POLIISI
POLICE OF FINLAND

Young people online

An educator's guide to cybercrime prevention and responsible online behaviour.

2026

CYBERCRIME EXIT

Co-funded by the European Union

Contents

1 Introduction

Technology is evolving at a rapid pace and, especially for young people, online platforms are a key part of everyday life. Some young people spend more than half their waking hours on various online platforms, using the web for schoolwork, hobbies, and to keep in touch with family and friends. Conversations and hobbies flick back and forth between the real world and online platforms, and digital life is a natural extension of a young person's everyday life.

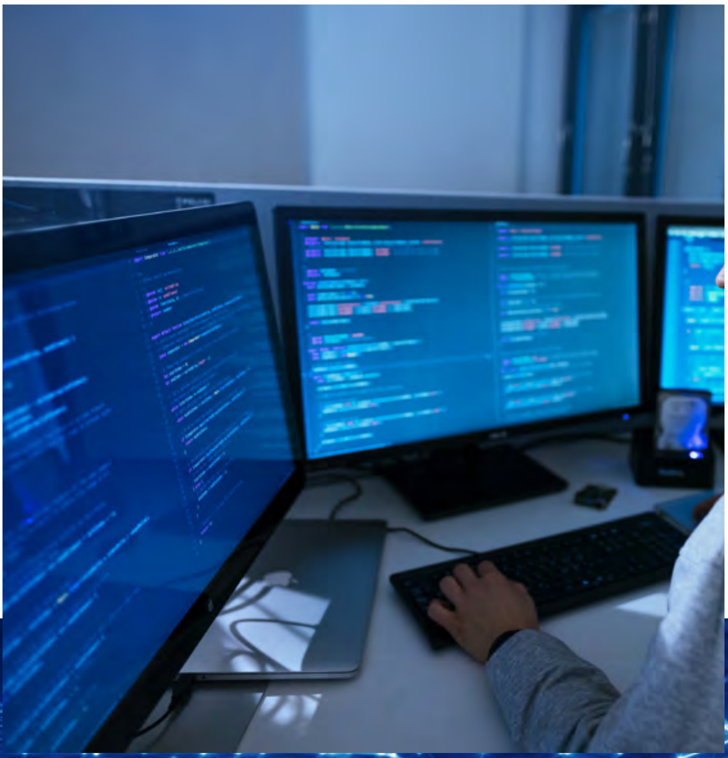
Digitalisation has created many opportunities, but it also poses challenges. With digitalisation, crime has also increasingly moved online, and cybercrime has exploded. Network technologies mean that crimes are no longer tied to a specific place – they can be committed anywhere, including at home on a computer or mobile device. The tools and instructions necessary to commit crimes are increasingly available on the open web, and committing a cybercrime does not necessarily require significant technical skill. In addition, first-time offenders of cybercrime in Finland are very young on average; some are even of primary school age.

This guide is for guardians, educators and others working with young people. It provides information on cybercrime among young people, how to support responsible online behaviour, and tips on legal opportunities in information technology. The guide aims to be an easy-to-use source of information on preventing cybercrime among young people and to provide support for discussing cyber issues with them. The guide approaches cybercrime specifically from the perspective of cyber-dependent crimes.

The National Bureau of Investigation’s programme to prevent cybercrime identified the need for easy-to-use, reliable materials to support discussions on cyber issues. For children and young people, being online is part of everyday life, and they can be highly skilled users of the web and of various applications and devices. However, their understanding of the rules of the web and the boundary between legal and illegal activities does not always develop as quickly as their technical skills. A young person may feel that no one supervises the internet, and they may not understand the consequences of their actions. Online activity may also be less visible in everyday conversations with adults. Lack of knowledge can lead to poor choices, and a young person could end up using their skills for criminal purposes if, for example, recruited by criminals. This is why adults play an important role in guiding children and young people on the safe and legal use of networks.

If you are unfamiliar with technology and the apps young people use, it may also feel challenging to discuss the topic. There is, however, no need to be nervous about discussing cyber matters. You do not need to be technically savvy to talk to a young person about what they do online. It is enough for an adult to be present, listen and talk to them, and perhaps enhance their own understanding of information networks as well. This guide presents information about cybercrime among young people, the legislation on cybercrime in Finland, support for discussing cyber issues, and advice on how to deal with various problems online. The guide also provides useful tips on materials to help those interested in the subject to explore the cyber world in more depth.

The guide was produced as part of the Cybercrime Exit project jointly funded by the National Bureau of Investigation in Finland and the European Union.



CYBERCRIME EXIT

Co-funded by the European Union

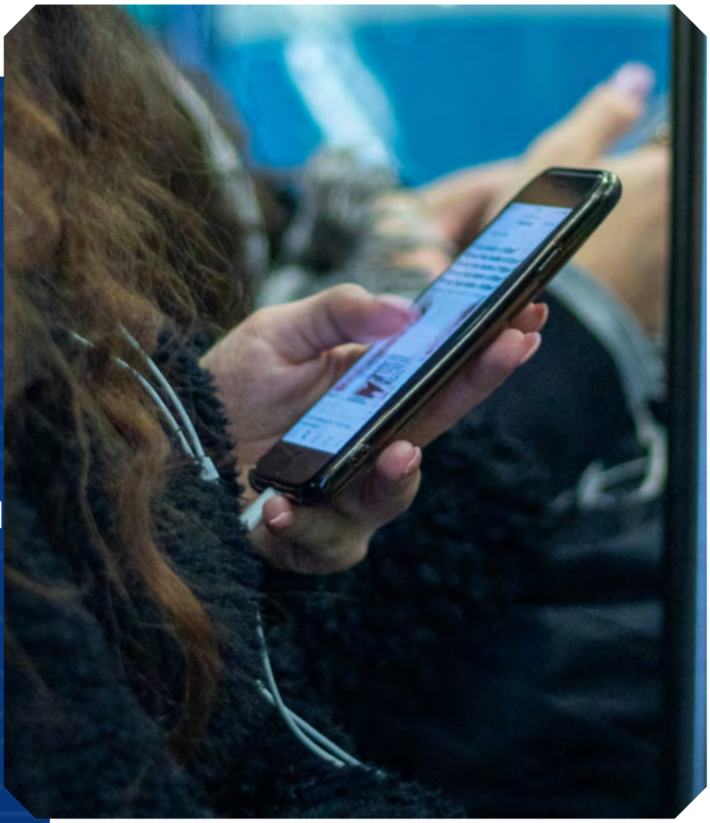
2 Young people online

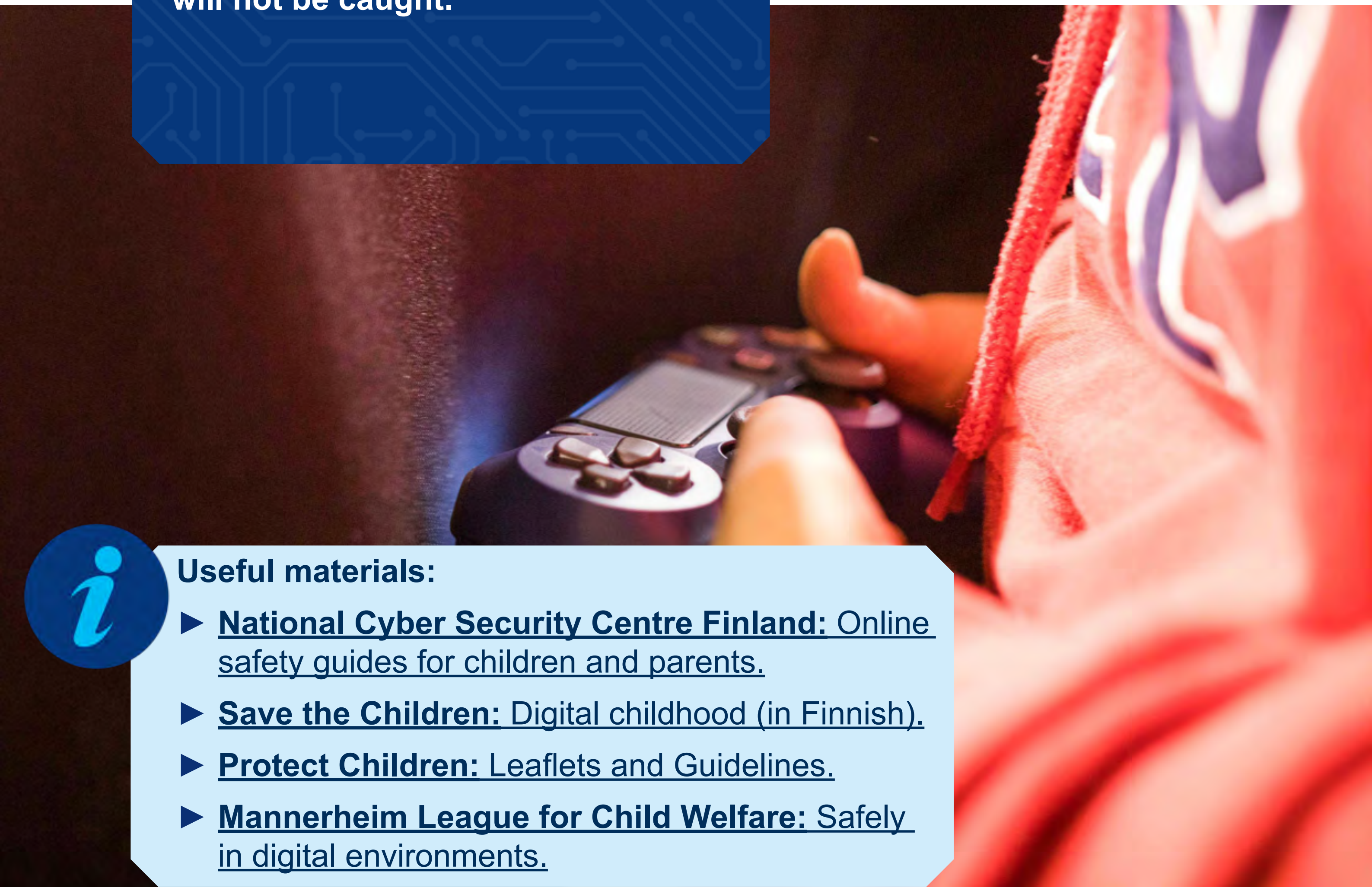
The digital environment is an integral part of young people's everyday lives. Most children and young people are active on various online platforms, such as social media, gaming platforms, chat rooms and websites. The online environment offers many opportunities, and cyber skills will only become more important as time goes on. However, active use of online platforms also exposes young people to various threats. The majority of young people have experienced some form of online abuse, such as phishing attempts, harassment, or content inappropriate for children. Various concerns about security and the safety of young people are a frequent topic of debate, and it is important to educate young people on how to protect themselves from various online threats. The Police's website and social media channels offer good materials, as do the websites of the National Cyber Security Centre Finland and several organisations, such as Save the Children and the Mannerheim League for Child Welfare.

It is equally important to teach children and young people how to act responsibly online. Young people can have highly advanced technical interests and skills. A young person interested in cyber issues might be curious to test their skills, explore how platforms and devices work, try out tools and techniques they find online, or, for example, learn how to build their own website, code or hack – all examples of creative problem-solving exercises online.

An interest in IT is a great thing, and cyber skills are increasingly important. However, while a young person may have a strong grasp of the technical aspects, the line between legal and illegal online activity may be less clear to them. **The online world lacks the signposting to clarify the difference between right and wrong, legal and illegal.** In the real world, a young person can be taught the rules of the road so they know how to stay safe. To a similar end, young people can learn online ground rules. However, they often find themselves alone in this endeavour. Young people are also at risk of committing harmful or criminal activities online, and adults need to provide guidance to help them understand the boundaries between legal and illegal activities in the online world.

> **Young people are often taught from an early age that they, for example, should not steal from a shop. In the real world, surveillance and control mechanisms are highly visible and shape how people act. Shops have sales assistants, CCTV cameras and guards who can intervene if they see a young person shoplifting. This type of supervision and control is more limited online and may be less visible to a young person. The young person may feel that there is no supervision online and that they will not be caught.**





Useful materials:

- ▶ **National Cyber Security Centre Finland:** Online safety guides for children and parents.
- ▶ **Save the Children:** Digital childhood (in Finnish).
- ▶ **Protect Children:** Leaflets and Guidelines.
- ▶ **Mannerheim League for Child Welfare:** Safely in digital environments.

3 What is cybercrime?

Cybercrime refers broadly to a variety of crimes that take place on or via networks. Cybercrime can be roughly divided into cyber-dependent and cyber-enabled crimes. Cyber-dependent crimes are crimes that target information networks and systems, while cyber-enabled crimes are crimes committed using information networks.

Cyber-enabled crimes are, in themselves, traditional crimes that can be committed in new ways due to networks. The crime does not target an information network, and it could also be committed without networks. **For example, cyber-enabled crimes include various forms of online fraud, such as romance scams, online drug trafficking, and the unauthorised sharing of sexually explicit images or using such images for blackmail.**

Cyber-dependent crimes are ‘pure’ cybercrimes that occur in an online environment and cannot be committed without networks. **These crimes include denial-of-service attacks and data breaches, such as unauthorised logins to another user's account.**

Cybercrime often involves elements of both cyber-dependent and cyber-enabled crimes, and it often serves as the first step in other criminal activity.

> **For example, an offender may use a data breach to gain access to personal data that they can later use to commit identity theft or fraud.**
> **A perpetrator could also, for example, hack into another person's digital device or social media account to get hold of material that can be used to blackmail the victim.**

Cyber-dependent crime

- A crime where computer networks or information systems are both the tool to commit the crime and the target of the crime.
- These crimes always take place in a cyber environment and cannot be committed without networks.
- They are often related to other crimes.
- Examples include data breaches and denial-of-service attacks.

Cyber-enabled crime

- An offence committed using computer networks or information systems.
- Traditional crimes that take place in an online environment.
- The offence does not actually target a computer network; it can also be committed offline.
- Examples include online fraud and online drug trafficking.

Read more:

- Criminal Code of Finland (39/1889).
- Cybercrime at Police website poliisi.fi.
- For up-to-date legislation, see finlex.fi.

3.1 Cybercrimes in Finnish legislation

In Finland, cybercrime is covered by the Criminal Code. Chapters 34, 35 and 38 of the Criminal Code, among others, contain specific provisions on cybercrime. In addition, other legislation, such as the Copyright Act, also contains provisions relating to cybercrime.

The law does not explicitly treat cybercrimes as a separate category. Instead, cybercrimes are largely included under legal classifications that cover both online and offline offences.

For example, the essential elements of fraud and identity theft are the same whether the act takes place online or in the real world.

Similarly, interference with communications can occur online, but could equally refer to offences such as nuisance calls to the emergency services or obstructing a postal worker.

3.2 Specific features of cybercrime

Cybercrime does not respect national borders. Crimes committed in Finland can target victims anywhere in the world and vice versa, without the offender ever having visited the country in question.

The economic damage caused by cybercrime is often greater than the harm caused by other types of crime committed by young people. A single, seemingly minor online infraction can cause widespread damage.

For example, distributed denial-of-service (DDoS) attacks are often described as mere congestion in digital traffic. In the worst case, however, a denial-of-service attack can cause serious damage to an individual or business, and even affect critical infrastructure in society, such as the electricity grid or emergency services.

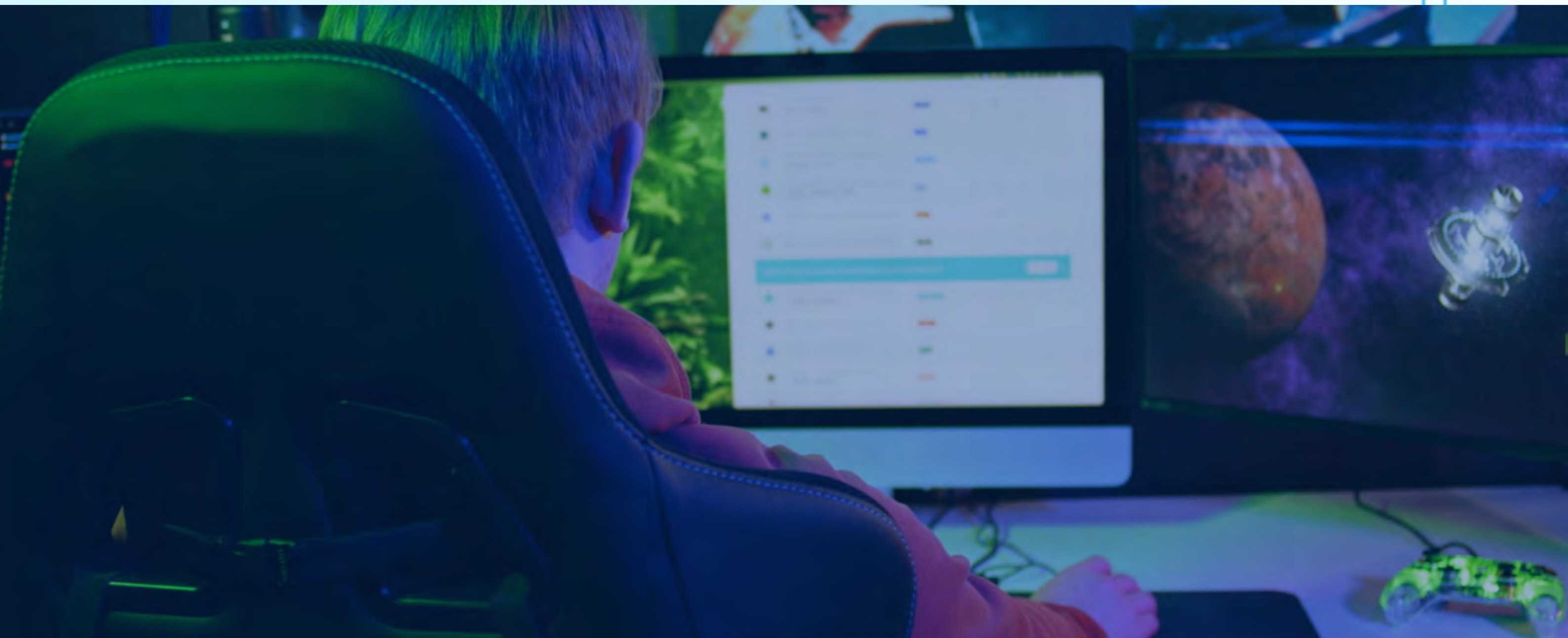
Denial-of-service attacks are very common among young people, especially in gaming environments where DDoSing is used to enhance the gaming experience, much as game modding and cheats do. For example, a young person may try to interfere with an opponent's actions in order to win a game.

It is fairly easy to find guides and tools on how to commit cybercrime using standard search engines**.** In addition, advice and tips are available to young people through various discussion forums and channels, such as Discord, a chat app, or YouTube, a video service.

Cybercrime can even be outsourced (**Crime as a Service, abbreviated to CaaS).** It is relatively easy for anyone to pay a Crime-as-a-Service vendor to attack their selected target without the user themselves requiring significant IT skills.

Attacks using automated tools are also crimes. In addition, when using automated tools, the perpetrator may not be able to ascertain the scale of the attack or the actual target in advance.

Failing to understand the consequences of an action does not exempt the perpetrator from criminal liability.



4 Youth cybercrime in Finland

4.1 Competences

News coverage often highlights cyberattacks by organised crime groups and state actors. It may come as a surprise to many people how much cybercrime is actually committed by individuals, such as young people. Crime statistics indicate that individuals and their user accounts are also the most common targets of cybercrime. Both in Finland and internationally, the average age of cybercrime offenders has fallen rapidly, with significant numbers of children under the age of criminal responsibility committing cybercrimes, some of whom are of primary school age. Every year, people under the age 15 are caught for cybercrimes.

Cybercrime does not necessarily require significant technical expertise, but can be as simple as an everyday act, such as the unauthorised use of a friend's account. Tools and guides for committing cybercrime are now easily available to young people on the open web. Cybercrime services can even be found with a simple search on a public search engine. The services are often inexpensive or free to try, making them easily accessible to young people. Younger and younger children are also being recruited into criminal activities online.

For example, a young person can use an outsourced service to carry out a very damaging denial-of-service attack from their computer with just a few clicks, without the young person even understanding how the attack is carried out or what damage it causes.

> **However, young people's technical skills should not be underestimated. Some young people who commit cybercrime are highly skilled in information technology and can carry out complex cyberattacks independently. In cases of serious cybercrime, the perpetrators often possess extensive technical expertise.**

4.2 Motives

Everyday motives

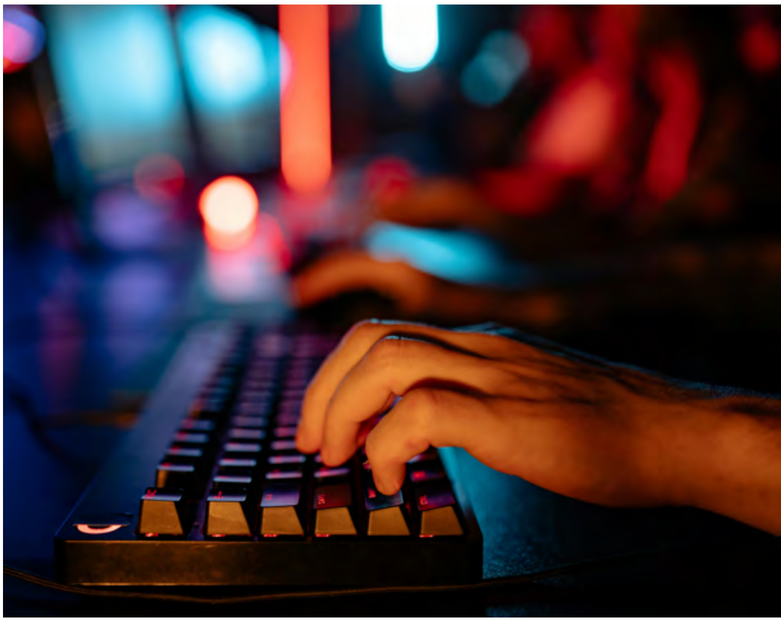
Particularly in the early stages of a young person's criminal career, the motives behind cybercrime are often quite innocuous and commonplace. Often, the young person does not initially seek financial gain or attempt to cause harm. Instead, they may be motivated by things such as seeking thrills, curiosity, mischief or jealousy. A young person may want to test their skills and push the limits, and may not understand or even care when the activity becomes illegal. However, even if the act is meant to be harmless, it can cause extensive damage. Financial motives also tend to come into play at some point, when young people realise they can earn money through cyber activities.

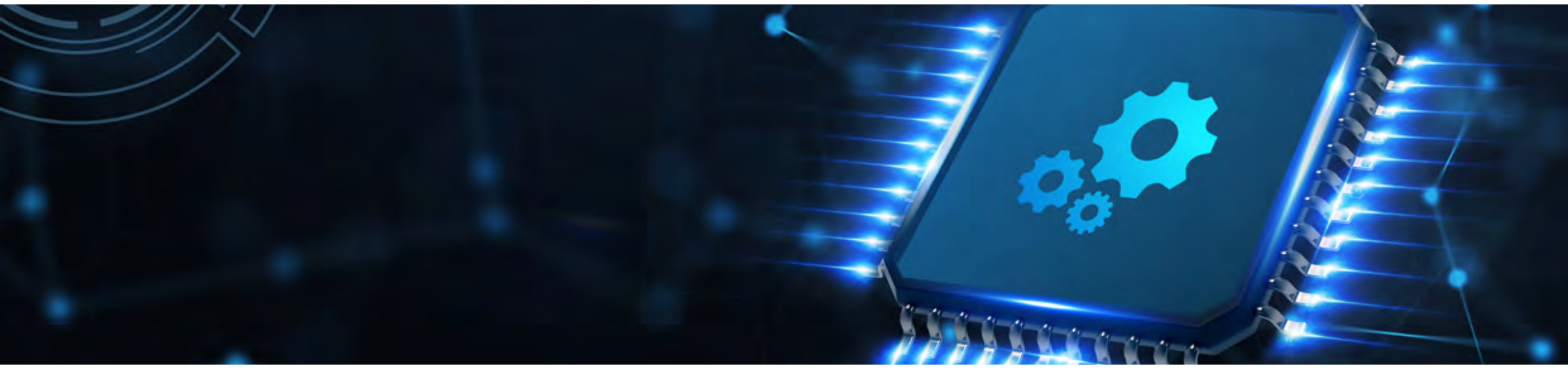
Normalisation of behaviour on online platforms

Certain types of behaviour on online platforms may be so normalised that a young person may not consider them disturbing or criminal. For example, DDoSing, which refers to denial-of-service attacks, is unfortunately common on gaming platforms. DDoSing is often perceived as merely mischief-making and may not be considered a criminal activity. However, research shows that DDoSing often serves as a young person's gateway into cybercrime and can normalise criminal activity online, setting the stage for a more serious criminal cycle.

Hacktivism

Young people can also be tempted to carry out cyber attacks under the guise of activism in the cyber environment. Hacktivism employs cyberattacks as tools for online activism in an attempt to demonstrate dissatisfaction or bring about change. Hacktivism is usually politically motivated. Typical forms of hacktivism include denial-of-service attacks against state actors. A young person taking part in an attack may think they are a force for good. In reality, however, it can be difficult for a young person to know the real target of the attack and the consequences it may have.





Online communities and the lure of criminal activity

A young person may also be involved in criminal activity as part of a larger local or international network. Criminal groups can spring up online in various forums, including gaming platforms. Criminal activity takes place both on and off the open network, such as on the Tor network. It is reasonably easy to join such groups, regardless of the geographical location, and young people can be drawn to online groups through popular games or other platforms. Group members may also actively approach young people on online platforms and entice them to join in criminal activities.

Young people can be lured by financial incentives or, for example, by **gamifying** activities, such as disguising criminal acts as technical challenges or games. The prominence of various criminal groups or witnessing an illegal shop online can also pique a young person's curiosity and strengthen their interest in criminal online groups.

Some online platforms use a **ranking system** where more experienced users have a higher status. A high-status user may be more likely to gain a young person’s trust and invite them to join a group outside the platform, for example, with the intention of recruiting them into criminal activity.

Young people are often easy targets for being lured into crime. Individuals under the age of 15 cannot be held criminally liable in Finland. In addition, the suspect’s age is taken into account when assessing the guilt and consequences of the offence if the suspected offender is under 21 years of age. Indeed, it is precisely because of their age that young people may be targeted to lure them into criminal activity online.

> **Young people can also be used on online platforms as a vehicle for crime, such as money laundering. For example, an online friend may send money in virtual currency and make up a reason for the young person to send it to another user or back to the person in real currency. They offer the young person a small amount of money as a thank you for their service. The young person may think they are making easy money and may not realise that anything bad has happened or be aware of the true extent of the activity.**

4.3 Damages

Cybercrime can cause significant harm. A crime can cause not only financial damage to the victim, but also long-term human suffering. Crime can also hamper the functioning of businesses or society as a whole, and the consequences can be very serious in the worst cases. A young person online may not realise the extent of the damage they can cause. In Finland, too, there have been cases in which an act that was intended to be merely mischievous has led to hundreds of thousands of euros in damages. When acting as part of an online group, the young person may not even know the true extent of the activity or the criminal damage caused. A child under the age of 15 can also be obligated to pay compensation for the damage caused.

> **A group of youths carried out denial-of-service attacks against a school server with the intention of causing trouble and disrupting the school's Wilma system. However, the attacks also crippled several other municipal systems, affecting the work of thousands of municipal employees. The repair work took several days, and the attack caused extensive financial damage to the municipality.**

4.4 Consequences

Cybercrime can be very serious and large-scale, even threatening the functioning of society and critical infrastructure. However, it does not take a large-scale act to cross the threshold into criminality, and something that may have been meant as a nuisance or a joke can constitute a criminal offence. Even an offence committed with mischief-making in mind can have far-reaching consequences for a young person.

Liability for damages: The damages from cybercrime can be substantial and affect a young person's life far into the future. A child under the age of 15 can also be obligated to pay compensation for the damage caused.

Criminal liability: A young person aged 15 or over is also criminally liable for the offence. Cybercrime can result in a fine, imprisonment, and a criminal record. A criminal record can make it difficult for a young person to apply for studies, training or a job, and can limit their ability to travel to certain countries.

Forfeiture of equipment: Any equipment used to commit an offence, such as a young person's phone, tablet or computer, can be confiscated and forfeited to the state.

Loss of access rights: Online platforms can block accounts used for criminal activities, such as a young person's game account, which may have taken a huge amount of time and possibly also money to build up.

4.5 Examples of cybercrimes committed by young people

Criminal damage to data, Criminal Code, chapter 35, section 3a

Unlawful destruction, corruption, concealment, alteration, damage or encryption of data on a storage medium or information system.

A young person has flunked a couple of exams and is annoyed by the poor grades he received. He eavesdrops on a teacher’s password for the Wilma system, logs in without permission, and upgrades the bad marks into better ones.

Interference with communications, Criminal Code, chapter 38, section 5

Interfering with or obstructing postal, telecommunications or radio communications, for example, by tampering with equipment or sending interfering messages.

A youth wants to cause a nuisance to his school and, using a program he found online, sends a huge amount of spam to the school’s mailbox, disrupting the school's email traffic.

Interference with an information system, Criminal Code, chapter 38, section 7a

Unlawfully preventing or disrupting the operation of an information system, for example, by entering, damaging, altering or deleting data.

A youth plays a team game online, and when his team loses, he is kicked out of the game. Angered by the defeat, the youth decides to use an online booter service to launch a denial-of-service attack on the game server, temporarily crashing it so that no one else could play.

Unlawful access to an information system, Criminal Code, chapter 38, section 8

Unlawfully breaking into an information system or accessing protected data on the system, for example, by using someone else's password without authorisation or by circumventing the system's security.

Some youths shared usernames for an online service. One of the young people discovers that the same account can be used to log in to another young person's social media account. A young person logs into the social media account without permission and sends defamatory messages in the name of another young person.

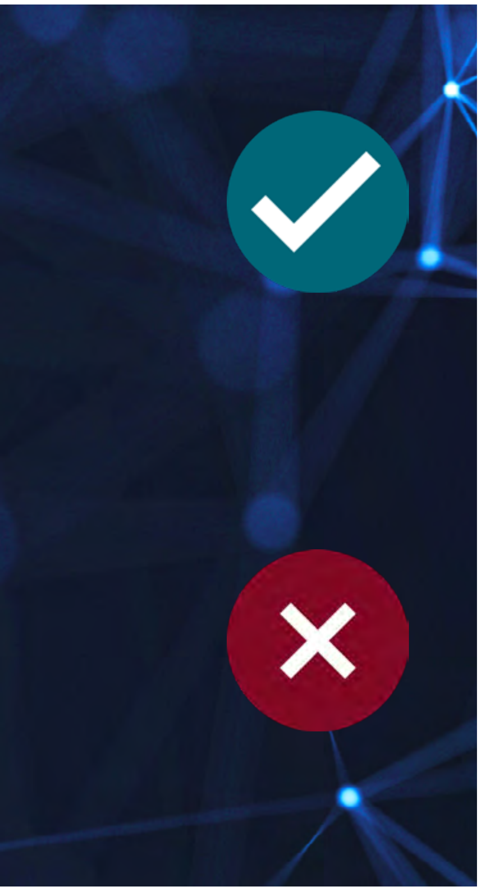
Violation of the secrecy of communications, Criminal Code, chapter 38, section 3

Opening a letter or message addressed to another person without authorisation, breaking into a secure electronic message or intercepting messages or calls.

A young person gets hold of a school friend's phone and reads their text messages and private social media messages without authorisation. The young person disseminates personal and sensitive information obtained from the messages to other students in the school.

4.6 Drawing the line between legal and illegal activities

Drawing the line between legal and illegal activities can be challenging, and a number of factors influence the assessment of the legality of an activity. The environment, the tools used, and the purpose of the activity also play a role, so the legality of an activity may need to be assessed on a case-by-case basis. It is therefore a good idea to talk to young people about the limits of online activities in different everyday situations. You can use the following situations as an example.



User accounts

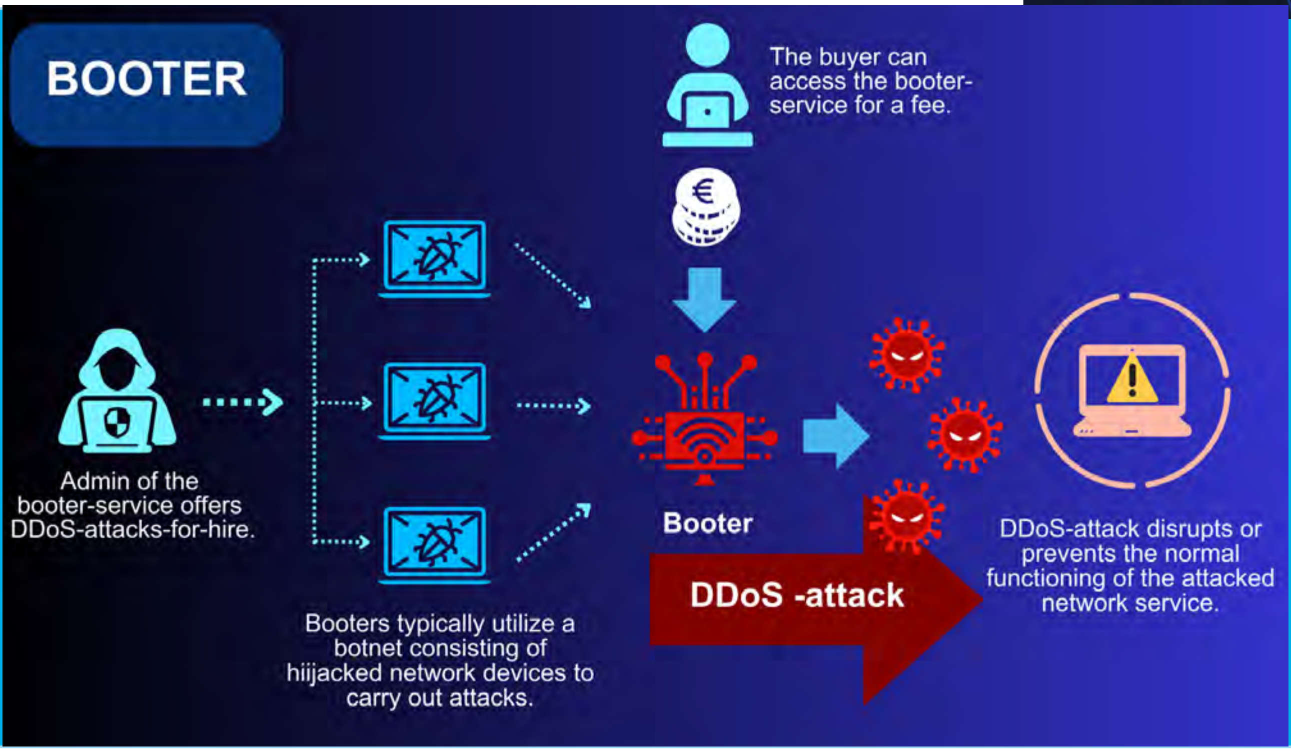
Young people may sometimes borrow each other's user accounts for various purposes, such as playing games online or viewing content on social media. You should never share your user account with anyone because it could be misused. However, it is not illegal to use another person's username or password with their permission. So the law does not explicitly prohibit young people from using each other's social media or gaming accounts, provided there is mutual consent. People may also lend each other their streaming service accounts, for example.

However, the right to use such services is limited to the agreed use. If a user account is used more beyond what was agreed, or someone attempts to use it to log in to services for which the account owner has not given permission, it may be a crime. Similarly, it may be illegal to buy a paid add-on in a service using someone else's account if the account owner has not given permission for this. It is also worth noting that activities that do not directly break the law may still be in breach of the terms of use of the service and cause problems. Among other things, many streaming services prohibit sharing user accounts with people in another household.

Load testing

Stress testing or load testing of a computer system is generally allowed, as long as the testing is done with the system owner's permission using legitimate tools and does not affect other services or devices on the network. Stress testing is a common part of corporate security testing, and many security companies offer related services. For example, you can load test your own website or game server, as long as the testing is done with legitimate tools and does not, for example, use a botnet or interfere with other systems. Before testing, it is, therefore, worth checking the legality and functionality of the tools you are using. In uncertain situations, it is safer to turn to an official security company for testing.

However, performing a denial-of-service attack without the system owner's permission or using a booter service is, in principle, illegal. Websites selling booter services may claim to offer security testing tools. In reality, however, booter services typically use illegal infrastructure, such as botnets hijacked by cybercriminals, to carry out denial-of-service attacks. When using booter services, it is also difficult to be sure what is actually affected by an attack. Using a booter service to test your own game server, for example, can therefore also unconsciously interfere with a server or other system that does not belong to you. Even legitimate tools, such as mass emailing tools, can be used illegally to interfere with communications, for example, by sending spam.



BOOTER

The buyer can access the booter-service for a fee.

Admin of the booter-service offers DDoS-attacks-for-hire.

Booters typically utilize a botnet consisting of hiijacked network devices to carry out attacks.

Booter

DDoS -attack

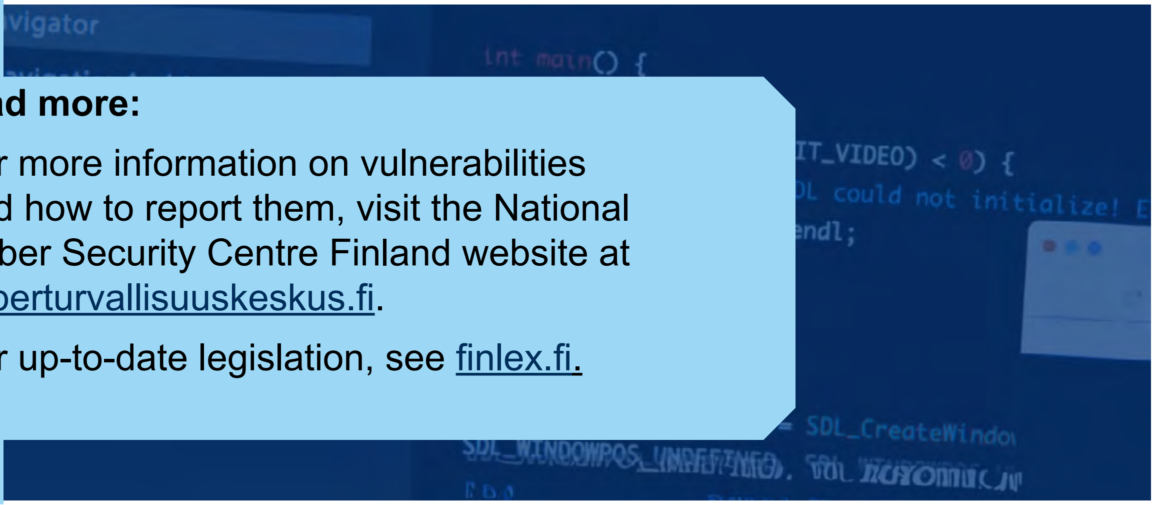
DDoS-attack disrupts or prevents the normal functioning of the attacked network service.

Searching for security holes

Searching for or discovering vulnerabilities is not in itself illegal. Security testing and penetration testing (pentesting) are often an important aspect of corporate cybersecurity. Companies may also organise bug bounty programmes, where hackers can, with the company's permission, search for security holes in the company's system. A skilled user may also stumble across a security hole by accident. The legality of the action depends on factors such as the measures used to identify the vulnerability, the extent to which the vulnerability is investigated, any harm caused by its use, and whether the vulnerability is exploited in an unauthorised way.

Keep in mind the following considerations when determining whether your activities are legal:

- **What environment am I in?** People increasingly spend their time in networked environments of some description, so it is important to consider what is allowed in those environments. For example, scanning your own system for vulnerabilities on an internal network may be allowed, but doing the same on an external network or virtual server may be illegal.
- **Who owns the system being tested?** Has the owner authorised the operation? It is one thing to study your own system, but another to study a system belonging to a school, for example.
- **When have I gone too far?** In principle, it is not worth investigating a vulnerability in depth unless you have permission, as it could cause you to cross the line into illegal activity.
- **Reporting the vulnerability is always a good idea.** Sometimes, it is possible to go too far in investigating a security vulnerability, either inadvertently or out of curiosity, and you may be concerned about reporting the vulnerability. However, you should always report a security hole you find, even if you have already investigated it. Reporting always causes less damage than not reporting.


vigator
int main() {
IT_VIDEO) < 0) {
DL could not initialize! E
endl;
SDL_CreateWindo
SDL_WINDOWPOS_UNDEFINED, SDL_WINDOWPO

Read more:

► For more information on vulnerabilities and how to report them, visit the National Cyber Security Centre Finland website at kyberturvallisuuskeskus.fi.

► For up-to-date legislation, see finlex.fi.

5 Supporting responsible online behaviour together

Children are often very skilled users of technology. However, it is important for them to receive support as they learn how to act in the digital world. In the same way that children and young people need to be taught traffic rules, they also need adult guidance to understand the rules of the internet and how to act responsibly and legally online.

5.1 Ask, listen, be present

Talking about a young person's online life need not be any different from talking about any other aspect of their life. More important than technical skills is being present, showing an interest in what the young person is doing, and a willingness to learn and understand. The young person is often happy to discuss the subject further if the adult shows interest in a topic that is important to them.

> **A large part of a young person's life and social relationships can take place online. For young people, online activities such as video games, and the friendships and communities they form online, are often just as important as the real world. For young people, the cyber environment and the real world are not separate realities but extensions of each other.**

✓ **Show interest in your child's hobbies and relationships online.**

Include their digital lives in everyday conversations, just as you would real-world events. It is also easier for young people to talk about the problems they face online if discussing the cyber environment is a normal part of their everyday life.

✓ **Get to know the platforms and apps that children and young people use, and discuss them regularly.** You do not need to know everything to discuss the safe use of apps with your child.

✓ **Familiarise yourself with the vocabulary of the online world.**

You do not need to know everything, but it is easier to strike up a conversation if you have at least some understanding of the cyber-related terms.

✓ **Be curious and ask questions.**

Most of us like to talk about our interests, and young people are no exception. A young person interested in IT is often happy to open up more if the adult shows interest and a willingness to learn.

Do not let a lack of knowledge hold you back. It is better to ask the young person to explain more about unfamiliar terms or how platforms work, for example, than to make assumptions and possibly misunderstand what is going on.

Discussion can help you learn more about the young person's hobbies and interests, and possibly also about the kinds of circles they are in online.

✓ **Discuss downloading new games and apps with your child, and explore the apps together.**

It is also worth looking at usage monitoring tools and talking to your child about whether they may be necessary.

✓ **Review the safety skills with your child in case of inappropriate approaches.**

For example, it is generally not a good idea to accept strangers as friends on social media or to post pictures of yourself to others. It is also worth discussing what kinds of information young people share about themselves online, and remembering that it is almost impossible to completely remove content posted online.

✓ **Support talented young people in developing their skills safely and legally.**

An interest in cyber matters is great, and young people interested in IT should be encouraged to develop their skills – as long as they do it legally. Familiarise yourself with the legislation about the internet, and discuss the ground rules and the limits of the law with your child.

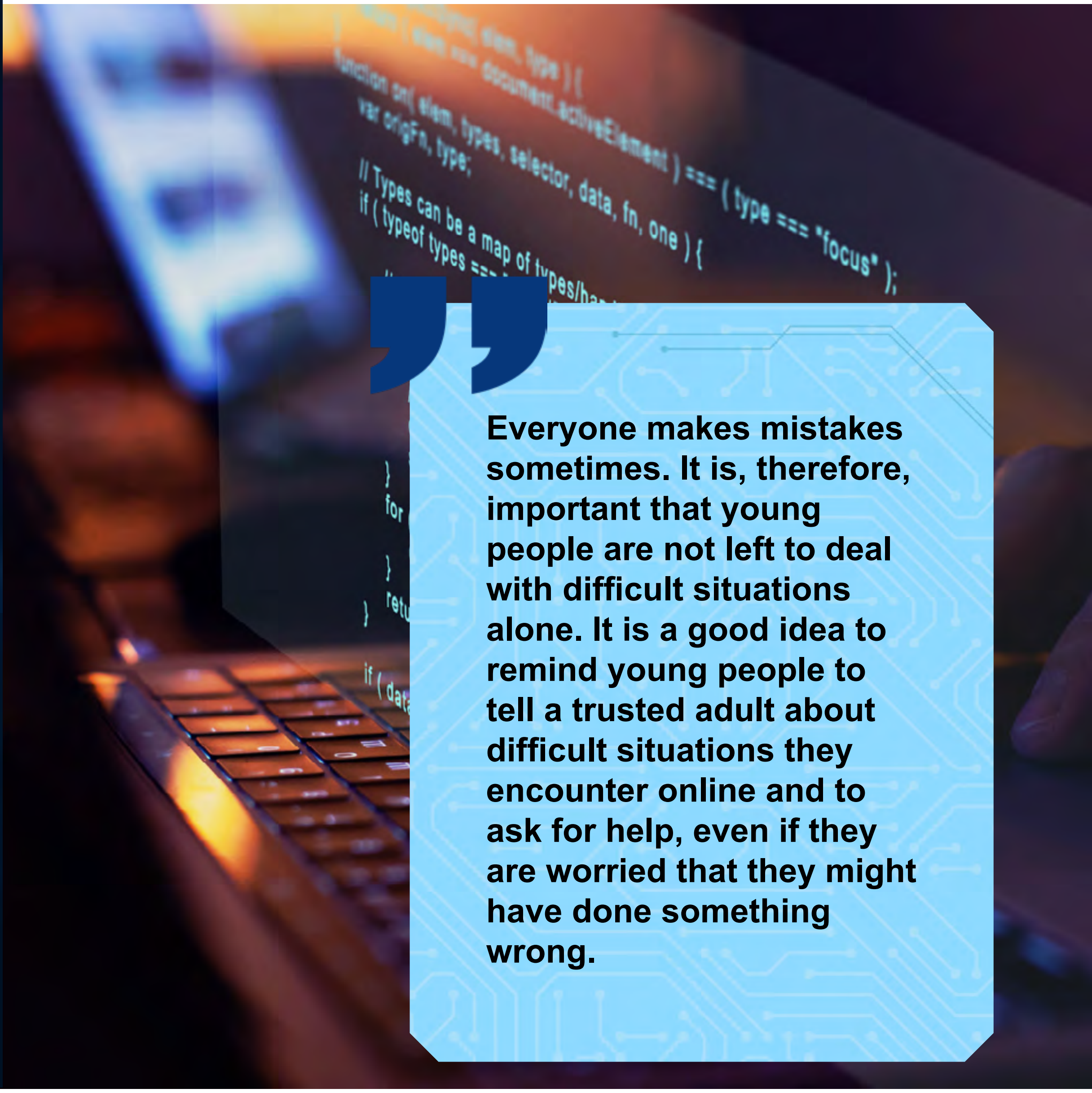
✓ **Talk to your child about responsible online behaviour and the boundaries between legal and illegal activities.**

If something is illegal offline, it is likely to be illegal online. Requests that seem to be rushed should also be treated with caution. Before taking any action, it is wise to stop and check whether the activity is legal and permitted. As a good rule of thumb for online activities, it is better not to engage in any activity if you are concerned about its legality.

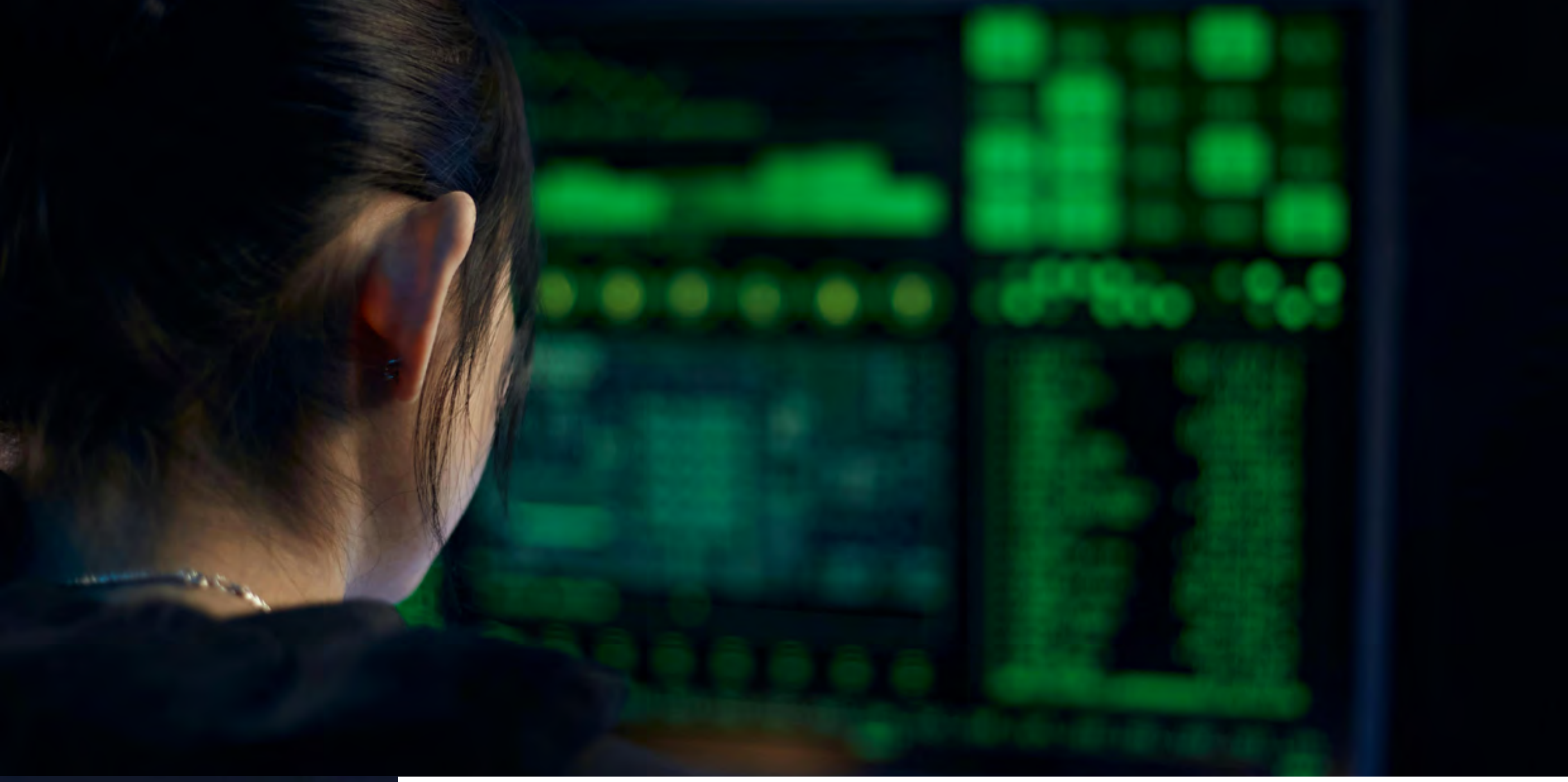
It is also a good idea to discuss what kinds of online communities the young person spends time in and to steer them away from harmful ones. The topic can be approached, for example, from a time management perspective. Cyber hobbies could be very useful in the future, and projects and competitions can help young people showcase their skills. Young people can expand their personal networks and make like-minded friends in positive online communities. They may even find interesting projects and job opportunities in the future.

However, it is difficult to highlight skills acquired through cybercriminal activity or cyber communities operating in a grey area. Cybercrime is not something to brag about in the security industry, and cybercrime is not something you can add to your CV, for example.

It is a good idea to clarify the cause-and-effect relationship of online activities at an early stage. Use the right terms, and explain them in a way that children and young people can understand. Especially with children, it is important to emphasise that criminal acts are wrong, without condemning the child for the act.



Everyone makes mistakes sometimes. It is, therefore, important that young people are not left to deal with difficult situations alone. It is a good idea to remind young people to tell a trusted adult about difficult situations they encounter online and to ask for help, even if they are worried that they might have done something wrong.

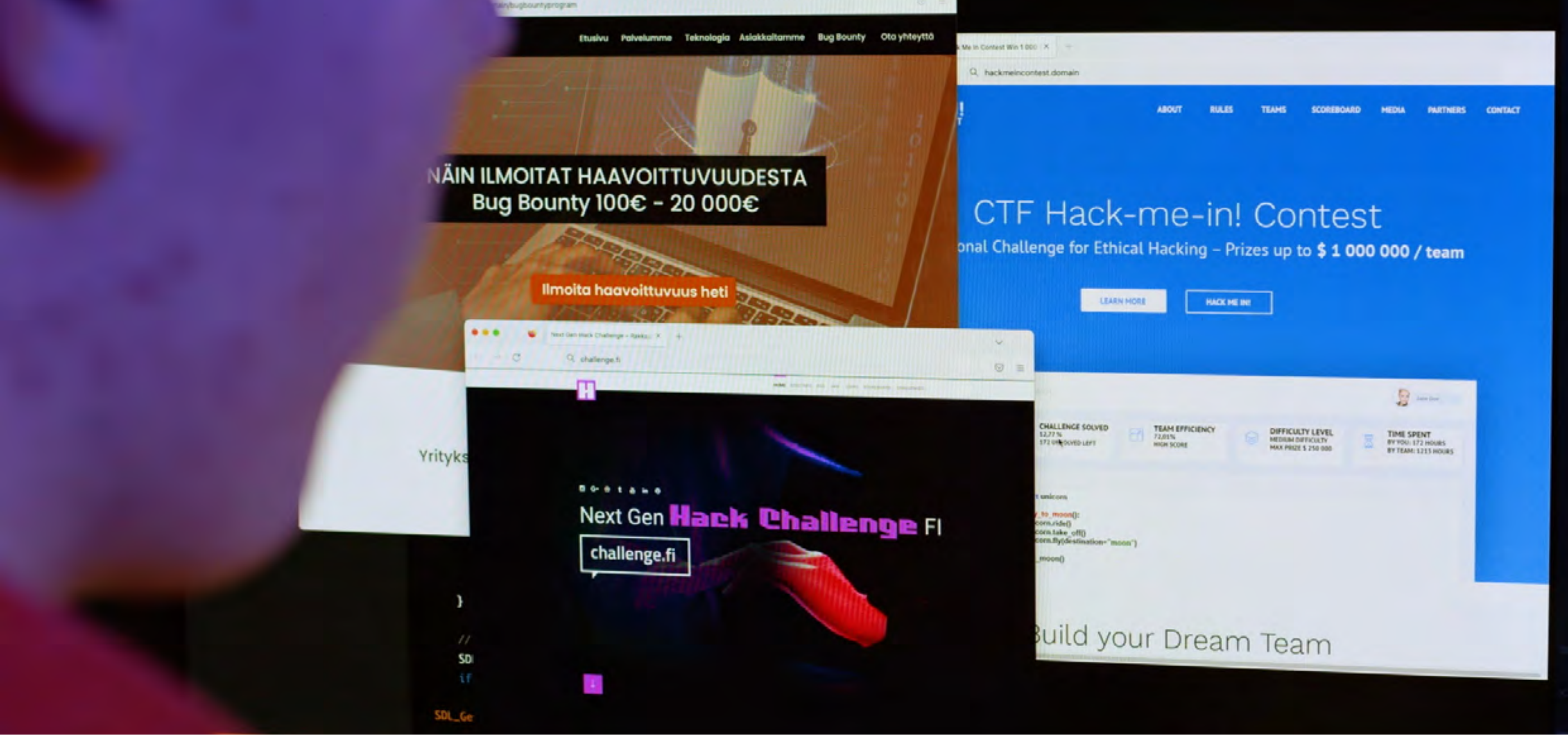


5.2 Is your child interested in hacking or security testing?

There are a huge number of interesting, legal opportunities to explore with a young person. The need for cybersecurity professionals is constantly growing, and cyber could become a career for young people interested in the field. Both in Finland and abroad, there are numerous companies in the information security sector that are in need of talent. In addition, cyber communities, such as local CitySec communities, are also growing in Finland.

This section provides some examples of legal options for practising and developing cyber skills. When considering options, it is a good idea to first try to understand the young person's skill level and interests.

Young people's technical skills can develop quickly to a very high level at any age by means such as online tutorials and hobby sites. It is therefore important to provide young people with enough interesting legal options and challenges.


NÄIN ILMOITAT HAAVOITTUVUUDESTA
Bug Bounty 100€ - 20 000€
Ilmoita haavoittuvuus heti
CTF Hack-me-in! Contest
onal Challenge for Ethical Hacking – Prizes up to $ 1 000 000 / team
Next Gen Hack Challenge FI
challenge.fi
uild your Dream Team

Sandbox environments

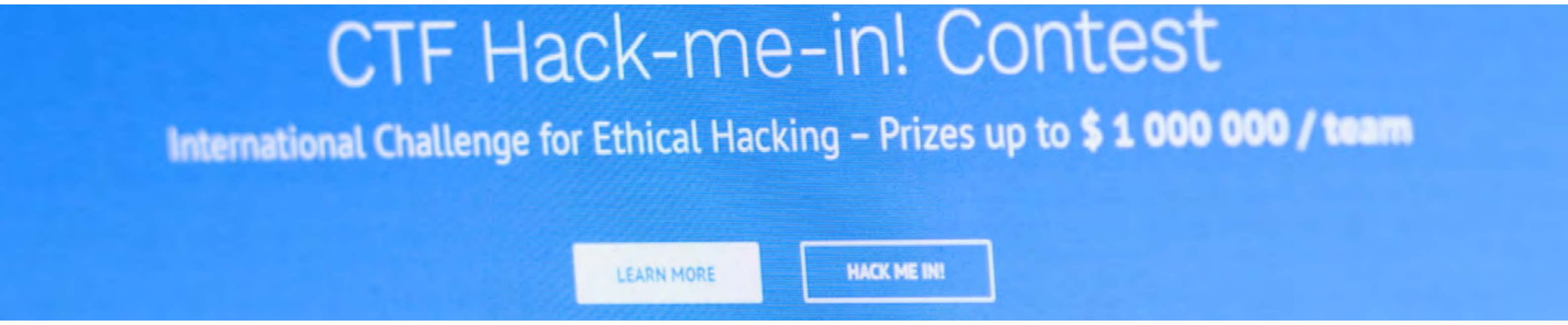
It is a bad idea to embark on security testing alone, as it always carries risks. In the worst case, independent testing could lead to criminal liability. However, hacking can be practised safely in a variety of sandbox environments.

Many sites offer virtual training environments, known as sandbox environments, where young people can put themselves to the test and practise their cyber skills safely and legally. Young people interested in hacking and security testing should be guided to develop their skills in secure, dedicated online environments. These can be found by searching for “ethical hacking”, “learn to hack”, “practise ethical hacking”, or “learn ethical hacking”, for example. If your child has already done some vulnerability scanning, it is a good idea to discuss how and where to report vulnerabilities, and talk about the limits of security testing.

CTF competitions

Young people can also take advantage of various CTF competitions, for example. Capture the Flag (CTF) competitions are hacking challenges, where the aim is to solve a challenge, or a set of security challenges, in a sandbox environment. The challenges involve various security scenarios, such as identifying vulnerabilities in code, reverse engineering, and decryption. After solving the challenge, the player receives a "flag" that, when returned, is worth the agreed number of points for completing the challenge. CTF competitions offer different levels of challenges and are a safe and inspiring way to learn about hacking.

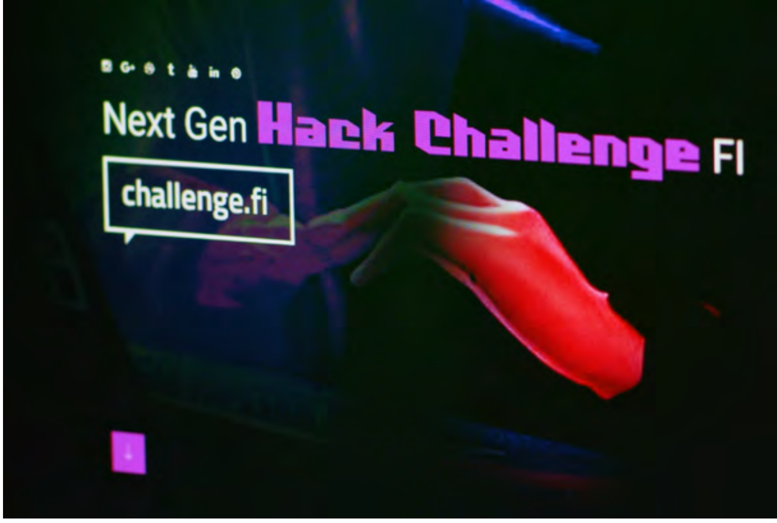
One well-known CTF competition is the European Cybersecurity Challenge, organised by ENISA, the European Union's network and security agency. You can join the Finnish team by going through the Finnish qualifying competition, organised by Next Gen Hack Finland ry.


CTF Hack-me-in! Contest
International Challenge for Ethical Hacking – Prizes up to $ 1 000 000 / team
LEARN MORE
HACK ME IN!

Bug bounty programmes

More experienced hackers can also test their skills by participating in bug bounty programmes. A bug bounty is a programme provided by an organisation or platform that allows participants to search for security vulnerabilities in a pre-arranged environment with permission. Anyone who finds a vulnerability is paid a reward, such as financial compensation. Bug bounty programmes are typically limited to a specific, predefined part of an organisation's system or platform, and usually require pre-registration. The programme can run for a limited time, or continuously. The size of the reward varies depending on the software and the severity of the vulnerability found.

Companies can use bug bounty platforms, that manage bug bounty programmes for multiple parties. Large companies such as Meta and Google often offer their own bug bounty programmes, and the rewards can be substantial.



Hackathon events

Hackathons (a portmanteau of “hacking” and “marathon”) are events where cyber experts come together to develop software or other innovations. Hackathons are often competitive, with pre-assembled teams competing against each other to find solutions or develop software around agreed themes. Hackathons are usually casual events and typically last 24–48 hours. At the end of the event, the teams present their products, and the best innovation receives an award.

Especially for young people who want to work on their ideas with other experts, hackathons can be a great way to network, collaborate, and meet other professionals, experts, or students.

Online courses and certificates

There is a huge variety of free online courses available, from beginner to advanced. Online courses can be a good option, especially for people who prefer a course-style learning experience. Courses can also give young beginners their first taste of the IT world.

Online courses can teach programming in different languages, web development, security monitoring and testing, or even data analysis.

Certain online courses also offer a certificate upon completion. This allows young people to demonstrate their skills.

Communities

While a lot of harmful content can be found online, there are also many positive and ethical communities. Young people interested in IT can meet like-minded people in online communities such as Discord and hacker forums. These communities can provide answers to the problems they face, as well as encouragement for their cyber hobby.

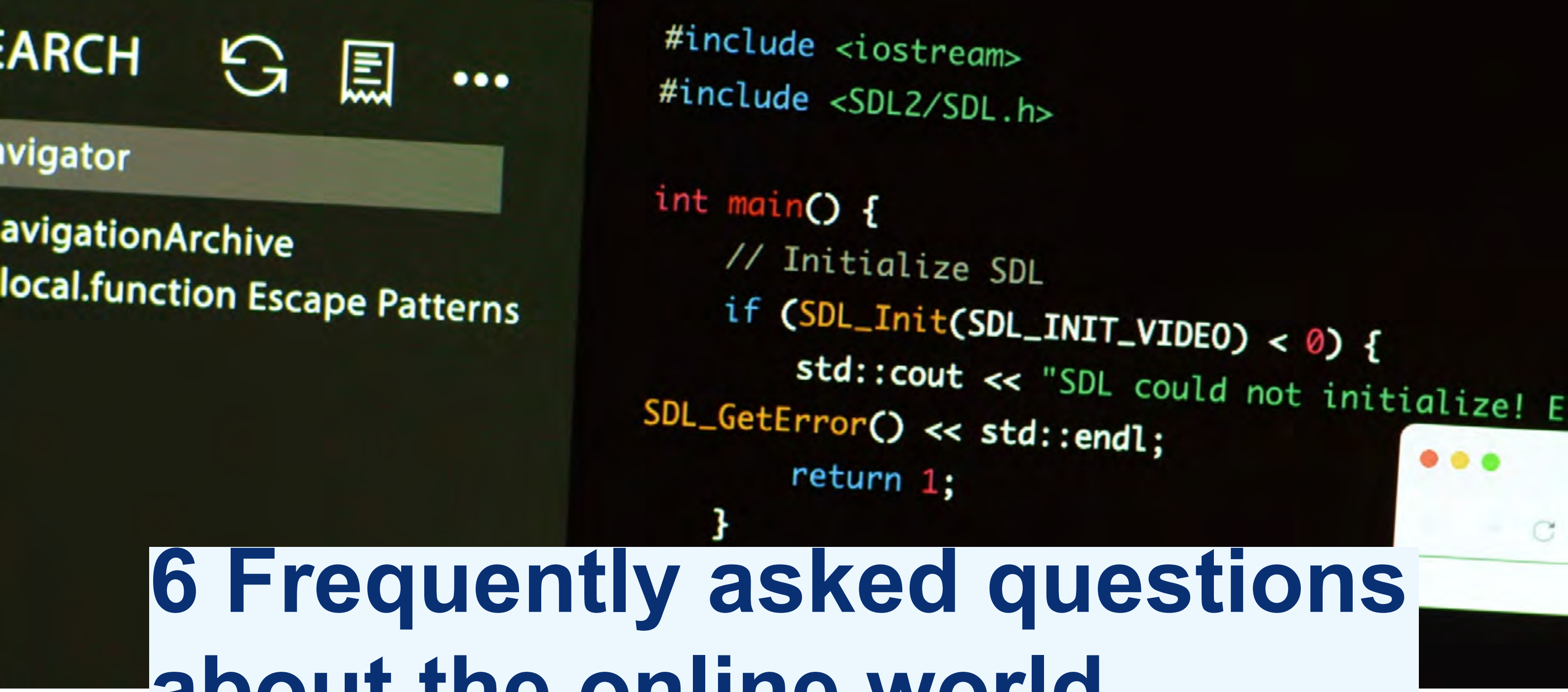
When looking for communities, pay attention to the content of the channels and the discussion culture. For example, ethical channels do not encourage the use of illegal tools such as booters or pressure anyone to engage in online activities that they are uncomfortable with. It is also a good idea to check whether the community is moderated and who is responsible for maintaining the group.

A young person's experience of community activities in general is a good reflection of the culture of the community. Good guiding questions include: Is there a supportive attitude towards online group members? Is the discussion between group members positive and respectful of others? How does the group deal with inappropriate discussion or bullying? Does the group encourage malicious or criminal activity, such as sharing malware or questionable links? How does the group react if one of its members starts bragging about criminal activity?

In addition to the online communities, many places have local communities or workshops where young people can work on their ideas or learn new ones with other like-minded enthusiasts. You can use search engines to check whether there are coding workshops or hacker clubs in your locality, for example.

Read more:

- European Union Agency for Cybersecurity (ENISA) website enisa.europa.eu
- Next Gen Hack Finland website nextgenhack.fi
- For up-to-date information on competitions and online courses, you can search for **“CTF”, “hacking challenge competition”, “CTF challenge”, “capture the flag exercise”, “Bug Bounty”, “vulnerability reward scheme”** or **“ethical hacking”**.



```
#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 Frequently asked questions about the online world

There are many questions and myths about information networks. Certain types of behaviour have become so normalised on online platforms that they are not even considered criminal. On the other hand, certain platforms and even the words they use may automatically create an image of criminal activity, even though they are used for legitimate purposes. In this section, we delve into some common questions and myths associated with the cyber environment.

6.1 What is hacking?

Hacking refers to creative problem-solving in a network and information system environment with the goal of finding and exploiting weaknesses in the environment. Unfortunately, hacking is often automatically perceived as a criminal activity. However, hacking can also be done within the law: ethical hacking is often an important part of corporate security. For example, an organisation might hire someone to find vulnerabilities in its system by attacking it. This helps the organisation to identify and correct weaknesses in its system. Some organisations run bug bounty programmes, in which attacks on their systems are permitted within certain parameters. They sometimes pay handsome rewards to those who find vulnerabilities.

However, hacking skills are sometimes also used for criminal activities, such as unauthorised access to information systems. The legality of hacking depends on the purpose of the activity, the target, and the methods used. It is important to understand the boundaries between legal and illegal security testing, and to raise awareness of how to report vulnerabilities and findings. Anyone interested in hacking should familiarise themselves with the legislation governing the online environment to avoid nasty surprises. As a rule of thumb, it is best not to independently investigate a vulnerability you have found. Instead, it is wise to report the discovery to the appropriate authority.

6.2 Can the dark web be used legally?

The dark web is the name given to the non-indexed part of the web that is beyond the reach of basic search engines and can only be accessed with a separate browser, such as the Tor browser. The Tor browser is free, open-source, volunteer-run software that enhances the network user's privacy. The Tor network anonymises network traffic through a global network of proxy servers, routing all network traffic through a series of encrypted servers called nodes. Each node decrypts only part of the route, so no server knows the entire route of the network traffic, making it difficult to determine the user's true location. The Tor network promotes the privacy and anonymity of communications, as users' locations and identities are more difficult to ascertain than on the open internet.

Dark web sites are accessed through the Tor browser or similar software. The dark web is often seen as a playground for criminals, but not all activity there is illegal. Using the Tor browser is legal, and many people use it to improve their online privacy. Especially in countries with strict state censorship, the dark web can be used to communicate more securely or access content that would otherwise be blocked. For example, human rights organisations and journalists may use the dark web to communicate and share content more safely.

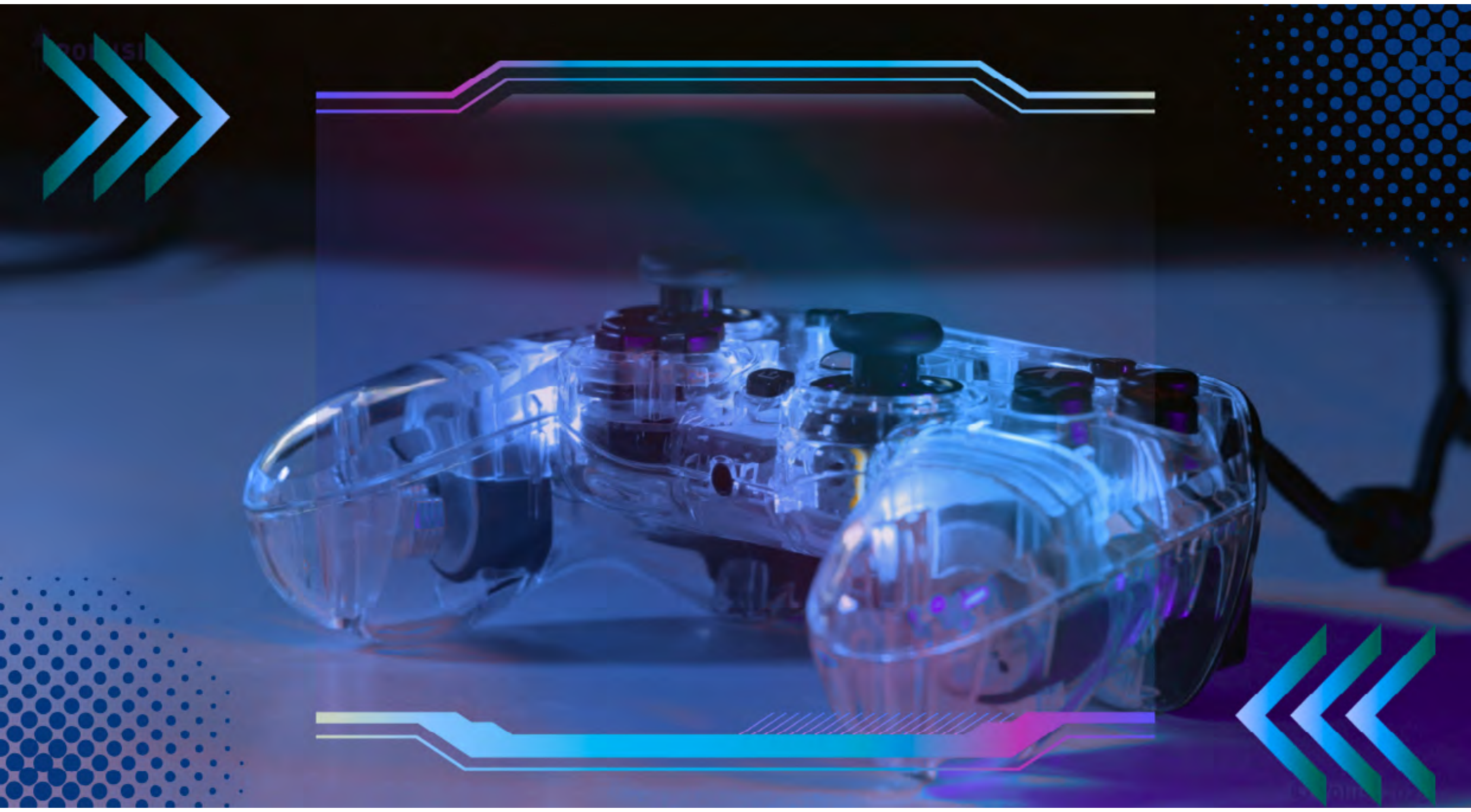
However, there are several risks associated with using the dark web.
A lot of criminal activity takes place on the dark web, including drug and arms trafficking and the distribution of illegal material. Criminals favour the dark web because of the higher level of privacy it offers, and dark web marketplaces are used to sell Crime as a Service, hacking and malware tools, or leaked data. Operating on the dark web is not as anonymous as one might think, and a user's identity may be disclosed to external actors despite the higher level of protection. In addition, the risk of being targeted by threats such as malware, scams, phishing or surveillance is high on the dark web.

The dark web may seem attractive to young people. It is therefore worth talking openly with your child about the dark web and the risks involved. Inexperienced users should not venture into the dark web, as without proper safeguards, they can easily fall prey to malicious activity. If your child has already used the dark web or is planning to use it, it is a good idea to discuss the reasons for using it, the benefits and risks, and weigh up together whether it is necessary for them to use it.

6.3 Are video games harmful?

It is often thought that video games are harmful and that young people should be steered away from them. Video game platforms, like other online platforms, are prone to disruptive and criminal behaviour, which is something to be aware of when playing. However, video games also have many positive effects and playing them can be a developmental hobby. Video games are a fun pastime and can develop learning, creativity, hand-eye coordination, and other useful skills. Video games bring together people from diverse backgrounds and can offer educational experiences as well as fun. Playing together can be a very communal activity and foster group and teamwork skills. Game characters can help the player process their own hopes, values and fears, and playing can also teach children and young people how to deal with feelings of frustration, for example.

Instead of giving up video games, parents should integrate the hobby of their child or young person into everyday conversations and get to know the games they play – for example, by playing them together. It is a good idea to discuss with your child the risks and problems they may encounter on game platforms and teach them how to act responsibly there. It is also good to discuss playing time and establish some ground rules. Any problems or disruptive behaviour should be reported to the platform and to a trusted adult.



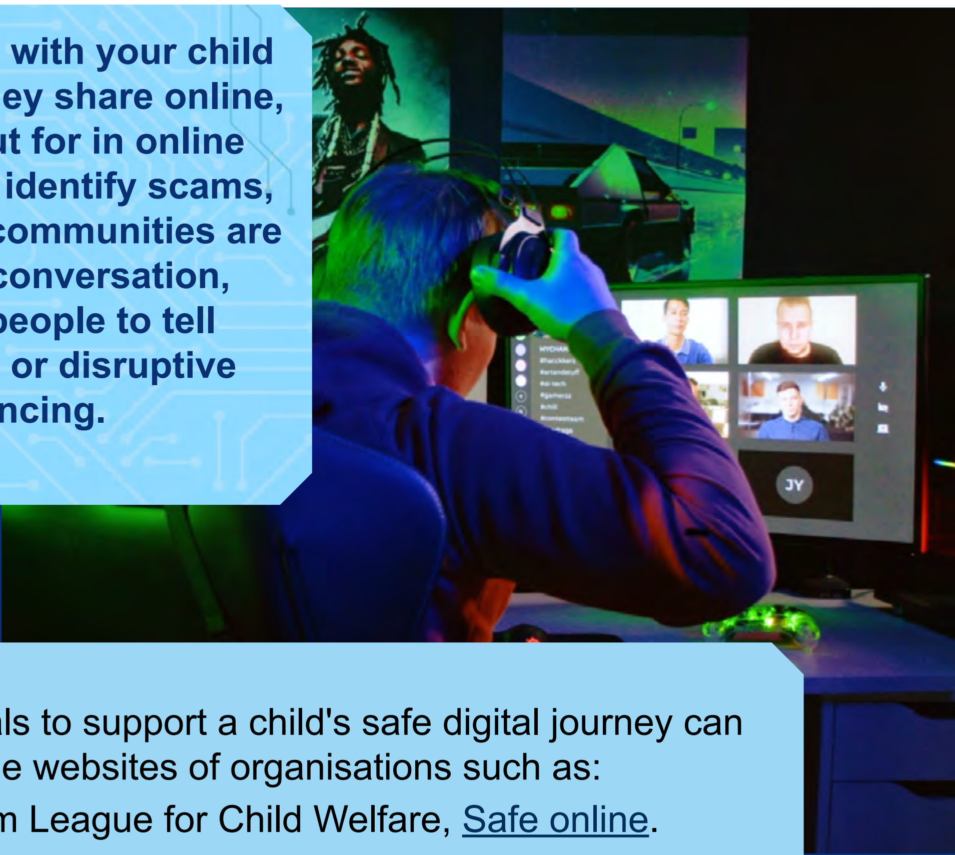
6.4 How should you approach interpersonal relationships among young people online?

It can sometimes be challenging for adults to react to a child's online relationships. Online friends may not be thought of as real, or they may be perceived as dangerous. It can be difficult to verify the identity of someone you are talking to online, and both children and adults should exercise caution when online and remember that the person behind an online profile may not be who they say they are.

In practice, however, the online behaviour of children and young people is highly social, and their online communities often include both real-world and online acquaintances. For many children and young people, online friendships can be really important and life-enriching. Online, it is possible to make like-minded friends from all over the world and receive support for topics of interest. Online friendships can be a very important way to support hobbies, especially for those young people who feel that they have no friends in their local community or area with similar interests. At the same time, young people from minority groups or in difficult life situations can receive crucial peer support online.

It is good to include your child's online relationships in your everyday conversations, just as you would with other friendships. Instead of automatically prohibiting or downplaying online friendships, it is wise to have an open discussion with the young person about who they spend time with on online platforms, and discuss age-appropriate personal boundaries and safe relationships online together.

It is a good idea to discuss with your child what kind of information they share online, what risk factors to look out for in online conversations, and how to identify scams, for example. When online communities are a normal part of everyday conversation, it can be easier for young people to tell an adult about any harmful or disruptive behaviour they are experiencing.



Read more:

Useful materials to support a child's safe digital journey can be found on the websites of organisations such as:

- Mannerheim League for Child Welfare, Safe online.
- Save the Children, Digital Childhood (in Finnish).
- Protecting children, A guide for parents on digital safety skills.

7 Where can I find help if...

7.1 I encounter an online security incident or malicious content, or if I find a vulnerability?

While online, you may encounter various types of malicious content, phishing attempts, or even vulnerabilities on a website. These types of problems should always be reported. The reporting process depends on the content or problem and the platform where it was found.

Content that violates the terms of use

If content violates the terms of use or is illegal, it can be reported directly to the platform that hosts it. Under the Digital Services Regulation (DSA), which came into force in February 2024, service providers must offer a channel for users to easily report content that breaches the terms of use or is suspected of being illegal. The reporting process varies, but platforms usually have a “Report this content” button.

You do not need to be certain of which terms of use or law the content violates. It is enough if you suspect that the content breaches the terms. The online platform or authority is responsible for investigating the content in more depth when they receive a report.

Information security incident

Information security incidents, such as phishing attempts or malware, should be reported to the authorities. Examples of incidents include malware that has infected your computer, a suspicious email link you received, or a text message asking for login credentials or bank details. You should report incidents even if they have not caused any damage.

- ► Submit a report to the National Cyber Security Centre Finland using the form on the Centre's website or by emailing cert@traficom.fi.
- ► If you suspect a crime, you should report it to the police without delay. You can report a crime electronically using the police’s online service or by visiting your nearest police station.

Security hole

If you find a security hole while online, it is vital that you do not exploit it. Exploiting vulnerabilities can, in the worst case, cause great harm to individuals, organisations or even society and lead to criminal sanctions. When a vulnerability is discovered, it is important to report it to the appropriate authority.

Report directly to the organisation

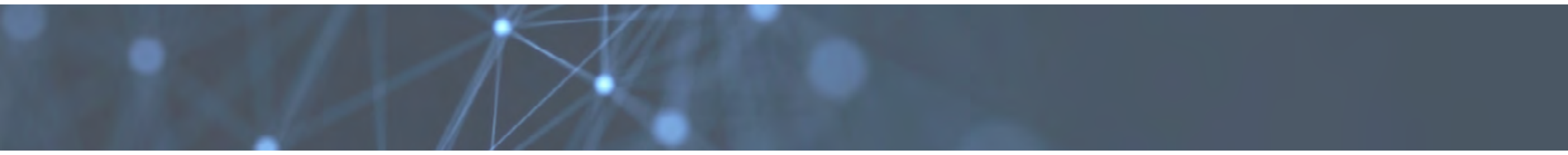
- ► Check whether the site has a separate email address or form for reporting vulnerabilities. If there are instructions for reporting a vulnerability on the website, the preferred method is to follow those instructions.
- ► Check if the site has a /.well-known/security.txt file that specifies the correct way to report a vulnerability.
- ► If the appropriate contact details cannot be found on the website, it is wise to report the vulnerability to the organisation's general email address and ask for further instructions. However, when using a general address, there is a risk that the information will not reach the right person.
- ► When making a report, patience and a matter-of-fact approach are key. Organisations have different approaches to handling reports. Some organisations respond to reports and may even offer a small reward for finding a security hole. Some organisations may not have a ready-to-go approach to handling reports, and a security breach notification may come as a complete surprise to them. It is, therefore, good to remember that you may not receive a response to your report, and the organisation may have taken action even if you do not receive a response.

If you are unsure what to do, it is a good idea to notify the National Cyber Security Centre Finland or, for example, send the report by email directly to both the organisation and the National Cyber Security Centre Finland.

Some organisations offer bug bounty programmes in which participants can search for security vulnerabilities in predefined environments. Bug bounty programmes usually require prior enrolment, have rules and limits for finding security holes, and pay rewards for vulnerabilities found.

Read more:

- ► For more information on vulnerabilities and how to report them, see the Vulnerability section of the National Cyber Security Centre Finland’s website.



Report to the National Cyber Security Centre Finland

- ► You can always report a vulnerability to the National Cyber Security Centre Finland. Reports can be submitted confidentially and anonymously.
- ► Report a vulnerability or security incident to the National Cyber Security Centre Finland online by completing the form “Report a security breach to us” on the website or by emailing cert@traficom.fi.
- ► You can report incidents to the National Cyber Security Centre Finland even if you have not first tried to report them directly to the organisation concerned. Reporting to the National Cyber Security Centre Finland is an easy option if you wish to remain anonymous or do not want to deal with the matter further. If you wish, you can also submit a report to the organisation concerned and the National Cyber Security Centre Finland at the same time by addressing an email to both parties.
- ► Support and further information on how to deal with security incidents is also available at this address.

7.2 I encounter suspicious or criminal activity online?

You should always report any suspicious activity you encounter online to the police.

If you suspect that you have been a victim of a crime, you should report it to the police without delay. You can report a crime electronically using the police’s online service or by visiting your nearest police station.

If you notice suspicious activity online or suspect you have come across illegal material or content, you can easily report your suspicions to the police using the online tip-off form at poliisi.fi/en/net-tip. The online tip-off form can be used to report non-urgent issues. The online tip-off form can be used to report suspicious activity, even if you are not sure whether it is a crime. When you submit a tip-off, describe in as much detail as possible the content or activity you have come across and where you found it. If you wish, you can leave the tip-off anonymously. The police deal with online tip-offs and, if necessary, take further action if there is reason to suspect a crime.

Read more:

- ► Report a security vulnerability to the National Cyber Security Centre Finland at kyberturvallisuuskeskus.fi.
- ► Submit an online tip-off at poliisi.fi/en/net-tip.
- ► You can report a crime electronically at poliisi.fi, or by visiting your nearest police station.

7.3 I have concerns about the online behaviour of a child or youth?

Are you concerned about a young person's behaviour online? Do you suspect that a young person's interests or activities have crossed the line into illegality? Do you need more information or support?

The National Bureau of Investigation’s preventive Cybercrime Exit programme prevents serious cybercrime among young people, raises awareness of how to recognise legal and illegal online activities, and supports young people in adopting a crime-free lifestyle as part of the police's specific prevention activities.

Cybercrime Exit provides information and guidance on prevention and early intervention in cybercrime. It also provides support for young people who may have already committed criminal acts online. Cybercrime Exit’s target group is young people aged 12–25 who have committed serious cybercrime or are at risk of committing it. A young person can approach Cybercrime Exit at their own initiative, or they may be referred by professionals, for example. The activities are voluntary and confidential. The starting point is to reinforce a crime-free lifestyle by helping young people to recognise the boundaries between legal and illegal activities, identify job and study opportunities that support their skills, access other possible support in their life situation, and guide them into networking activities that support a legal approach to their interests. An individual plan is drawn up with each client, taking into account their situation and interests.

Contact us

Cybercrime Exit can be contacted by email at **cybercrime.exit.krp@poliisi.fi**.

For more information on the project and cybercrime prevention, visit the **Cybercrime Exit website.**

In the words of young people

What young people would like parents and educators to know about the internet

Young people are experts in their fields and know best what challenges they face online. **Testausserveri ry** is a non-profit association founded by young people for young people interested in information technology. It aims to inspire young people to take up an IT and cyber hobby and provide support for their cyber projects through the Discord community. We asked members of Testausserveri ry to tell us what they would like parents and educators to know about IT hobbies, and what kind of support they would like adults to give them. The main themes that emerged were understanding and showing an interest in the young person's hobby, and supporting them in learning to act ethically.

What young people would like adults to know about IT as a hobby

- ► Hacking as a hobby is not illegal, and the purpose of hacking is not to cause harm, as long as you remain within the permitted limits.
- ► A consensus about what is legal and harmless behaviour, and less unjustified fear.
- ► There is value and potential in IT as a hobby to develop useful skills for the world of work.

> **"My relative used to go through my code in his spare time and always improved it. This helped me learn the best practices. I cannot imagine any better support than this."**

Read more:

- ► Find out more about Testausserveri at testausserveri.fi.

What kind of support would young people like to have from adults for their IT hobby?

- ► Show interest in the person's hobby. Adults can show interest by asking about the software or tools the young person uses or what they have learned, for example. This allows the adult to show an appreciation for the young person's hobby and helps them to understand the young person's behaviour. Adults could also suggest coding project ideas for the young person.
- ► A young person may be interested in a cyber hobby but need help finding resources for ethical learning and hobbies. It is easy for a young person to run into bad influences online, but they could do exciting things with permission, as long as they know where to find the right places.

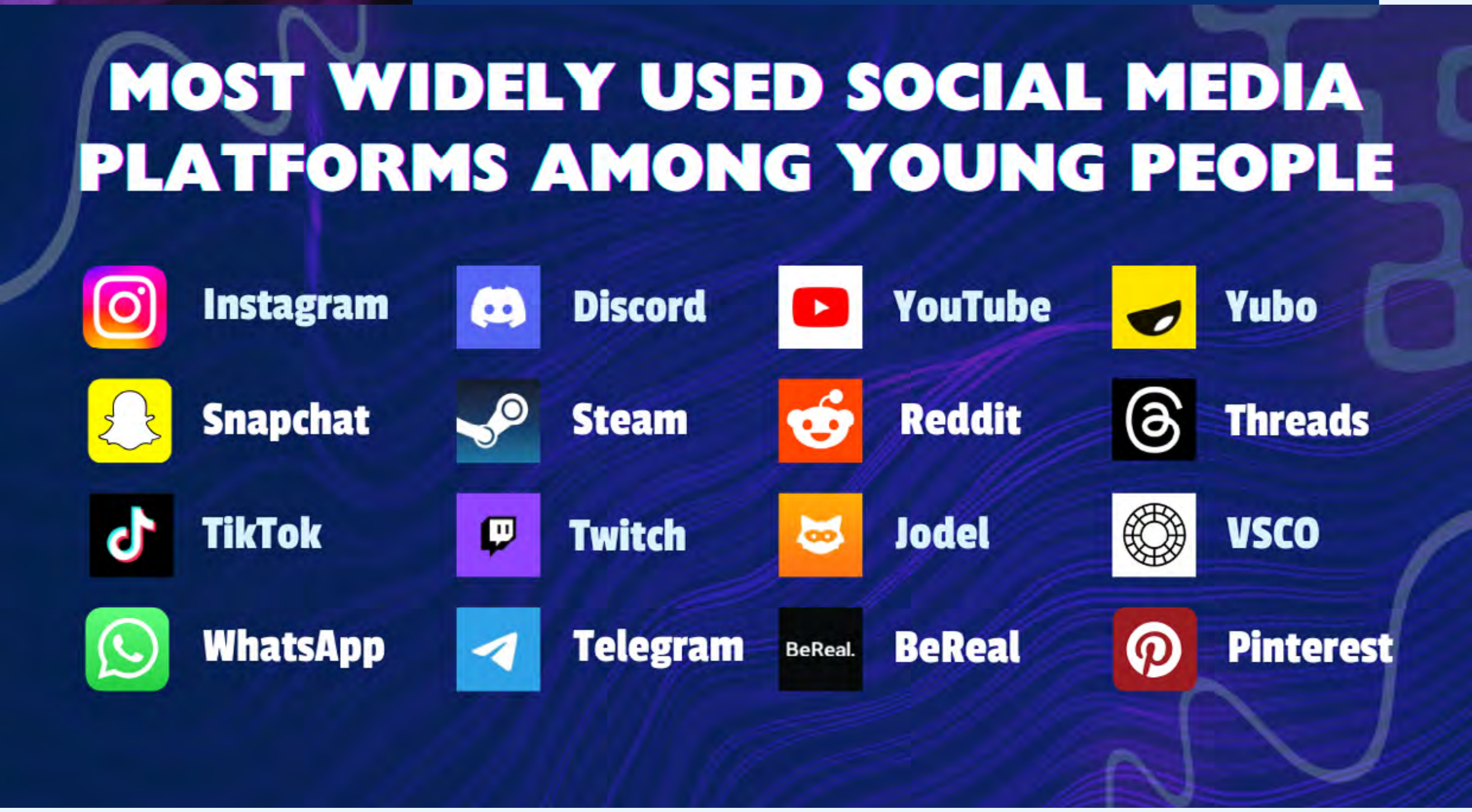
> **"I could have done with more guidance in finding things. I mean, it would have been nice to have support in solving problems using search engines."**

Social media channels popular among young people

The most popular apps among children and young people change at a rapid pace, as new apps emerge constantly. In 2024, young people in Finland were most active on Snapchat, WhatsApp and TikTok. Adults often perceive messaging apps such as WhatsApp and Telegram as discussion channels, but they also offer communities to follow and other social media features that even children of primary school age actively use.

It is a good idea to talk to your child about the platforms they use actively.

This section lists some of the social media channels that are popular among young people, so adults are advised to familiarise themselves with the channels.



MOST WIDELY USED SOCIAL MEDIA PLATFORMS AMONG YOUNG PEOPLE

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

Glossary of cyber terms

Booter

A tool that allows the user to perform denial-of-service attacks against a target of their choice on a network. The booter sends so much traffic to the selected target that the target's service, such as a website, is overwhelmed and becomes unavailable during the attack. Attacks by booter services typically exploit network devices that are illegally hijacked by means such as data breaches to form a botnet.

Booter and stresser services are readily available on the open web via public search engines for a fee or even for free. Booter and stresser sites may claim to sell products suitable for security testing. In reality, however, the services provide illegal tools that allow denial-of-service attacks to be carried out from anywhere in the world.

Botnet

A group of networked IT devices that have been hijacked to carry out network attacks. A person building a botnet takes control of devices connected to other parties' networks by means such as malware or exploiting weak security on devices, such as a bad password or the lack of a password. The hijacked devices are assembled into a remotely managed network, which can be used to send data traffic to the selected target upon command.

A botnet can consist of a range of everyday connected devices such as computers, smart TVs, speakers, fridges or electric toothbrushes. The device owner may not even realise that the device is being used in a botnet. Botnets can be used for purposes such as phishing, denial-of-service attacks, malware or spam.

Bug bounty

A bug bounty is a programme provided by an organisation or platform that allows participants to search for security vulnerabilities in a pre-arranged environment with permission. Anyone who finds a vulnerability is paid a reward, such as financial compensation. Bug bounty programmes are usually limited to a specific, predefined part of an organisation's system or platform, and often require pre-registration. The programme can run for a limited time, or continuously. The size of the reward varies depending on the software and the severity of the vulnerability found.

Companies can use bug bounty platforms to manage bug bounty programmes for multiple parties. Large companies such as Meta and Google often offer their own bug bounty programmes, and the rewards can be substantial.

Crime as a Service (CaaS)

Automated crime tools are available online that can be used to commit various crimes, such as denial-of-service attacks, as an outsourced service (Crime as a Service). Crime-as-a-Service providers can also be easily found through general search engines, and they allow cybercrime to be committed even without significant IT skills.

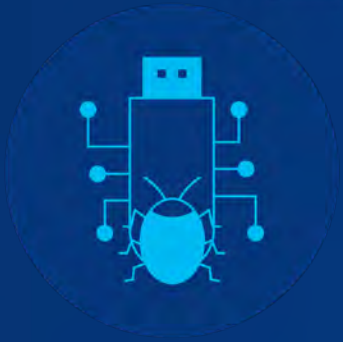
Capture the Flag (CTF)

Capture the Flag (CTF) competitions are hacking challenges, where the aim is to solve a challenge, or a set of security challenges, in a sandbox environment. The challenges involve various security scenarios, such as identifying vulnerabilities in code, reverse engineering, and decryption. After solving the challenge, the player receives a "ticket" that, when returned, is worth the agreed number of points for completing the challenge. CTF competitions offer different levels of challenges and are a safe and inspiring way to learn about hacking.

Vulnerability, Security hole

A vulnerability, or security hole, is a weakness in a system that allows an outsider to exploit or cause damage to the target system. Vulnerabilities can be found in software, information systems, applications or hardware. A security hole may be caused by outdated software, for example, and software updates often fix vulnerabilities.

Vulnerabilities vary in severity. Security vulnerabilities can be minor, and the software provider may discover and fix the vulnerability before any harm occurs. At their worst, vulnerabilities can be critical, effectively allowing an outsider to gain unfettered access to the system and do anything on it.



Malware

Malware is malicious software designed to damage or exploit information systems or devices. Common types of malware include viruses, worms, spyware, ransomware, keyloggers and trojans. A device can become infected with malware if the user opens a malicious email attachment, downloads the wrong software, or clicks on a polluted link. Malware can also spread through a vulnerability, so it may be able to spread without the user taking any action. For example, malware can be used to fish for information, steal bank or credit card details, take over a device for extortion purposes, or use an infected device as part of a botnet.

Hacker

A person who is adept at using information technology and has creative problem-solving skills to deal with information technology challenges. A hacker could use their skills to make the internet safer. They could also use their skills for criminal purposes – for example, by hacking into a protected system.

Hacking

Creative problem solving in a network and information system environment with the goal of finding and exploiting weaknesses in the environment. Hacking is often perceived as illegal, but it can also be done within the limits of the law. Ethical hacking is an important part of security testing.

Distributed denial-of-service (DDoS) attacks

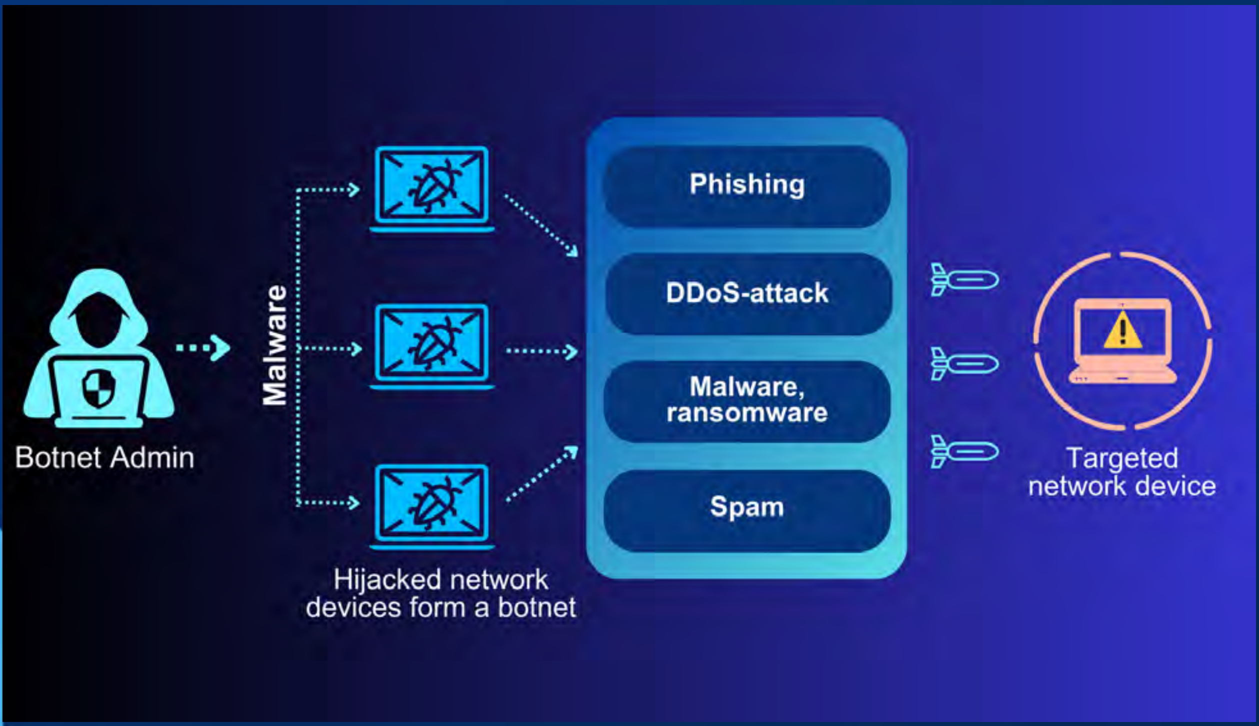
A cyber attack that is intended to disrupt or prevent the normal functioning of a particular network service. A distributed denial-of-service attack is carried out by sending so much traffic to a website that the site becomes overwhelmed and can no longer operate normally. A denial-of-service attack can be carried out directly from a single source, or in a distributed manner, for example, by exploiting a botnet. Denial-of-service attacks can also be carried out without extensive technical knowledge using automated tools such as a booter, which can be found on the open web.

Script kiddie

An amateur hacker who does not have extensive technical knowledge themselves, but uses tools or scripts created by others to carry out cyber attacks. Script kiddies are usually beginners who do not know how to build code from scratch, but rely on pre-built tools to perform attacks.

Read more:

- Cybersecurity glossary, National Cyber Security Centre Finland.
- Vocabulary of Cyber Security, Finnish Terminology Centre.
- The websites of telecom operators and information security companies also provide more information on security and the latest cyber phenomena.



Young people online – An educator's guide to cybercrime prevention and responsible online behaviour

This guide was created as part of the **Cybercrime Exit project**, co-funded by the European Union. This guide was created in response to a request from project stakeholders for an easy-to-use resource for educators, such as carers and teachers, on how to prevent cybercrime among young people. The necessity and content of the guide were also discussed with the National Bureau of Investigation’s Cybercrime Centre, the National Police Board, the Ministry of the Interior, and Testausserveri, among others, and these parties were invited to comment on the draft version of the guide. In addition, the members of the Testausserveri association wrote a short section in the guide on young people’s wishes towards educators. The guide was produced by the National Bureau of Investigation’s Cybercrime Exit project.

The National Bureau of Investigation launched a programme of cybercrime prevention for young people in 2020. The activities continued from 2023 to 2025 with Cybercrime Exit 3, a client and education pilot project to prevent youth cybercrime, co-funded by the European Union. The project piloted and developed interventions to prevent cybercrime among young people and created up-to-date operating conditions to detect the specific characteristics of cybercrime and intervene in the cycle of cybercrime among young people. The National Bureau of Investigation will continue its work on cybercrime prevention in 2026 with a consolidation project as part of the implementation of the police's preventive action strategy and the national cybersecurity strategy.

Cybercrime Exit project team:

Viivi Lehtinen, Project Manager
Sari Latomaa, Chief Inspector
Aki Somerkallio, Chief Inspector

Police
Written by: Sari Latomaa, National Bureau of Investigation.

Photos in the guide: Police, Canva C00, Pexels CC0, Unsplash C00.

ISBN 978-951-53-3934-8

Published 3/2026, translated by Semantix Finland Oy.

The hyperlinks were checked on 20 November 2025.