millaisissa piireissä nuori verkossa liikkuu.

✓ **Keskustele uusien pelien ja sovellusten lataamisesta lapsen ja nuoren kanssa, ja tutustu sovelluksiin yhdessä.**

Myös käytönvalvontatyökaluihin kannattaa tutustua, ja keskustella niiden mahdollisesta tarpeellisuudesta lapsen ja nuoren kanssa.

✓ **Käy lapsen ja nuoren kanssa läpi turvaintoja asiattoman lähestymisen varalta.**

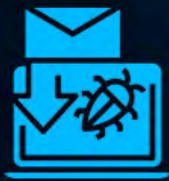
Esimerkiksi tuntemattomia henkilöitä ei lähtökohtaisesti kannata hyväksyä kaveriksi sosiaalisessa mediassa, eikä itsestään kannata lähettää kuvia muille. On myös hyvä keskustella siitä, millaista tietoa nuori jakaa itsestään verkossa, ja muistuttaa, että verkkoon julkaistua sisältöä on miltei mahdotonta täysin poistaa verkosta.

✓ **Tue tietoteknisesti lahjakasta nuorta kehittämään taitojaan turvallisesti ja laillisesti.**

Kiinnostus kyberiin on hieno juttu, ja tietotekniikasta kiinnostunutta nuorta kannattaa kannustaa kehittämään taitojaan - kunhan sen tekee laillisesti. Tietoverkkoja koskevaan lainsäädäntöön kannattaa tutustua, ja yhdessä nuoren kanssa keskustella verkon pelisäännöistä ja lain rajoista.

✓ **Keskustele nuoren kanssa vastuullisesta verkossa toimimisesta ja laillisen ja laittoman toiminnan rajoista.**

Jos jokin asia on laitonta verkon ulkopuolella, on se todennäköisesti laitonta myös verkkoympäristössä. Myös pyyntöihin, joilla tuntuu olevan kova kiire kannattaa suhtautua varauksella. Ennen toimimista onkin hyvä pysähtyä ja tarkistaa, onko toiminta laillista ja sallittua. Hyvänä sääntönä verkossa toimimiselle pätee, että sellainen toiminta, jonka sallittavuus mietityttää, on parempi jättää tekemättä.



On myös hyvä keskustella, millaisissa nettiyhteisöissä nuori viettää aikaa, ja ohjata nuorta pois haitallisista verkkoyhteisöistä. Aihetta voi lähestyä esimerkiksi ajankäytön näkökulmasta. Kyberharrastuksesta voi olla paljon hyötyä tulevaisuudessa, ja erilaiset projektit ja kilpailut voivat auttaa nuorta tuomaan esille omaa osaamistaan. Positiivisten verkkoyhteisöjen kautta voi verkostoitua ja tutustua samanhenkisiin kavereihin, sekä mahdollisesti löytää mielenkiintoisia projekteja ja työmahdollisuuksia tulevaisuudessa.

Kyberrikollisen toiminnan tai harmaalla alueella toimivien verkkoyhteisöjen kautta hankittua osaamista sen sijaan on hankala tuoda esille. Kyberrikoksilla ei voi tietoturva-alalla kehuskella, eikä kyberrikollista toimintaa voi esimerkiksi lisätä ansioluetteloonsa.



Verkossa tehtyjen toimien syy ja seuraussuhde on hyvä selkeyttää jo varhaisessa vaiheessa. Käytä oikeita termejä, ja selitä ne lapselle ja nuorelle ymmärrettävästi. Etenkin lasten kanssa on tärkeää korostaa rikollisten tekojen olevan väärin, kuitenkin tuomitsematta lasta teosta.



Jokainen tekee joskus virheitä. Onkin tärkeää, ettei nuori jää hankalien tilanteiden kanssa yksin. Nuorta on hyvä muistuttaa, että verkossa vastaan tulleista hankalista tilanteista kannattaa aina kertoa turvalliselle aikuiselle ja pyytää apua, myös silloin kun epäilee itse tehneensä jotain väärää.

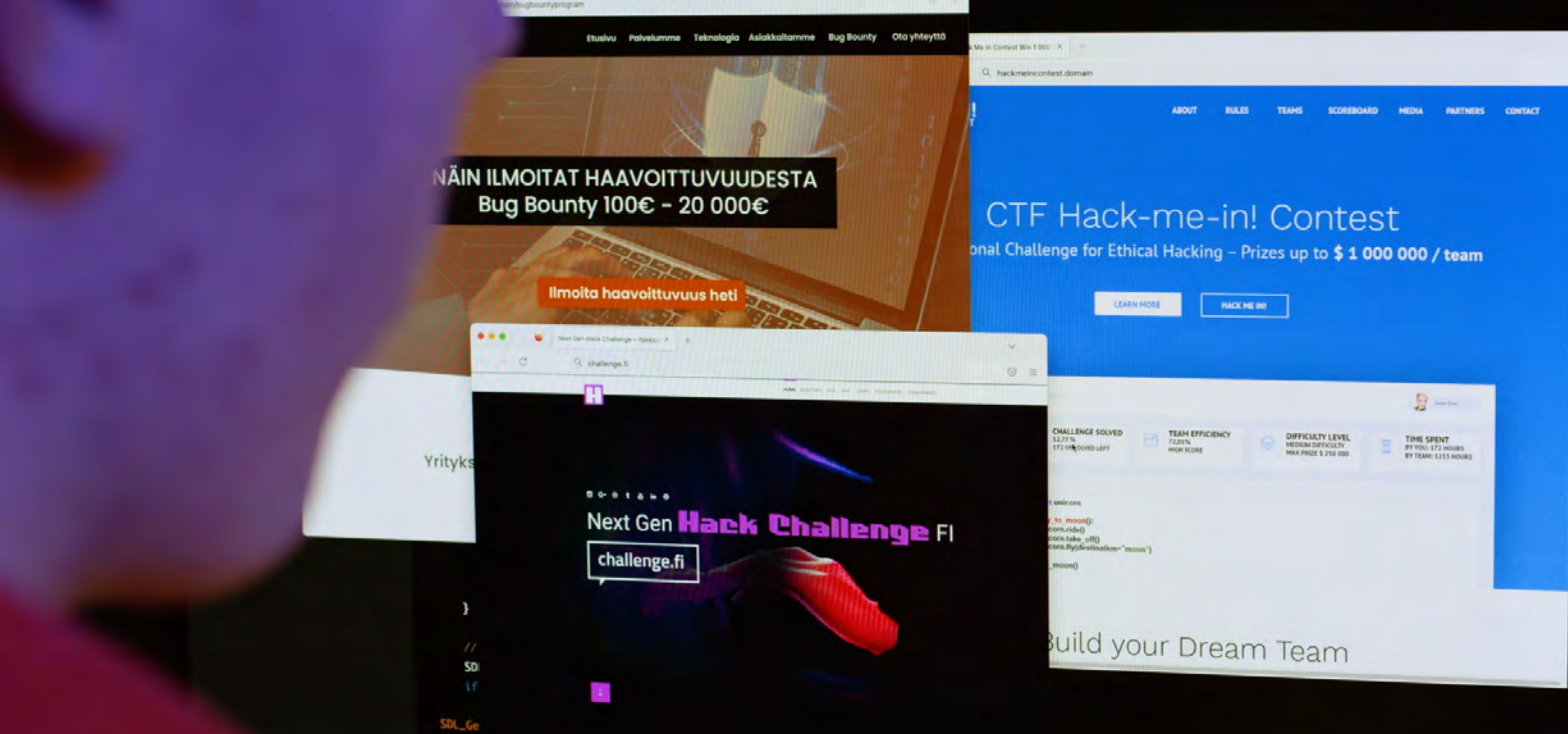


5.2 Onko lapsi kiinnostunut hakkeroinnista tai tietoturvatestaamisesta?

Kyberin parissa on valtavasti kiinnostavia, laillisia mahdollisuuksia, joihin nuoren kanssa voi yhdessä tutustua. Tarve tietoturva-alan ammattilaisille kasvaa jatkuvasti, ja kyberistä voi muodostua alasta kiinnostuneelle nuorelle myös ammatti. Sekä Suomesta että ulkomailta löytyy joukko erilaisia tietoturva-alan yrityksiä, joissa tarvitaan osaajia. Lisäksi kyberalan yhteisöt, kuten paikalliset CitySec-yhteisöt ovat lisääntymässä myös Suomessa.

Tähän osioon on koottu muutamia esimerkkejä laillisista vaihtoehtoisista harjoitella ja kehittää kybertaitoja. Vaihtoehtoja miettiessä on hyvä ensin pyrkiä hahmottamaan nuoren taitotaso ja kiinnostuksen kohteet.

Nuoren tekniset taidot voivat nuoresta iästä riippumatta kehittyä nopeasti hyvinkin korkealle tasolle esimerkiksi verkosta löytyvien tutoriaalien ja harrastusta tukevien sivustojen kautta. Onkin tärkeää, että nuorelle on tarjolla riittävästi kiinnostavia laillisia vaihtoehtoja ja haasteita.



Hiekkalaatikkoympäristöt

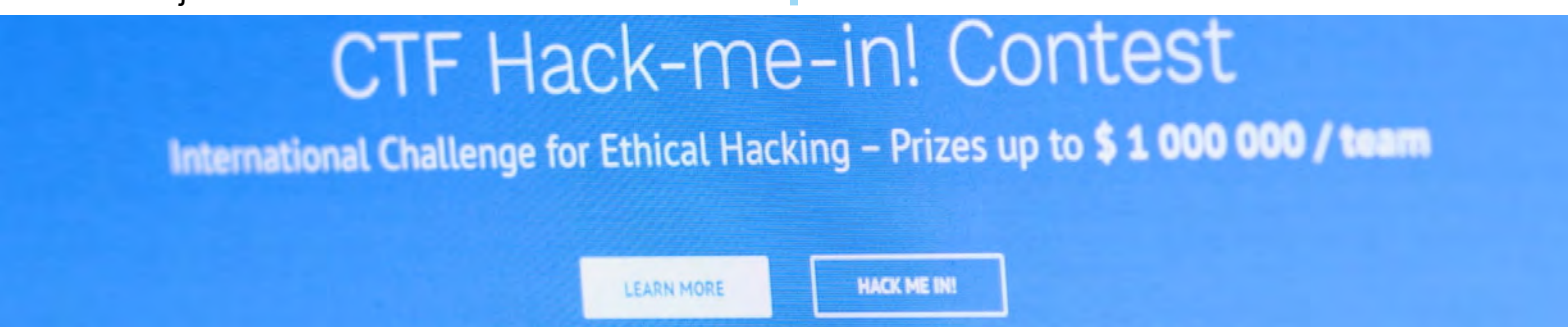
Tietoturvestaaminen omin päin ei kannata, sillä siinä on aina omat riskinsä. Pahimassa tapauksessa omin päin testailu voi johtaa rikosvastuuseen. Hakkerointia voi kuitenkin harjoitella turvallisesti erilaisissa hiekkalaatikkoympäristöissä.

Useat sivustot tarjoavat virtuaalisia harjoitusympäristöjä, niin sanottuja hiekkalaatikkoympäristöjä, joissa nuori voi testata taitojaan ja harjoitella kyberosaamista turvallisesti ja laillisesti. Hakkeroinnista ja tietoturvestaamisesta kiinnostunutta nuorta kannattaa opastaa kehittämään taitojaan turvallisissa, toimintaa varten tarkoitetuissa verkkoympäristöissä. Näitä löytyy verkosta esimerkiksi yleisten hakukoneiden kautta hakusanoilla: eettinen hakkerointi, opi hakkeroimaan, harjoittele eettistä hakkerointia, learn ethical hacking. Mikäli nuori on jo harrastanut tietoturva-aukkojen etsimistä, on nuoren kanssa hyvä käydä läpi, miten ja minne tietoturva-aukoista ilmoitetaan, ja keskustella yhdessä tietoturvestaamisen rajoista.

CTF -kilpailut

Nuori voi myös hyödyntää esimerkiksi erilaisia CTF-kilpailuja. Capture the Flag, ”lipunryöstö”, eli CTF -kilpailut ovat hakkerointihaastekilpailuja, jossa pyritään hiekkalaatikkoympäristössä selvittämään haaste, tai joukko tietoturva haasteita. Haasteet liittyvät erilaisiin tietoturvatilanteisiin, kuten haavoittuvuuden etsimiseen koodista, takaisinmallinnukseen, tai vaikkapa salauksen purkuun. Ratkaistuaan haasteen pelaaja saa ”lipun”, jonka palauttamalla saa haasteen suorittamisesta sovitun pistemäärän. CTF-kilpailut tarjoavat eri taseisia haasteita, ja ovat turvallinen ja innostava tapa tutustua hakkerointiin.

Yksi tunnettu CTF -kilpailu on European Cybersecurity Challenge, jota järjestää Euroopan unionin verkko- ja turvallisuusvirasto ENISA. Suomen kisatiimiin voi päästä mukaan pärjäämällä Suomen karsintakilpailussa, jonka järjestää Next Gen Hack Finland ry.



Bug bounty -ohjelmat

Kokeneempi hakkeri voi testata taitojaan myös osallistumalla erilaisiin Bug bounty -ohjelmiin. Bug bounty, eli haavoittuvuuspalkinto-ohjelma on organisaation tai alustan tarjoama ohjelma, jossa osallistujat voivat luvallisesti etsiä tietoturva-aukkoja ennalta sovitusta ympäristöstä. Haavoittuvuuksien ilmoittajille maksetaan palkkioita, kuten rahallista korvausta, haavoittuvuuden löytämisestä. Bug bounty -ohjelmat on tyypillisesti rajattu tiettyyn, ennalta määriteltyyn osaan organisaation järjestelmää tai alustaa, ja ohjelmiin täytyy yleensä rekisteröityä etukäteen. Ohjelma voi olla käynnissä rajatun ajan, tai jatkuvasti. Palkkioiden suuruus vaihtelee ohjelmasta ja löydetyn haavoittuvuuden vakavuudesta riippuen.

Yritykset voivat hyödyntää bug bounty -alustoja ohjelmien järjestämiseen, jolloin alusta hallinnoi useiden eri toimijoiden bug bounty -ohjelmia. Suuret yritykset, kuten Meta ja Google tarjoavat usein omia bug bounty -ohjelmiaan, ja palkkiot saattavat kohota mittaviin summiin.



Hackathon -tapahtumat

Hackathonit (englannin sanoista hacking ja marathon) ovat tapahtumia, joissa kyberalan osaajat kokoontuvat yhteen kehittämään esimerkiksi ohjelmistoa tai muuta innovaatiota. Hackathonit ovat usein kilpailutyypisiä, joissa ennalta kootut joukkueet kilpailevat keskenään, etsien ratkaisuja tai kehittäen ohjelmia sovittujen teemojen puitteissa. Hackathonit ovat yleensä rentoja tapahtumia ja kestävät tyypillisesti 24-48 tuntia. Tapahtuman päätteeksi joukkueet esittelevät tuotoksensa, ja paras innovaatio palkitaan.

Etenkin nuorelle, joka haluaa päästä työstämään ideoitaan yhdessä muiden osaajien kanssa, hackathonit voivat olla loistava keino verkostoitua, kehittää yhdessä ja tavata muita alan ammattilaisia, osaajia tai opiskelijoita.

Verkkokurssit ja sertifikaatit

Verkossa on tarjolla valtavasti erilaisia ilmaisia verkkokursseja, joista löytyy oppia niin aloittelijoille kuin kokeneemmillekin konkareille. Etenkin kurssityyppisestä oppimisesta pitävälle verkkokurssit voivat olla hyvä vaihtoehto. Aloitteleva nuori voi myös kurssien kautta saada ensikosketuksen tietotekniikan maailmaan.

Verkkokursseilla voi opetella esimerkiksi ohjelmointia eri koodikielillä, web-kehitystä, tietoturvalvontaa ja -testaamista, tai vaikkapa data-analyysia.

Tietyistä verkkokursseista on mahdollista saada myös sertifikaatti kurssin suorittamisesta, jolla nuori voi osoittaa osaamistaan.

Yhteisöt

Vaikka verkosta voi löytää paljon haitallista sisältöä, löytyy alustoilta myös paljon positiivisia ja eettiseen toimintaan kannustavia yhteisöjä. Tietotekniikasta kiinnostunut nuori voi löytää samanhenkistä seuraa esimerkiksi erilaisista verkkoyhteisöistä, kuten Discord-kanavilta, ja hakkerifoorumeilta. Yhteisöistä voi hakea vastauksia kohtaamiinsa ongelmiin, ja saada kannustusta kyberharrastukseensa.

Yhteisöjä etsiessä huomiota kannattaa kiinnittää kanavien sisältöön ja keskustelukulttuuriin. Eettisesti toimivilla kanavilla ei esimerkiksi kannusteta käyttämään laittomia työkaluja, kuten bootereita, tai painosteta osallistumaan verkkotoimintaan, joka itsestä tuntuu kyseenalaiselta. On myös hyvä tarkistaa, onko kyseessä moderoitu yhteisö, ja kuka vastaa ryhmän ylläpidosta.

Nuoren kokemus yhteisön toiminnasta yleensä kuvastaa hyvin sitä, millainen toimintakulttuuri yhteisössä vallitsee. Hyviä ohjavia kysymyksiä ovat esimerkiksi: Onko suhtautuminen verkkoryhmän jäseniin kannustavaa? Onko keskustelu ryhmän jäsenten välillä positiivista ja muita kunnioittavaa? Miten ryhmässä suhtaudutaan asiattomaan keskusteluun tai kiusaamiseen? Kannustetaanko ryhmässä haitalliseen tai rikolliseen toimintaan, kuten haittaohjelmien tai kyseenalaisten linkkien jakamiseen? Miten ryhmässä suhtaudutaan, jos ryhmän jäsen rehentelee rikollisella toiminnalla?

Verkosta löytyvien yhteisöjen lisäksi useilla paikkakunnilla on paikallisia yhteisöjä tai työpajoja, joissa nuori pääsee työstimään ideoitaan tai oppimaan uutta muiden samanhenkisten harrastajien kanssa. Hakukoneiden kautta voi tarkistaa, löytyykö omalta paikkakunnalta esimerkiksi koodaus työpajoja tai hakkerikerhoja.



Lue lisää:

- ▶ Euroopan unionin kyberturvallisuusvirasto ENISAn verkkosivut enisa.europa.eu
- ▶ Next Gen Hack Finland -yhdistyksen verkkosivut nextgenhack.fi
- ▶ Ajantasaista tietoa kilpailuista ja verkkokursseista voit etsiä avoimien hakukoneiden kautta esimerkiksi hakusanoilla **CTF, hakkerointihaastekilpailu, CTF challenge, capture the flag exercise, Bug Bounty, haavoittuvuuspalkinto-ohjelma** tai eettinen hakkerointi.




```
#include <iostream>
#include <SDL2/SDL.h>
```

```
int main() {
    // Initialize SDL
    if (SDL_Init(SDL_INIT_VIDEO) < 0) {
        std::cout << "SDL could not initialize! E
        SDL_GetError() << std::endl;
        return 1;
    }
}
```

6 Usein kysyttyä tietoverkoissa toimimisesta

Tietoverkkoihin liittyy paljon kysymyksiä ja myyttejä. Tietäntyyppinen toiminta voi olla verkkoalustoilla niin normalisoitua, ettei sitä edes mielletä rikolliseksi. Toisaalta tietyt alustat ja jopa termit saattavat automaattisesti luoda mielikuvan rikollisesta toiminnasta, vaikka niitä käytetään myös laillisiin tarkoituksiin. Tässä osiossa on avattu muutamia kyberympäristöön usein liittyviä yleisiä kysymyksiä ja myyttejä.

6.1 Mitä ihmettä on hakkerointi?

Hakkeroinnilla tarkoitetaan tietoverkko- ja tietojärjestelmäympäristössä tapahtuvaa luovaa ongelmanratkaisua, jossa päämääränä on löytää ja hyödyntää ympäristöstä löytyviä heikkouksia. Hakkerointi valitettavan usein automaattisesti mielletään rikolliseksi toiminnaksi. Hakkeroida voi kuitenkin myös lain puitteissa, ja niin sanottu eettinen hakkerointi onkin usein tärkeä osa yritysten tietoturvasta huolehtimista. Organisaatio saattaa esimerkiksi palkata henkilön etsimään haavoittuvuuksia järjestelmästäan hyökkäämällä siihen. Näin organisaatio pystyy löytämään epäkohdat järjestelmästäan ja korjaamaan ne. Jotkut organisaatiot järjestävät niin sanottuja bug bounty -ohjelmia, sallien järjestelmiinsä hyökkäämisen tiettyjen säättöjen puitteissa, ja maksavat joskus mittaviakin palkkioita haavoittuvuuksien löytäjille.

Hakkerointitaitoja kuitenkin toisinaan käytetään myös rikolliseen toimintaan, kuten luvattomaan tietojärjestelmiin tunkeutumiseen. Hakkeroinnin laillisuus riippuu toiminnan tarkoituksesta, kohteesta, ja käytetyistä menetelmistä. Tärkeää onkin ymmärtää laillisen ja laittoman tietoturvan testaamisen rajat, ja lisätä tietoisuutta siitä, miten haavoittuvuuksista ja löydöksistä tulee ilmoittaa. Hakkeroinnista kiinnostuneiden kannattaa tutustua verkkoympäristöön liittyvään lainsäädäntöön välttyäkseen mahdollisilta yllätyksiltä. Hyvänä periaatteena on, ettei löytämäänsä haavoittuvuutta kannata itsenäisesti tutkia syvemmin, vaan ilmoittaa löydöksestä asianmukaiselle taholle.





6.2 Voiko pimeää verkkoa käyttää laillisesti?

Pimeäksi verkoksi kutsutaan indeksoimatonta verkon osaa, joka on perushakukoneiden ulottumattomissa, ja jonka käyttämiseen tarvitaan erillinen selain, kuten TOR-selain. TOR-selain on ilmainen, vapaaehtoisten ylläpitämä avoimen lähdekoodin ohjelmisto, joka lisää verkkokäyttäjän yksityisyyttä. Tor-verkossa verkkoliikenne anonymisoidaan maailmanlaajuisen välityspalvelinverkon avulla, ohjaamalla kaikki verkkoliikenne useiden salattujen palvelimien, niin sanottujen solmujen kautta. Kukin solmu purkaa vain yhden osan reitin salauksesta, eikä yksikään palvelin näin tiedä verkkoliikenteen koko reittiä, jolloin käyttäjän todellinen sijainti on vaikea selvittää. Tor-verkko edistää viestinnän yksityisyyttä ja anonymiteettiä, sillä käyttäjän sijainti ja henkilöllisyys eivät ole selvitettävissä yhtä helposti kuin avoimessa verkossa.

Pimeän verkon sivustoja käytetään Tor-selaimen tai muun vastaavan ohjelman kautta. Pimeä verkko usein mielletään rikollisten leikkikentäksi, mutta kaikki pimeässä verkossa tapahtuva toiminta ei suinkaan ole laitonta. Tor-selaimen käyttö on laillista, ja monet toimijat käyttävät sitä parantamaan yksityisyyttään verkossa. Etenkin maissa, joissa valtiollinen sensuuri on vahva, pimeää verkkoa voidaan käyttää turvallisempaan viestintään tai saadakseen pääsyn sisältöön, joka muutoin olisi maassa estetty. Esimerkiksi ihmisoikeusjärjestöt ja journalistit saattavat käyttää pimeää verkkoa pystyäkseen turvallisemmin viestimään ja jakamaan sisältöä.

Pimeän verkon käyttämiseen kuitenkin liittyy useita riskejä. Pimeässä verkossa tapahtuu paljon rikollista toimintaa, kuten huumausaine- ja asekauppaa sekä laittoman aineiston levittämistä. Rikolliset toimijat suosivat pimeää verkkoa sen tarjoaman korkeamman yksityisyyden vuoksi, ja pimeän verkon markkinapaikoilla kaupitellaan niin rikoksia ostopalveluna kuin hakkerointi- ja haittaohjelmatyökaluja tai tietovuotomateriaaleja. Toiminta pimeässä verkossa ei ole niin anonyymiä kuin saatetaan ajatella, ja käyttäjän henkilöllisyys voi päättyä ulkoisten toimijoiden tietoon korkeammasta suojaustasosta huolimatta. Lisäksi riski joutua erilaisten uhkien, kuten haittaohjelmien, huijausten, tietojenkalastelun tai tarkkailun kohteeksi on pimeässä verkossa suuri.

Pimeä verkko saattaa vaikuttaa nuorista kiinnostavalta. Nuoren kanssa kannattaakin keskustella avoimesti pimeän verkon käyttämisestä ja siihen liittyvistä riskeistä. Koke mattoman käyttäjän ei kannata lähteä tutkimaan pimeää verkkoa, sillä ilman asianmukaisia suojatoimia voi helposti joutua haitallisen toiminnan kohteeksi. Pimeää verkkoa jo käyttäneen tai käyttämistä suunnittelevan nuoren kanssa on hyvä keskustella miksi ja mihin nuori pimeää verkkoa käyttää, millaisia hyötyjä ja riskejä käyttöön liittyy, ja punnita yhdessä, onko pimeän verkon käyttäminen nuorelle tarpeellista.

6.3 Ovatko videopelit haitallisia?

Usein ajatellaan, että videopelit olisivat haitallisia, ja nuoria tulisi ohjata pois videopelien maailmasta. Videopelialustoilla, siinä missä muillakin verkkoalustoilla, tapahtuu häiriökäyttäytymistä ja rikollista toimintaa, mikä on toki hyvä huomioida pelatessa. Videopeleillä on kuitenkin myös paljon positiivisia vaikutuksia ja pelaaminen voi olla kehittävä harrastus. Videopelit ovat hauskaa ajanvietettä ja voivat kehittää oppimista, luovuutta, silmä-käsikoordinaatiota, sekä muita hyödyllisiä taitoja. Videopelit yhdistävät erilaisia ja eritaustaisia ihmisiä, ja voivat elämysten lisäksi tarjota opettavaisia kokemuksia. Yhdessä pelaaminen voi olla hyvinkin yhteisöllistä, ja pelaamisen kautta voi harjoitella ryhmätyöskentelyä ja joukkueena toimimista. Pelihaamojen kautta voi käsitellä omia toiveitaan, arvojaan ja pelkojaan, ja pelaaminen voi opettaa lapselle ja nuorelle myös, miten käsitellä vaikkapa turhautumisen tunteita.

Videopeleistä luopumisen sijasta onkin tärkeää sisällyttää lapsen tai nuoren peliharrastus osaksi arkisia keskusteluja ja tutustua lapsen pelaamiin peleihin esimerkiksi pelaamalla niitä yhdessä. Lapsen kanssa on hyvä keskustella, millaisia riskejä ja ongelmia pelialustoilla saattaa tulla vastaan, ja opastaa lasta toimimaan pelialustoilla vastuullisesti. Myös pelaamiseen käytetystä ajasta on hyvä keskustella ja luoda yhteiset pelisäännöt. Kohtaamistaan ongelmista tai häiriökäyttäytymisestä kannattaa aina ilmoittaa pelialustalle ja turvalliselle aikuiselle.



6.4 Miten suhtautua nuoren ihmissuhteisiin verkossa?

Aikuisten voi joskus olla haasteellista suhtautua lapsen ihmissuhteisiin verkossa. Verkko-tuttavuuksia ei ehkä koeta todellisina, tai ne mielletään vaarallisiksi. Verkossa voi olla hankalaa varmistua keskustelukumppanin henkilöllisyydestä, ja niin lasten kuin aikuistenkin on hyvä noudattaa verkossa toimiessaan varovaisuutta ja muistaa, että verkkoprofiiliin takana oleva henkilö ei välttämättä ole kuka hän väittää olevansa.

Käytännössä lasten ja nuorten verkkokäyttäytyminen kuitenkin on hyvin sosiaalista, ja nuoren verkkoyhteisöt usein sekoitus reaali maailman ja verkkoympäristön tuttavuuksia. Monille lapsille ja nuorille verkossa muodostetut ystävyssuhteet voivat olla todella tärkeitä ja elämää rikastuttavia. Verkosta on mahdollista löytää samanhenkisiä kavereita ympäri maailmaa, ja saada tukea omalle kiinnostukselle. Etenkin nuorille, jotka kokevat, ettei heidän lähipiiristään tai omalta alueeltaan löydy samoista asioista kiinnostuneita kavereita, verkossa muodostetut kaveruus suhteet voivat muodostua erittäin tärkeiksi harrastusta tukemaan. Samoin esimerkiksi vähemmistöön kuuluville tai hankalassa elämäntilanteessa oleville nuorille verkkoympäristöstä saatu vertaistuki voi muodostua ensiarvoisen tärkeäksi.

Nuoren ihmissuhteet verkossa on hyvä sisällyttää arkiseen keskusteluun samalla tavalla kuin muutkin nuoren kaverisuhteet. Verkkoystävien automaattisen kieltämisen tai vähätteleminen sijasta lapsen ja nuoren kanssa on hyvä pyrkiä avoimesti keskustelemaan siitä, kenen kanssa nuori viettää aikaa verkkoalustoilla, sekä ikätasoon sopivasti pohtia yhdessä henkilökohtaisia rajoja ja turvallisia ihmissuhteita verkossa.

Lapsen kanssa on hyvä käydä läpi esimerkiksi millaisia tietoja lapsi jakaa itsestään verkkoon, millaisia riskitekijöitä verkkokeskusteluissa kannattaa huomioida, ja miten tunnistaa vaikkapa huijausyrityksiä. Kun verkkoyhteisöt ovat tavanomainen osa arkista keskustelua, voi nuoren olla helpompi kertoa aikuiselle myös kohtaamastaan haitallisesta toiminnasta tai häiriökäyttäytymisestä.



Lue lisää:

Hyödyllisiä materiaaleja tukemaan lapsen turvallista digiarkea löydät esimerkiksi seuraavien järjestöjen verkkosivuilta.

- Mannerheimin Lastensuojeluliitto, [Turvallisesti verkossa](#).
- Pelastakaa Lapset ry, [Digitaalinen lapsuus](#).
- Suojellaan lapsia, [Opas vanhemmille digiturvataidoista](#).

7 Mistä apua, jos...

7.1 Kohtasin verkossa tietoturvapoikkeaman, haitallista sisältöä, tai löysin haavoittuvuuden

Verkossa liikkuessi vastaan voi tulla erilaista haitallista sisältöä, tiedonkalasteluyrityksiä, tai vaikkapa haavoittuvuuksia sivustolla. Kohtaamistasi epäkohdista kannattaa aina tehdä ilmoitus. Ilmoittamisprosessi riippuu siitä, mitä ja millä alustalla sisältöön tai poikkeamiin on törmännyt.

Käyttöehtojen vastainen sisältö

Voit ilmoittaa käyttöehtojen vastaisesta tai laittomasta sisällöstä suoraan sille verkkoalustalle, josta sisältö löytyi. Helmikuussa 2024 voimaan tulleen digipalveluasetuksen (DSA) mukaan palveluntarjoajien tulee tarjota kanava, jonka kautta käyttäjät voivat helposti ilmoittaa kohtaamastaan käyttöehtojen vastaisesta tai laittomaksi epäilemästään sisällöstä. Ilmoittamisprosessi vaihtelee, mutta useimmiten tapahtuu esimerkiksi käyttämällä verkkoalustalta löytyvää "ilmoita" tai "raportoi" painiketta.

Sinun ei tarvitse olla varma, mitä käyttöehtoa tai lakia sisältö rikkoo. Riittää, että epäilet sisällön olevan ehtojen vastaista. Tarkempi selvitys sisällöstä on verkkoalustan tai viranomaisen vastuulla heidän saatuaan ilmoituksen käyttöehtojen vastaisesta sisällöstä.

Tietoturvapoikkeama

Erilaisista tietoturvapoikkeamista, kuten tietojenkalasteluyrityksistä tai kohtaamistasi haittaohjelmista kannattaa tehdä ilmoitus viranomaisille. Poikkeama voi olla esimerkiksi koneelle tullut haittaohjelma, saamasi epäilyttävä sähköpostilinkki tai tekstiviesti, jossa pyydetään antamaan kirjautumistunnuksia tai pankkitietoja. Poikkeamasta kannattaa ilmoittaa, vaikka vahinkoa ei olisi aiheutunut.

- Tee ilmoitus Kyberturvallisuuskeskukselle sähköisellä lomakkeella Kyberturvallisuuskeskuksen verkkosivuilla tai sähköpostilla cert@traficom.fi.
- Mikäli epäilet rikosta, kannattaa asiasta tehdä viipymättä rikosilmoitus poliisille. Rikosilmoituksen voit tehdä sähköisesti poliisin sähköisessä asiointipalvelussa tai asioimalla lähimmällä poliisiasemalla.

NÄIN ILMOITAT HAAVOITTUVUUDESTA
Bug Bounty 100€ - 20 000€



Tietoturva-aukko

Jos verkossa liikkeessaan löytää tietoturva-aukon, on ensiarvoisen tärkeää, ettei käytä löytämäänsä haavoittuvuutta hyväkseen. Haavoittuvuuden hyödyntäminen voi pahimmassa tapauksessa aiheuttaa suurta vahinkoa yksityishenkilöille, organisaatioille tai jopa yhteiskunnalle sekä johtaa rikosoikeudellisiin seuraamuksiin. Löytyneestä haavoittuvuudesta on tärkeää ilmoittaa asianmukaiselle taholle.

Ilmoitus suoraan organisaatiolle

- Tarkista, onko sivustolla käytössä erillinen sähköposti tai lomake, jonne haavoittuvuudesta voi ilmoittaa. Jos sivustolta löytyy ohjeet haavoittuvuudesta ilmoittamiseen, tulee ilmoittamisessa ensisijaisesti käyttää pyydettyä väylää.
- Tarkista, onko sivustolla /.well-known/security.txt tiedostoa, josta löytyy oikea toimitapa haavoittuvuudesta ilmoittamiseen.
- Mikäli sivustolta ei ole löydettävissä sopivia yhteystietoja, voi haavoittuvuudesta ilmoittaa myös esimerkiksi organisaation yleiseen sähköpostiin ja pyytää lisäohjeita. Yleistä osoitetta käytettäessä on kuitenkin vaara, ettei tieto löydy perille oikealle taholle.
- Ilmoitusta tehdessä kärsivällisyys ja asiallinen lähestymistapa ovat valttia. Organisaatioilla on erilaisia toimintamalleja ilmoitusten käsittelyyn. Osa organisaatioista vastaa ilmoittajalle ja saattaa jopa tarjota pienen palkinnon tietoturva-aukon löytämisestä. Osalla organisaatioista ei välttämättä ole valmista toimintamallia ilmoitusten käsittelyyn, ja ilmoitus tietoturva-aukosta voi tulla organisaatiolle täytenä yllätyksenä. Onkin hyvä muistaa, ettei tekemäänsä ilmoitukseen välttämättä saa vastausta, ja ilmoitukseen on voitu reagoida, vaikkei vastausta kuuluisikaan.

Epävarmoissa tilanteissa ilmoitus kannattaa tehdä myös Kyberturvallisuuskeskukselle, tai esimerkiksi lähettää ilmoitus sähköpostitse suoraan sekä organisaatiolle että Kyberturvallisuuskeskukselle.

Jotkut organisaatiot tarjoavat bug bounty -ohjelmia, joissa osallistujat voivat etsiä tietoturva-aukkoja ennalta määritellystä ympäristöstä. Bug bounty -ohjelmiin täytyy yleensä ilmoittautua etukäteen, ohjelmassa on asetettu säännöt ja rajat tietoturva-aukkojen etsimiselle, ja ilmoittajille maksetaan palkkiota löydetyistä haavoittuvuuksista.



Lue lisää:

- Lisätietoja haavoittuvuuksista ja niistä ilmoittamisesta löydät Kyberturvallisuuskeskuksen verkkosivuilla osiosta [Haavoittuvuudet](#).

Ilmoitus Kyberturvallisuuskeskukselle

- ▶ Voit aina ilmoittaa haavoittuvuudesta Kyberturvallisuuskeskukselle. Ilmoituksen voi tehdä luottamuksellisesti, myös nimettömänä.
- ▶ Tee ilmoitus haavoittuvuudesta tai tietoturvapoikkeamasta Kyberturvallisuuskeskukselle sähköisellä [ilmoita meille tietoturvaloukkauksesta](#) -lomakkeella Kyberturvallisuuskeskuksen verkkosivuilla tai sähköpostilla osoitteeseen cert@traficom.fi.
- ▶ Ilmoituksen Kyberturvallisuuskeskukselle voi tehdä riippumatta siitä, oletko ensin yrittänyt lähestyä sivustoa suoraan. Kyberturvallisuuskeskukselle ilmoittaminen on vaivaton vaihtoehto, mikäli haluat pysyä nimettömänä tai et halua hoitaa asiaa enempää. Ilmoituksen voi halutessaan myös laittaa yhtä aikaa sekä organisaatiolle että Kyberturvallisuuskeskukselle esimerkiksi yhteisellä sähköpostilla.
- ▶ Osoitteesta on myös saatavilla tukea ja lisätietoa erilaisten tietoturvapoikkeamien käsittelystä.

7.2 Kohtasin verkossa epäilyttävää tai rikollista toimintaa

Verkossa kohtaamastaan epäilyttävästä toiminnasta kannattaa aina ilmoittaa poliisille.

Mikäli epäilet joutuneesi rikoksen uhriksi, kannattaa asiasta tehdä viipymättä rikosilmoitus poliisille. Rikosilmoituksen voit tehdä sähköisesti poliisin sähköisessä asiointipalvelussa, tai asioimalla lähimmällä poliisiasemalla.

Mikäli havaitset verkossa epäilyttävää toimintaa tai epäilet törmänneesi laittomaan aineistoon tai sisältöön, voi epäilyistä helposti ilmoittaa poliisille Nettivinkki-palvelussa osoitteessa poliisi.fi/nettivinkki. Nettivinkkiä voi käyttää kiireettömistä asioista ilmoittamiseen. Nettivinkkiä voi käyttää epäilyttävästä toiminnasta ilmoittamiseen, vaikka ei olisi varma, onko kyseessä rikos. Nettivinkkiin kannattaa kuvailla mahdollisimman yksityiskohtaisesti millaiseen sisältöön tai toimintaan on törmännyt ja missä. Vinkin voi halutessaan jättää nimettömänä. Poliisi käsittelee nettivinkit ja ryhtyy tarvittaessa jatkotoimenpiteisiin, jos asiassa on aihetta epäillä rikosta.



Lue lisää:

- ▶ Ilmoita tietoturva-aukosta Kyberturvallisuuskeskukselle osoitteessa kyberturvallisuuskeskus.fi.
- ▶ Tee nettivinkki osoitteessa poliisi.fi/nettivinkki.
- ▶ Tee rikosilmoitus sähköisesti osoitteessa poliisi.fi, tai asioimalla lähimmällä poliisiasemalla.



**Tee rikos-
ilmoitus**

**Näin estät
rikoksen**

7.3 Lapsen tai nuoren verkkokäyttäytyminen huolettaa

Huolettaako nuoren käyttäytyminen verkossa? Epäiletkö, että nuoren kiinnostus tai toiminta on saattanut kääntyä laittomalle puolelle ja kaipaavat lisätietoa tai tukea?

Keskusrikospoliisin kyberrikollisuutta ennalta estävässä toiminnassa ennalta ehkäistään nuorten vakavaa tietoverkkorikollisuutta, lisätään tietoisuutta laillisen ja laittoman verkkotoiminnan tunnistamisesta, sekä tuetaan nuoria rikoksettoman elämäntavan omaksumisessa osana poliisin ennalta estävää erityistoimintaa.

Toiminta tarjoaa tietoa ja opastusta tietoverkkorikollisuuden ennalta ehkäisyyn ja varhaiseen puuttumiseen. Lisäksi toiminta tarjoaa tukea nuorille, jotka ovat ehkä jo syyllistyneet rikollisiin tekoihin verkossa. Toiminta on kohdistettu noin 12-25-vuotiaille nuorille, jotka ovat tehneet, tai vaarassa syyllistyä vakaviin tietoverkkorikoksiin. Nuori voi hakeutua toimintaan omasta aloitteestaan, tai toimintaan voidaan ohjata esimerkiksi ammattilaisten toimesta. Toiminta on vapaaehtoista ja luottamuksellista. Toiminnan lähtökohtana on vahvistaa rikoksetonta elämäntapaa tukemalla laillisen ja laittoman toiminnan rajojen tunnistamisessa, kartoittamalla osaamista tukevia työ- ja opiskelumahdollisuuksia ja mahdollista muuta elämäntilanteen tukea, sekä ohjaamalla nuorta laillista toimintakulttuuria tukevaan verkostotoimintaan nuoren kiinnostuksen kohteiden mukaisesti. Jokaisen asiakkaan kanssa laaditaan yksilöllinen suunnitelma asiakkaan tilanne ja kiinnostuksen kohteet huomioiden.



Ota yhteyttä:

Kyberrikollisuutta ennalta estävään toimintaan voi matalalla kynnyksellä ottaa yhteyttä sähköpostitse osoitteeseen **cybercrime.exit.krp@poliisi.fi**.

Lisätietoja hankkeesta ja kyberrikollisuuden ennalta ehkäisystä löydät **[Cybercrime Exit -toiminnan verkkosivuilla](#)**.

Nuorten suusta

Mitä nuoret toivoisivat vanhempien ja kasvattajien tietävän kyberistä

Nuoret ovat oman asiansa asiantuntijoita ja tietävät parhaiten, millaisia haasteita he verkossa kohtaavat. **Testausserveri ry** on nuorten perustama ja tietotekniikasta kiinnostuneista nuorista koostuva voittoa tavoittelematon yhdistys, jonka tavoitteena on innostaa nuoria tietotekniikka- ja kyberharrastuksen pariin ja tarjota nuorille tukea heidän kyberprojekteihinsa muun muassa Discord-yhteisön kautta. Pyysimme Testausserveri ry:n jäseniä kertomaan, mitä nuoret toivoisivat vanhempien ja kasvattajien tietävän tietotekniikkaharrastukseen liittyen, ja millaista tukea nuoret toivoisivat aikuisilta tietotekniikkaharrastukseen. Keskeisinä teemoina esille nousivat ymmärrys ja kiinnostus nuoren harrastusta kohtaan, ja tuki eettisen toiminnan opetteluun.

Mitä nuoret toivoisivat aikuisten tietävän tietotekniikkaharrastuksesta

- ▶ Hakkerointiharrastus ei ole laitonta eikä hakkeroinnin tarkoitus ole aiheuttaa haittaa, kun noudattaa sallittuja rajoja.
- ▶ Yleisymmärrystä siitä, mikä on lainmukaista ja vaaratonta toimintaa, ja vähemmän perusteetonta pelkoa.
- ▶ Tietoteknisessä harrastuksessa on arvoa ja potentiaalia kehittää hyödyllisiä työelämän taitoja.

”Sukulaiseni kävi koodini läpi vapaa-ajalla ja kirjoitti aina siitä paremman version, josta opin hyviä käytäntöjä. En osaa kuvailla, miten minua oltaisiin voitu tukea enemmän.”

Lue lisää:

- ▶ Tutustu Testausserverin toimintaan osoitteessa testausserveri.fi.

Millaista tukea nuoret toivoisivat aikuisilta tietotekniikkaharrastukseen?

- ▶ Kiinnostusta nuoren harrastukseen. Kiinnostusta voi osoittaa esimerkiksi kysymällä, mitä ohjelmia tai työkaluja nuori käyttää tai mitä hän on oppinut. Näin aikuinen voi osoittaa arvostusta nuoren harrastukseen ja auttaa tuntemaan nuoren käyttäytymistä. Nuorelle saa myös ehdottaa ideoita koodausprojekteille.
- ▶ Nuori voi olla kiinnostunut kyberharrastuksesta, mutta kaipaa apua löytämään resursseja eettiseen oppimiseen ja harrastamiseen. Nuoren on helppoa törmätä huonoihin vaikutteisiin netissä, vaikka luvallisestikin pääsee tekemään jännittäviä asioita, kun vain tietää mistä luvallisia paikkoja löytää.

”Olisin kaivannut enemmän ohjausta asioiden etsimisessä. Tarkoitan, että mukavaa olisi ollut saada tukea ongelmien ratkomisessa hakukoneiden kautta.”

Nuorten suosimia sosiaalisen median kanavia

Lasten ja nuorten suosiossa olevat sovellukset vaihtuvat usein nopeaan tahtiin, ja uusia sovelluksia nousee esille jatkuvasti. Vuonna 2024 suomalaisten nuorten aktiivisimmin käyttämät sosiaalisen median sovellukset olivat Snapchat, WhatsApp ja TikTok. Viestintäsovellukset, kuten WhatsApp ja Telegram mielletään usein aikuisten keskuudessa keskustelukanaviksi, mutta myös niistä löytyy seurattavia yhteisöjä ja muita sosiaalisen median elementtejä, joita ala-asteikäisetkin lapset seuraavat aktiivisesti.



Nuoren kanssa on hyvä keskustella hänen aktiivisesti käyttämistään alustoista.

Tähän osioon on listattu muutamia nuorten suosimia sosiaalisen median kanavia, joihin aikuisten voi olla hyvä tutustua.

NUORTEN ENITEN KÄYTTÄMIÄ SOSIAALISEN MEDIAN ALUSTOJA



Instagram



Discord



YouTube



Yubo



Snapchat



Steam



Reddit



Threads



TikTok



Twitch



Jodel



VSCO



WhatsApp



Telegram



BeReal.

BeReal



Pinterest

Kyber-sanastoa

Booter

Työkalu, joka mahdollistaa käyttäjälleen palvelunestohyökkäysten tekemisen käyttäjän haluamaan kohteeseen tietoverkoissa. Booteria käyttämällä haluttuun kohteeseen lähetetään niin paljon tietoliikennettä, että kohteen tarjoama palvelu, kuten verkkosivusto, kaatuu, eikä ole hyökkäyksen aikana käytettävissä. Booter -palvelut hyödyntävät tyypillisesti hyökkäyksissä laittomasti haltuun otettuja, kuten tietomurtojen avulla kaapattuja tietoverkkolaitteita, ns. bottiverkkoa.

Booter ja stresser palveluja on helpposti saatavilla avoimesta verkosta yleisten hakukoneiden kautta maksua vastaan tai jopa ilmaiseksi. Booter ja stresser -sivustot voivat väittää myyvänsä tietoturvatestaamiseen soveltuvia tuotteita. Todellisuudessa palvelut kuitenkin tarjoavat laittomia työkaluja, jotka mahdollistavat palvelunestohyökkäysten tekemisen mistä ja minne päin maailmaa tahansa.

Bottiverkko (botnet)

Joukko tietoverkoissa olevia tietoteknisiä laitteita, jotka on kaapattu verkkohyökkäysten toteuttamiseksi. Bottiverkon kokoaja ottaa haltuunsa toisten tietoverkkoon yhdistämiä laitteita esimerkiksi haittaohjelman avulla tai hyödyntämällä laitteiden heikkoa tietoturvaa kuten huonoa salasanaa tai salasanan puutetta. Kaapatut laitteet kootaan etähallittavaksi verkoksi, jota voidaan komentamalla hyödyntää esimerkiksi tietoliikenteen lähettämiseksi haluttuun kohteeseen.

Bottiverkko voi koostua useista arkisista verkkoyhteyden omaavista laitteista kuten tietokoneista, älytelevisioista, kaiuttimista, jääkaapeista tai sähköhammasharjoista. Laitteen omistaja ei välttämättä edes huomaa, että laitetta käytetään osana bottiverkkoa. Bottiverkkoja voidaan hyödyntää esimerkiksi tietojenkalasteluun, palvelunestohyökkäysten tekemiseen tai haittaohjelmien tai roskapostin levittämiseen.

Bug bounty

Bug bounty, eli haavoittuvuuspalkinto-ohjelma on organisaation tai alustan tarjoama ohjelma, jossa osallistujat voivat luvallisesti etsiä tietoturva-aukkoja ennalta sovitusta ympäristöstä. Haavoittuvuuksien ilmoittajille maksetaan palkkioita, kuten rahallista korvausta, haavoittuvuuden löytämisestä. Bug bounty -ohjelmat on yleensä rajattu tiettyyn, ennalta määritettyyn osaan organisaation järjestelmää tai alustaa, ja ohjelmiin täytyy usein rekisteröityä etukäteen. Ohjelma voi olla käynnissä rajatun ajan, tai jatkuvasti. Palkkioiden suuruus vaihtelee ohjelmasta ja löydetyn haavoittuvuuden vakavuudesta riippuen.

Yritykset voivat hyödyntää bug bounty -alustoja ohjelmien järjestämiseen, jolloin alusta hallinnoi useiden eri toimijoiden bug bounty -ohjelmia. Suuret yritykset, kuten Meta ja Google tarjoavat usein omia bug bounty ohjelmiaan, ja palkkiot saattavat kohota mittaviin summiin.

Crime-as-a-Service (CaaS)

Verkosta on saatavilla automatisoituja rikoksentekovälineitä, joita voi käyttää erilaisten rikosten, kuten palvelunestohyökkäysten tekemiseen niin sanotusti ostopalveluna (crime-as-a-service). Crime-as-a-service -palveluita voi helposti löytää myös yleisten hakukoneiden kautta, ja palvelut mahdollistavat tietoverkkorikosten tekemisen myös ilman merkittävää tietoteknistä osaamista.



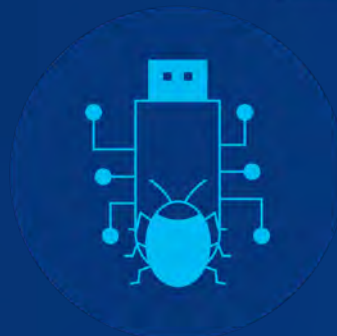
CTF (Capture the flag)

Capture the Flag, ”lipunryöstö”, eli CTF -kilpailut ovat hakkerointihaastekilpailuja, jossa pyritään niin sanotussa hiekkalaatikkoympäristössä selvittämään haaste, tai joukko tietoturva haasteita. Haasteet liittyvät erilaisiin tietoturvatilanteisiin, kuten haavoittuvuuden etsimiseen koodista, takaisinmallinnukseen, tai vaikkapa salauksen purkuun. Ratkaisutuaan haasteen pelaaja saa ”lipun”, jonka palauttamalla saa haasteen suorittamisesta sovittun pistemäärän. CTF-kilpailut tarjoavat eri tasoisia haasteita, ja ovat turvallinen ja innostava tapa tutustua hakkerointiin.

Haavoittuvuus, Tietoturva-aukko

Haavoittuvuudella, eli tietoturva-aukolla tarkoitetaan järjestelmässä olevaa heikkoutta, jonka avulla ulkopuolinen voi päästä hyödyntämään tai aiheuttamaan vahinkoa kohdejärjestelmälle. Haavoittuvuuksia voi löytyä esimerkiksi ohjelmistoista, tietojärjestelmistä, sovelluksista tai laitteista. Tietoturva-aukko saattaa johtua esimerkiksi vanhentuneesta ohjelmistosta, ja haavoittuvuudet pyritään usein korjaamaan ohjelmistopäivityksillä.

Haavoittuvuuksien vakavuusaste vaihtelee. Tietoturva-aukot voivat olla lieviä, ja ohjelmiston tarjoaja saattaa huomata ja korjata haavoittuvuuden ennen kuin siitä on ehtinyt aiheutua haittaa. Pahimmillaan haavoittuvuudet voivat olla kriittisiä, ja käytännössä mahdollistaa ulkopuoliselle vapaan pääsyn tehdä järjestelmässä mitä vain.



Haittaohjelma

Haittaohjelmalla tarkoitetaan erilaisia haitallisia ohjelmistoja, joilla pyritään vahingoittamaan tai käyttämään hyödyksi tietojärjestelmiä tai laitteita. Yleisiä haittaohjelmia ovat esimerkiksi virukset (virus), madot (worms), vakoiluohjelmat (spyware), kiristyshaittaohjelmat (ransomware), näppäilytallentimet (keylogger) ja troijalaiset (trojans). Haittaohjelma voi tarttua muun muassa sähköpostin liitteen tai ohjelmistolatauksen kautta tai napsauttamalla saastunutta linkkiä. Haittaohjelma voi levitä myös haavoittuvuuden kautta, eikä välttämättä vaadi levitäkseen toimenpiteitä käyttäjältä. Haittaohjelmalla voidaan pyrkiä esimerkiksi kalastelemaan tietoja, varastamaan pankki- tai luottokorttitietoja, ottamaan laite haltuun kiristystarkoituksessa, tai hyödyntämään saastunutta laitetta osana bottiverkkoa.

Hakkeri

Henkilö, joka on taitava käyttämään tietotekniikkaa ja omaa luovaa ongelmanratkaisutaitoa tietoteknisissä haasteissa. Hakkeri voi käyttää taitojaan esimerkiksi internetin turvallisuuden lisäämiseen. Taitoja voi käyttää myös rikollisesti vaikkapa tunkeutumalla suojattuun järjestelmään.

Hakkerointi

Tietoverkko- ja järjestelmäympäristössä tapahtuvaa luovaa ongelmanratkaisua, jossa päämääränä on löytää ja hyödyntää ympäristöstä löytyviä heikkouksia. Hakkerointi mielletään usein laittomaksi toiminnaksi, mutta hakkeroida voi myös lain puitteissa. Eettinen hakkerointi on tärkeä osa tietoturvatestaamista.



Palvelunestohyökkäys (DDoS)

Tietoverkkohyökkäys, jolla pyritään häiritsemään tai estämään tietyn verkkopalvelun normaali toiminta. Hajautettu palvelunestohyökkäys toteutetaan esimerkiksi kohdistamalla verkkosivustolle niin paljon liikennettä, että sivusto ylikuormittuu ja sivuston normaali käyttö estyy. Palvelunestohyökkäys voidaan tehdä suoraan yhdestä lähteestä, tai hajautetusti hyödyntämällä esimerkiksi bottiverkkoa. Palvelunestohyökkäyksiä on mahdollista tehdä myös ilman laajempaa teknistä osaamista avoimesta verkosta löytyvien automatisoitujen työkalujen, kuten booterin avulla.

Skript Kiddie

Harrastelijahakkeri, jolla ei itsellään ole laajaa teknistä osaamista, vaan joka käyttää muiden tekemiä työkaluja tai skriptejä kyberhyökkäysten tekemiseen. Skript kiddiet ovat yleensä aloittelijoita, jotka eivät osaa itse rakentaa koodia alusta asti, vaan turvautuvat valmiisiin työkaluihin hyökkäyksiä tehdäkseen.



Lue lisää:

- [Kyberturvallisuuden perussanasto](#), Kyberturvallisuuskeskus.
- [Kyberturvallisuuden sanasto](#), Sanastokeskus.
- Lisätietoa tietoturvasta ja ajankohtaisista kyberilmiöistä löydät myös esimerkiksi teleoperaattoreiden ja tietoturvalan yritysten verkkosivuilta.





Nuoret verkossa - Kasvattajan opas kyberrikosten ehkäisyyn ja vastuulliseen verkkokäyttämiseen.

Tämä opas on luotu osana Euroopan unionin osarahoittamaa **Cybercrime Exit -hanketta**. Opas on luotu vastaamaan hankkeen sidosryhmien suunnalta tulleeseen toiveeseen kasvattajille, kuten huoltajille ja opettajille suunnatusta helppokäyttöisestä tiedonlähteestä nuorten kyberrikollisuuden ennalta ehkäisyyn. Oppaan tarpeellisuudesta ja sisällöstä käytiin myös keskustelua muun muassa Keskusrikospoliisin Kyberrikostorjuntakeskuksen, Poliisihallituksen, Sisäministeriön ja Testausserverin kanssa, ja oppaan luonnosversio lähetettiin kyseisille tahoille kommentoitavaksi. Lisäksi Testausserveri-yhdistyksen jäsenet kirjoittivat oppaaseen lyhyen osion nuorten toiveista kasvattajia kohtaan. Oppaan on toteuttanut Keskusrikospoliisin Cybercrime Exit -hanke.

Nuorten kyberrikollisuutta ennalta estävä toiminta käynnistyi Keskusrikospoliisissa vuonna 2020. Toiminnan jatkumona hankekaudella 2023-2025 toteutettiin Euroopan unionin osarahoittama Cybercrime Exit 3 - nuorten kyberrikollisuuden ehkäisyn asiakas- ja koulutuspilottihanke. Hankkeessa pilotoitiin ja kehitettiin nuorten tietoverkkorikollisuutta ennalta estäviä interventioita, ja luotiin ajantasaisia toimintaedellytyksiä tietoverkkorikollisuuden erityispiirteiden havainnointiin ja nuorten kyberrikoskierteeseen puuttumiseen. Kyberrikollisuutta ennalta estävä toiminta jatkuu Keskusrikospoliisissa vuonna 2026 toiminnan vakiinnuttamishankkeena osana poliisin ennalta estävän toiminnan strategian ja kansallisen kyberturvallisuusstrategian toimeenpanoa.

Cybercrime Exit-hanketiimi:

Viivi Lehtinen, projektipäällikkö
Sari Latomaa, tarkastaja
Aki Somerkallio, tarkastaja

Poliisi

Oppaan tekijä: Sari Latomaa, Keskusrikospoliisi

Oppaan kuvat: Poliisi, Canva C00, Pexels CC0, Unsplash C00.

ISBN 978-951-53-3932-4

© Keskusrikospoliisi 2026.

Julkaistu 3 / 2026

Hyperlinkkien toimivuus on tarkistettu 20.11.2025.