POLISEN

Ungdomar på nätet

Guide för fostrare för att förebygga cyberbrott och främja ansvarsfullt beteende på nätet.

2026

CYBERCRIME EXIT

Medfinansieras av Europeiska unionen

Innehållsförteckning

1 Inledning

Tekniken utvecklas i en hisnande takt, och i synnerhet för unga är det en central del av var-dagen att agera på olika typer av webbplattformar. De unga tillbringar upp till hälften av den vakna tiden av dygnet på olika webbplattformar och använder nätet för både skoluppgifter, hob-byer och kontakter med familj och vänner. Sam-talen och hobbyerna i den verkliga världen fort-sätter på webben och vice versa, och det digitala livet är en naturlig del av den ungas vardag.

Digitaliseringen har medfört många möjligheter, men också utmaningar. Med digitaliseringen har också brottsligheten i allt högre grad överförts till nätet, och nätbrottsligheten har ökat explosionsartat. På grund av webben är brotten inte längre bundna till en viss plats, utan brotten kan begås var som helst, inklusive hemma vid datorn eller den mobila enheten. Hjälpmedel och anvisningar för att begå brott är allt lättare tillgängliga också på öppna nätverk, och det krävs inte nödvändigtvis stort tekniskt kunnande för att begå ett nätbrott. Även i Finland är förstagångsförbrytare som gör sig skyldiga till nätbrott i genomsnitt mycket unga, till och med i lågstadieåldern.

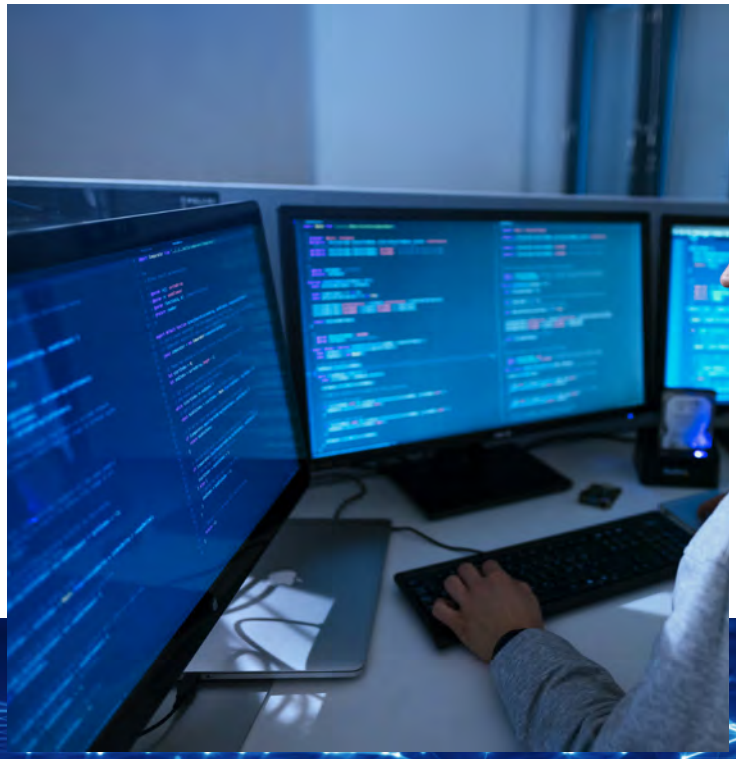
Denna guide ger vårdnadshavare, fostrare och andra som arbetar med ungdomar information om ungdomars cyberbrottslighet, ger stöd för ett ansvarsfullt beteende på nätet samt tips om lagliga möjligheter inom informat-ionsteknik. Syftet med guiden är att vara en lättförståelig informationskälla för att förebygga cyberbrottslighet bland unga samt att erbjuda stöd för att diskutera cyberfrågor med unga. Guiden tar upp cyberbrottslighet uttryckligen med tanke på nätverksbundna brott.

I det åtgärdsprogram för förebyggande av cyberbrotts-lighet bland unga som genomfördes vid centralkriminalpolisen upptäcktes ett behov av lättförståeligt och tillförlitligt material till stöd för diskussionen om cyberteman. För barn och unga är det vardag att vara aktiv på nätet, och unga kan vara mycket skickliga användare av datanät och olika applikationer och anordningar. Förståelsen för spelreglerna och gränserna för laglig och olaglig verksamhet växer dock inte alltid lika snabbt som den tekniska kompetensen. De unga kanske anser att det inte finns någon som övervakar nätet och de kanske inte förstår konsekvenserna av gärningarna. Att röra sig på nätet kan

också bli mindre uppmärksammat i vardagliga diskussioner med vuxna. Okunnighet kan leda till dåliga val, och ungdomar kan till och med välja att använda sina färdigheter för brottsliga syften, till exempel lockade av brottslingar. Därför betonas vuxnas roll när det gäller att vägleda barn och unga i säker och laglig användning av nätet.

Om tekniken och de applikationer som ungdomarna använder känns främmande för dig själv, kan det också kännas svårt att diskutera ämnet. Du ska inte i onödan oroa dig för cybersamtal. Du behöver inte vara tekniskt begåvad för att kunna tala med den unga om hur man ska agera på nätet. Det räcker med att en vuxen är närvarande, lyssnar och diskuterar, och på så sätt kanske du också ökar din egen förståelse om datanäten. I denna guide hittar du information om cyberbrottslighet bland unga, lagstiftning om verksamhet i datanät i Finland, stöd för att diskutera cyber-teman samt anvisningar för olika problemsi-tuationer i webbmiljöer. Guiden ger också dem som är intresserade nyttiga tips om material genom vilka man kan fördjupa sig i cybervärlden.

Guiden har producerats som en del av Cybercrime Exit-projektet som medfinansieras av Centralkriminalpolisen och Europeiska unionen.



CYBERCRIME EXIT

Medfinansieras av Europeiska unionen

2 Ungdomar på nätet

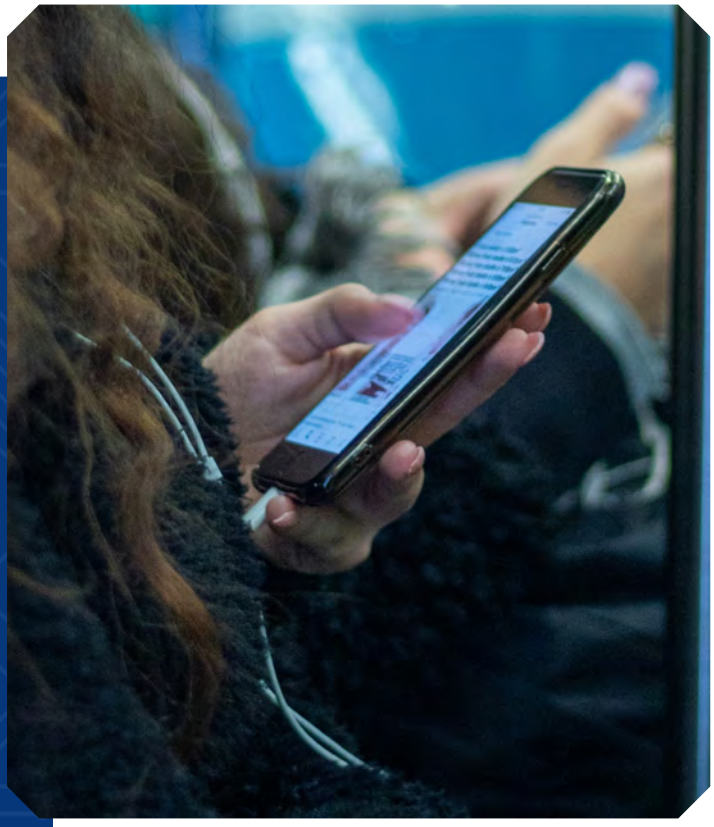
Den digitala miljön är en integrerad del av de ungas vardag. Största delen av barnen och de unga rör sig på olika webbplattformar, såsom sociala medier, spelplattformar, chattrum och webbsidor. Webbmiljön medför många möjligheter och cyberkompetensen behövs alltmer i framtiden. En aktiv användning av webbplattformar utsätter dock unga också för olika slags hot. Största delen av de unga har därför stött på någon form av ofog på nätet, såsom nätfiskeförsök, trakasserier eller innehåll som är olämpligt för barn. Olika orosmoment som gäller informationssäkerheten och de ungas säkerhet syns ofta i diskussionerna, och det är viktigt att den unga vägleds att skydda sig mot olika slags näthot. Det finns bra material om detta på polisens webbplats och i sociala medier, samt till exempel på Cybersäkerhetscentrets och på flera organisationers, såsom Rädda barnen rf:s och Mannerheims Barnskyddsförbunds webbplatser.

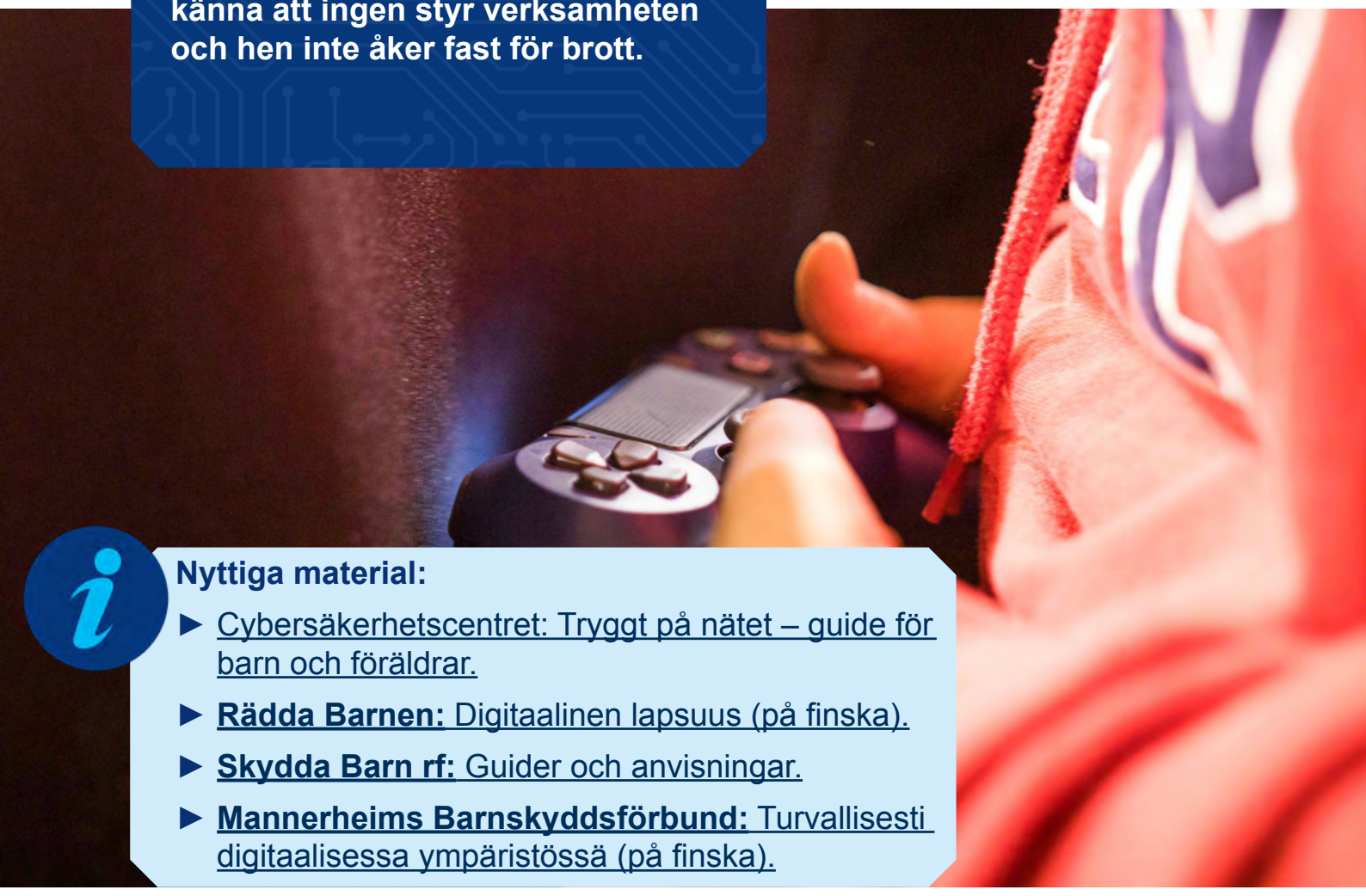
Det är lika viktigt att barn och unga vägleds att själv agera ansvarsfullt på webben. En ung persons tekniska intresse och kunnande kan vara mycket starkt. En ung person som är intresserad av cyberteman kan vara nyfiken på att testa sina färdigheter, undersöka hur plattformar och anordningar fungerar, testa verktyg och tekniker som hen hittar på nätet eller lära sig till exempel att skapa, koda eller hacka egna webbplatser, dvs. att lösa kreativa problem med datanät.

Att vara intresserad av datateknik är en bra sak, och cyberkompetens som en färdighet blir allt viktigare. Även om man mycket väl behärskar det tekniska kunnandet, är gränsen mellan laglig och olaglig nätverksamhet dock inte nödvändigtvis lika tydlig för en ung person. **Webbvärlden ger inte själv riktlinjer om vad som är rätt eller orätt eller vad som är lagligt eller olagligt.**

Medan man i den verkliga världen brukar lära ungdomar till exempel trafikregler för att de ska fungera tryggt i trafiken, måste man på samma sätt lära dem spelreglerna på nätet. Men här lämnas den unga personen ofta ensam. Ungdomar löper också risk att själva göra sig skyldiga till ofog eller brottslig verksamhet på nätet, och vuxnas vägledning behövs också i webbvärlden för att unga ska förstå gränserna för laglig och olaglig verksamhet.

Unga lär sig ofta från tidig ålder att man till exempel inte får stjäla i butiker. I den reella världen är dessutom övervakning och kontrollmekanismer starkt närvarande som styr verksamheten. I butiken finns försäljare, övervakningskameror och väktare som kan ingripa när de upptäcker att en ung person gör sig skyldig till snatteri. I datanät är motsvarande övervakning och kontroll mer begränsad och syns inte nödvändigtvis för den unga personen. Den unga personen kan känna att ingen styr verksamheten och hen inte åker fast för brott.





Nyttiga material:

- Cybersäkerhetscentret: Tryggt på nätet – guide för barn och föräldrar.
- **Rädda Barnen:** Digitaalinen lapsuus (på finska).
- **Skydda Barn rf:** Guider och anvisningar.
- **Mannerheims Barnskyddsförbund:** Turvallisesti digitaalisessa ympäristössä (på finska).

3 Vad är cyberbrott?

Med cyberbrott avses i relativt stor utsträckning olika brott som begås i eller utnyttjar datanät. Datanätsbrott kan grovt indelas i datanätsbundna och datanätsstödda brott. Med datanätsbundna brott avses brott som riktar sig mot datanät och informationssystem och med datanätsstödda brott som begås med hjälp av datanät

Datanätsstödda brott är i sig traditionella brott, och datanäten har gjort det möjligt att begå dem på nya sätt. Brottet riktar sig alltså inte egentligen mot ett datanät, och det är möjligt att begå brottet också utan datanät. **Till exempel olika nätbedrägerier, såsom så kallade romansbedrägerier, narkotikahandel på nätet eller otillåten delning av eller utpressning genom sexrelaterade bilder, är datanätsstödda brott.**

Datanätsbundna brott har däremot varit så kallade rena cyberbrott som begås i en datanätsmiljö, och det är inte möjligt att begå dem utan datanät. **Sådana brott är till exempel överbelastningsattacker och dataintrång, såsom olovlig inloggning på någon annans användarkonto.**

I cyberbrotten ingår ofta element av både datanätsbundna och datanätsstödda brott, och cyberbrotten är ofta förberedande brott för annan brottslig verksamhet

Gärningsmannen kan till exempel genom dataintrång försöka få reda på personuppgifter som gärningsmannen senare kan utnyttja för identitetsstöld eller bedrägeri. Gärningsmannen kan också till exempel bryta sig in i en annan persons digitala enhet eller på ett konto i sociala medier för att få tillgång till material med hjälp av vilket gärningsmannen kan utpressa offret.

Datanätsbundna brott

- **Brott som riktar sig mot och äger rum i datanät eller informationssystem.**
- **Sker alltid i en datanätsmiljö, det är inte möjligt att begå brottet utan datanät.**
- **Har ofta anknytning till andra brott.**
- **Till exempel dataintrång, överbelastningsattack.**

Datanätsstödda brott

- **Brott som begås med hjälp av datanät eller informationssystem.**
- **Så kallade traditionella brott som begås i en webbmiljö.**
- **Brottet riktar sig egentligen inte mot datanätet, brottet kan också begås utanför ett datanät.**
- **Till exempel nätbedrägeri, narkotikahandel på nätet.**

Läs mer:

- Strafflagen 39/1889
- Cyberbrottslighet, Polisens webbplatts, poliisi.fi.
- Uppdaterad lagstiftning finns på finlex.fi.

3.1 Cyberbrott enligt finsk lagstiftning

I Finland finns bestämmelser om nätbrott i strafflagen. I 34, 35 och 38 kap. i strafflagen finns det bland annat särskilda bestämmelser om nätbrott.

Dessutom finns det bestämmelser om datanätsbundna brott också i annan lagstiftning, såsom upphovsrättslagen.

Lagen specificerar inte direkt cyberbrott som en egen helhet, utan nätbrott har i huvudsak tagits in som en del av benämningar som omfattar gärningssätten både i och utanför datanät.

Till exempel är rekvisiten för bedrägeri eller identitetsstöld desamma oberoende av om gärningen sker i en webbmiljö eller i den reella världen.

Likaså kan störning av datatrafiken ske på nätet, men på samma sätt avses till exempel störningssamtal till nödcentralen eller förhindrande av en postanställds verksamhet.

3.2 Särdragen hos cyberbrott

Cyberbrott struntar i statsgränser. Brott kan begås från Finland var som helst i världen och omvänt utan att gärningsmannen ens har besökt landet.

Den ekonomiska skada som orsakas genom cyberbrott är ofta större än vid andra typer av brott som begås av unga. En enskild cyberhandling som också verkar harmlös kan orsaka omfattande skada.

Till exempel överbelastningsattacker (DDoS, distributed denial of service) beskrivs ofta som en ofarlig digital trafikstockning. I värsta fall kan en överbelastningsattack dock orsaka allvarlig skada för en individ eller ett företag och till och med påverka verksamheten i samhällets kritiska infrastruktur, såsom elnätet eller nödcentralsverket.

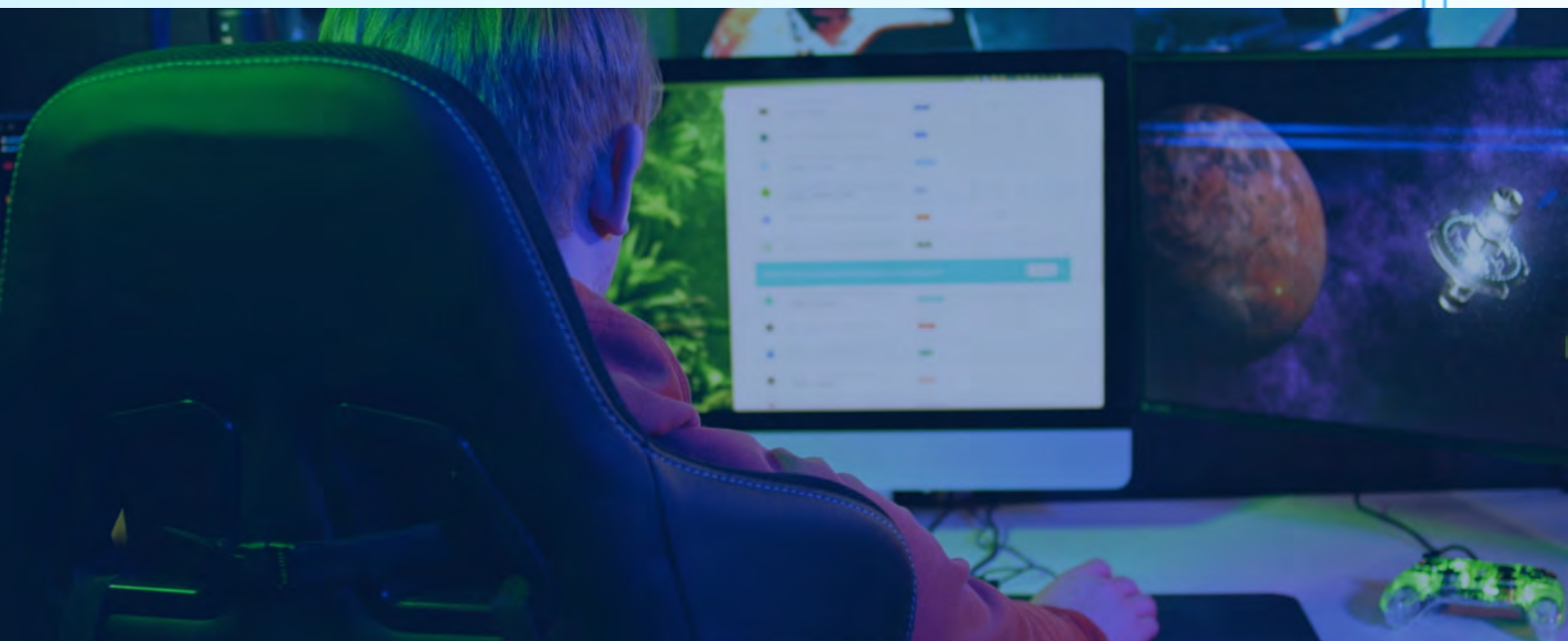
Överbelastningsattacker är mycket vanliga bland unga i synnerhet i spelmiljöer där så kallad doxing utnyttjas som en effekt inom spelupplevelser på samma sätt som spelmodifieringar och bedrägerier. En ung person kan till exempel försöka störa motspelarens verksamhet för att vinna spelet.

Via de allmänna sökmotorerna är det relativt lätt att hitta **anvisningar och verktyg som lämpar sig för att begå cyberbrott.** Dessutom finns anvisningar och tips tillgängliga för unga i olika diskussionsforum och kanaler, såsom en diskussionsapplikation i Discord eller en videotjänst i YouTube.

Det är möjligt att beställa nätbrott som köpta tjänster (**Crime-as-a-Service, CaaS**). Vem som helst kan med hjälp av köpta tjänster relativt enkelt angripa ett visst mål utan att användaren själv behöver ha betydande datateknisk kompetens.

Även ett angrepp med automatiserade verktyg är ett brott. Dessutom kan gärningsmannen vid användning av automatiserade verktyg inte nödvändigtvis själv på förhand försäkra sig om omfattningen av eller det verkliga föremålet för attacken.

Oförmåga att förstå konsekvenserna av verksamheten undanröjer inte straffansvaret.



4 Cyberbrottslighet bland unga i Finland

4.1 Kompetens

I nyheterna framhävs ofta cyberattacker som utförs av organiserade kriminella grupper och statliga aktörer. Många kan bli förvånade över hur stor del av cyber-brotten som i verkligheten begås av enskilda personer, såsom unga. Också föremålet för cyberbrott är enligt brottsstatistiken oftast en enskild person och dennes användarkonto. Både i Finland och internationellt har den genomsnittliga åldern för dem som begår cyberbrott sjunkit snabbt, och också barn under straffansvarsåldern, till och med barn i lågstadieåldern, gör sig skyldiga till cyberbrott varje år. Också i Finland grips personer under 15 år årligen för cyberbrottsliga gärningar.

För att ett cyberbrott ska kunna begås krävs inte nödvändigtvis stor teknisk kompetens, utan i ett cyberbrott kan det som enklast vara fråga om en mycket vardaglig gärning, såsom olovlig användning av en väns användarkonto. Verktyg och anvisningar som används för att begå cyberbrott är numera lättillgängliga för unga på ett öppet nät. Sådana tjänster kan till och med hittas genom enkel sökning i allmänna sökmotortjänster. Tjänsterna är ofta billiga eller också kan det vara möjligt att testa dem gratis, vilket gör tjänsterna lättillgängliga också för unga. Allt yngre barn rekryteras också till brottslig verksamhet på olika webbforum.

En ung person kan till exempel genom att använda köpta tjänster i praktiken utföra en mycket skadlig överbelastningsattack från sin egen dator genom att trycka på några knappar, utan att den unga personen kanske själv ens förstår hur attacken sker och vilken skada den orsakar.

> **De ungas tekniska kompetens får dock inte underskattas. En del unga som gör sig skyldiga till cyber-brott är mycket kunniga i datateknik och kan självständigt genomföra komplicerade cyberattacker. Förövarna av allvarliga cyberbrott har också ofta omfattande teknisk kompetens..**

4.2 Motiv

Vardagliga motiv

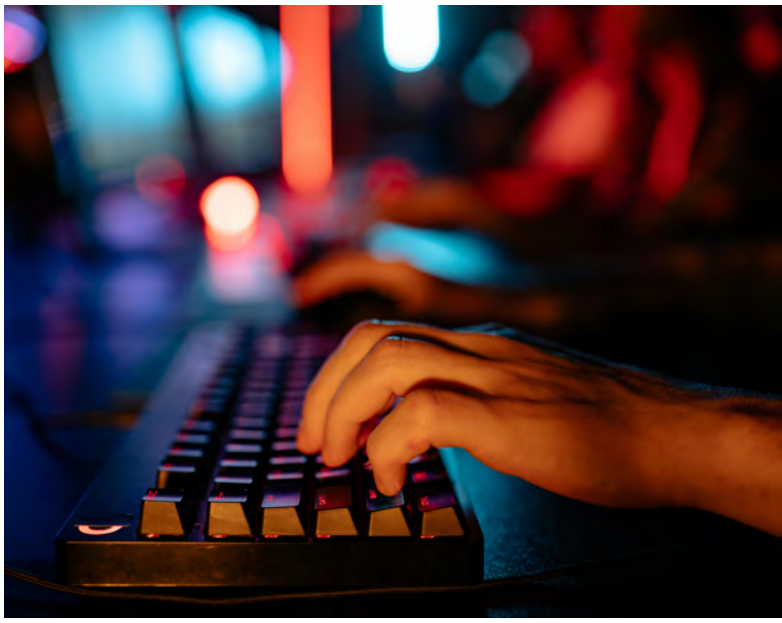
I synnerhet i början av den brottsliga verksamheten är motiven för ett cyberbrott som en ung person begått ofta ganska harmlösa och vardagliga. Till en början strävar den unga ofta inte efter ekonomisk vinning och försöker inte orsaka skada, utan bakgrunden till gärningen kan vara till exempel spänning, nyfikenhet, ofog eller till exempel svartsjuka. En ung person kanske vill testa sina färdigheter och pröva gränser och kanske inte förstår eller bryr sig om verksamheten blir olaglig. Även en gärning som är avsedd att vara ofarlig kan dock orsaka omfattande skada. Också ekonomiska motiv kommer i allmänhet i något skede med i verksamheten, när den unga upptäcker att hen genom verksamheten kan tjäna pengar.

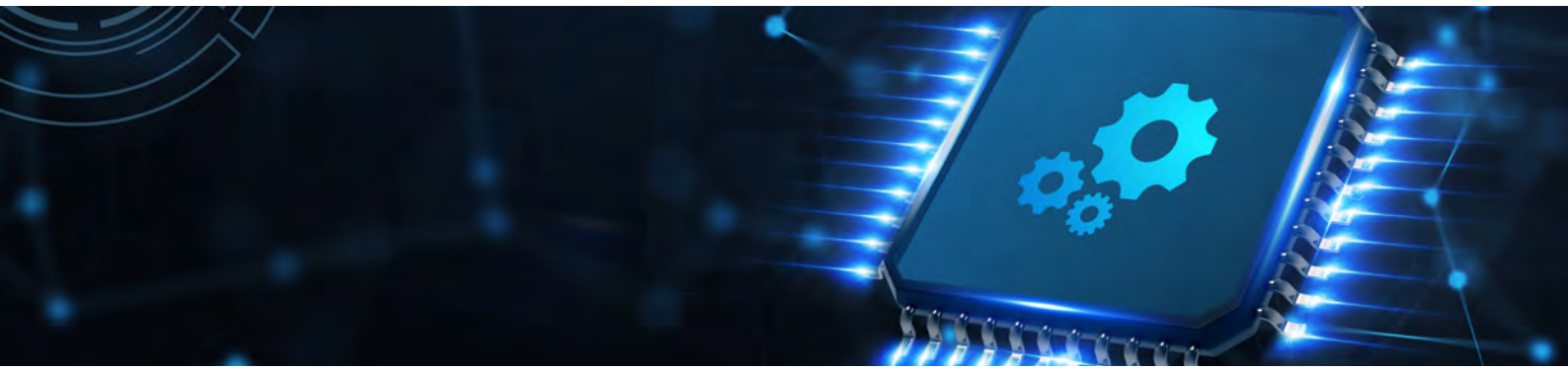
Beteendet blir vanligt på webbplattformar

En viss typ av beteende på webbplattformar kan vara så vanligt att den unga inte nödvändigtvis uppfattar verksamheten som störande eller brottslig. Till exempel på spelplattformar är det beklagligt vanligt med doxing, dvs. överbelastningsattacker. Det är ofta rent ofog som ligger bakom doxingen, och den unga kanske inte uppfattar det som brottslig verksamhet. Enligt undersökningar fungerar dock doxingen ofta som den ungas första kontakt med cyberbrott och kan normalisera brottslig verksamhet på nätet, vilket skapar grund för en allvarligare brottsspiral.

Haktivism

Ungdomar kan också lockas att göra cyberattacker under förevändning av aktivism i cybermiljö. I hacktivism utnyttjas cyberattacker som ett verktyg för aktivism på nätet, som ett försök att visa missnöje eller åstadkomma förändringar. Motiven till hacktivism är oftast politiska. Typiska former av hacktivism är till exempel överbelastningsattacker mot statliga aktörer. En ung person som deltar i en attack kan tro att hen handlar för en god sak. Men i verkligheten kan det vara svårt för en ung person att veta vad som är det verkliga målet för ett angrepp och vilka konsekvenser det får.





Nätgemenskaper och lockande till kriminell verksamhet

Unga kan delta i brottslig verksamhet också som en del av en större lokal eller internationell nätgrupp. Kriminella grupper kan bildas på nätet i olika forum eller till exempel på spelplattformar. Brottslig verksamhet bedrivs både i och utanför det öppna nätet, till exempel i TOR-nätet. Det är relativt lätt att gå med i grupper oberoende av geografiskt läge, och en ung person kan hamna i nätgrupper bland annat genom spel som är populära bland unga eller genom andra populära plattformar. Medlemmarna i nätgruppen kan också aktivt närma sig en ung person på webbplattformarna och locka hen att delta i brottslig verksamhet.

En ung person kan lockas med ekonomiska motiv eller bland annat genom att göra verksamheten **spelbetonad**, dvs. genom att kamouflera brottsliga gärningar till tekniska utmaningar eller spel. Olika synligt aktiva kriminella grupper eller bevittnande av olaglig handel på nätet kan också väcka ungas nyfikenhet och öka intresset för kriminella nätgrupper. Vissa webbplattformar har ett så kallat **rankingsystem** där mer erfarna användare har högre status. En användare med hög status kan lättare få den ungas förtroende och kan locka med den unga personen att delta i en grupp utanför webbplattformen i syfte att till exempel rekrytera den unga personen till brottslig verksamhet.

Kriminella grupper vill gärna ofta locka ungdomar att utföra brott. Unga under 15 år är inte straffrättsligt ansvariga i Finland. Dessutom beaktas den misstänktes ålder vid bedömningen av skuld och konsekvenserna av brottet, om den misstänkte är under 21 år. Ungdomar kan därför lockas till brottslig verksamhet på nätet just på grund av sin unga ålder.

På webbplattformar kan unga också användas som hjälpmedel för brott till exempel vid penningtvätt. En vän som är bekant från nätet kan skicka pengar till en ung person till exempel i virtuell valuta och genom påhittade orsaker be den unga personen att skicka pengarna vidare till en annan användare eller tillbaka till personen i reell valuta. Den som ber om tjänsten erbjuder den unga personen en liten summa pengar som tack för tjänsten. Den unga personen kan tro att hen tjänar lätta pengar, och hen kanske inte förstår att något fel har begåtts eller är inte medveten om verksamhetens verkliga omfattning.

4.3 Skador

Ett cyberbrott kan orsaka betydande skada. Brottet kan orsaka offret utöver ekonomisk skada också långvarigt mänskligt lidande. Brott kan också försvåra verksamheten i företag eller hela samhället, och konsekvenserna kan i värsta fall vara mycket allvarliga. När en ung person är verksam på nätet förstår hen inte nödvändigtvis hur omfattande skada verksamheten kan orsaka. Även i Finland har det förekommit fall där en gärning som begåtts i syfte att provocera har orsakat skador på hundratusentals euro. När den unga personen agerar som en del av en nätgrupp kanske hen inte ens känner till verksamhetens verkliga omfattning eller den brottsskada som har orsakats. Också ett barn under 15 år är skyldigt att ersätta den skada som det orsakat.

Ungdomar utförde överbelastningsattacker på skolans server i syfte att störa skolans Wilma-system. Attackerna lamslog också flera andra kommunala system, vilket påverkade arbetet för tusentals kommunala arbetstagare. Reparationsarbetet tog flera dagar och attacken orsakade kommunen omfattande ekonomisk skada.

4.4 Konsekvenser

Cyberbrotten kan vara mycket allvarliga och omfattande och till och med utgöra ett hot mot samhällets funktion och kritisk infrastruktur. Överskridandet av brottströskeln kräver inte omfattande verksamhet, och gärningar som var avsedda som ofog eller skämt kan uppfylla rekvisitet för brott. Även ett brott som har begåtts som ofog kan ha långvariga konsekvenser för den unga personen.

Skadeståndsansvar: Skadestånd till följd av cyberbrott kan bli omfattande och påverka den ungas liv långt in i framtiden. Också ett barn under 15 år är skyldigt att ersätta den skada som det orsakat.

Straffrättsligt ansvar: En ung person över 15 år är också straffrättsligt ansvarig för ett brott. Ett cyberbrott kan leda till böter eller fängelse samt en anteckning i straffregistret. En anteckning i straffregistret kan medföra svårigheter för den unga att få en studie-, praktik- eller arbetsplats samt begränsa möjligheterna att resa till vissa länder.

Förlust av utrustning: Utrustning som används för att begå ett brott, såsom den ungas telefon, surfplatta eller dator, kan beslagtas och förverkas till staten.

Förlust av åtkomst: Webbplattformar kan blockera konton som används för brottslig verksamhet, till exempel en ung persons spelkonto, som den unga kan ha satsat mycket tid och eventuellt också pengar för att bygga upp.

4.5 Exempel på cyberbrott som begåtts av unga

Dataskadegörelse SL 35:3 §

Obehörigt förstörande, försämrande, döljande, ändrande av data på ett datamedium eller i ett informationssystem.

Ett par prov har gått dåligt, och den unga personen är arg över de dåliga vitsorden hen fått. Den unga personen loggar utan tillstånd in i lärarens Wilma-system med ett lösenord som hen snokat fram och ändrar de dåliga vitsorden till bättre.

Störande av post- och teletrafik SL 38:5 §

Att störa eller hindra post-, tele- eller radiotrafik till exempel genom att ingripa i anordningars funktion eller sända störande meddelanden.

En ung person vill orsaka förtret för sin skola, och med hjälp av ett program som hen hittar på nätet skickar hen en mycket stor mängd skräppost till skolans e-postlåda och stör skolans e-posttrafik.

Systemstörning SL 38:7 a §

Obehörigt hindrande eller störande av informationssystemets funktion till exempel genom att mata in, skada, ändra eller undertrycka data.

En ung person spelar ett lagspel på nätet, och när hens lag förlorar hamnar hen ur spelet. Den unga personen är arg över förlusten och med hjälp av en booter-tjänst på nätet att gör hen en överbelastningsattack på spelservern som för en stund avbryter verksamheten på spelservern så att inte heller andra kan spela.

Dataintrång SL 38:8

Att obehörigt göra intrång i ett informationssystem eller ta reda på skyddade uppgifter i ett system, till exempel genom att olovligen använda någon annans lösenord eller genom att kringgå systemets skydd.

Unga personer har sinsemellan delat användarkoder till en webbtjänst. En av de unga kommer på att hen med samma koder också kan logga in på en annan ung persons konto i sociala medier. Den unga personen loggar in på ett konto i sociala medier utan tillstånd och skickar fräcka meddelanden i en annan ung persons namn.

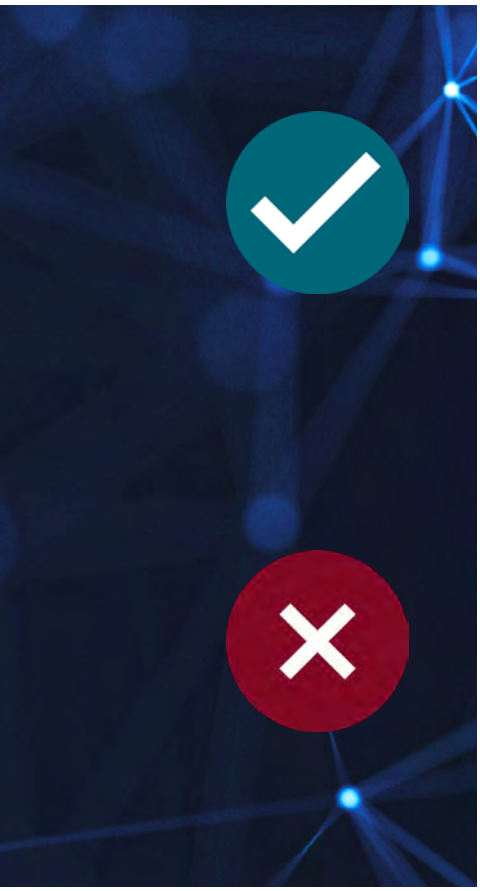
Kränkning av kommunikationshemlighet SL 38:3 §

Obehörigt öppnande av brev eller meddelanden till någon annan, intrång i skyddade elektroniska meddelanden eller avlyssning av meddelanden eller samtal.

En ung person får tillgång till sin skolkamrats telefon och läser obehörigt sms på telefonen och privata meddelanden i sociala medier. Den unga personen sprider personlig och känslig information i meddelandena till andra elever i skolan.

4.6 Kännedom om gränsen mellan laglig och olaglig verksamhet

Gränsdragningen mellan laglig och olaglig verksamhet kan ibland vara svår, och flera faktorer påverkar bedömningen av lagligheten. Också verksamhetsmiljön, de verktyg som använts och verksamhetens syfte har betydelse, och verksamhetens laglighet kan behöva bedömas från fall till fall. Det lönar sig därför att tillsammans med den unga fundera över gränserna för verksamhet på nätet i olika vardagliga situationer. Som hjälp kan man använda till exempel följande situationer.



Användarkoder

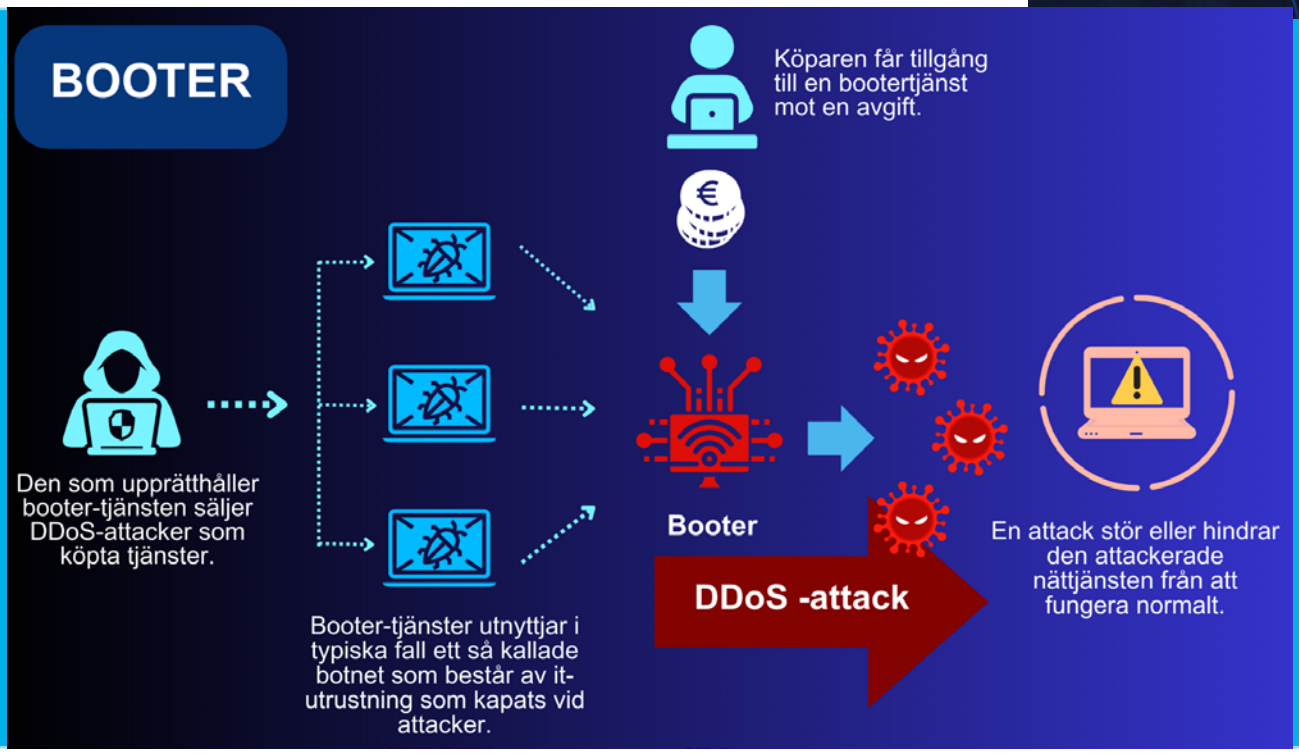
Ungdomar kan ibland låna varandras användarkonton för olika ändamål, till exempel för att spela spel på nätet eller för att titta på innehåll i sociala medier. Det lönar sig aldrig att dela ut sina egna användarkoder till någon, eftersom delning av användarkoder kan leda till missbruk. Användningen av en annan persons användarkoder är i princip inte olaglig, om den som äger användarkoderna har gett sitt tillstånd att använda dem. Lagen förbjuder alltså inte direkt unga att till exempel använda varandras koder för sociala medier eller spelkonton, om båda parter har gett sitt samtycke till användningen av koderna. Många kan också låna sinsemellan till exempel koder för strömningstjänster.

Nyttjanderätten är dock begränsad till en gemensamt överenskommen användning. Om koderna används i större utsträckning än vad som avtalats eller om man med koderna försöker logga in i tjänster som innehavaren av koderna inte har gett lov till, kan man göra sig skyldig till brott. På samma sätt kan det vara olagligt att köpa en avgiftsbelagd tilläggsdel i en tjänst med någon annans koder, om kontoinnehavaren inte har gett sitt tillstånd till köpet. Det är också bra att beakta att verksamhet som inte direkt bryter mot lagen dock kan strida mot användningsvillkoren för tjänsten och orsaka problem. Flera strömningstjänster förbjuder bland annat att koder delas ut utanför det egna hushållet.

Belastningstestning

Så kallade **stress- eller belastningstester** av informationssystem är i princip tillåten, förutsatt att testningen utförs med tillstånd av systemägaren och med lagliga medel och testningen inte påverkar andra tjänster eller anordningar på nätet. Stresstester är en vanlig del av företagens informationssäkerhetstester, och flera företag inom informationssäkerhetsbranschen tillhandahåller tjänster i anslutning till detta. Till exempel funktionen på en egen webbplats eller spelserver kan alltså i princip testas, förutsatt att testningen utförs med lagliga verktyg och att testningen till exempel inte utnyttjar ett botnet eller stör andra system. Före testningen lönar det sig därför att försäkra sig om att de verktyg som används är lagliga och fungerar. I tveksamma situationer är det vid testning säkrare att vända sig till ett officiellt företag inom informationssäkerhet.

Däremot är det i regel olagligt att göra en överbelastningsattack utan tillstånd av systemägaren eller med hjälp av en booter-tjänst. BWebbplatser som säljer booter-tjänster kan hävda att de erbjuder verktyg som lämpar sig för säkerhetstester. I själva verket utnyttjar bootertjänsterna dock vanligen olaglig infrastruktur för att fungera, såsom ett botnet som har kapats genom dataintrång och med hjälp av vilka överbelastningsattacker utförs. Vid användning av booter-tjänster är det också svårt att fastställa vad som i verkligheten påverkas av attacken. Genom att använda en booter-tjänst till exempel för att testa sin egen spelserver kan man alltså omedvetet också störa funktionen hos en server som man inte har rätt till eller något annat system. Det är i regel också olagligt att använda lagliga verktyg, såsom verktyg för massmejl, för att störa datatrafiken till exempel genom att skicka skräppost.

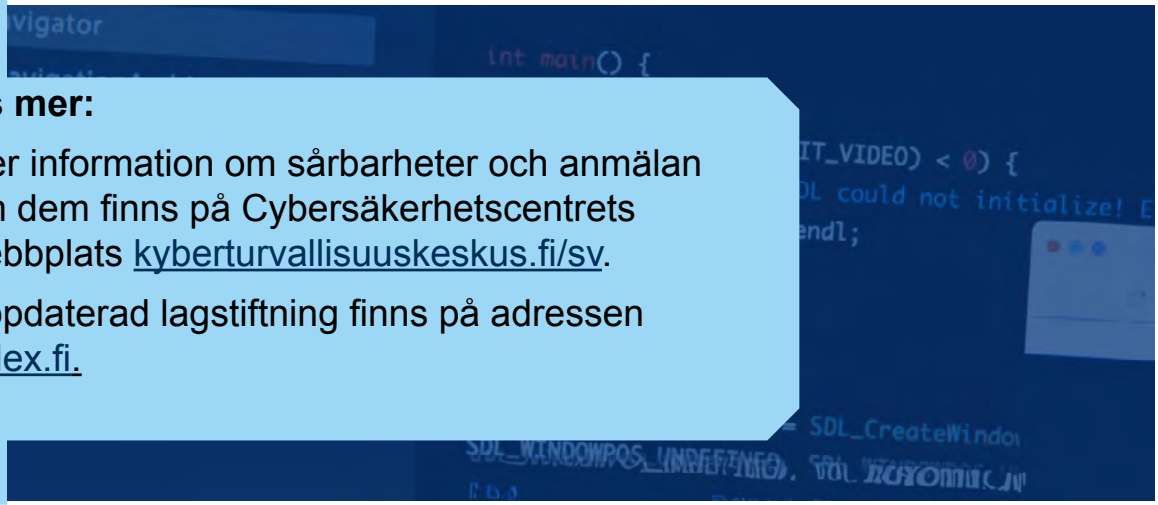


Sökning efter säkerhetshål

Det är inte i sig olagligt att söka eller upptäcka sårbarheter. Informationssäkerhetstester och sökande av sårbarheter (på engelska penetration testing, pentesting) är ofta en viktig del av tryggandet av företagens informationssäkerhet. Företagen kan också anordna bug bounty-program där hackare med företagets tillstånd kan söka efter sårbarheter i företagets system. En skicklig användare kan också råka stöta på en sårbarhet. Verksamhetens laglighet beror bland annat på vilka åtgärder som används för att söka en sårbarhet, hur långt man undersöker om sårbarhetens användning orsakar skada och om sårbarheten på något sätt utnyttjas olovligt.

När man bedömer om den egna verksamheten är tillåten är det bra att beakta till exempel följande faktorer:

- **I vilken verksamhetsmiljö jag rör mig.** Allt oftare agerar man i någon form av nätverksmiljö, och då måste man fundera över vad som är tillåtet just i denna nätverksmiljö. Det kan till exempel vara tillåtet att skanna sårbarheter i det egna systemet i ett internt nätverk, men samma verksamhet i ett externt nätverk eller via en virtuell server kan redan vara olaglig.
- **Vem som äger det system som testas** och om systemets ägare har gett sitt tillstånd. Det är en sak att undersöka sitt eget system, än till exempel skolans system.
- **När går verksamheten för långt.** Det lönar sig i regel inte att undersöka sårbarheter utan tillstånd, eftersom en undersökning av sårbarheten kan leda till olaglig verksamhet.
- **Det lönar sig alltid att göra en anmälan.** Ibland är det möjligt att en brist i informationssäkerheten av misstag eller nyfikenhet undersöks längre än vad som kanske är tillåtet, och därför tvekar du kanske att anmäla en sårbarhet. Det lönar sig dock alltid att anmäla en identifierad brist i informationssäkerheten, även om du redan hunnit undersöka bristen. Anmälan orsakar alltid mindre skada än om du låter bli att att göra en anmälan.



Läs mer:

- Mer information om sårbarheter och anmälan om dem finns på Cybersäkerhetscentrets webbplats kyberturvallisuuskeskus.fi/sv.
- Uppdaterad lagstiftning finns på adressen finlex.fi.

5 Vi ska tillsammans stödja ansvarsfullt beteende på nätet

Barn är ofta mycket skickliga på att använda teknik. Det är dock viktigt att barnet får stöd när det lär sig att agera i den digitala världen. På samma sätt som man med barnet går igenom till exempel trafikregler, behöver barnet och den unga också handledning av vuxna för att förstå spelreglerna på nätet och kunna agera ansvarsfullt och lagligt på nätet.

5.1 Fråga, lyssna, var närvarande

Att diskutera den ungas verksamhet på nätet behöver inte vara konstigare än att tala om något annat delområde i den ungas liv. Viktigare än teknisk kompetens är att vara närvarande, visa intresse för den ungas angelägenheter och vilja att lära sig och förstå. En ung person berättar ofta gärna mer om ämnet, om någon visar intresse för ett ämne som är viktigt för den unga.

En stor del av den ungas liv och sociala relationer kan finnas på nätet. För den unga är olika hobbyer på nätet, såsom videospel, samt relationer och gemenskaper som bildats på nätet ofta lika viktiga som i verkligheten. Cybermiljön och den riktiga världen är inte olika verkligheter för den unga, utan fungerar som en komplettering av varandra.

- **Intressera dig för den ungas hobbyer och relationer på nätet**.

  Inkludera den ungas digitala liv i era dagliga diskussioner på samma sätt som diskussioner om livet i den reella världen. Det är också lättare för unga att berätta om problem som de stöter på i nätet, om diskussioner om cybermiljön är en normal del av vardagen.

- **Lär känna de plattformar och appar som den unga använder och diskutera med hen regelbundet om dessa**.

  Du behöver inte veta allt för att diskutera trygg användning av appar med den unga.

- **Bekanta dig med den terminologi som används i webbvärlden**.

  Allt behöver du inte veta, men det är lättare att inleda en diskussion om du som vuxen har en uppfattning om termer som används i samband med datanät.

- **Var nyfiken och ställ frågor**.

  De flesta av oss tycker om att diskutera sina egna intressen, och ungdomar är inget undantag. En ung person som är intresserad av informationsteknik tycker ofta om att berätta mer om ämnet, om du visar intresse för den ungas hobby och du vill lära dig. Du ska inte vara rädd för att visa din okunnighet.

  Det är bättre att ställa frågor och be den unga personen förklara till exempel främmande termer eller plattformarnas funktion än att du gör antaganden och eventuellt missförstår vad det är fråga om.

Genom diskussionerna kan du lära dig mer om den ungas hobby och intressen och eventuellt också få mer information om i vilka kretsar den unga rör sig på nätet.

- **Diskutera laddningen av nya spel och appar med barnet och den unga personen och bekanta er med apparna tillsammans**.

  Det lönar sig också att bekanta sig med verktyg för åtkomstkontroll och diskutera med barnet och den unga personen om de eventuellt behövs.

- **Gå igenom integritetskunskap tillsammans med barnet och den unga personen med tanke på obehörigt närmande**.

  Det lönar sig till exempel i regel inte att godkänna okända personer som vänner i sociala medier, och det lönar sig inte att skicka bilder av sig själv till andra. Det är också bra att diskutera vilken typ av information den unga personen sprider om sig själv på webben och påminna om att det nästan är omöjligt att helt ta bort innehåll som publicerats på webben.

- **Stöd en digitalt begåvad ung person att utveckla sina färdigheter på ett tryggt och lagligt sätt.**

  Att en ung person är intresserad av cyber är en fin sak, och det är värt att uppmuntra hen att utveckla sina färdigheter – inom laglighetens gränser. Det är bra att känna till lagar om datanät och tillsammans med den unga diskutera spelreglerna och gränserna för vad som är lagligt.

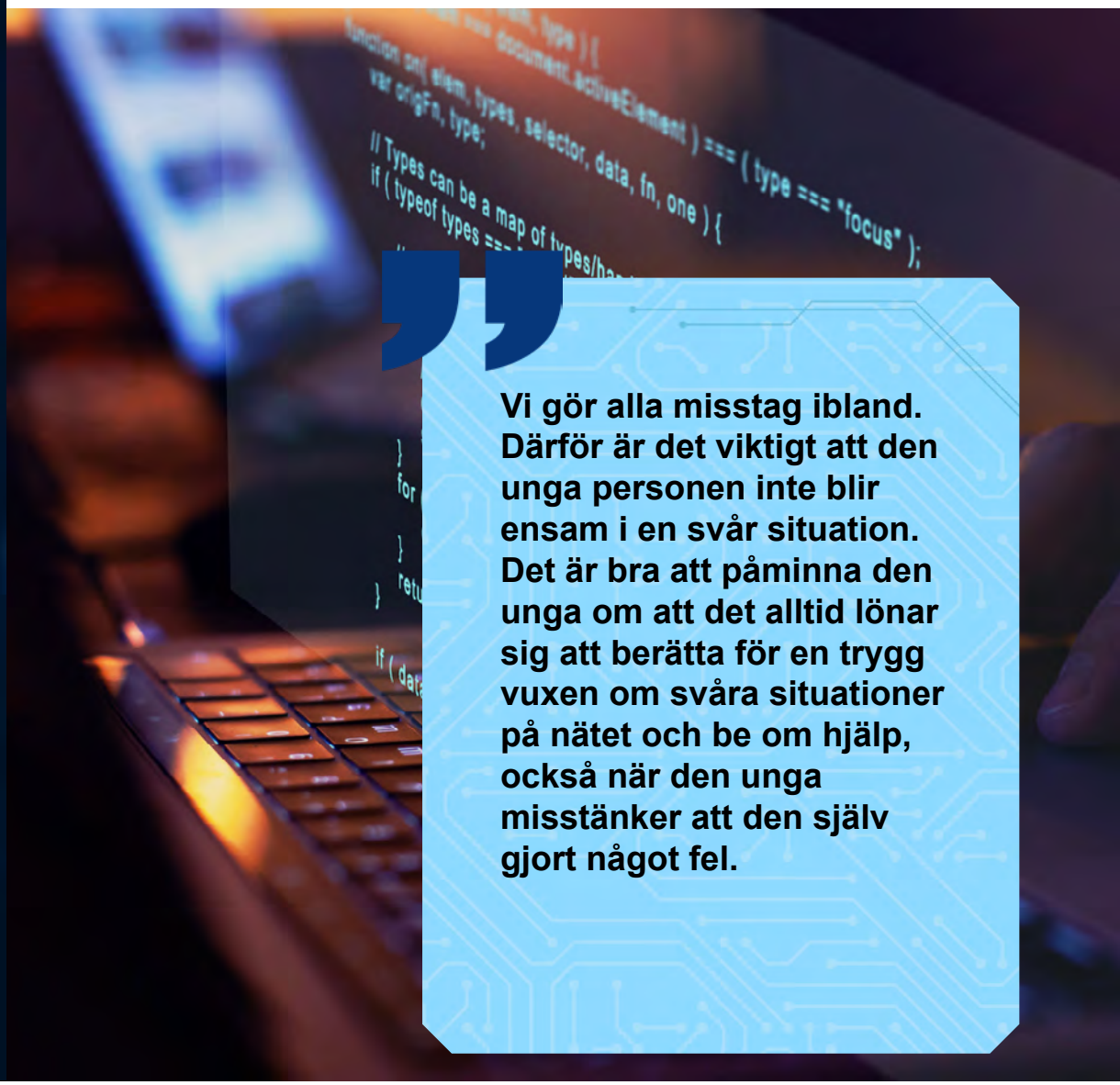
- **Diskutera med den unga om ansvarsfull verksamhet på nätet och gränserna för laglig och olaglig verksamhet.**

  Om något är olagligt utanför nätet är det sannolikt olagligt också i nätmiljön. Det lönar sig också att förhålla sig skeptisk till en begäran som låtsas vara brådskande. Innan man agerar är det bra att stanna upp och kontrollera om verksamheten är laglig och tillåten. En bra regel för verksamhet på nätet är att det är bättre att låta bli sådan verksamhet som väcker funderingar på om den är tillåten.

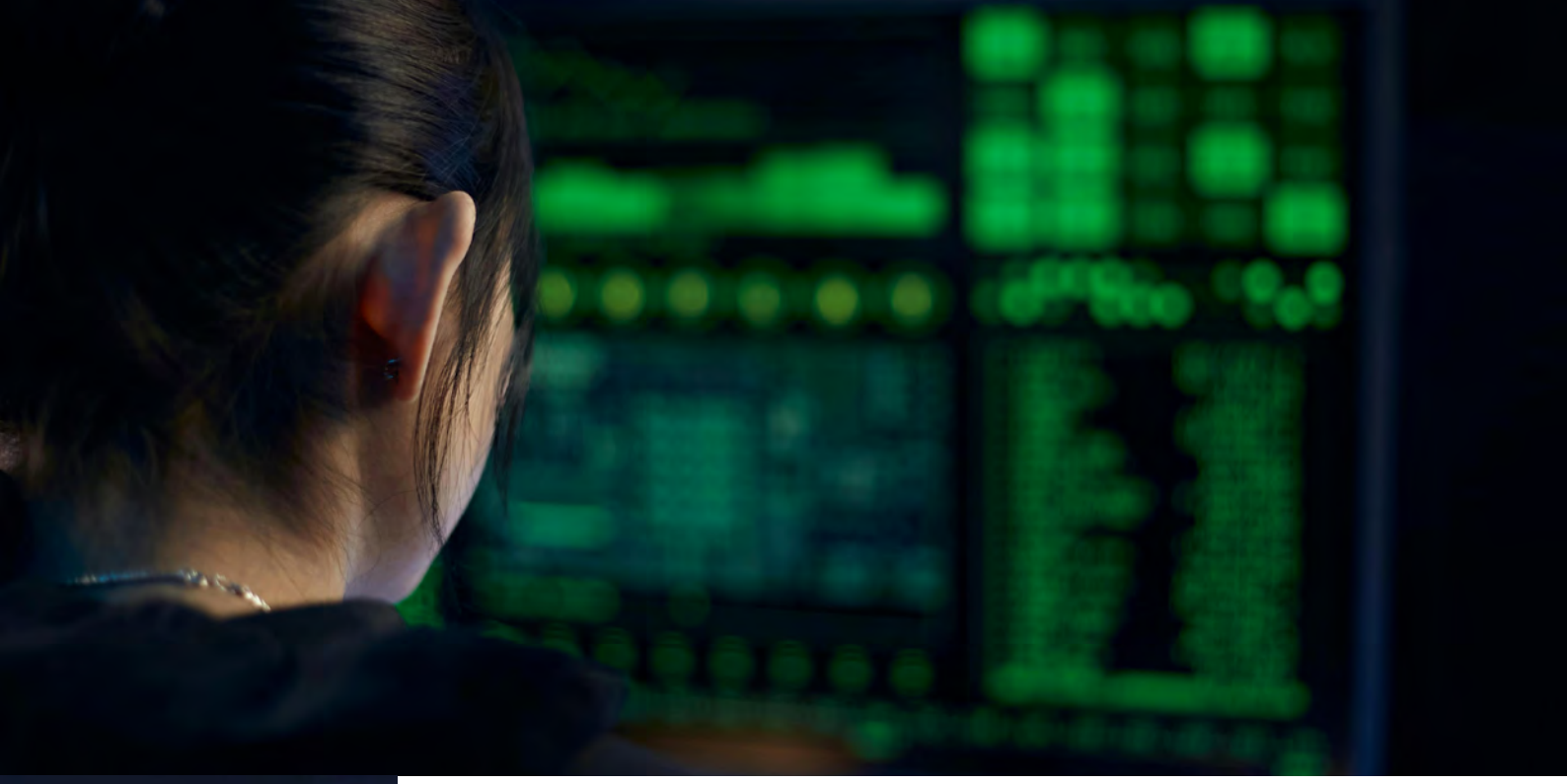
Det är också bra att diskutera i vilka webbgemenskaper den unga tillbringar sin tid och styra den unga bort från skadliga webbgemenskaper. Man kan närma sig ämnet till exempel utifrån tidsanvändningen. Cyberhobbyer kan vara till stor nytta i framtiden, och olika projekt och tävlingar kan hjälpa den unga att lyfta fram sitt kunnande. Genom positiva webbgemenskaper kan den unga bilda nätverk och bekanta sig med likasinnade vänner samt eventuellt hitta intressanta projekt och arbetsmöjligheter i framtiden.

Däremot är det svårt att lyfta fram kunnande som förvärvats genom cyberbrottslig verksamhet eller webbgemenskaper som är verksamma i gråzonen. Inom informationssäkerhetsbranschen kan den unga inte skryta med cyberbrott, och cyberbrottslig verksamhet kan till exempel inte läggas till i meritförteckningen.

Det är bra att redan på ett tidigt stadium klargöra sambandet mellan de åtgärder som vidtas på nätet och deras konsekvenser. Använd de rätta termerna och förklara dem på ett begripligt sätt för barnet eller den unga personen. Särskilt med barn är det viktigt att betona att det är fel att begå brottsliga gärningar, utan att för den skull döma barnet för en gärning.



Vi gör alla misstag ibland. Därför är det viktigt att den unga personen inte blir ensam i en svår situation. Det är bra att påminna den unga om att det alltid lönar sig att berätta för en trygg vuxen om svåra situationer på nätet och be om hjälp, också när den unga misstänker att den själv gjort något fel.

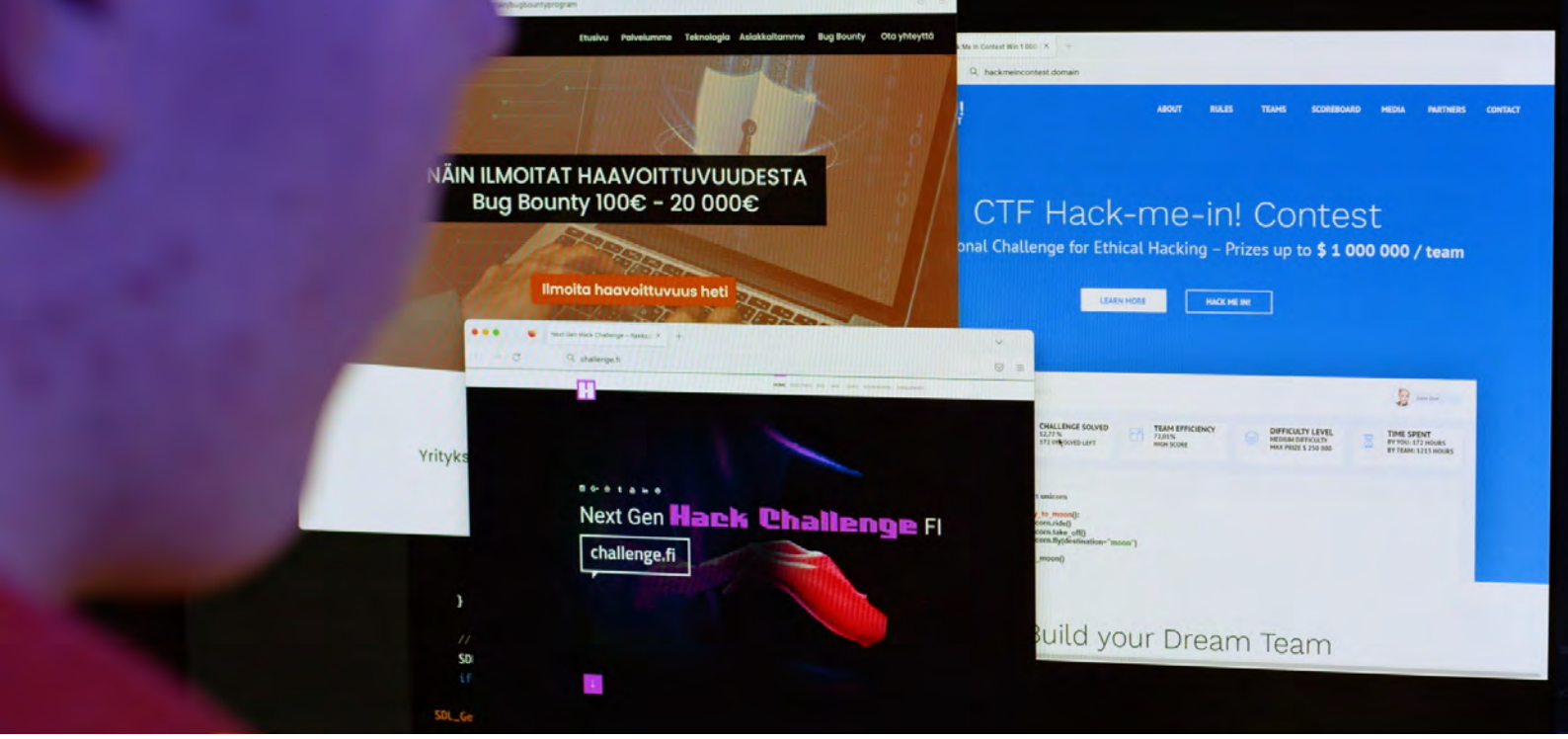


5.2 Är barnet intresserat av hackning eller datasäkerhetstestning?

I cybermiljöer finns många intressanta, lagliga möjligheter som man kan bekanta sig med tillsammans med en ung person. Behovet av utbildade inom informationssäkerhetsbranschen ökar hela tiden, och cyberteknik kan också bli ett yrke för unga som är intresserade av branschen. Både i Finland och utomlands finns det ett stort antal olika företag inom informationssäkerhetsbranschen där det behövs experter. Dessutom ökar sammanslutningar inom cyberbranschen, såsom lokala CitySec-sammanslutningar, också i Finland.

I detta avsnitt ges några exempel på lagliga alternativ för att öva och utveckla cyberfärdigheter. När man överväger alternativen är det bra att först försöka gestalta den ungas kompetensnivå och intressen.

En ung persons tekniska färdigheter kan, trots den unga åldern, snabbt utvecklas till en mycket hög nivå till exempel via tutorialer på webben och webbplatser som stöder hobbyn. Därför är det viktigt att den unga har tillräckligt med intressanta lagliga alternativ och utmaningar.



Sandlådemiljöer

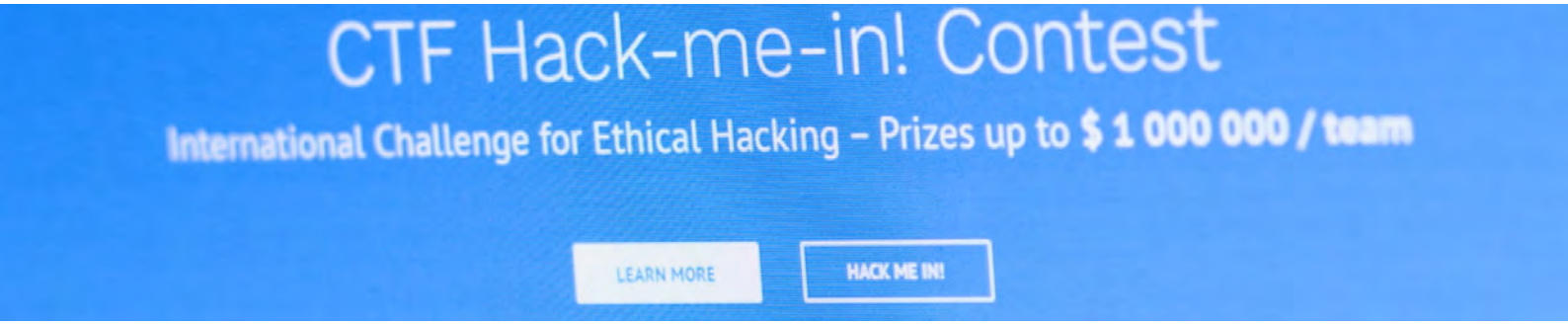
Det lönar sig inte att testa informationssäkerheten på egen hand, eftersom det alltid innebär risker. I värsta fall kan testning på eget initiativ leda till straffansvar. Hackning kan dock provas på ett säkert sätt i olika sandlådemiljöer.

Flera webbplatser erbjuder virtuella träningsmiljöer, så kallade sandlådemiljöer, där den unga kan testa sina färdigheter och öva cyberkompetens på ett säkert och lagligt sätt. Det lönar sig att vägleda unga som är intresserade av hackning och informationssäkerhetstester att utveckla sina färdigheter i trygga webbmiljöer som är avsedda för verksamheten. Dessa hittar man på webben till exempel via allmänna sökmotorer med sökord: etisk hackning, lär dig hacka, öva etisk hackning, learn ethical hacking. Om den unga redan har sökt efter brister i informationssäkerheten, är det bra att tillsammans med den unga gå igenom hur och var dessa anmäls och diskutera gränserna för informationssäkerhetstestningen tillsammans.

CTF -tävlingar

Den unga kan också utnyttja till exempel olika CTF-tävlingar. Capture the Flag, ”Fånga flaggan”, det vill säga. CTF-tävlingar, är hackningsutmaningstävlingar där man försöker lösa en utmaning i en sandlådemiljö eller en rad utmaningar som gäller informationssäkerheten. Utmaningarna gäller olika informationssäkerhetssituationer, såsom sökning efter sårbarhet i en kod, återmodellering eller till exempel dekryptering. Efter att ha löst utmaningen får spelaren ”flaggan”, och genom att lämna tillbaka flaggan får spelaren ett överenskommet poängtal för utmaningen. CTF-tävlingarna innebär utmaningar på olika nivåer och är ett säkert och inspirerande sätt att bekanta sig med hackning.

En känd CTF-tävling är European Cybersecurity Challenge, som arrangeras av Europeiska unionens byrå för nät- och informationssäkerhet ENISA. Man kan delta i Finlands tävlingsteam genom att klara sig i Finlands uttagningsprov, som ordnas av Next Gen Hack Finland ry.



Bug bounty-program

En mer erfaren hackare kan också testa sina färdigheter genom att delta i olika bug bounty-program. Bug bounty, dvs. bugbelöningsprogram, är ett program som tillhandahålls av en organisation eller plattform och där deltagarna med lov kan söka efter brister i informationssäkerheten i en på förhand avtalad miljö. De som anmäler sårbarheter får belöningar, såsom penningbelöningar, för att upptäcka sårbarheter. Bug bounty-programmen är vanligen begränsade till en viss på förhand definierad del av organisationens system eller plattform, och programmen måste i allmänhet registreras i förväg. Programmet kan pågå under en begränsad tid eller kontinuerligt. Storleken på belöningarna varierar beroende på programmet och hur allvarlig den identifierade sårbarheten är.

Företag kan använda bug bounty-plattformar för att ordna program, vilket innebär att plattformen förvaltar flera olika aktörers bug bounty-program. Stora företag som Meta och Google erbjuder ofta sina egna bug bounty-program, och belöningarna kan uppgå till stora belopp.

Hackathon -evenemang

Hackathoner (av de engelska orden hacking och marathon) är evenemang där cyberexperter samlas för att utveckla till exempel programvara eller andra innovationer. Hackathoner är ofta tävlingar där på förhand bildade lag tävlar mot varandra, söker lösningar eller utvecklar program inom ramen för överenskomna teman. Hackathoner är vanligtvis lekfulla evenemang och pågår vanligen 24–48 timmar. I slutet av evenemanget presenterar lagen sin produkt, och den bästa innovationen belönas.

I synnerhet för unga som vill bearbeta sina idéer tillsammans med andra experter kan hackathoner vara ett utmärkt sätt att bilda nätverk, utvecklas tillsammans och träffa andra sakkunniga, experter eller studerande inom branschen.

Webbkurser och certifikat

På webben finns ett stort utbud av avgiftsfria webbkurser där man kan lära sig av både nybörjare och mer erfarna experter. Webbkurser kan vara ett bra alternativ, särskilt för dem som tycker om kursliknande inlärning. En ung nybörjare kan också genom kurser få första kontakten med it-världen.

På webbkurserna kan man till exempel lära sig programmering på olika programspråk, webbutveckling, övervakning och testning av informationssäkerheten eller till exempel dataanalys.

För vissa kurser på nätet är det också möjligt att få ett intyg över att den unga personen har genomgått en kurs genom vilken hen kan bevisa sin kompetens.

Sammanslutningar

Även om man kan hitta mycket skadligt innehåll på webben, finns det också många positiva och sporrande sammanslutningar på plattformarna. En ung person som är intresserad av informationsteknik kan hitta likasinnat umgänge till exempel i olika nätgemenskaper, såsom Discord-kanaler och hackarforum. Den unga kan av sammanslutningar få svar på de problem hen stöter på och få uppmuntran för sin cyberhobby.

När man söker sammanslutningar lönar det sig att fästa uppmärksamhet vid kanalernas innehåll och diskussionskultur. Etiska kanaler uppmuntrar till exempel inte till användning av olagliga verktyg, såsom booter, eller utövar påtryckningar för att delta i nätverksamhet som man själv anser vara tvivelaktig. Det är också bra att kontrollera om det är fråga om en modererad sammanslutning och vem som ansvarar för gruppens underhåll.

Den unga personens erfarenhet av sammanslutningens verksamhet i allmänhet återspeglar bra den verksamhetskultur som råder i sammanslutningen. Goda vägledande frågor är till exempel: är inställningen till medlemmarna i nätgruppen uppmuntrande? Är diskussionen mellan gruppmedlemmarna positiv och respektfull? Hur förhåller man sig i gruppen till osaklig diskussion eller mobbning? Uppmuntrar gruppen till skadlig eller brottslig verksamhet, såsom delning av sabotageprogram eller tvivelaktiga länkar? Hur förhåller man sig i gruppen om dess medlem skryter med brottslig verksamhet?

Utöver de sammanslutningar som finns på webben finns det på flera orter lokala sammanslutningar eller workshoppar där den unga kan prova på sina idéer eller lära sig nytt tillsammans med andra likasinnade hobbyutövare. Via sökmotorer kan man kontrollera om det på den egna orten finns till exempel workshoppar i programmering eller hackarklubbar.

Läs mer:

- Europeiska unionens byrå för cybersäkerhet ENISAS webbplats enisa.europa.eu.
- Next Gen Hack Finland-föreningens webbplats nextgenhack.fi.
- Aktuell information om tävlingar och webbkurser kan sökas via öppna sökmotorer till exempel med sökorden **CTF, hackningsutmaning, CTF challenge, capture the flag exercise, bug bounty, buggbelöningsprogram eller etisk hackning**.

6 Vanliga frågor om agerande i datanät

Det finns många frågor och myter om datanät. En viss typ av verksamhet kan vara så normaliserad på webbplattformar att den inte ens uppfattas som brottslig. Å andra sidan kan vissa plattformar och till och med termer automatiskt skapa en bild av brottslig verksamhet, även om de också används för lagliga ändamål. I detta avsnitt ger vi svar på några vanliga frågor och myter som ofta anknyter till cybermiljön.

6.1 Vad är hackning?

Med hackning avses kreativ problemlösning i en datanäts-och informationssystemmiljöer, där målet är att upptäcka och utnyttja de sårbarheter som finns i miljön. Hackning uppfattas beklagligt ofta automatiskt som brottsligt. Hackning kan dock också ske inom ramen för lagen, och så kallad etisk hackning är ofta en viktig del av tryggandet av företagens informationssäkerhet. Organisationen kan till exempel anställa en person för att söka sårbarheter i sitt system genom att personen angriper det. På så sätt kan organisationen upptäcka och åtgärda brister i sitt system. Vissa organisationer ordnar så kallade bug bounty-program, tillåter angrepp på sina system inom ramen för vissa regleringar och betalar ibland stora belöningar till dem som upptäcker sårbarheter.

Hackningsfärdigheter används dock ibland även förbrottslig verksamhet, såsom obehöriga intrång i informationssystem. Huruvida hackningen är laglig beror på syftet med och föremålet för hackningen och de metoder som används. Det är därför viktigt att förstå gränserna för laglig och olaglig testning av informationssäkerhet och att öka medvetenheten om hur sårbarheter och upptäckter av dem ska rapporteras. Det lönar sig för dem som är intresserade av hackning att bekanta sig med lagstiftningen om webbmiljöer för att undvika eventuella överraskningar. En god princip är att det inte lönar sig att självständigt djupare undersöka den sårbarhet som man upptäckt, utan att informera den behöriga parten om upptäckten.

6.2 Kan man använda det mörka nätet lagligt?

Det mörka nätet kallas den icke-indexerade delen av nätet som är utom räckhåll för de vanliga sökmotorerna och som kräver en separat webbläsare, såsom en TOR-webbläsare. TOR-webbläsaren är ett gratis program med öppen källkod som upprätthålls av frivilliga och som ökar nätanvändarens integritet. I Tor-nätet anonymiseras nättrafiken med hjälp av ett globalt nätverk av proxyservrar, genom att all nättrafik styrs via flera krypterade servrar, så kallade noder. Varje nod avkodar endast en del av ruttkrypteringen och ingen server känner till hela rutten för nättrafiken, vilket gör det svårt att fastställa användarens verkliga position. Tor-nätet främjar kommunikationens integritet och anonymitet, eftersom användarens position och identitet inte kan fastställas lika lätt som i ett öppet nät.

Webbplatser i det mörka nätet används via en Tor-webbläsare eller något annat motsvarande program. Det mörka nätet anses ofta som en lekplats för brottslingar, men all verksamhet på det mörka nätet är långt ifrån olaglig. Det är lagligt att använda en Tor-webbläsare och många aktörer använder den för att förbättra sin integritet på nätet. I synnerhet i länder där den statliga censuren är stark kan det mörka nätet användas för säkrare kommunikation eller för att få tillgång till innehåll som annars skulle ha blockerats i landet. Människorättsorganisationer och journalister kan till exempel använda det mörka nätet för att på ett säkrare sätt kunna kommunicera och dela med sig av innehåll.

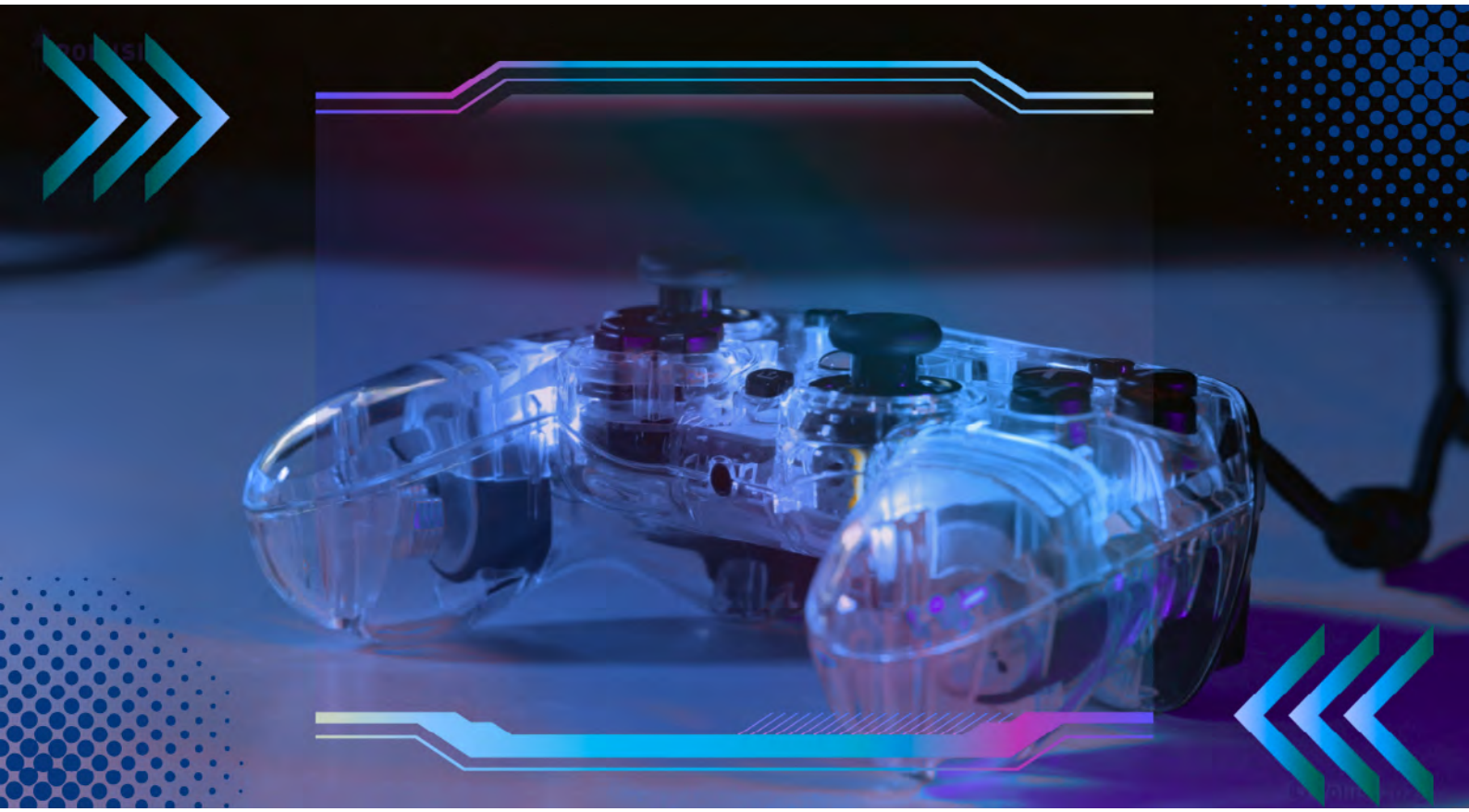
Användningen av det mörka nätet är dock förknippad med flera risker. I det mörka nätet förekommer många brottsliga handlingar, såsom narkotika- och vapenhandel samt spridning av olagligt material. Brottsliga aktörer föredrar det mörka nätet på grund av den högre integritetsnivån, och på marknadsplatser för det mörka nätet säljs både brott som köpta tjänster och verktyg för hackning och sabotageprogram eller material från dataläckage. Verksamheten i det mörka nätet är inte så anonym som man kanske tror, och användarens identitet kan komma till externa aktörers kännedom trots en högre skyddsnivå. Dessutom är risken stor att utsättas för olika hot, såsom sabotageprogram, bedrägerier, nätfiske eller att man blir föremål för observation i det mörka nätet.

Det mörka nätet kan verka intressant för ungdomar. Det lönar sig därför att med den unga att öppet diskutera användningen av det mörka nätet och riskerna med det. Det lönar sig inte för en oerfaren användare att undersöka ett mörkt nät, eftersom det utan lämpliga skyddsåtgärder är lätt att utsättas för skadlig verksamhet. Det är bra att diskutera varför en ung person använder eller planerar att använda det mörka nätet, vilka fördelar och risker användningen medför och att tillsammans överväga om det är nödvändigt för den unga att använda det mörka nätet.

6.3 Är videospel skadliga?

Man anser ofta att videospel är skadliga och att ungdomarbör styras bort från videospelens värld. På videospelsplattformar, liksom på andra webbplattformar, förekommer störande beteende och brottslig verksamhet, vilket naturligtvis är bra att beakta när man spelar. Videospel har dock också många positiva effekter och spelandet kan vara en utvecklande hobby. Videospel är rolig underhållning och kan utveckla inlärning, kreativitet, ögon-hand-koordinationen och andra nyttiga färdigheter. Videospel förenar människor med olika bakgrund, och utöver upplevelser kan de också ge lärorika erfarenheter. Att spela tillsammans kan vara mycket socialt, och genom spelandet kan spelarna lära sig grupparbete och laganda. Genom spelfigurer kan man hantera sina egna önskemål, värderingar och rädslor, och spelandet kan också lära barn och unga hur man hanterar till exempel frustrationskänslor.

I stället för att förbjuda videospel är det viktigt att inkludera barnets eller den ungas spelhobby som en del av de dagliga diskussionerna och bekanta sig med de spel som barnet spelar till exempel genom att spela dem tillsammans. Det är bra att diskutera med barnet vilka risker och problem som kan uppstå på spelplattformarna och att instruera barnet att agera ansvarsfullt på spelplattformarna. Det är också bra att diskutera den tid som ägnas åt spelandet och skapa gemensamma spelregler. Det lönar sig alltid att informera spelplattformen och en trygg vuxen om problem eller störande beteende som de stöter på.



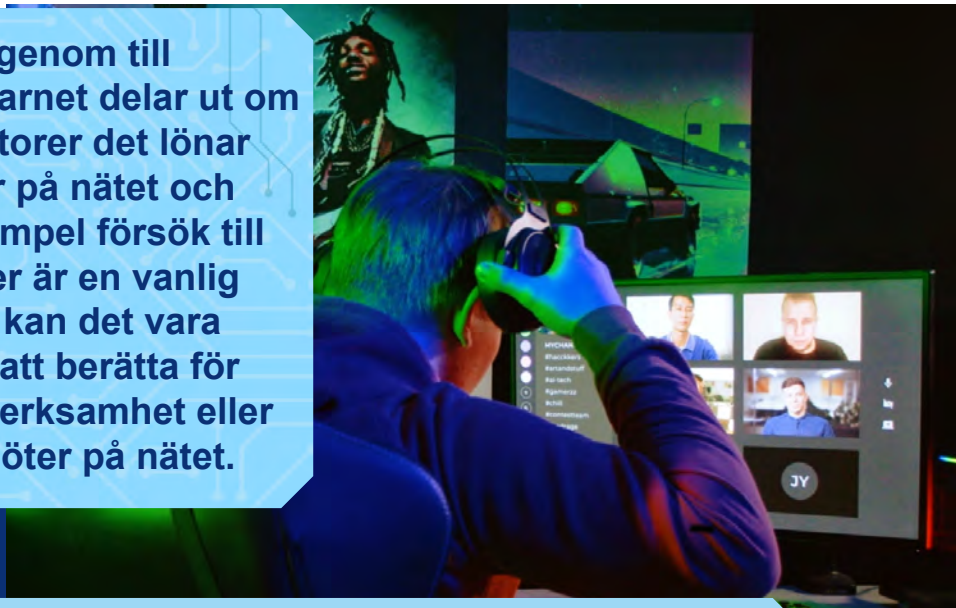
6.4 Hur ska man förhålla sig till den ungas relationer på nätet?

Det kan ibland vara svårt för vuxna att veta hur de ska förhålla sig till barnets relationer på nätet. Bekantskaper på nätet kanske inte upplevs som verkliga eller uppfattas som farliga. Det kan vara svårt att på nätet försäkra sig om en samtalspartners identitet, och det är bra att både barn och vuxna iakttar försiktighet när de agerar på nätet och kommer ihåg att den person som ligger bakom nätprofilen inte nödvändigtvis är den han eller hon påstår sig vara.

I praktiken är dock barns och ungas beteende på nätet mycket socialt, och den ungas nätgemenskaper är ofta en blandning av personer som är bekanta från den reella världen och webbmiljön. För många barn och unga kan vänskapsförhållanden på nätet vara mycket viktiga och berika livet. På nätet är det möjligt att hitta likasinnade vänner runt om i världen och få stöd för sitt eget intresse. Särskilt för unga som upplever att det inte i deras närmaste krets eller där de bor inte finns vänner som är intresserade av samma saker, kan de vänskapsförhållanden som skapats på nätet bli mycket viktiga för att stödja hobbyn. På samma sätt kan kamratstöd från webbmiljön bli ytterst viktigt till exempel för unga som hör till en minoritet eller som befinner sig i en svår livssituation.

Det lönar sig att i de dagliga diskussionerna ta upp den ungas relationer på nätet på samma sätt som den ungas övriga kompisrelationer. I stället för att automatiskt förbjuda eller förringa nätvänner är det bra att öppet sträva efter att diskutera med barnet och den unga vem den unga tillbringar tid med på webbplattformar samt att på ett sätt som lämpar sig för åldersnivån tillsammans fundera över de individuella gränserna och trygga människorelationer på nätet.

Med ett barn är det bra att gå igenom till exempel hurdan information barnet delar ut om sig själv på nätet, vilka riskfaktorer det lönar sig att beakta vid diskussioner på nätet och hur man kan identifiera till exempel försök till bedrägeri. När nätgemenskaper är en vanlig av de dagliga diskussionerna, kan det vara lättare för den unga personen att berätta för den vuxna också om skadlig verksamhet eller störande beteende som hen möter på nätet.



Läs mer:
Användbart material för att stödja en trygg digital vardag för barn hittar du till exempel på följande organisationers webbplatser.

- Mannerheims Barnskyddsförbund, Turvallisesti verkossa (på finska).
- Rädda Barnen rf, Digitaalinen lapsuus (på finska).
- Skydda Barn rf, En guide för föräldrar om digitala säkerhetsfärdigheter.

7 Var får jag hjälp, om…

7.1 Jag stötte på en informationssäkerhetsincident, skadligt innehåll eller så upptäckte jag en sårbarhet

När man rör sig på nätet kan man stöta på olika skadliga innehåll, nätfiskeförsök eller till exempel sårbarheter på webbplatsen. Det lönar sig alltid att anmäla missförhållanden. Anmälningsprocessen beror på vad och på vilken plattform du har sett innehållet eller avvikelserna.

Innehåll som strider mot användningsvillkoren

Du kan anmäla innehåll som strider mot användningsvillkoren eller olagligt innehåll direkt till den webbplattform där du hittade innehållet. Enligt förordningen om digitala tjänster (DSA), som trädde i kraft i februari 2024, ska tjänsteleverantörerna erbjuda en kanal genom vilken användarna lätt kan anmäla innehåll som de ser och som strider mot användningsvillkoren eller misstänks vara olagligt. Anmälningsprocessen varierar, men oftast kan man göra det till exempel med hjälp av en ”anmäl”- eller ”rapportera”-knapp som finns på webbplattformen.

Du behöver inte vara säker på vilket användningsvillkor eller vilken lag innehållet bryter mot. Det räcker att du misstänker att innehållet strider mot villkoren. Efter att ha fått en anmälan om innehåll som strider mot användningsvillkoren ansvarar webbplattformen eller myndigheten för en närmare utredning av innehållet.

Informationssäkerhetsincident

Det lönar sig att anmäla olika informationssäkerhetsincidenter, såsom nätfiskeförsök eller sabotageprogram, till myndigheterna. Incidenten kan vara till exempel ett sabotageprogram som installerats på datorn, en misstänkt e-postlänk eller ett textmeddelande där man ber om inloggnings- eller bankuppgifter. Det lönar sig att anmäla incidenten även om ingen skada har uppkommit.

- Lämna en anmälan till Cybersäkerhetscentret på en elektronisk blankett på Cybersäkerhetscentrets webbplats eller per e-post till cert@traficom.fi.
- Om du misstänker ett brott lönar det sig att utan dröjsmål göra en polisanmälan. Anmälan om brott kan göras elektroniskt via polisens e-tjänst eller genom att besöka närmaste polisstation.

Lucka i informationssäkerheten

Om du upptäcker en lucka i informationssäkerheten när du rör dig på nätet är det av största vikt att du inte utnyttjar den sårbarhet som du upptäcker. Att utnyttja sårbarheten kan i värsta fall orsaka stor skada för privatpersoner, organisationer eller till och med samhället och leda till straffrättsliga påföljder. Det är viktigt att informera den behöriga myndigheten om den sårbarhet som upptäckts.

Anmälan direkt till organisationen

- Kontrollera om det på webbplatsen finns en separat e-postadress eller separat blankett till vilken sårbarheter kan anmälas. Om det på webbplatsen finns anvisningar om hur man anmäler sårbarheter, ska du i första hand använda denna kanal för anmälan.
- Kontrollera om det på webbplatsen finns filen /.well-known/security.txt där du hittar förfaringssätt för att anmäla sårbarheter.
- Om det inte går att hitta lämpliga kontaktuppgifter på webbplatsen, kan du också anmäla sårbarheten till exempel via organisationens allmänna e-post och be om ytterligare anvisningar. När du kontaktar en allmän adress finns det dock en risk för att informationen inte når fram till rätt aktör.
- Tålamod och ett sakligt förhållningssätt är en fördel när du gör en anmälan. Organisationerna har olika verksamhetsmodeller för behandling av anmälningar. En del organisationer ger ett svar till anmälaren och kan till och med ge en liten belöning till den som hittar en lucka i informationssäkerheten. En del organisationer har inte nödvändigtvis en färdig verksamhetsmodell för behandling av anmälningar, och en anmälan om en brist i informationssäkerheten kan komma som en fullständig överraskning för organisationen. Det är därför bra att komma ihåg att du inte nödvändigtvis får något svar på din anmälan och att organisationen har kunnat reagera på den även om den inte gav dig något svar.

I osäkra situationer lönar det sig att göra anmälan också till Cybersäkerhetscentret eller till exempel skicka anmälan per e-post direkt till både organisationen och Cybersäkerhetscentret.

Vissa organisationer har bug bounty-program där deltagarna kan söka efter säkerhetshål i en förutbestämd miljö. I Bug bounty-programmen måste man i allmänhet anmäla sig i förväg, i programmet fastställs regler och gränser för hur man ska söka efter luckor i informationssäkerheten och anmälarna belönas för upptäckta sårbarheter.

Läs mer:

- Mer information om sårbarheter och anmälan om dem finns på Cybersäkerhetscentrets webbplats i avsnittet Sårbarheter.

Anmälan till Cybersäkerhetscentret

- Du kan alltid informera Cybersäkerhetscentret om sårbarheter. Anmälan kan du göra konfidentiellt, också anonymt.
- Gör en anmälan om sårbarheter eller informationssäkerhetsincidenter till Cybersäkerhetscentret på e-blanketten Anmäl en informationssäkerhetsincident på Cybersäkerhetscentrets webbplats eller per e-post till adressen cert@traficom.fi.
- Du kan göra en anmälan till Cybersäkerhetscentret oberoende av om du först har försökt kontakta webbplatsen direkt. Anmälan till Cybersäkerhetscentret är ett enkelt alternativ, om du vill förbli anonym eller inte själv vill sköta ärendet. Anmälan kan också lämnas in samtidigt till både organisationen och Cybersäkerhetscentret till exempel med ett gemensamt e-postmeddelande.
- Via adressen fås också stöd och ytterligare information om hanteringen av olika informationssäkerhetsincidenter.

7.2 Jag stötte på misstänkt eller brottslig verksamhet på nätet

Det lönar sig alltid att anmäla misstänkt verksamhet på nätet till polisen.

Om du misstänker att du har fallit offer för ett brott lönar det sig att utan dröjsmål göra en polisanmälan. Polisanmälan kan göras elektroniskt via polisens e-tjänst eller genom att besöka närmaste polisstation.

Om du upptäcker misstänkt verksamhet på nätet eller misstänker att du har stött på olagligt material eller olagligt innehåll, kan du enkelt anmäla misstankarna till polisen via tjänsten Nättips på adressen poliisi.fi/sv/nattips. Nättips kan du använda för att anmäla icke-brådskande ärenden. Nättips kan du använda för att anmäla misstänkt verksamhet, även om du inte är säker på att det är fråga om ett brott. I Nättips lönar det sig att så detaljerat som möjligt beskriva hurdant innehåll eller hurdan verksamhet du stött på och var. Tipset kan du lämna anonymt om du så önskar. Polisen behandlar nättips och vidtar vid behov fortsatta åtgärder, om det finns skäl att misstänka brott i ärendet.

Läs mer:

- Meddela Cybersäkerhetscentret om luckor i informationssäkerheten på adressen kyberturvallisuuskeskus.fi/sv.
- Lämna ett nättips på adressen poliisi.fi/sv/nattips.
- Gör en polisanmälan elektroniskt på adressen poliisi.fi/sv, eller genom att besöka närmaste polisstation.

7.3 Barns eller ungas beteende på nätet oroar

Oroar du dig för den ungas beteende på nätet? Tror du att den ungas intresse eller verksamhet riktar sig på illegal verksamhet och att du behöver mer information eller stöd?

I centralkriminalpolisens verksamhet för att förebygga cyberbrottslighet förebyggs allvarlig nätbrottslighet bland unga, ökas medvetenheten om identifiering av laglig och olaglig nätverksamhet samt stöds unga i att tillägna sig en brottsfri livsstil som en del av polisens förebyggande specialverksamhet.

Verksamheten erbjuder information och handledning för att förebygga och ingripa i it-brottslighet i ett tidigt skede. Dessutom ger verksamheten stöd till ungdomar som kanske redan har begått brottsliga handlingar på nätet. Verksamheten riktar sig till unga i åldern 12–25 år som har begått eller löper risk att göra sig skyldiga till allvarliga datanätsbrott. Den unga kan söka sig till verksamheten på eget initiativ eller också kan till exempel yrkesutbildade personer styra unga till verksamheten. Verksamheten är frivillig och konfidentiell. Utgångspunkten för verksamheten är att stärka en brottsfri livsstil genom att stödja identifieringen av gränserna för laglig och olaglig verksamhet, kartlägga arbets- och studiemöjligheter som stöder kompetensen och eventuellt annat stöd för livssituationen samt genom att hänvisa den unga till nätverksverksamhet som stöder den lagliga verksamhetskulturen i enlighet med den ungas intressen. Med varje kund utarbetas en individuell plan med beaktande av kundens situation och intresseområden.

Ta kontakt:

Du kan med låg tröskel kontakta verksamhet som förebygger cyberbrottslighet per e-post till **cybercrime.exit.krp@poliisi.fi.**

Mer information om projektet och förebyggande av cyberbrottslighet finns på webbplatsen Cybercrime Exit.

Ungas åsikter

Vad ungdomar vill att föräldrar och fostrare ska veta om cybervärlden

De unga är experter på det som gäller dem själva och vet bäst vilka utmaningar de möter på webben. Testausserveri ry är en icke-vinstdrivande förening som grundats av unga och som består av unga som är intresserade av informationsteknik. Syftet med föreningen är att inspirera unga att delta i it- och cyberhobbyer och erbjuda unga stöd för deras cyber-projekt bland annat via sammanslutningen Discord. Vi bad medlemmarna i Testausserveri ry att berätta vad de unga önskar att föräldrar och fostrare ska veta om it-hobbyn och hurdant stöd de unga önskar av vuxna för it-hobbyn. Centrala teman som lyftes fram var förståelse och intresse för den ungas hobby och stöd för att lära sig etisk verksamhet.

Vad ungdomar vill att vuxna ska veta om it-hobbyn

- Hackning som hobby är inte olagligt och syftet med hackning är inte att skada, så länge som de tillåtna gränserna iakttas.
- Allmän förståelse för vad som är lag-lig och ofarlig verksamhet och mindre ogrundad rädsla.
- It-hobbyn har värde och potential att utveckla nyttiga färdigheter för arbetslivet.

”Min släkting gick igenom min kod på fritiden och skrev alltid en bättre version av den. Jag kan inte beskriva hur jag kunde ha fått mer stöd.”

Läs mer:

- Se Testausserveris verksamhet på adressen testausserveri.fi.

Hurdant stöd önskar de unga av vuxna för sin it-hobby?

- Visa intresse för den ungas hobby. Vux-na kan visa intresse till exempel genom att fråga vilka program eller verktyg den unga personen använder eller vad den unga har lärt sig. På så sätt kan en vuxen visa uppskattning för den ungas hobby och lära känna den ungas bete-ende. Vuxna kan för den unga också ge förslag om kodningsprojekt.
- Den unga kan vara intresserad av cy-berhobbyer, men behöver hjälp med att hitta resurser för att lära sig och utöva hobbyn på ett etiskt sätt. Det är lätt för en ung person att stöta på dåligt inflytan-de på nätet, trots att den unga på nätet också kan göra spännande lovliga saker, förutsatt att den unga vet var den kan hitta lovliga platser.

”Jag hade velat få mer vägledning i sökandet efter saker. Jag menar, det hade varit trevligt att få hjälp med att lösa problem via sökmotorer.”

Sociala medier som är populära bland unga

Appar som är populära bland barn och unga varierar i snabb takt och nya appar dyker upp hela tiden. År 2024 var de sociala medieappar som de finländska ungdomarna mest aktivt använde Snapchat, WhatsApp och TikTok. Kommunikationsappar som WhatsApp och Telegram uppfattas ofta som chattrum för vuxna, men också i dem finns det grupper som unga följer och andra element i sociala medier som också barn i lågstadiet aktivt följer.

Det är bra att diskutera med den unga om de plattformar som hen aktivt använder.

I detta avsnitt finns en förteckning över några av de sociala medier som är populära bland ungdomar och som vuxna gärna kan bekanta sig med.

PLATTFORMAR FÖR SOCIALA MEDIER SOM DE UNGA ANVÄNDER MEST

- Instagram
- Discord
- YouTube
- Yubo
- Snapchat
- Steam
- Reddit
- Threads
- TikTok
- Twitch
- Jodel
- VSCO
- WhatsApp
- Telegram
- BeReal
- Pinterest

Cyber-ordlista

Booter

Ett verktyg som gör det möjligt för användaren att utföra överbelastningsattacker på ett valt mål i datanät. Med booter skickas så mycket trafik till det valda målet att den tjänst som målet tillhandahåller, till exempel en webbplats, kraschar och är inte tillgänglig under attacken. Booter-tjänster utnyttjar i typiska fall datanätutrustning, så kallad botnet, som olagligt tagits i besittning genom attacker, till exempel med hjälp av dataintrång.

Booter- och stresser-tjänster är enkelt tillgängliga via ett öppet nät via allmänna sökmotorer mot betalning, eller till och med gratis. Booter- och stresser-webbplatser kan påstå att de säljer produkter som lämpar sig för säkerhetstester. I verkligheten erbjuder tjänsterna dock olagliga verktyg och gör det möjligt att utföra överbelastningsattacker varifrån som helst och vart som helst i världen.

Botnet (botnät)

Ett antal datatekniska apparater i datanät som har kapats för att genomföra cyberattacker. Den som sammanställer ett botnet tar till exempel med hjälp av sabotageprogram eller genom att utnyttja svag datasäkerhet på enheterna, såsom svagt lösenord eller avsaknad av lösenord, i besittning anordningar som andra anslutit till datanätet. De kapade enheterna samlas till ett fjärrmanövrerat nätverk som på kommando kan utnyttjas till exempel för att sända datakommunikation till ett valt mål. Ett botnet kan bestå av flera vardagliga nätanslutna anordningar, såsom datorer, smarta tv-apparater, högtalare, kylskåp eller eltandborstar. Ägaren av apparaten kanske inte ens märker att den används som en del av ett botnet. Ett botnet kan utnyttjas till exempel för nätfiske, överbelastningsattacker eller spridning av sabotageprogram eller skräppost.

Bug bounty

Bug bounty, dvs. sårbarhetsbelöningsprogram, är ett program som erbjuds av en organisation eller plattform och där deltagarna lovligen kan söka efter brister i informationssäkerheten i en på förhand avtalad miljö. De som anmäler sårbarheter får en belöning, till exempel en penningbelöning, för att upptäcka sårbarheter. Bug bounty-programmen är i allmänhet begränsade till en viss på förhand definierad del av organisationens system eller plattform och deltagare måste registrera sig i förväg. Programmet kan pågå en begränsad tid eller kontinuerligt. Storleken på belöningarna varierar beroende på programmet och hur allvarlig den identifierade sårbarheten är.

Företagen kan använda bug bounty-plattformar för att ordna program, vilket innebär att plattformen förvaltar flera olika aktörers bug bounty-program. Stora företag som Meta och Google erbjuder ofta sina egna bug bounty-program, och belöningarna kan stiga till stora belopp.

Crime-as-a-Service (CaaS)

På nätet finns automatiserade hjälpmedel för brott som kan användas för att begå olika brott, såsom överbelastningsattacker, så att säga som köpta tjänster (crime-as-a-Service). Crime-as-a-Service-tjänster kan man lätt hitta också via allmänna sökmotorer, och tjänsterna gör det möjligt att begå datanätsbrott också utan betydande datatekniskt kunnande.

CTF (Capture the flag)

Capture the Flag, ”Fånga flaggan”, dvs. CTF-tävlingar, är tävlingar med hackningsutmaningar där man försöker lösa en utmaning i en så kallad sandlådemiljö, eller en rad utmaningar som gäller informationssäkerheten. Utmaningarna gäller olika informationssäkerhetssituationer, såsom sökning efter sårbarhet i koder, återmodellering eller till exempel dekryptering. Efter att ha löst utmaningen får spelaren ”flaggan”, och genom att återlämna flaggan får spelaren ett överenskommet poängtal för utmaningen. CTF-tävlingarna bjuder på utmaningar på olika nivåer och är ett tryggt och inspirerande sätt att bekanta sig med hackning.

Sårbarhet, lucka i informationssäkerhet

Med sårbarhet, dvs. lucka i informationssäkerheten, avses en sårbarhet i systemet som gör det möjligt för utomstående att utnyttja eller skada målsystemet. Sårbarheter kan finnas till exempel i programvara, informationssystem, applikationer eller anordningar. Luckor i informationssäkerheten kan bero till exempel på föråldrad programvara, och man strävar ofta efter att avhjälpa sårbarheter genom programuppdateringar.

Sårbarheternas allvarlighetsgrad varierar. Luckorna i informationssäkerheten kan vara lindriga och programleverantören kan upptäcka och åtgärda sårbarheten innan den har hunnit orsaka skada. I värsta fall kan sårbarheterna vara kritiska och i praktiken gör det möjligt för utomstående att fritt göra vad som helst i systemet.

Sabotageprogram

Med sabotageprogram avses olika skadliga program som syftar till att skada eller utnyttja informationssystem eller anordningar. Vanliga sabotageprogram är till exempel virus (virus), maskar (worms), spionprogram (spyware), utpressningsprogram (ransomware), tangentregistrerare (keylogger) och trojaner (Trojans). Sabotageprogram kan sprida sig bland annat via en bilaga i ett mejl eller genom nedladdning av programvara eller genom att klicka på en smittad länk. Sabotageprogram kan också spridas via sårbarheter och kräver inte nödvändigtvis att användaren vidtar åtgärder för att sprida den. Sabotageprogrammet kan till exempel syfta till att fiska efter uppgifter, stjäla bank- eller kreditkortsuppgifter, ta en apparat i besittning i utpressningssyfte eller utnyttja den förorenade apparaten som en del av ett botnet.

Hackare

En person som är skicklig på att använda informationsteknik och sin egen kreativa förmåga att lösa problem i samband med it-utmaningar. Hackaren kan använda sina färdigheter till exempel för att öka säkerheten på internet. Skickligheten kan också användas kriminellt, till exempel för att göra intrång i ett skyddat system.

Hackning

Kreativ problemlösning i en nätverks- och systemmiljö som syftar till att upptäcka och utnyttja de svagheter som finns i miljön. Hackning uppfattas ofta som olaglig verksamhet, men hackning kan också ske inom ramen för lagen. Etisk hackning är en viktig del av informationssäkerhetstestningensa.

Överbelastningsattack (DDoS)

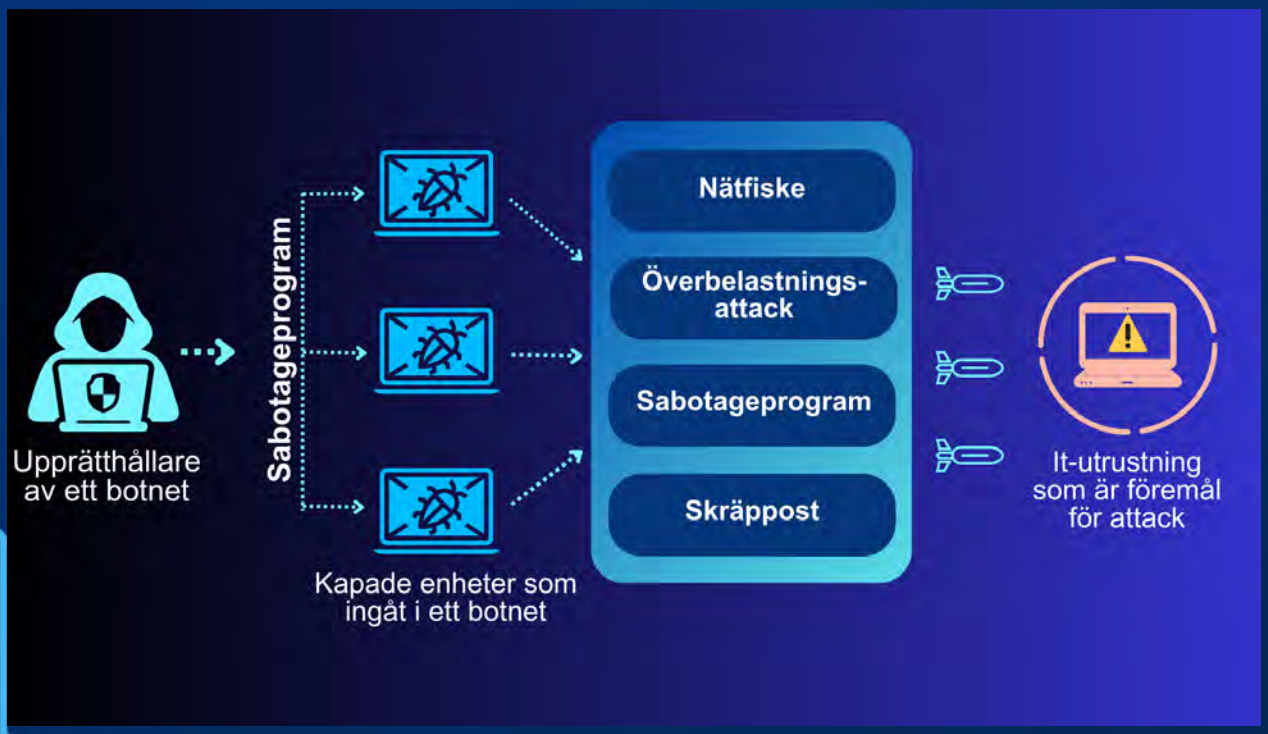
En cyberattack som syftar till att störa eller hindra en viss nättjänst från att fungera normalt. En decentraliserad överbelastningsattack genomförs till exempel genom att webbplatsen utsätts för så mycket trafik att webbplatsen blir överbelastad och normal användning av webbplatsen förhindras. En överbelastningsattack kan göras direkt från en enskild källa eller decentraliserat till exempel med hjälp av ett botnet. Det är också möjligt att utföra överbelastningsattacker utan mer omfattande teknisk kompetens med hjälp av automatiserade verktyg som finns i det öppna nätet, såsom booter.

Skript Kiddie

Amatörhackare som inte själv har omfattande teknisk kompetens, utan som använder verktyg eller skript som andra gjort för att utföra cyberattacker. Skript kiddies är i allmänhet nybörjare som inte själva kan skapa koden från början, utan använder sig av färdiga verktyg för att utföra attacker.

Läs mer:

- Basordlista för cybersäkerhet, Cybersäkerhetscentret.
- Ordlista om cybersäkerhet, Terminologicentralen.
- Mer information om informationssäkerhet och aktuella cyberfenomen finns också på till exempel teleoperatörernas och företag inom informationssäkerhetsbranschens webbplatser.



Ungdomar på nätet – Guide för fostrare för att förebygga cyberbrott och främja ansvarsfullt beteende på nätet.

Denna guide har utarbetats som en del av **Cybercrime Exit-projektet**, som medfinansieras av Europeiska unionen. Guiden har skapats för att svara på det tydliga önskemålet från intressentgrupperna i projektet om en lättförståelig informationskälla för fostrare, såsom vårdnadshavare och lärare, för förebyggande av cyberbrottslighet bland unga. Behovet av och innehållet i guiden diskuterades också med bland annat Centralkriminalpolisens Centralen för bekämpning av cyberbrott, Polisstyrelsen, inrikesministeriet och Testausserveri, och utkastet till guiden sändes till dessa instanser för kommentarer. Dessutom skrev medlemmarna i Testausserveri-föreningen i guiden ett kort avsnitt om ungdomars önskemål gentemot fostrare. Guiden har genomförts av Centralkriminalpolisens Cybercrime Exit-projekt.

Verksamheten för att förebygga cyberbrottslighet bland unga inleddes vid Centralkriminalpolisen 2020. Som en fortsättning på verksamheten genomfördes under projektperioden 2023–2025 det av Europeiska unionen medfinansierade kund- och utbildningspilotprojektet Cybercrime Exit 3 för förebyggande av cyberbrottslighet bland unga. Inom projektet gjordes pilotförsök med och utvecklades åtgärder för att förebygga it-brottslighet bland unga, och det skapades uppdaterade verksamhetsförutsättningar för att upptäcka särdrag hos it-brottslighet och ingripa i de ungas cyberbrottsspiral. Den verksamhet som förebygger cyberbrottslighet fortsätter vid Centralkriminalpolisen 2026 som ett projekt för etablering av verksamheten som en del av genomförandet av polisens strategi för förebyggande verksamhet och den nationella cybersäkerhetsstrategin.

Cybercrime Exit-projektteamet:

Viivi Lehtinen, projektchef
Sari Latomaa, inspektör
Aki Somerkallio, inspektör

Polisen
Guiden har utarbetats av: Sari Latomaa, Centralkriminalpolisen.
Bilder i guiden: Polisen, Canva C00, Pexels CC0, Unsplash C00.
ISBN 978-951-53-3933-1

Publicerad 3/2026, översättning Käännös-Aazet Oy.
Hyperlänkarnas funktion har kontrollerats 20.11.2025.