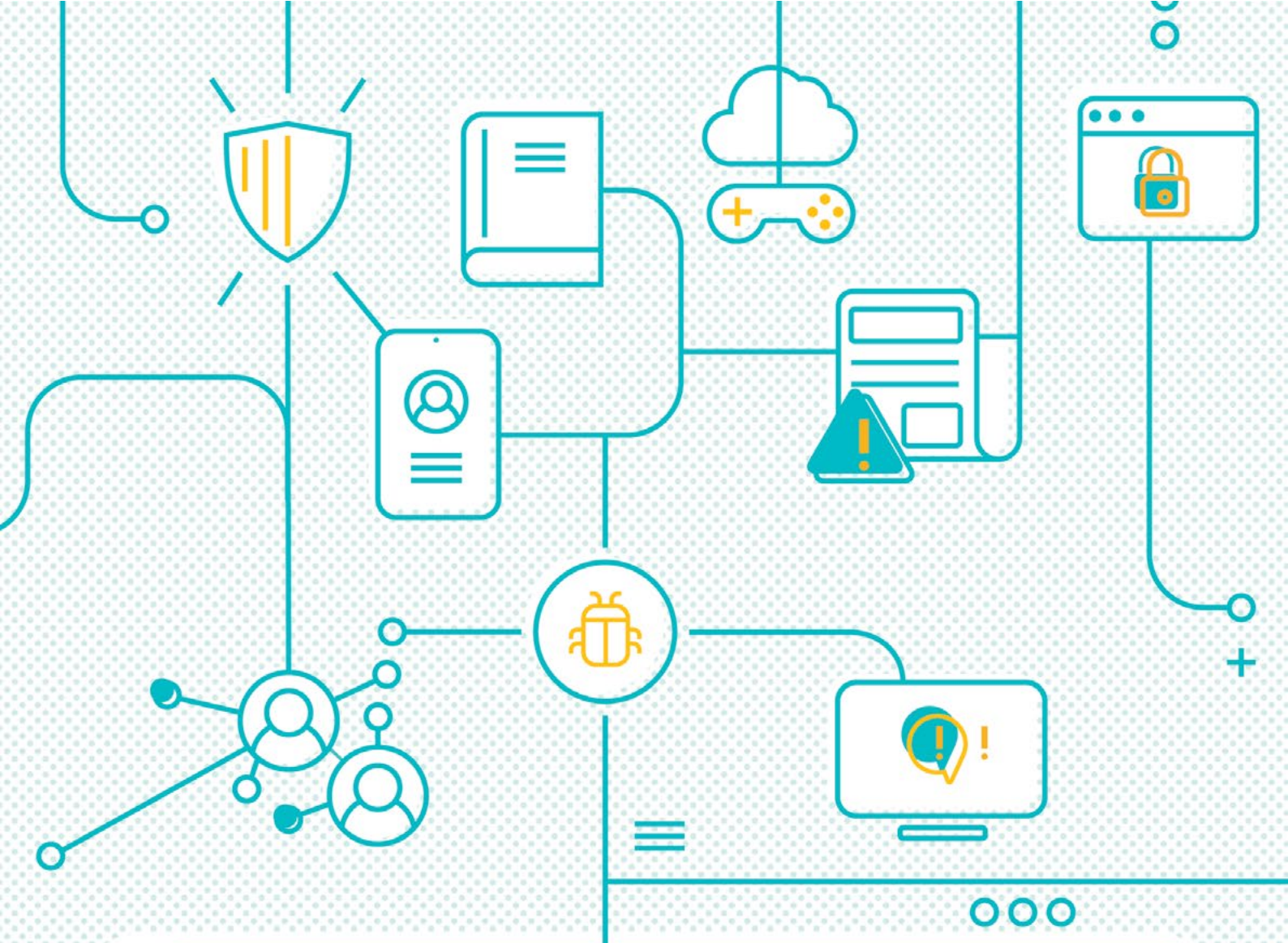


DIGITAL SECURITY HANDBOOK

FOR TEACHERS

saferkidsonline by ESET

ISBN 978 – 80 – 973884 – 0 – 9

Contents

Mobile device security 8

Selfies 12

Cyberbullying 14

Trolling and cyberhate 22

Social networks 25

Social networks and digital security 26

Social networks and psychological resilience 30

Influencers 36

Real vs. online world 40

Disinformation, hoaxes and fake news 47

Digital identity and privacy 55

Online, not everyone is who they seem to be 61

Browser security 63

Surface web, deep web, dark web 68

Illegal downloads 69

Online games 70

Malware and other malicious activities 73

Security solution (antivirus) 79

Internet connection security 82

Passwords 86

Updates 91

Glossary 95

Biography of the authors 98

Acknowledgements

We would like to thank all **ESET staff** who have contributed their professional advice, suggestions and organisational skills to help create this handbook.

We would also like to thank psychologist **Jarmila Tomková** for contributing several key chapters reflecting her professional and practical knowledge.

And last but not least, we want to thank **all the teachers** who, despite adverse conditions, keep educating and preparing the new generation for life in the digital age. Special thanks go to **Peter Kučera** who managed to take time out of his busy schedule to provide us with very useful feedback.

Introduction

The internet and digitalisation have changed the world. Smartphones, apps and social networks have introduced profound changes in the way children and young people are growing up. These technologies open up new, previously unforeseen horizons but also introduce risks and threats unknown to past generations.

In this situation, elementary school teachers find themselves on the front lines but are often left without any useful material or information. Still, it remains their task to impart knowledge of both the digital and real world and prepare students for a life in both of them.

ESET is here to help.

As a global leader in the digital security field, with more than 30 years of experience and more than 110 million protected users worldwide, we believe it is possible for parents to enjoy a digital life without fearing for the safety of their children. However, to achieve that, it is paramount to raise awareness of the importance of online safety among kids.

With that in mind, we have created the SaferKidsOnline platform full of educational and engaging content for kids, parents and teachers. An important part of that long-term and extensive effort is this handbook, based on our renowned, award-winning experts' knowledge, experience, and insights. It provides elementary school teachers with basic theoretical understanding of online security and safe use of the internet. It also contains practical exercises that they can use to present the topics covered in the handbook in an interesting and interactive manner, emphasizing modern didactic methods.

This handbook looks at digital security from two different viewpoints:

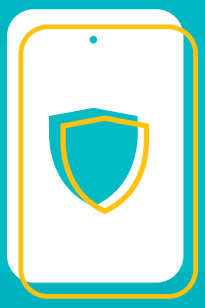
- The technical viewpoint, based on ESET's 30 years of expertise in developing security solutions for digital equipment.
- The psychological viewpoint, with the focus on various digital threats, such as cyberbullying, which cannot be resolved using technology alone, as they often spill over from the online to the offline world.

One of the obstacles to education can be the so-called generation gap. Today's children and young people are constantly in direct contact with the latest technologies, which gives them far more detailed knowledge and skills in this field. That does not mean, however, that teachers cannot keep up with them and bridge the generation gap:

- It is not the teacher's task to match the children's knowledge in every aspect. However, they can reasonably complement one-another and coordinate their mutual learning experience.
- Besides imparting knowledge, teachers should also take advantage of the most recent experience of learning methods, project-based learning, peer learning and more.
- Teachers can introduce difficult topics, initiate debate and spark interest in the issues. They don't always have to present solutions—they can just moderate the debate in which a group of students finds suitable solutions, or, at the very least, starts thinking about the existence of the issues.

We believe this handbook will become a useful tool for teachers in preparing and shaping their lessons.

Certain theory chapters are supported by proposed practical activities that can be found in The Digital Security Handbook Activities (further as “Activities”). They are a series of activities designed by ESET experts, computer science teachers and child psychologists, which present the topics of digital security and safe internet use by children in an engaging and practical form. If you find this icon throughout this Handbook, make sure to find an activity for it under the corresponding topic.



Mobile device security

application | cloud | mobile antivirus | mobile security solution | mobile device | factory reset | operating system | PIN code | follower | developer | smartphone | tablet

Issues covered in this chapter:

- What are the basic rules of mobile device security?
- Why should you lock the screen and which method is the safest?
- Why update apps and the operating system?
- Why download apps from the official Android/Apple app store only?
- How can you safely download apps and what should you watch for?
- Does a mobile phone/tablet need antivirus protection?
- Why should you back up your data and how should you safely store it?

What are the basic rules of mobile device security?

One of the first things every user/pupil/student can do to increase their security is to choose a quality mobile device from a reputable manufacturer.

Many of the following recommendations apply to the two most commonly-used operating systems—Android and iOS. On Android, users can take advantage of both the built-in security and third-party security software. Mobile devices have several layers of security (in particular, tablet and smartphone):

1. **Device access:** You should always lock your device in case it gets lost or stolen, but also to protect the stored data from unauthorised third-party access. Currently available locking mechanisms include the unlock pattern[1], PIN code, face ID and fingerprint ID. Fingerprint ID in combination with a four- to six-digit PIN code is currently considered the most secure form of protection. If the device doesn't have a fingerprint scanner, then at least one of the other options should be available for activation under "Settings".

2. **Physical device security:** Modern mobile devices store a lot of sensitive data which, if the device is lost or stolen, can end up in the wrong hands. Users should thus take advantage of services allowing them to remotely locate, lock or erase the device. Here's how to activate this type of service:

    a. Android devices
    b. Apple devices

3. **Backups:** Some malicious attacks can affect the functioning of the mobile device to such an extent that it requires a factory reset. This will automatically erase **all user data** including contacts, pictures, videos and stored settings. This is one of the reasons why users should regularly (e.g. once a month) copy all their valuable data from the mobile device to another location and create backups.

    There are several ways to do this:

    a. One of the user-friendliest methods is to use a cloud backup offered for a modest monthly fee by the manufacturers, such as Google and Apple, or to use another app available on Google Play or the App Store.

    b. As an alternative, users can back up data to a hard drive not connected to the internet, and thus not accessible to any attackers who would usually misuse vulnerabilities or weak security to access a connected storage. An example of this is an external hard drive which the user disconnects from the computer immediately after creating the backup.

4. **Sensitive app protection:** A fingerprint and PIN code combination can also be used to secure access to some applications, such as internet banking or cryptowallets[2]. This should be a separate PIN code different from the one used for device access.

1 The user has to connect some of the nine dots displayed by the device in the correct order.
2 An application which can store cryptocurrencies such as bitcoin, Monero, Ethereum and others.

5. **Be careful about applications from unofficial app stores:** For maximum device security, we recommend using only apps from the official app store for the given platform (Google Play for Android and the App Store for iOS). Users should avoid unofficial app stores and forums, which are the most common channels for attackers to spread malware.

6. **User app reviews:** Before installing an app from the official app store, always read the reviews posted by other users. If they refer to the app as fake, malware or a virus, you should postpone the installation and at least do a simple online search to check whether the app has not been tagged as unsafe. Special attention should be paid to all negative reviews. The positive ones are often created by the attackers themselves to improve their chances of success. Fake apps also often promise what they cannot deliver, such as the quick and free increase of the number of friends/followers on a social network or easy money in exchange for installing the app on the device.

7. **App permissions:** Before starting the installation, every app notifies the user which data and features it needs to access to be fully functional. Suspicious apps often request access to features completely unrelated to their purpose. If, for example, an image viewer app requests access to the microphone, this can suggest an attempt to stalk the user.

8. **Operating system and app updates:** Developers constantly find new weaknesses and vulnerabilities in applications and regularly issue updates to fix them. Users should thus regularly update both the operating system and the apps installed on their device. Users can set up automatic device updates or set the device to automatically offer updates which are then installed manually by the user (all options are available under "Settings"). For more information on this topic, see the chapter Updates.

9. **Mobile security solution (antivirus):** To further improve the security of Android devices, we recommend using a security application—commonly referred to as mobile antivirus. A reliable security application can notify the user of the harmful nature or behaviour of apps and protect them from malicious links or data theft. This also applies when the harmful nature of the app is revealed only after it has been installed on the device. Some security applications also notify the user of weak or incorrect security settings or can help them retrieve a lost or stolen device. For more information on this topic, see the chapter Securtiy solution (antivirus).

BONUS TIP: What else should mobile device users watch out for?

Even the official app stores can be infiltrated by malicious actors or malware that is difficult to spot. One of the signs that can give away a fake version of a popular app is the developer's name. This can differ from the real developer name by just a single character (e.g. the capital "I" (as in the name Ivan) can be replaced with a small "l" (as in the word letter)). Another approach used by attackers is to name their developer account in a way that increases their trustworthiness. An example of this are names which look like the number of user downloads (See Figure 1 and Figure 2).

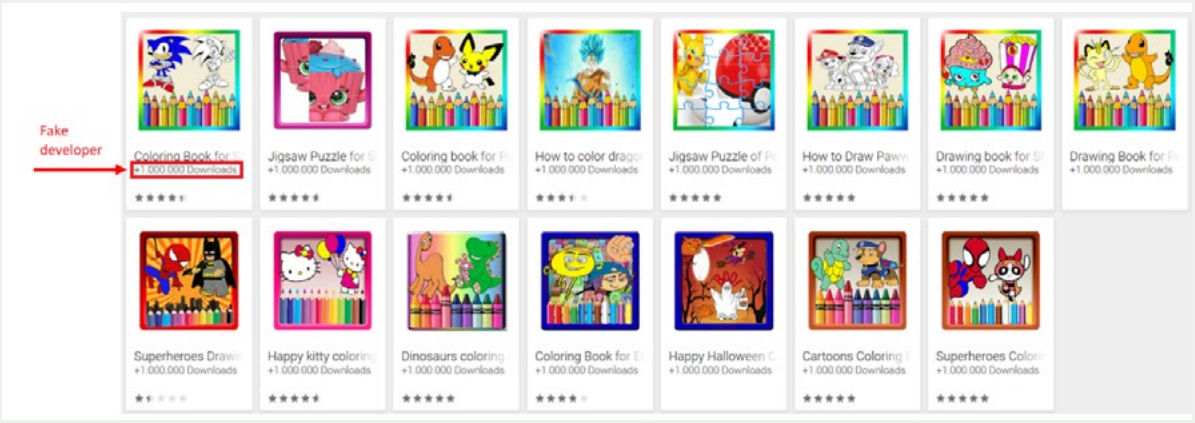


FIGURE 1 *"+1,000,000 Downloads" is a fake developer name. It creates the impression that this app has been downloaded by millions of users while in reality it was only downloaded by a couple of hundred. Source: Google Play Store*

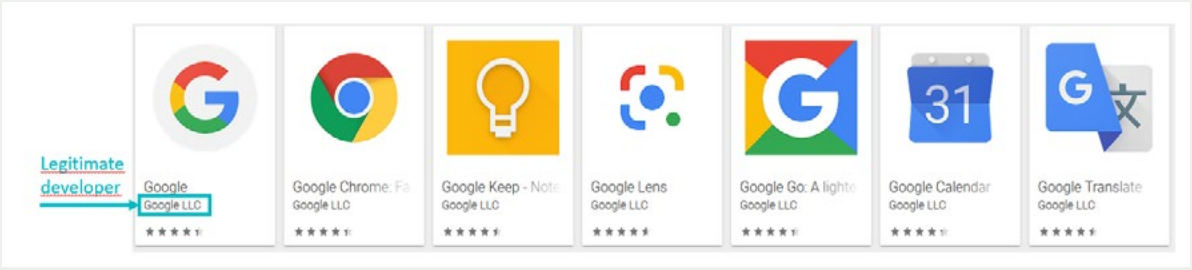


FIGURE 2 *Normally, here it shows the name of the legitimate developer (as is the case with these Google apps), not the number of downloads. Source: Google Play Store*

Rules for children using a mobile device

Teachers should advise pupils/students of the risks associated with mobile phone use or emergency line abuse:

- Children should never use an emergency line unless there's an emergency. Otherwise they block the line for those who really need help and run the risk of incurring a fine or more severe punishment.
- When a child gets a call from an unknown person, they should never give out any personal or otherwise sensitive information. A bank, technical support and other professionals never call their customers and request such information.
- A person calling a child should introduce themselves first.

- In their voicemail message, children should never state their own or other people's contact information.
- Children should always think about who they give their phone number to.
- If a child receives unwanted messages via Bluetooth, they should disable Bluetooth and make the device non-discoverable in the "Settings".
- If a child does not know the sender of an SMS message, they should not click any links in such a message or reply to it.

Selfies

selfie | selfie stick | viral image

Issues covered in this section:

What is a selfie and what risks does it entail? What rules should you follow when taking a selfie?

What is a selfie and what risks does it entail?

A selfie is a self-portrait photograph typically taken with a smartphone which may be held in the hand or supported by a selfie stick. Despite the modern name, selfies have been around for quite some time. Hundreds of years before the first mobile phone or social network was invented, "selfies", or self-portraits, had been made by many renowned artists such as Leonardo da Vinci, Rembrandt and Vincent van Gogh.

Unlike the great painters of the past, many present-day users (regardless of their age) don't pay much attention to what is visible in the shot when taking selfies, and without even checking the image they post it on their social network profiles. By doing so, they expose themselves to various risks. Mainly the image can contain things which the user did not intend to publish, or it can depict them in an unflattering pose.

Let's look at the recipe for a good (and in particular safe) selfie by da Vinci, Rembrandt and van Gogh. When painting their self-portraits and creating other works of art, they invested days into what should be in the foreground as well as in the background. Users probably don't need to take days but should give at least some thought before taking selfies and always scrutinise the final image just like an investigating officer or a detective would.

Not observing a simple set of rules can lead to a number of problems, such as ridicule from their peers, cyberbullying or the publishing or sale of intimate images in online forums.

What rules should you follow when taking a selfie?

1. First of all, you should be aware of your surroundings and what they look like. As many people have learned the hard way, a selfie can be fatal. Statistics show that each year, more people die from taking selfies than from shark attacks.
2. When taking a selfie, you should also focus on the details, such as: What is on the table, on the windowsill or on the floor in the background? Does the image capture my ID card, insurance card, passport or a concert ticket with a QR code? Does the image disclose my location to someone who should not know it?
3. Before publishing a selfie, you should realise that the image will remain on the internet forever and that it will not be possible to completely remove it. To illustrate this, teachers can use the fact that many photographs of common people have inadvertently become viral and cannot be controlled anymore by their authors/owners. A good rule of thumb is to first answer the question: "Would I want my grandmother, parents, acquaintances or my future employer to see this photograph/selfie?"
4. Users of all ages should also protect their privacy by adjusting their profile settings. For more information on this topic, see the chapter on social networks.
5. When it comes to selfies, teachers should act as role models and follow the rules they advocate.

BONUS TIP:

If you want to take a selfie with another person (a celebrity), ask them for their permission first. We are all entitled to privacy and the same applies to well-known YouTubers, musicians, movie stars and other celebrities you may meet on the street. There is even a video devoted to this topic shot by Kirsten Dunst.

Cyberbullying

lack of restraint in the online environment (disinhibition effect) | cyberbullying | outing | cyberstalking | happy slapping | troll | trolling | cyber-hate

Issues covered in this chapter:

How is lack of restraint shown in the online environment?
What is cyberbullying and what are its basic signs?
What do cyberbullies do?
How does cyberbullying differ from face-to-face bullying?
Why do we need to know about cyberbullying and do something about it?
Are there more male or female bullies?
How can teachers tell that a child is being bullied?
What can teachers do against cyberbullying?
How should teachers react when a child tells them that s/he is being bullied?
What environments pose a higher risk of (cyber)bullying?
What should you pay attention to when teaching about preventing (cyber)bullying?

How is lack of restraint shown in the online environment?

Electronic communication is specific in several ways:

- **People don't communicate in real time.** This applies to chats as well as to comments on social media content and replies to emails. An exception to this is videogames.
- **Electronic communication is often anonymous** and people may feel above the law.
- **It makes it difficult to feel empathy**. Unless the two parties are in a videocall, the child does not see the other party's face, body, movement or reactions and doesn't fully understand the consequences of their actions and communication.
- **When nobody can see the child (or user), they loosen up, feel less restrained, more courageous and less limited by social norms**. This can be beneficial to the shy among us, however, it can cause too much "loosening up" with others and lead to expressions of aggression. Without the usual inhibitions and guilty conscience, people often let their emotions, desires and behaviour run fee.

This "lack of online restraint" is also called the **disinhibition effect.** People on the internet often show a lack of restraint and caution due to their perceived anonymity. It is this loosening up that causes people to often act with more courage or even aggression in online communication. They often confront people they would never dare to challenge face-to-face. This can result in expressions of aggression and improper communication:

- This can either take the form of isolated incidents, such as trolling or cyberhate,
- or systematic cyberbullying or cyber-stalking.

What is cyberbullying and what are its basic signs?

Nowadays, bullying can take place both online and offline. When electronic means are used, we call it **cyberbullying, electronic bullying, mobile and internet bullying or electronic aggression.**

However, research shows that when cyberbullying takes place, the victim is often also being bullied in the real world and their peer relationships are disrupted and less satisfactory. Cyberbullying is thus not completely disconnected from the offline realities. The digital tools just give the attackers another possibility to hurt the victim.[1]

Bullying, either in cyberspace or face-to-face, has the following basic traits:

- **There is a disproportion of power between the attacker and the victim**.
  The attacker's dominance and the victim's helplessness can be real or apparent, emanating from physical strength, self-confidence, feelings of inferiority or from the superiority of a group. The dominance can be real or subjective. When it comes to cyberbullying, superiority can also take the form of technical skills and reactions of the audience to the hurtful acts.
- **It involves intentional harm** inflicted on one or multiple persons.
- The aggressor can be a **single child or a group of children**.
- **Repeated ill-treatment**. A one-off act of aggression in a face-to-face environment is usually

not deemed bullying. With cyberbullying, the matter is more complicated. The bully can add a single ridiculing post which others can like, comment on and share with other users. There has only been a single post, however, all the other reactions and interactions can also be deemed hurtful, which is further multiplied by the size of the audience.**Is influenced by group dynamics**. It is not just about the attacker and the victim, but also about the audience—**the bystanders**—who are a source of feedback for the attacker (admiration, encouragement, refusal, ignoration) and witness to the victim's humiliation on social networks. The passivity or activity of the witnesses determine whether the victim becomes isolated or gets backed by their friends. It is the bystanders' attitudes or actions/lack thereof that can alleviate or completely stop the bullying, or, vice-versa, legitimise it and contribute to it.

- Cyberbullying, just like any other form of physical or psychological abuse, is a **violation of the child's rights**.

Cyberbullying involves the abuse of the internet and digital technologies, i.e. smartphones, mobile devices, the internet, websites, apps and online activities to intentionally inflict harm on others.

Cyberbullying can take the following forms:

- **instant messages, SMS and emails,**
- **blogs**, published opinions and observations hurtful to the victim,
- **photographs, images and videos** hurtful to the victim,
- **(online) surveys, quizzes or prompts** attacking the victim,
- **social network likes** representing approval of harmful or hurtful content, i.e. siding with the aggressor.
- **offensive comments,**
- **happy slapping** also known as "slapping for fun". This is a new form of ill-treatment which combines face-to-face bullying with cyberbullying. The aggressor physically attacks the victim while recording the incident on a mobile phone. The recorded video is then uploaded to the internet or disseminated to peers in messages. With happy slapping, the aggressor is often a group, not just an individual. The group members are "having fun" and encouraging each other in harming the victim. This form of aggression has a devastating effect on the victim's psyche.

Cyberbullying most frequently happens:

- on social networks
- in chat groups,
- via messages sent to the victim's mobile device,
- via email messages.

What do cyberbullies do?

The objective of cyberbullying is for the aggressor to (repeatedly) assert their dominance over the victim. In order to do so, they can use different forms of ill-treatment that:

- **Provokes the victim with messages and posts** containing offensive, false, unacceptable and/or vulgar text. The nature and contents of such messages attract the victim's attention. The victim disapproves of them but is unable to take them lightly. By doing so, the attacker involves the victim in an improper dialogue and repeatedly asserts their dominance.
- **Threatens and blackmails the victim**, e.g. by hacking their social network profile, changing the password and misusing the profile. They can, for example, modify original messages, communicate with the victim's contacts on their behalf or publish inappropriate posts harmful to the victim and their friends. The aggressor can also use the hijacked profile to manipulate and blackmail the victim.
- **Humiliates and ridicules the victim** in front of others, e.g. on social networks and in chat groups.
- **Defames or bad-mouths the victim**, e.g. by spreading rumours and lies with the objective to damage the victim's reputation and relationships.
- **Pretends to be a different person/the victim (steals their identity)** and inflicts harm on others or the victim.
- **Publishes the victim's private or intimate information (outing)** without their consent. The leaked information can be images or intimate videos which discredit the victim in public.
- **Intentionally excludes the victim from the online community**, either on social networks, in chat rooms or in discussion forums. Such exclusion from the group is not gradual, but quick and distinct, so the victim will definitely notice and feel isolated.
- **Harasses and stalks the victim,** eroding their feeling of security. The aggressor makes the victim uncomfortable by spamming, resending photographs, sending messages in chats, leaving likes and comments or by ringing their phone. This kind of attention can be positive, however, due to its intensity is usually intrusive. In some cases, the communication can become negative and damaging and may even include threats of physical harm, false accusations, the damaging of data or identity theft, offline stalking, monitoring the victim's computer etc. The intensity of the harassment usually increases and doesn't stop, even if the attacker is prompted to stop or after the victim blocks them. From the online environment it often extends offline.

How does cyberbullying differ from face-to-face bullying?

The feeling of anonymity lifts inhibitions and increases the level of cruelty.
People feel anonymous on the internet, so they can pretend to be someone else and feel immune to punishment. This lifts inhibitions, which is why the attackers are often people who in the real world could not gain the upper hand.

Cyberbullying can reach the victim anywhere.
While face-to-face bullying is more or less bound to certain locations, i.e. more predictable, cyberbullying can reach the victim anywhere, any time and repeatedly. This omnipresence of bullying deprives the victim of all safe spaces and the feeling of danger spreads through many areas otherwise perceived as safe.

A large number of aggressors can cyberbully a single victim.
While with offline bullying the aggressors are where they physically meet the victim, on the internet anyone can actively join in.

The number and nature of the audience members ("bullying witnesses") is changing.
With face-to-face bullying, the audience is usually clear cut: the victim knows who beat them up or embarrassed them, who saw it and how far the information about those events can travel, e.g. classmates and school students. It is basically impossible to guesstimate the size of a cyberbullying audience, as the contents become part of the digital world and can spread again and again. The victim cannot be certain who saw their humiliation, which can have mentally devastating effects and is much more damaging.

The possibility to remain anonymous behind a monitor or a display reinforces the **"social loafing phenomenon"**. The audience feels little responsibility to act against injustice. The witnesses have a feeling of not being involved in the situation personally and only very few will defend the victim.

With cyberbullying, it is much more difficult to identify the aggressor and punish them for their acts.

Because it is complicated to expose the true identity of the aggressor, cyberbullying often remains unresolved, further contributing to those involved not realising the consequences or their share of guilt. This applies to both the aggressors and the bystanders, whether they are peers or figures of authority. Besides that, cyberbullying often takes place outside the school grounds. Teachers and school psychologists thus feel less pressure to resolve these incidents.

Why do we need to know about cyberbullying and do something about it?

According to several international surveys (HBSC, EUKO, TIMSS, GSHS and PISA) we can state that roughly **every third child** has had some kind of experience with cyberbullying. And it is becoming even more prevalent. When bullying remains unresolved or is only partially resolved, it permanently negatively alters the identity of the victims, aggressors and bystanders.

When you experience power or helplessness, when you see that violence and passivity in interpersonal relationships become legitimised, these experiences become engraved in your memory until they are "overwritten" by a more positive experience. Such positive experience can be when ill-treatment is stopped, when the attackers are exposed, when peer relationships get fixed, when people make up, when they see acts of friendship and courage to stand up for the weak, etc. This is something that adults should do together with children.

Cyberbullying, just like any physical or psychological abuse, is a violation of the child's rights and thus unacceptable.

Are there more male or female bullies?

Evidence shows that among the attackers, there are more boys than girls and these gender differences can be perceived in all age groups of children and adolescents. This applies to both online and offline bullying. When it comes to the number of attackers, these gender-based differences become less pronounced with 11 to 13-year olds, when it becomes more difficult for girls in puberty to control their own impulses and they too can significantly hurt their peers; this is also the time when they start using social networks, which offer more opportunities for cyberbullying.

Still, in general boys display bullying behaviours more frequently than girls. Just like among attackers, also among victims there are more boys than girls.

Most girls fall victim to cyberbullying ages 12-17 when they are most active on social networks. Presumably because social standards judge acts of violence against/among women and girls more strictly, young women fall victim to and attack others online (where they lose their inhibitions and the perception of social standards is weaker) more frequently than offline.

How can you tell that a child is being bullied?

Teachers should explain to children how to notice when someone is being bullied. This way, children can learn to see the early signs and prevent extensive psychological damage to the victim.

To a child, cyberbullying is a significant stress factor causing anxiety, depression, fear and the feeling of helplessness. These conditions often have external symptoms which parents, teachers and peers should notice.

Their worries can manifest as follows:

- **psychosomatic symptoms**—stomach ache, headache, eating and sleeping disorders,
- **uncertainty, reduced self-confidence and self-respect**, feeling threatened by social contact, neurotic behaviour and avoiding company,
- **changes in behavioural patterns—**less contact with their peers, fewer hobbies and activities, increased apathy, seclusion, loss of interest in school activities, inferior grades and behaviour,
- **new harmful patterns in the child's behaviour**—taking risks, use of addictive substances, self-harm, delinquency, truancy,
- **stressful reactions when using a computer or a smartphone** or when talking about them. Display of stress when using digital tools, however, doesn't always have to be caused by cyberbullying. It can be caused by other difficulties a young person is going through, or by changes related to puberty. Don't forget that cyberbullying is more about relationships than about the internet.

Each child reacts to worries and stress differently. The important thing is that both the classmates and the adults at school **remain observant** in order to notice that something is wrong. At school, the children and the teachers are constantly in contact, which increases the chances of them noticing changes in behaviour.

What can teachers do against cyberbullying?

Parents and teachers can emphasise the following objectives:

1. **Teach children what (cyber)bullying is**
   - The teacher needs to teach children the limits between fun and (cyber)bullying.
   - The teacher needs to teach children how to reduce the risk of (cyber)bullying.

2. **Teach children how to proceed if they experience (cyber)bullying**
   - The teacher should recommend specific people children can turn to if they run into problems, such as their parents, an older sibling or a peer for emotional support, or a computer science teacher for technical support.
   - The teacher needs to teach children exactly how to proceed when something bad is happening to them on the internet.

3. **Improve children's social skills, support their self-perception and empathy**
   - The teacher can help children by teaching them to distinguish their own feelings, so they are more sensitive to their own experiences and the experiences of others.
   - The teacher can help children to improve their self-perception and social skills so they can build and maintain healthy relationships.
   - Within the classroom, the teacher can endorse values such as friendship, acceptance and belonging.

4. **Encourage children to help those who are weaker**
   - The teacher develops children's ability to actively defend themselves and others if someone is hurting them.

5. **Develop children's safe internet use skills**
   - The teacher explains how to better protect oneself using the available technical means.

6. **Create safe places and zones on the internet for the victim**
   - The teacher helps create safe zones where bullied children can operate without fear of more attacks.

7. **Assure children that it is good to confide**
   - The teacher explains that it is key that adults or at least some of the more mature peers know of the issue. If nobody knows about the problem, nobody can offer a helping hand.

How should teachers react when a child tells them that s/he is being bullied?

How to proceed with regard to the victim:

The child needs the help of someone who provides social support and is qualified to resolve the incident. Besides providing emotional support, listening and helping the child to express their feelings, the teacher can also explain what to do next:

1. **Store the bullying communication**, such as SMS messages, chat messages, humiliating photographs, comments or screenshots of online applications. This is an important step, because the child may, understandably, wish to delete all derogatory online contents and mentions to prevent them from spreading. However, it is exactly this content that is the evidence necessary to take action against the aggressor.
2. **Do not communicate with the aggressor,** block them and remove them from your contacts. At this point, the bullying may stop, however, it is necessary to help the child resolve any existing conflicts and maintain functioning relationships with their peers.

How to proceed with regard to school, parents, professionals and the authorities:

1. The teacher must not overlook or withhold information about ill-treatment between students, because it represents a violation of the child's rights. In similar cases, the teacher should always contact the headmaster and the child's legal representatives.
2. The teacher must act immediately and try to help the child in collaboration with the relevant school system members, i.e. the parents, child, classmates, headmaster, other school professionals such as the school psychologist or social pedagogue or the police.

How to proceed with regard to the classroom where the (cyber)bullying has occurred:

1. The teacher immediately requests **help within the classroom.**
2. He/she helps to **transform the negative experience into a comprehensible lesson** which explains what has happened, how the specific behaviour is (cyber)bullying, why this is not permissible and what the classroom can do to fix their relationships.
3. The teacher helps the children **restore the feeling of safety and healthy relationships** using group activities. With cyberbullying, the perpetrators don't have to be the victim's classmates, however, the classmates can help the victim feel more included and supported.
4. The successful involvement of students who participated in the ill-treatment in fixing the peer relationships can be a **way to share responsibility** and reduce the punishment for the violation of classroom/school rules.
5. The teacher can also recommend individual **psychological support to students** or their families.
6. It is useful if the school has a clear set of rules on how to handle (cyber)bullying. These rules should include **sanctions**, as they help children learn to be responsible for their actions.

Trolling and cyberhate

trolling | troll | cyberhate

Issues covered in this section:

Who is a troll? How can users avoid trolls? What is cyberhate? What should teachers aim for in terms of preventing trolling and cyberhate?

In the digital environment, users often feel a false sense of security as they think nobody will be able to link them to their actions. In many situations, this feeling leads to harassment and even acts of aggression. Some individuals, however, knowingly post inflammatory remarks and even create fake accounts for this purpose. Using such accounts, they attack others and instigate hatred, disputes and chaos. Such a disruptive user in an online discussion is called a **troll**.

Who is a troll?

Troll is the designation for a disruptive user who:

- instigates disputes and arguments, provoking others on the internet,
- deliberately posts offensive, irritating, false or irrelevant posts,
- tries to provoke a strong reaction from other users (source),
- knowingly disrupts or thwarts discussion and posts digressive messages (source).

To a troll, the objective is to gain attention and the feeling of power. The best course of action for a user is to deny the troll this opportunity.

Research shows that trolls are usually narcissistic and may also show some personality disorder traits (psychopathy, sadism, Machiavellianism, schizophrenia), and are more impulsive. However, we should be careful not to overgeneralise. Not every person with a personality disorder must also be a troll and vice versa – not every troll has to have a personality disorder. Still, the probability of having one is higher.

How can users avoid trolls?

Users can most commonly encounter trolls on social networks, in chat groups and in individual chats. There are ways to avoid them:

- Use the correct privacy settings on social networks. If possible, don't use public profiles on any of the social networks.
- On social networks, only add as contacts people you personally know or have several mutual friends with.
- Identify fake profiles and don't react to them. Sometimes a fake account user can pretend to be your friend just to get into a group. You should also be careful when an unknown social network profile:
  - doesn't have a photograph where the user's face is recognisable,
  - doesn't have any mutual friends or contacts with the user they are trying to friend,
  - contains aggressive, suspicious or malicious previous activity, or traits of intolerance and hate speech in their comments or the contents they share,
  - has significantly more friends than the average user. For a child/student, a good reference number is the number of friends of a popular peer,
  - doesn't create any of their own content, only shares other users' messages, videos or photographs and adds pointless comments.

How should you deal with trolls?

When in contact with a troll, there is one simple rule: don't react. There is no reasonable debate with a troll. You cannot logically reason with them because they like to do harm and enjoy the attention they get online. Once you know you are dealing with a troll, your best course of action is not to respond to their comments and end the debate. To them, each response to their content is a "reward".

If your response is positive, the troll is glad someone agrees with them. If your response is negative, the troll is glad they managed to make someone miserable or angry. By ignoring them, you show that their post doesn't affect you in a positive or negative way and refuse to reward them.

If your "lack of reaction" doesn't dissuade the troll and they continue in their malicious activity, you should save screenshots of their posts and report them to the administrators. A responsible user will do so regardless of whether the troll is bothering them or someone else in the online environment. For this purpose, social networks usually offer a "Report" feature. By reporting malicious activity, you can contribute to creating a safer online environment for all.

1. Once you have reported the troll, block them and remove them from your contacts if you previously added them.
2. The best course of action is to talk to someone you trust about everything that bothers you both online and offline.
3. If the harassment continues through other "channels", you should keep saving screenshots and messages and immediately contact an adult or older peer. Screenshots and other evidence can then be provided to the police.

What is cyberhate?

Cyberhate originates from stereotypes and prejudice against certain groups of people which can often turn into hatred.

Acts of hatred—communication and types of behaviour in which the attacker discriminates against, defames or strives to exclude someone on the grounds of race, ethnicity, language, nationality, complexion, religion, sex, gender, gender affinity, sexual orientation, political affiliation, socio-economic status, age or mental or physical health.

Their behaviour often shows traits of chauvinism, racism, xenophobia, anti-Semitism, Islamophobia and homophobia. All schools are bound to prevent **acts of hatred** in the learning process and teach a culture of tolerance and the observance of human rights both online and offline.

Acts of hatred are a violation of human rights and elementary freedoms which apply equally to all people from their birth, are protected on a global level and are clearly described in the Universal Declaration of Human Rights.

Compared to trolling, cyberhate is more serious because it violates human rights and freedoms, discriminates against people or directly disseminates extremist attitudes and can thus qualify as an offence or a crime.

What should teachers aim for in terms of preventing trolling and cyberhate?

Teachers can systematically lead children towards active digital citizenship, which can briefly be characterised as follows: "To disagree with injustice is only the first step, the important thing is our actions". The message to children is: "Whenever you notice cyberhate, it's necessary to report it using the Report button". In this way, passive bystanders can become active creators of a better online environment.

In educating children/students, schools should focus on:

- building relationships around respect, empathy, and healthy self-confidence,
- imparting knowledge about human rights and freedoms,
- tearing down stereotypes and prejudice,
- constructive conflict solving,
- how to be a proactive internet user and how to react to cyberhate properly.

Social networks

chat | discoverability | end-to-end encryption | screenshot | social network | link | FOMO | cyberbullying | social network bubbles | influencer | YouTuber | vloger | blogger | hate-speech | problematic use of the internet | internet addiction | game transfer phenomenon | selfie dysmorphia

Issues covered in this chapter:

What are the rules of social network security?

What psychological risks do social networks pose and how to handle them?

Who is an influencer and how do they influence the lives of children?

Reals vs. online world—when do we speak of problematic use of internet and social networks?

Social networks and digital security

chat | discoverability | end-to-end encryption | screenshot | social network | link

Issues covered in this section:

What are the basic elements of social network security? How can you improve social network security? Which features can help you improve account security on social networks? Which data and facts should not be shared on social networks? What should you take into account when choosing a social network? What properties should you focus on when selecting a chat app? Who can you turn to if you run into problems on social networks? How do attackers misuse social networks?

What are the basic elements of social network security?

With social networks, just like with the whole internet, the following holds true: what goes online stays online forever. Even if you remove the information from your social network profile, it can pop up in a different form as a screenshot, as part of a video or embedded in another form of digital content. Even if you cannot find that particular piece of information online, that does not mean it is not out there.

How can you improve social network security?

1. **When you set up a profile, set it to private** and share your content (statuses, posts, photographs, videos) only with a restricted group of users. The smaller the group, the more secure your profile is. You can also set the option to only "show posts to friends". If you select the option to "show posts to friends of friends", the content will also be visible to people you don't directly know.

2. **Carefully select which content to share.** Not all photographs or posts are suitable for the internet. Carefully scrutinise every photograph, video and post just like an investigating officer would. This way you can prevent the disclosure of sensitive or private information. A good and simple rule is: *"Don't share anything you would not show to your (grand)parents."*

3. **Regularly check your shared content.** On Facebook, an option in the settings (see Figure 3) allows you to download all information the social network has stored about you. A similar option is also offered by other social networks like Snapchat or Instagram. The best-case scenario is that you only find minimum personal information in the downloaded data. That means strangers should not be able to find out your birth date or your place of residence, work or study.

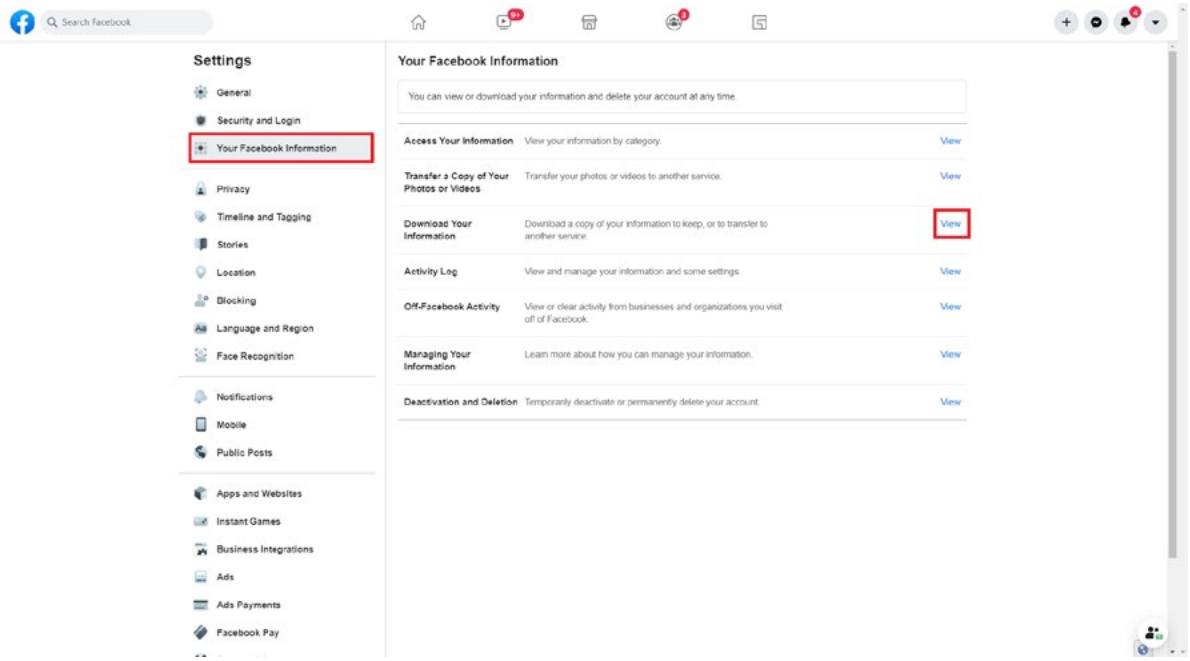


FIGURE 3 *How to download all information that Facebook has gathered on a user.*

4. **Regularly check group membership.** Groups on social networks (Facebook Pages and similar) can change their contents or focus. As you get older, your opinions also change and you may find yourself in a group whose opinions you don't share any more. Some groups are even intentionally set up to gather as many members as possible as quickly as possible and are then sold to the highest bidder. The new owner can then change the group's name and focus sending unsolicited content to its members.

5. **Look before you click.** If a social network user receives a message or a link from one of their friends, they should always think first about whether that person would actually send such content. If possible, you should always first check what the link points to (without clicking it, just hover the mouse over the link and the address it points to will be displayed). If the sent content or the link itself look suspicious or either of them is in a language the given friend doesn't use, you should avoid clicking it and warn the friend who sent it to you.

6. **Check and correctly set up how people can find you.** Under the social network settings, you can set up stricter rules for who can find your profile—ideally it should only be your family, friends or a specific group of people.

7. **Adjust your behaviour on social networks.** If you want to be sure that you don't disclose too much information about yourself, you can choose an approach where you treat your profile or the device as if it is being monitored by someone. Naturally, no sensitive data should be stored in such places.

Which features can help you improve account security on social networks?

Besides the correct setup and safe behaviour, the account needs to be secured using additional security features. These are, in particular, a **strong password** and **two-factor authentication**, which can protect the data stored in a social network account. For more details on this topic, see the chapte Passwords.

Which data and content should not be shared on social networks?

You should not publish any **private or otherwise sensitive content**. The following should not be published on social networks, blogs or in other public places:

- number and photograph of a driver's license, ID card or other official document,
- phone number,
- your school, home or work address and the addresses of your relatives and acquaintances,
- vehicle registration plate,
- contracts and other official documents (school reports, etc.)

You also shouldn't publicly share any travel tickets or tickets to events, as many of them contain QR codes which the attacker can simply copy from the photograph or video and use. The same attention you pay to the things you photograph and record should be paid to the background of your recordings, photographs and videos.

It is not recommended to publish data or other sensitive information related to your close ones (including family members and classmates) and acquaintances as this can violate personal data protection laws.

It has been demonstrated that it is not advisable to publish and share your current position on social networks, as this can be easily misused. An example of this is the robbery in which Kim Kardashian lost jewellery worth millions because she disclosed way too much about herself on social networks. Users can unknowingly share their position by publishing photographs or posts on social networks, but such data can also be collected by numerous applications. To limit collection of location data, you can adjust the device "Settings" or the settings of individual apps.

What should users take into account when choosing a social network?

Pupils/students should only use those social networks whose age restriction and terms they meet. When selecting a network, they should not only consider how many people from their social circle already have a profile on that network, but also the level of security the service provides.

To verify this, ask yourself the following simple questions:

- Can the profile be set up as private and can I limit who can see the content I share?
- How is my account secured: is it just a username and a password, or can another verification factor be added (numeric code, app or SMS verification, fingerprint)?

If you answered no to both questions yet still want to connect to a social network with such inferior security, you should adapt the shared content accordingly and avoid any sensitive information in your posts.

What properties should you focus on when selecting a chat app?

If pupils/students use chat services (apps), they should focus on those offering **end-to-end encryption**[3]. This technology protects their communication and only makes the contents visible to the end users (thus end-to-end) of that particular communication. This significantly complicates any attempts to monitor messages "in transit". Even with these services, the shared contents can end up online without your knowledge or consent (e.g. if published by the user on the other end of the communication).

When selecting a chat application, you should always check how the service provider uses your data, and how it is stored and further used. The terms and conditions are usually available on the app website, however, in some cases they are accessible directly in the app's settings or in the description of its features. If you disapprove of some of the conditions, you should try to opt out of them or avoid using the service completely.

When downloading apps you should always verify whether you are downloading them from the official website or a trusted store and in particular from the profile of the actual developer (for more information see the chapter Mobile device security). The store for the Android platform, in particular, previously had issues with fake versions and imitations of popular chat applications (WhatsApp, Messenger, Snapchat, Hangouts, etc.) which aimed to collect and steal sensitive user data.

Who can you turn to if you run into problems on social networks?

You should always request help from someone you trust. For children, this is usually their parents, older siblings or a teacher. Depending on the seriousness of the issue they can seek further help or turn to the police.

How do attackers misuse social networks?

1. They identify and stalk their future victims.
2. They collect sensitive data.
3. They spread (malicious) ads and hoaxes.
4. They spread malicious code (through posts, photographs, groups, and message links).

3 This can be verified on Google or in the app description in the Google Play Store or in the App Store.

Social networks and psychological resilience

link | FOMO | cyberbullying | social network bubbles

Issues covered in this section:

What psychological risks do social networks pose and how should children handle them? How does negative and insufficient feedback on social networks influence children? How can teachers help children overcome negative or insufficient feedback? Why do some children use social networks without any issues and some face problems or even addictions? How are children influenced by the beauty and lifestyle conventions of social networks? How can a child protect themselves from these risks? What is FOMO and how is it related to social network use? How can teachers help children overcome FOMO?

What psychological risks do social networks pose and how can children handle them?

To their users, in particular teenagers, social networks are very attractive. To them, presentation through their profile appears safe, plus they can share different types of content, stay in touch with others, and present themselves while not having to face their peers directly. They also can post whatever they are proud of—or the improved versions thereof—which can help them avoid embarrassing situations.

Positive reactions from others (e.g. in the form of likes and interactions) temporarily boost their self-confidence. However, this is something one easily gets used to, and may even cause addictions. It can be hurtful when the feedback is not positive or not as good as expected. The user can be led to believe that on social networks everyone looks even more amazing and happy. Children need to be taught how to perceive these social media phenomena and they must build psychological resilience against the following risks:

1. Negative or insufficient feedback
2. Compulsive and problematic behaviour
3. Pressure of beauty and lifestyle conventions
4. Fear of missing out (FOMO)
5. Number of friends and popularity
6. Social network bubbles

Negative or insufficient feedback

In extreme cases this can involve (cyber)bulling, trolling or hate speach on social networks.

Children using social networks encounter cyberbullying more often than those who don't use them. In this regard, social networks are often a platform where children publicly shame their peers in front of a much larger audience then they could "face-to-face". The aggressor wants to show their power in public.

Teachers should lead children to form an audience which does not empower the aggressor and does not join the shaming; on the contrary, it should have the victim's back both online and offline. Children should also realise that if they learn about a similar act, they should tell an adult. For more information, see the chapter Cyberbulling.

Social networks (e.g. Snapchat) allowing so-called ephemeral content which only remains accessible for a brief period of time (e.g. photographs and videos) pose a high-risk environment. This can induce risky behaviour in users, because they know all traces of their posts will shortly disappear. Such risky behaviour on social networks includes sending intimate photographs, sexting, as well as improper and bullying content.

It is important to emphasise to children that those who want to misuse photographs published on social networks can take a screenshot before the photograph disappears or record the photograph using other digital equipment. The content can then be misused, e.g. to ridicule or extort the victim. Children don't just perceive ill-treatment as stressful—insufficient feedback can be equally problematic.

How can teachers help children overcome negative or insufficient feedback?

Teachers can systematically lead children to:

- focus on good relationships with their peers,
- learn to resolve conflicts and make up and reconcile following an argument,
- not to share anything they don't want to be ridiculed for; the fewer digital footprints, the less materials which can be misused,
- know why they should carefully set the privacy of their posts,
- know how to proceed when something unpleasant happens to them on social networks.

Social media use—compulsive and problematic behaviour and addictions

Children can use social media freely even if they spend a lot of time using them. The important thing is what exactly the child is doing, whether they are satisfied with how much time they spend on social networks or whether they are not satisfied with it but cannot control it.

Why do some children use social networks without any issues and some face problems or even addictions?

Whether a child becomes addicted to social media depends on their particular situation—how satisfied they are with themselves and their relationships. The more a child is vulnerable on the inside, the less satisfied and integrated with their peers, the more their well-being can depend on what helps them improve their self-perception—e.g. success on social networks. For more information, see the chapte Real vs. online world.

Children who are too uncertain or anxious can obsessively check reactions to their posts. Sometimes children turn to social media because of boredom or loneliness or to distract themselves when they have worries.

THE PRESSURE OF BEAUTY AND LIFESTYLE CONVENTIONS

How are children influenced by the beauty and lifestyle conventions of social networks?

Social media profiles often look like showcases of perfect appearances and exciting lives compared to which a teenager can feel inadequate. This is particularly true for social networks based primarily on photographs, such as Instagram. Because children are particularly vulnerable and often use social networks, they are more prone to feeling anxiety, feeling bad about their appearance or the fear of missing out. Social networks based on sharing videos, such as YouTube, have a less negative impact on children's well-being and can enrich them in many ways.

When used too much, the pressure of social media on well-being can be significant. In this case, children who are not happy before using social media are the most vulnerable.

How can a child protect themselves from the pressures of beauty and lifestyle conventions?

- Users should choose social media appropriate to their age, taking into account the recommendations of professional developers.
- Social media should be used for interaction rather than just passively browsing other people's posts. Even on Instagram, a social network typical for passive viewing, you can create things like stories, which increase the level of interaction with other users.
- Users can usually profit more from social media offering varied and more realistic content (such as YouTube).
- With the less interactive social media (such as Instagram), the user should be active and prudent in selecting friends and subscriptions. Besides influencers, one can follow posts from different categories such as hobbies, travel, arts, sports, etc. The choice of subscriptions is entirely up to you and will influence what you will see and surround yourself with.

FEAR OF MISSING OUT (FOMO)

What is FOMO and how is it related to social network use?

Fear of missing out (FOMO) is the fear that something interesting or important can happen and one can miss it. Fear of missing out also relates to offline experiences—people usually want to be where something is happening and stay in touch. On the internet, fear of missing out can relate to many things, not just social networks. Someone, for example, may obsessively check the news in fear of missing out on social affairs. Children and adolescents, however, are usually more interested in what is going on among their peers or on their own profile than in the economic and political situation and don't want to miss out on that. It's easy to feel fear of missing out on social networks, because one can keep checking for social status updates and interactions non-stop.

Users are also regularly notified of events and actions they could potentially be interested in or those which their friends are interested in. Constantly checking what their friends are doing or are planning to do and comparing it what they are doing often puts children under pressure or makes them feel inadequate. If they didn't know about the activities of their friends, perhaps it would come as natural to them to stay at home and spend the time resting.

How can teachers help children overcome FOMO?

- A teacher can help children to know themselves better and discover what their real needs and preferences are.
- The teacher can explain what FOMO is, thus reducing the impact of the phenomenon. Adolescent users also need to be reminded that social networks are a showcase of condensed, exclusive moments which don't offer a balanced image of the individual's life that also includes bad moments and everyday chores.

NUMBER OF FRIENDS AND POPULARITY

For young people, having a lot of friends may seem fantastic. But are these real friends? Or are they just users who were added at random to pose as "friends"? And should these "friends" really know everything the user wants to share with their closest friends? The answer to this question most probably is "no", but most young users don't realise this when writing individual posts. Sharing usually happens in a certain mood when the user doesn't stop and think about the possible consequences. Besides that, subconsciously they can think: the more people see this, the better the chance of (good) feedback. This, however, is usually not the best solution.

Who should you add as your contacts on social networks?

- The basic rule for all social network users is to only add/friend people they already know in real life or with whom they at least have several mutual friends in real life.
- If you are interested in the opinions of someone you don't know in person, you can "follow" their activities without friending them on social networks (e.g. Facebook) or without allowing that person to follow your content (e.g. Instagram). "Following" allows you to be inspired by other people's insights while not sharing too much of your private life.

- Similarly, without your knowledge, someone else can start following your activities on social networks even without sending you a friend request. Such a person can also be someone with bad intentions. To avoid this, you can change your privacy settings, e.g. on Facebook under "Settings" → "Privacy" → "Who can send you friend requests?" and "Who can look you up?".

A social network friend is not automatically a close friend

- If possible, take enough time to create contact/friend categories on your social networks. Relationships keep naturally evolving and someone you got along with at 13 doesn't have to be your friend at all at 15. That is why you should regularly update your friend list and its subcategories. On Facebook, each friend on your list can be assigned one of the following categories: "Restricted", "Acquaintances", "Close friends" (see Figure 4).

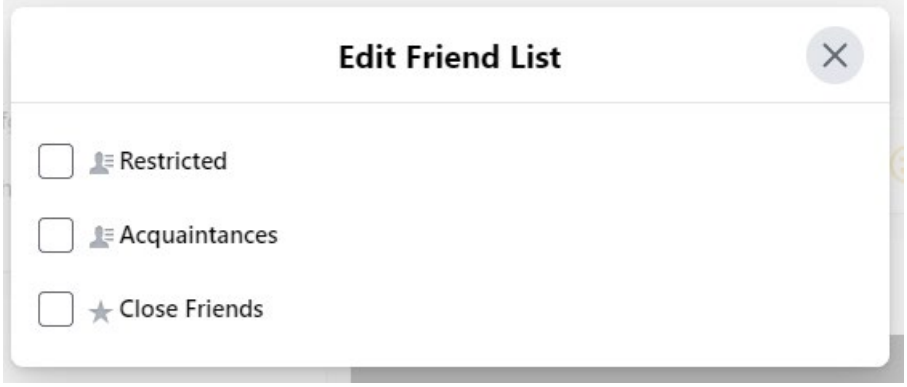


FIGURE 4 *Friend categories on Facebook.*

- Facebook also offers the option to "receive notifications" about the posts of your contacts on social networks. This is usually used for contacts you want to be particularly well informed about.
- Then there is the option to "Unfriend" a Facebook friend. When you unfriend someone, this is done discreetly, i.e. that person will not learn that you unfriended them and it will not hurt their feelings. Thus you don't have to worry and can adjust the contact settings as you please.

When reviewing social network contacts, you should consider the following:

- Am I still friends with this person?
- Am I still interested in what they do?
- What does it give me?
- Do I want to surround myself with their opinions or do I dislike them?
- Should they know everything I sometimes feel like sharing?

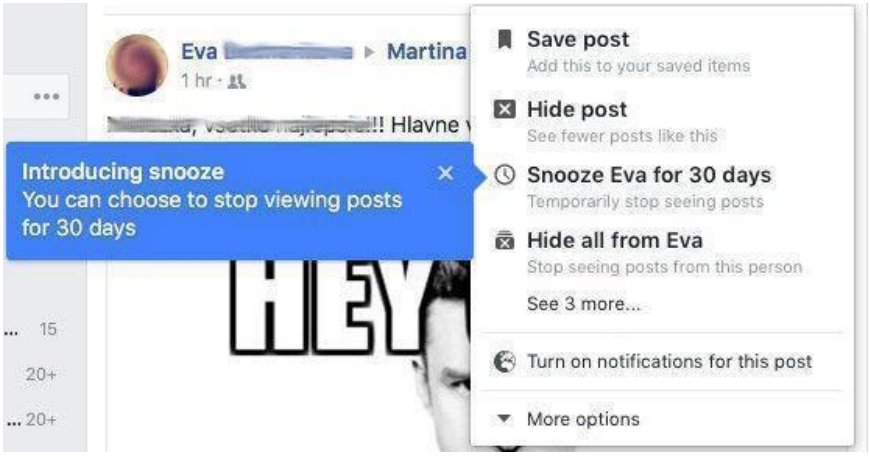
Social network bubbles

The algorithm for displaying content in your News Feed adjusts depending on what posts you most often interact with and what (and whose) posts you click, rate and comment on. The social network algorithm evaluates all these interactions and then displays matching and similar posts in your News Feed, suppressing other types of posts you have not interacted with in the past.

However, this creates a selection of a certain type of posts shown to the user. This is sometimes referred to as creating social networking bubbles. That means the user is mostly surrounded by what interests them both in terms of content and opinions. Other opinions or content are shown less, and the topics become less varied, enclosing the user in their own bubble. This also gives the user a feeling that their opinions are true and confirmed by their surroundings, weakening their critical thinking and making the user more susceptible to disinformation and hoaxes.

The effect of social bubbles can be reduced:

- By regulating what the user is surrounded by on social networks.
- By more frequent interactions on social networks and maintaining varied interpersonal relationships offline.
- By intentionally looking up topics and friends with which/whom the user recently didn't have much contact, even if the social network algorithm didn't include their posts in the user's News Feed.
- On Facebook, by occasionally (temporarily) disabling posts from certain persons. If the user feels that their News Feed contains too many posts of a certain type, they either have the option to block a friend, hide all their posts, or request that the social network doesn't show their posts for a month in the News Feed. If the user knows that they want a longer pause, they can "unfollow" a person or limit the display of certain types of posts. This can be done by setting the options for a particular post, not in the friendship settings.



Influencers

influencer | YouTuber | vlog | vlogging | blog | blogging | blogger | hate-speech

Issues covered in this section:

Who is an influencer and how do they influence the lives of children? What power do influencers have? How should you perceive the psychological help of influencers? How do influencers influence a child's self-perception and identity? How can you choose the right influencer? How can you spot advertising co-authored by influencers? How can you maintain critical thinking when watching your favourite influencers? What does it take to be an influencer?

VIDEO FOR TEACHERS: https://www.youtube.com/watch?v=8LEJovZ2Diw

Who is an influencer and how do they influence the lives of children?

An **influencer** is someone who has become popular through social media, has a lot of followers and has high viewing rates. Their posts can thus significantly influence the opinions and behaviour of others.

Children are discovering their own identity and it often helps if they can identify with someone their own age. An influencer can often be a teenager as well. They talk about what many children are interested in but don't yet know much about. This helps children to grasp many things, inspires them and gives them advice. At the same time, the influencer's posts can be trendy and entertaining and help children relax.

The influencers' posts can take several forms:

1. **Photographs**, e.g. on Instagram and Snapchat—two social networks based primarily on sharing and rating photographs and video stories.

2. **Blog**—a website allowing registered users (bloggers) to chronologically publish their posts in the form of articles which may contain additional multimedia content, such as photographs and videos. The content and topics can be very varied—from reflections on society, to scientific articles, tips and tricks, a diary, all the way to a school or company blog. Blogs usually allow users to comment, rate and share individual posts which further increases their view rates and chances of having an impact.

3. **Videos** shared on social networks—sometimes also called **vlogs**. A vlog (short for video blog) is a form of blog where the user's **(vlogger's)** communication is not written, rather oral; they record themselves and their surroundings while talking about something. The recorded video blogs (vlogs) are most often shared on YouTube, which is why vloggers that share their posts on YouTube are also called **YouTubers**.

For some users, it is simpler and more natural to record vlogs instead of writing text. Similarly, for some target groups, watching a video is more appealing than reading text. Influencers vlog on different topics, thus creating their specific content and forming their identity. The topics can be very varied, e.g. instructions, video game tutorials, humorous or educational videos, regular news recaps, travel, fitness, etc.

Following influencers also involves certain risks, which is why we need to develop children's ability to face the risks. Children need to know about the associated risks so they can "see through" the influencers and not just blindly follow them. This also requires critical thinking and media literacy, because it is useful to interconnect such topics and activities.

What power do influencers have?

To their fans, influencers are the living embodiment of values, trends, ideals of beauty and lifestyle. Children start noticing things about themselves and their surroundings that are based most on what influencers do and speak about. This is the hidden power the influencers acquire after becoming popular. It can be used for noble causes, e.g. to spread good, tear down prejudices or support healthy or ecological causes, to help others, etc. However, it can also be used to endorse products from brands the influencers cooperate with.

How should you perceive the psychological help of influencers?

It can be useful when influencers help children to see they are OK the way they are. Influencers can do so by talking about both the positive and the negative experiences they had to deal with. Some influencers openly talk about what it takes to face hate-speech or bullying, psychological crises and difficulties, break-ups, and their own fears and how they handled them. Such posts show children they don't have to be ashamed for what they are going through, and sometimes they can even find advice on how to handle their own issues. Still, their posts cannot serve as some kind of universal advice.

How can you maintain critical thinking when watching your favourite influencers?

Regularly following influencers and celebrities is a common leisure time activity which used to be popular with previous generations as well. What has changed is the medium, form and frequency at which

today's children can follow them—thanks to smartphones, this basically means non-stop. On social media, one can more often than not see a condensed version of stylised and retouched posts and the prototypes of amazing lives and perfect looks of other users and influencers.

When imagining the influencers' lives, teenagers presumably think about amazing pictures and videos from holidays, trips and collaborations with big brands and free products. Children can even be led to believe that there are no problems in the world of their idols.

The risk for a child is that such posts are served through a medium which, in the absence of critical thinking, can create an appearance of authenticity.

Unlike photographs, videos provide more stimuli and a more consistent image than the stylised and edited images. Videos also contain non-verbal communication and are thus closer to reality. From time to time, in a video the influencer may do something imperfect, laugh at themselves and not be perfect all the time.

How do influencers influence a child's self-perception and identity?

- **Self-confidence**
  Children may not realise that a video or a post are just a tiny fraction of the influencer's life. They are not always perfectly dressed and witty, they too can be bored, depressed or just normal. That, however, is usually not captured in photographs and video. When children fall victim to this illusion without realising it, they can feel inferior and ordinary.
  - Children need to be reminded that the influencers' posts don't show the whole truth, that the videos have been edited, that the photos have been stylised and that many influencers only show the icing on the cake.
- **Imitation**
  - During adolescence, it is natural that children want to imitate their idols. However, they need to be constantly reminded that each of them is a unique personality and it would be a pity if this uniqueness got lost. Children also need to get to know themselves better, i.e. realise what makes them unique.

How can a child choose the right influencer?

Influencers have great power and the ability to influence public opinions and values. This power is not self-proclaimed, on the contrary, there is something the audience likes about them and this "something" helped them gather a following of users. The more fans they have, the stronger they influence the public and people who may not even know what makes the influencer "so unique and attractive". They basically follow them because they follow trends and keep up with the times.

Following influencers just because they are popular and trendy doesn't have to be the most reasonable solution. Subliminally, the influencer has different opinions, taste and values, which is why choosing the right influencer is important. Some celebrities may inspire children to take up sports, adopt a healthier lifestyle, show courage or support charities, while others offer a controversial lifestyle associated with numerous risks.

The teacher should discuss the following with their students:

- Whose opinions, language and personality do they want to be regularly in touch with?
- What is of value for them?
- What do they want to see and hear from their influencer?
- How could the influencer disappoint them beyond repair?

How can you spot advertising co-authored by influencers?

Today's influencers collaborate with certain brands and earn profits from promoting their products. This turns their posts into adverts. When viewers see an advert on TV, e.g. for a cosmetic product, they clearly realise that this is advertising. However, if a popular influencer mentions in one of her videos how a certain cream helped her, it has the appearance of experience and reality. To her follower this may not look like advertising, rather a fact. The follower likes the influencer, trusts her and is more likely to believe what she says about the products. This lack of explicitness turns the influencers into very strong advertising tools. The promoted products usually include fashion brands, drinks, healthy nutrition, fitness products, electronic products, games, jewellery or travel agencies. And of course, their own brands and products, if they have them (clothing, music albums and so on).

What does it take to be an influencer?

Children and teenagers often only perceive the benefits of being an influencer and don't think about the hard work and risks their role models face. Many dream of such an attractive and seemingly easy career path. A dream job survey conducted among 11 to 16-year-olds shows that doctor still remains the most popular profession (18%) closely followed by influencer (17%) and YouTuber (14%). This shift in the popularity of professions is only natural considering what the digital age and existence of social media have brought.

However, their opinions are distorted by constantly seeing popular influencers, i.e. the outcome of a long-term effort by several people who managed to succeed. Besides them, there are a lot of those who failed or "lost interest" after a couple of months of exhausting work on social media with poor results. Success does not come easy. The popular influencers did not become popular in a week and the competition keeps growing. Moreover, even though they are popular, being an influencer entails many **negatives which the fans don't see:**

1. **Pressure to perform.** The influencer needs to remain constantly active and creative. To maintain their followers, they need a detailed concept and plan on what to focus and how to achieve that through their posts. They need to fill their visions with content and one should not forget that preparing, recording and promoting their posts is real work requiring time and energy. Work that needs to be done even if the influencer is not in the mood.

2. **Pressure for feedback.** Despite great effort by the influencer, the feedback on their posts can be weak or average, sometimes disproportionately bad considering the energy invested.

3. **Bullying and trolling.** Probably all influencers on social media experience negative feedback, cyberbullying and trolling.

4. **Threat of burnout.** After several months or years, influencers often experience burnout syndrome, lose the energy to continue and feel tired and put off by the negative reactions.

5. **Loss of privacy.** With all the popularity and excessive sharing of content about their lives, they run the risk of losing all privacy, which jeopardizes their well-being and safety.

6. **Relationship and real-life issues.** Their focus on work and their fans takes away the time, attention and energy they could devote to their loved ones and family. Some friendships will be put to the test or jeopardized by the burden of popularity and jealousy of their friends. And we should also remember that swarms of fans don't necessarily mean one has enough close friends who are valuable.

Real vs. online world

problematic use of the internet | internet addiction | game transfer phenomenon | selfie dysmorphia

Issues covered in this section:

Is there such a thing as internet addiction? What do we consider problematic when using the internet? When do you become addicted to online activities? How can a teacher spot that a child is addicted to online activities? Is there a real threat that by playing frequently, a child could get lost in virtual reality? When do we speak of problematic use of social networks? Are children more themselves or the images of themselves presented on social media? What causes fear of missing out in children? How do beauty conventions influence the self-perception of children? Do children perceive their actual experiences or are they just choosing the background for their "photoshoot"? Are children running a risk of communication overload?

Is there such a thing as internet addiction?

Internet addiction (considering the internet as a medium) does not exist. The online and offline world are just two different environments where people experience different things, and just like there is no such thing as being addicted to "being offline" there is no addiction to "being online". There are only addictions to specific online activities or the overuse/problematic use of such activities. With children and teenagers, this particularly involves the following online activities:

- playing digital games,
- looking up information,
- use of social networks and chat,
- excessive video watching,
- online shopping.

What do we consider problematic when using the internet?

There are many activities on the internet you can enjoy, however, under certain circumstances you can become absorbed by them to such an extent that you keep repeating them and cannot stop. This is the so-called problematic use of the internet, i.e. the kind that disrupts both private and social life and leads to inferior results at work or in school.

Problematic use of the internet is not yet an addiction, however, it is a kind of grey, critical zone. With a better online regime it can get better without any permanent consequences. Yet there are also cases where the problematic use of the internet develops into a full-blown addiction similar to alcohol addiction. When such problematic use of the internet is detected we need to be careful and try to prevent it from developing into an addiction. Overuse of the internet is prevalent especially among teenagers and young adults (13-20 years of age).

What turns a popular online activity into a problem or an addiction? The issue is not just the intensity and the time that the child devotes to such activities, we also need to look at their particular situation and vulnerability.

The following are risk factors for the problematic use of the internet:

- genetic vulnerability (history of addictions in the family),
- current psychological vulnerability (difficult period, lots of stress, depression),
- overall satisfaction with one's life, family situation and quality of peer and other relations,
- psychological resilience of the child, stress and conflict-coping strategies,
- situational factors (breakup, quarrels, loss of security, strong negative experience),
- lack of varied activities the child can enjoy in the offline world,
- the nature of the online activity.

When do you become addicted to online activities?

The amount of time devoted to the activity alone is not necessarily an indication of addiction. The most important indicator is the child's relationship to the given activity, i.e. whether that relationship is relatively free or whether the child's "life depends on it". The decisive factor is the priority that the child assigns to the online activity and whether the activity deprives them of life's other important aspects.

As with all other addictions, online addictions also need to have the following 6 indicators:

1. **Importance.** The given activity becomes the number one priority for the person and all other activities become irrelevant. The person devotes most of their energy to the one activity and to thinking about it. If the person in question is a child, those around them may notice a decrease in the variety of hobbies and activities which were previously part of their life.

2. **Mood swings.** If the child's mood depends on the activity s/he is addicted to or the lack thereof.

3. **Growing need** to do one specific activity. In order for the activity to keep bringing joy to the person, they need to do it more and more frequently, with increasing intensity.

4. **Withdrawal symptoms.** This is an unpleasant condition which starts when the addict cannot pursue, or has to limit, the activity to which they are addicted. The side-effects—just like with substance addictions—are bad moods, irritability, aggressiveness, nervousness, and inability to focus.

5. **Conflict.** This is one of the basic symptoms of addiction. Repeated addictive behaviour introduces problems in relationships, in school results and there can also be an internal conflict (feelings of guilt, self-loathing).

6. **Loss of control.** Following a period during which one strives to limit online activities, there are usually stretches of time where one completely loses control and the addiction becomes overwhelming.

The basic differentiator between addictions and online activities is the conflict and loss of control. That means the person does realise that the given behaviour is causing them problems, but despite all their efforts they cannot control it and keep returning to it. The symptoms of internet addiction are often signs of other mental issues which may also require attention.

Fortunately, such non-substance-based addiction to online activities is rather rare, and in most cases we are dealing with "problematic use of the internet" which affects a rather large portion of the population, in particular young people.

How can a teacher spot that a child is addicted to online activities?

A child will almost never contact a teacher if they start losing control over their online activities. Also, it is not easy to spot this problem, because the internet and digital technologies have become an integral part of our lives. Children also talk about them a lot, so the topic is basically ubiquitous. A teacher can, however, notice some changes in the child's behaviour:

- the child is sleepy and restless,
- their marks are getting worse and they lose interest in school,
- the child is frequently ill-tempered, upset, aggressive and distracted,
- they have significantly fewer friends,
- they don't talk about anything else,
- they lose interest in all other hobbies,
- the only thing they look forward to is their favourite online activity.

These changes in the child's behaviour can help the teacher identify an online addiction. It is usually possible to determine which specific online addiction we are dealing with from what the child most frequently talks about, such as playing games, social networks, etc.

Because other mental problems may also be involved, the teacher should consult the issue with the child's parents, who usually know best what is going on with their child. They can also turn to the school psychologist and recommend that the student's parents seek family therapeutic help.

What can the teacher do?

- build a good relationship with the children based on respect and trust,
- show reasonable interest in how they are doing and what they do in their free time,
- be attentive to notice possible changes in individual children's behaviour,
- if they suspect an issue, they should talk to the parents about the child's worries. Then it is up to the parents to set rules at home regarding online activities and digital tools,
- during lessons, involve students in activities which point out the different risks,
- raise awareness of addictions to online activities,
- use simple peer prevention programmes,
- improve their own knowledge and competencies and keep track of the use of individual online activities and applications,
- teach students how to perceive their own user habits in the broader sense—e.g. how they relate to their mood, engagement in offline activities, success or failure, life situations and so on. An aware internet user is better prepared to take control of their online life.

Problematic videogame playing

Nowadays, almost all children play some videogames, either on computers, tablets, game consoles, smartphones or elsewhere. Girls and boys seem to show roughly equal levels of interest in electronic entertainment. Parents and teachers would certainly prefer it if children only played educational games, but the fact is that children mainly want to play for fun. When children play age-appropriate games and the time and importance games have in their lives are tracked, this is just harmless entertainment. However, there are also children who play excessively, who refuse to do anything else and for whom gaming has become priority number one. These may be signs of addictive gaming. Only roughly 3-5% of children suffer from this problem.

Addictions most frequently develop among MOBA (multiple online battle arena) players. These are short battle sequences played mostly by boys (e.g. League of Legends, World of Tanks).

The second most at risk are MMORPG (massively multiple online role-playing games) games, which involve constant improvement of your own avatar (e.g. World of Warcraft).

Very popular among children are also creative building games, such as Minecraft. Here, the player can shape the environment their character is placed in. With games such as Minecraft, the probability of addiction is much lower, because the game is creative, non-aggressive and the sequence of in-game movements is slower. This game is very popular also among younger children. If parents support varied activities and hobbies, online addictions at a young age are quite rare.

Is there a real threat that by playing frequently, a child could get lost in virtual reality?

Game transfer phenomenon

When people frequently play online or computer games, even after the videogame is turned off, they still respond to real world stimuli as if they were the game stimuli. Everyday situations can remind them of the challenges they were facing in the game, and they react to them the same way. This can be either an emotional response (a rush of adrenaline, readiness for action) or a verbal/mental response. Sometimes people can perceive themselves as the game heroes and see the world through their eyes. They can see life bars hanging over the heads of people in the real world or expect to find a hidden treasure just around the corner.

Still, this does not necessarily mean they have developed an addiction. This can be just a natural adaptation of the mind to the way the brain perceives the in-game world. This can also involve repeating obtrusive game-related thoughts—a kind of flashback. This is usually the case with long gaming sessions or when binging TV shows. Once you take a break from these activities, your mind will reset back to the real world.

The risk is when your mind wants to stay in the environment to which it has grown accustomed. This is often the basis for obsessive playing and in some cases a driver of addiction. Not every child that spends a lot of time playing games is addicted—they can enjoy it and still enjoy a variety of other activities in their life.

When do we speak of problematic use of social networks?

Children can use social media freely even if they spend a lot of time using them. The important thing is what exactly the child is doing and why, and whether they are satisfied with how much time they spend on social networks. Sometimes they are not satisfied with it, but they cannot control it. The more a child is vulnerable on the inside, and the less satisfied and integrated with their peers, the more their mood and well-being can depend on their success on social networks.

Children who are anxious and lack self-confidence can obsessively check reactions to their posts. Sometimes children turn to social media because of boredom or loneliness, or to distract themselves when they have worries.

How do beauty conventions influence the self-perception of children?

The audience often cannot tell when photographs have been edited. This has a negative impact on the self-assessment of users who, after looking at the edited photographs, feel ugly and imperfect. In teenagers, excessive use of social media can cause discontent and feelings of inadequacy and loneliness.

This also shifts the beauty ideal towards unrealistic images. When children have less contact with reality, with what is natural, real and authentic, they can gradually start perceiving the altered appearance as a norm and they will do anything to achieve the same look.

Are children more themselves or the images of themselves presented on social media?

Some people use the internet to show what they like to do, but others pretend to be someone they are not. Such pretence can indirectly create anxiety and cause internal conflict and the rejection of oneself. If you present yourself only through edited images, you put yourself under pressure and become disappointed in experiences which don't match this altered image of yourself.

Do children perceive their actual experiences or are they just choosing the background?

To young people, selfies are fun. However, they often don't experience the moment and instead just focus on taking a good photograph. For example, when taking a walk through a city, the teenager will focus more on what will make a good composition for their photograph, rather than the walk itself or the company of their friends. There have even been cases of young people becoming addicted to taking and sharing edited selfies.

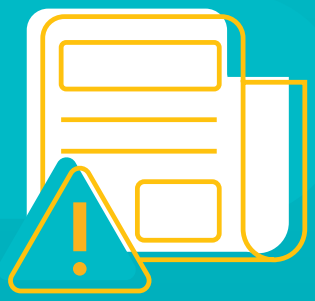
What causes fear of missing out (FOMO) in children?

Fear of missing out (FOMO) is the fear that you could miss something interesting or important, such as a concert, a friend's celebration, a trip, a sports practice, etc. This can cause anxiety and other negative feelings. Similar feelings may be, and have been, also caused by the user's/child's fear of missing out on the most recent gossip on social networks. Because of this fear, the child is nervous and checks their device way too often.

Are children running a risk of communication overload?

"Being always available" on multiple different platforms often gives teenagers the yearned-for feeling of community inclusion and being on top of things, however, it can be quite mentally exhausting. They often obsessively check their smartphones, which distracts them, overloads them with information, and puts them under pressure. The average student will check their smartphone every three minutes. The level of pressure, however, also depends on the number and nature of the platforms they are following.

Adults can help children acquire inner balance, boost their self-confidence, and develop their peer skills so they have enough good friends offline and can find a meaningful way to spend their leisure time. If a child repeatedly experiences conflict and issues with family and friends, they will require confidential advice, possibly the professional help of a psychologist.



Disinformation, hoaxes and fake news

hoax | disinformation | fake news | intelligence wars | confirmation bias | conspiracy | disinformation media vs. traditional media | analytic skills

Issues covered in this chapter:

How is misinformation different from disinformation?
Who produces disinformation and why?
What are disinformation media?
What information spreads faster and why?
What is confirmation bias?
How does our mind try to find answers to unfamiliar questions?
What are hoaxes?
What forms do disinformation and hoaxes take?
How can you identify a hoax/fake news?
How can you protect yourself from hoaxes?
How can you stop fake news? Where can you verify news?
What should you do with a piece of fake news? What threat do hoaxes pose?

How is misinformation different from disinformation?

These two notions are often used interchangeably, however, they don't have the same meaning. In both cases, incorrect or made-up information is disseminated, but in the case of misinformation the person disseminating the information is honestly convinced or does not know if the information is true and it is not their intention to cause any harm. Disinformation is also incorrect, but the person who created and disseminates it knows this and despite that knowingly continues to do so with the objective to cause harm.

Disinformation can also be information which at its core is true, but is spread without any context—resulting in a single portal or profile creating a distorted view of the issue at hand. Isolated cases may be picked and accumulated in one place. Disinformation can lead to incorrect conclusions or decisions. It is one of the tools used in so-called psychological warfare.

Who produces disinformation and why?

Disinformation is commonly used in unfair competition by political parties in intelligence wars between different political systems or enemy states. Disinformation can also be part of military conflicts. The objective of disinformation is to deceive the opponent and make them believe whatever the disinformation author deems beneficial. Often, the objective is to create an atmosphere of chaos and doubt as to what is true, thus reducing the public's confidence in the state or other authorities. Some disinformation creators may aim to disrupt the functionality of a certain system.

Business too can be one of the reasons—the market is hungry for information not presented in the traditional media. However, the main reason why such issues are not covered is not because of an attempt to withhold information, rather the fact that the information is untrue, of poor quality, or cannot be verified. By filling this void, disinformation media can gather a huge following, generating significant income from advertising.

What are disinformation media?

Disinformation media focus on the dissemination of disinformation. Sometimes they are also called conspiracy media. Their primary objective is to disseminate conspiracy theories, hoaxes, or unverified or manipulated information. They usually push one main topic—in particular, these currently include immigrants, anti-COVID-19 and anti-EU information.

In terms of presentation they strive to imitate the traditional media, and many of them also publish real news. However, while the traditional media depict the world in a more complex and comprehensive manner, the disinformation media focus on selected topics which they present in ways allowing them to negatively impact the readers' minds. They often publish stories from other sources or translate them with more shocking headlines. When they do interviews, they usually interview people holding the same views and supporting the same goals. They don't care about ethics or trustworthiness. Their objective is not to inform, rather to control the public authorities or wage a campaign against the democratic system. Often, intentional mistakes are introduced, or part of the information is withheld or presented out of context.

A large portion of the disinformation media are not just news portals, but also media devoted to health. One of the most popular articles on the Czech internet was one headlined "Hydrogen peroxide—a cancer cure" and in Slovakia "Secret revealed: Cancer not a disease rather a business.
This is how you can get rid of it."

Besides the standard media, disinformation media are active in almost every country of the world. Despite the risk they pose, we should know them so we can avoid them and stop spreading the news they publish.

What information spreads faster and why?

Research published in March 2018 by the journal *Science* confirmed that lies spread on the internet much faster than the truth (https://science.sciencemag.org/content/359/6380/1146). The authors compared how information spreads on Twitter and found out that false rumours spread six times faster. People like to share and disseminate information with a hint of sensation. This conveys social status upon the author, suggesting that they are "in the know" or have access to unique "inside" information.

Many questions can be answered easily, but the truth is often less appealing and more boring than falsehoods. Verified information explaining or disproving falsehoods spreads much slower and often doesn't even reach the people who have read the original fake news. As a result, it is often very difficult if not impossible to fix the damage caused by those spreading disinformation. False information is often populist and spreads quickly on the internet also due to a lack of trust in official sources.

Also, people prefer information that matches their own views and existing opinions, which creates so-called confirmation bias.

What is conformation bias?

Confirmation bias is a natural way of thinking, a judgement error. It is the tendency to favour, search for and recall information which confirms our existing beliefs or hypotheses. People tend to pay much less attention to alternative views.

Experiments have shown that people don't seek information, rather opinions confirming what they believe—a confirmation of their ideas. Confirmation bias is even stronger with emotionally significant topics and deeply rooted beliefs. People tend to focus on one possibility only and ignore the alternatives. Because of confirmation bias, we are often convinced that false information is true and we disseminate it in good faith as the truth. We disseminate misinformation. And because we are convinced that the news is true, we don't see why we should fact-check it. Knowing about confirmation bias and constantly doubting whether facts are true and checking them is therefore very important. Only by constantly verifying and comparing information with trustworthy sources can we avoid spreading fake news.

How does our mind try to find answers to unfamiliar questions?

When making judgements, we prefer simpler and easier solutions to ones that require more thinking and effort. We are too lazy to read more complex information.

When asked a question we don't know the answer to, our mind will transform it into something that is easier to assess. In the assessment process we recall situations that are the easiest to remember. Try answering this question: Which job is more dangerous—policeman or fisherman? Most people will presumably say policeman, because they will recall all the action movies where policemen are involved in gunfights. In reality, though, we should be answering the question by considering in how many dangerous situations have we seen a policeman and in how many a fisherman. According to statistical data, being a fisherman is one of the riskiest jobs in the world. You can find out more about how our mind works and about judgement errors in Daniel Kahneman's book *Thinking, Fast and Slow*.

Gordon Pennycook and David Rand, experts studying the human mind, have confirmed that our tendency to believe fake news is based on a lack of analytical skills.

What are hoaxes?

A hoax is a piece of news with false, fake or otherwise incorrect contents (i.e. disinformation) which aims to evoke negative emotions and manipulate the recipient into forwarding and disseminating the message. A hoax is a specific type of disinformation inciting us to propagate it. Through manipulation, hoax spreaders can be convinced that what they spread is true, essentially making it misinformation. The author often poses as a trustworthy source (a company, a state authority, or misuses their name, e.g. "American scientists have found", or "according to Interpol") and warns of the catastrophic consequences of a made-up event. In doing so, they use claims not based on scientific data or any verifiable facts. The objective of the hoax creator is to spread fear, anxiety and the feeling of danger, forcing the victim to act without thought.

What forms do disinformation and hoaxes take?

Disinformation and hoaxes can take several forms—below you can find examples of the most common ones.

- **Hoaxes appealing to your compassion—**this type of hoax appeals to the recipient's compassion and promises a made-up reward, saved lives or other benefits for spreading and liking the hoax.
- **Fake news and disinformation—**using modified, twisted or made-up information these aim to manipulate public opinion, most frequently with political or ideological objectives. Social networks which don't regulate similar content further increase the power of fake news and disinformation because, due to their highly viral nature, the networks' algorithms spread them even faster.
- **Made-up quotes by famous people—**the author disseminates the information as a quote (statement) by someone who is famous and trusted in the given country (location) and who is often seen as an opinion leader. A photograph of this person is often added to an article or information to make it look more trustworthy. This can be a celebrity who is older and is not (very) active on social networks, which makes the news difficult to verify.

- **Disinformation disseminated by celebrities—**sometimes fake news is spread by celebrities with numerous supporters who are not experts on the given subject. This can be a singer, politician, or well-known doctor. For example, falsehoods about COVID-19 were spread by a well-known doctor specializing in lifestyle medicine. Donald Trump proposed the use of disinfectants as a COVID-19 remedy, which reportedly resulted in one case of poisoning.
- **Technology hoaxes**—most of these are spread through email and warn of a made-up virus or technological threat. They will often ask you to do something that will damage your device, e.g. they will ask you to delete a specific operating system file (which is a standard part of the system), claiming that if you find this file on your device it has already been infected by a virus.
- **Joke hoaxes, hoaxes created on special occasions when they are deemed socially acceptable**—most of these are created as April Fools' Day pranks or practical jokes which aim to outwit people. However, sometimes people will believe the information and keep spreading it. This form of hoax is basically harmless.
- **Chain letters**—in the past these were spread by post but have now moved to the internet. They will ask you to continue spreading the message, taking advantage of human superstitions. They can, for example, claim that if you don't send the message to at least five people you will have bad luck, or promise good luck if you do.
- **Modified or old photographs (videos)**—when creating disinformation, old photographs are often used, which are real but tied to a completely different event. Sometimes the photograph or parts of it may be modified, creating a fake one. The author can also add text compiled from articles published by controversial websites that regularly disseminate hoaxes. A typical example of this is the photograph depicting a ship named Vlora. The photograph was taken in 1991 but has been used in connection with the 2015 immigration crisis.

Images publicly searchable through Google

Adding deceptive text to an old photograph is a very simple and effective method of misleading people. The image does not even have to be modified, as it looks trustworthy enough on its own.

How can you identify a hoax/fake news?

There are some typical signs which can help you identify fake news. They often originate from doubtful or controversial sources or there is no source specified at all. Websites that disseminate fake news usually don't list any contact information for the author or the editorial office, and the grammar and style are often poor.

However, sometimes such texts and websites can appear very professional. In this case the only way to unveil the fake nature of the news is to keep verifying and cross-examining information using multiple trustworthy sources. Trustworthy sources are usually the mainstream media who work in a transparent manner, check their facts and follow a code of ethics. A good source can also be independent (international) organizations, non-governmental institutions, universities or the scientific institutes of democratic states.

Articles which don't specify the date and place of the event they describe should also be treated as suspicious. We should also remain alert regarding posts on politically sensitive topics that encourage sensationalism and controversy.

The more shocking the news, the higher the probability that it is disinformation. Let's not forget that the number of likes and shares has nothing to do with the veracity and trustworthiness of the news.

How can you protect yourself from hoaxes? How can you stop fake news?

Everyone should learn to distinguish between true and fake news. This is not just so that you can know what is true, but also so that you can avoid spreading disinformation. The following steps can help you to identify fake news and stop it from spreading.

- **Check the source—**review the purpose of the website and it the published contact information—check these using a search engine. Is the source a mainstream medium or did you find it listed among disinformation media?
- **Check the author—**look for information about the author. Is he/she trustworthy? What topics does he/she normally deal with? Is it an actual person or a made-up one?
- **Check the date—**is the date included? Is it a new or an old article? Be careful about old news. Just because it was true in the past does not mean it is still relevant today. Scientific knowledge may have evolved significantly in the given area.
- **Think about your bias**—what are your convictions? Does the news support your point of view? Be careful about confirmation bias.
- **Read the whole story, not just the headline—**the headline may look shocking to motivate you to click on it (clickbait). What's the whole story? Is the headline misleading you just to capture your attention?
- **Check the source quality**—does the article contain links to other sources? Check whether the listed sources don't contradict what is written in the article.
- **Is this just a joke**—does the content appear strange? Think about whether this could just be satire or irony. Check the website and the author to make sure it's not just a joke.
- **Ask an expert—**verify with an expert, consultant or a fact-checking website.

Where can you verify news?

To check whether a news article is true or not, you can use websites specializing in exposing hoaxes. For example: snopes.com or stopfake.org, FactCheck.org, hoax.cz. In Slovakia, current hoaxes are exposed by the police at their Facebook page: https://www.facebook.com/hoaxPZ/. Claims made by Slovak politicians can be verified at demagog.sk.

When a post/article contains an image, you can check whether it's true using the Google reverse image search.

What should you do with a piece of fake news?

If you determine that a news article is fake, don't spread it. If you know the author of the message (these often originate from people you know), you should inform them that the news is fake. Social networks provide tools you can use to report fake news, hoaxes and disinformation published on social media. You can find the option to "Report a post" right next to the post and then you can select "False news" from the available options.

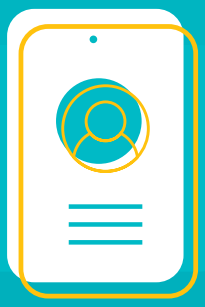
What threat do hoaxes pose?

Hoaxes and disinformation are not just made up information you can send or tell anyone. It is no excuse if your motivation to disseminate falsehoods is just to have fun or play practical jokes. Disinformation can cause great damage to both property and health. If you believe some bizarre information or someone obtains your sensitive data (e.g. your credit card number) on a social network through disseminating a hoax, a hoax can also cause you to lose money.

The spread of health-related hoaxes is also a very dangerous phenomenon. If you believe a hoax and refuse medication or vaccination, this can not only damage your own health but pose a threat to society more widely.

And let's not forget that creating and disseminating hoaxes and disinformation can also be considered a criminal act. You may have encountered information on social networks that the police are looking for authors of hoaxes. They may, for example, ask social network users to help identify a voice on a recording.

SOURCE: https://www.ifla.org/publications/node/11174
DETAILED HANDBOOK: https://unesdoc.unesco.org/ark:/48223/pf0000265552



Digital identity and privacy

cloud | digital citizenship | digital footprint | email account | location

Issues covered in this chapter:

What is a digital identity?
What is a digital footprint and what types of digital footprints are there?
Can you remove your digital footprint?
How can you find out where and what digital footprints you have left?
What is digital citizenship?
What is a digital signature?
Are we going to vote online in the future?

What is a digital identity?

On the internet, anyone can create a basically unlimited number of digital identities. Some of them can, in many aspects, match the actual person—e.g. a Facebook or Instagram profile—however, they can also differ significantly—a gamer profile in Fortnite or Steam concealed behind a made-up nickname. Some identities can be intentionally different to prevent the original owner from being tracked down—like a fake email to subscribe to newsletters.

The key with a digital identity is reputation. A person builds their reputation with their behaviour and interactions with other users on a given platform. If their reputation is good, they are more trustworthy and can make deals and conclude agreements online or obtain better terms. An example of this is a user offering their flat for short-term rental (e.g. Airbnb). If the user is reliable, the flat is always clean and the customers are satisfied, they will get a good rating from their customers. If there are many of these ratings, this builds their reputation and they can gain advantages from the online platform and attract better customers. The same applies to the customers. If they are known for leaving a mess or trying to dodge payment, their reputation gets worse and along with that their chances of finding accommodation.

What is a digital footprint and what types of digital footprints are there?

If you have an email account, if you use a social network, if you play online games or just browse different entertainment, news and other websites, you are creating your own digital footprints. That does not automatically mean someone knows your identity in the real world. A digital identity is an anonymous reflection of your behaviour in the digital world which in connection with other information—digital footprints—can lead to a specific person.

The data which forms a digital footprint can be provided **actively** or **passively**:

- **A passive digital footprint** consists of information which the user leaves in the online space unknowingly and which is not directly visible. An example of a passive digital footprint can be the type of browser, device model, language settings, operating system or IP address stored in the internet provider's database or on the servers of the provider whose service you are using. The IP address helps identify the approximate location or the internet provider, however, it can be unreliable, as it can be masked on purpose (by using a virtual private network, or VPN).
- **An active digital footprint** includes all data knowingly provided and published on the internet. If you send an email, publish a blog, like a photograph/comment, share a video or a text on social network, or send a chat message, this and similar information becomes your active digital footprint. You should also realise that large providers of online services such as Google and Facebook use their code on a number of websites to help the website owner analyse their visitors. Such data also helps these companies collect a wide spectrum of digital footprints to obtain a more detailed image of the user's online behaviour.

Whether a given footprint is deemed active or passive often depends on the user's technical level. A more experienced user is aware that their behaviour on the web can be monitored and knowingly avoids certain websites or online services or uses tools to prevent such monitoring.

Can you remove your digital footprint?

A digital footprint is a permanent and indelible part of our online existence. In accordance with the General Data Protection Regulation (GDPR), every EU citizen has the "right to be forgotten", however, this is a rather lengthy process. Moreover, even though at the end of the process the given service or provider doesn't own any of the user's data, some data may still be stored in another database or be part of a data package which, in the meantime, is in the hands of another organisation. An improper email or an embarrassing photograph of the user can also be preserved on the hard-drive of someone who has taken a screenshot. So despite being erased from the primary source, the information may reappear on the internet in the future and become a burden, e.g. complicating the user's future job applications or making it difficult to start new relationships.

How can you find out where and what digital footprints you have left?

Thanks to the existing legislation, this is possible, but quite difficult. According to the GDPR, companies collecting data about their users (this applies to EU residents only) have an obligation to provide the user with such data, should they request it. This is one of the reasons why large online services provide an option—typically available under user settings—through which an individual can request all the information stored about them by any given provider.

What is digital citizenship?

Just as we are citizens of a country in the real world, we are also becoming citizens in the digital world. Estonia, the Netherlands and Britain are just some examples of European countries that provide many government services online. This introduces a number of advantages, such as non-stop service availability, the time saved by citizens who would otherwise have to wait at various local branches of government authorities, financial savings by the state that it would otherwise have to spend on clerks, as well as fewer mistakes and the tirelessness of these automated systems. The advantages of such online services were clearly felt during the coronavirus pandemic.

Because the services are electronic, people don't have to repeatedly provide their data to different authorities, as state employees can look them up in centralised government systems. Digitalised authority services also simplify administrative acts, such as change of vehicle ownership, change of permanent residence address or establishment of a business. Instead of having to visit an authority, wait your turn, and hand over documents at the counter, people now can fill in forms at home, sign them using a chip in their ID card and submit them with a few clicks.

Naturally, centralisation and automation also have their downsides. IT systems are also prone to failures, at times they can be overloaded and the service availability can be limited. Another risk is that such systems may not be sufficiently protected from external attacks or can leak sensitive data due to incorrect setup. An example of this was the mass leak of the data of 6.5 million Israeli voters, which was made available online due to an error in an app used by a political party.

If you are setting up a business, you should also think about having to process customer data—thus having to follow strict legislation requirements (e.g. GDPR). The legislation doesn't only determine how the data is to be collected, stored and protected, it also introduces severe penalties in case of a data leak or theft.

What is (not) a digital signature?

When the world was ruled by kings and noblemen, they secured their mail with wax seals bearing the impression of their coat of arms or another recognisable emblem. If the letter was delivered to the addressee with the seal broken, it was clear someone had opened and read the letter in transit, possibly changing its contents.

A similar system is also used in the digital world where messages, emails and sensitive documents bear a so-called digital signature.

Important to note: A digital signature is not a user's name written or "drawn" in digital form in one of the graphical editors or written in a document in a text editor (e.g. Word) or even a scan of their hand-written signature. Had the user only drawn/written/scanned the signature, an attacker could easily imitate it and sign contracts or documents on their behalf or steal their identity.

A real digital signature is a mathematical scheme for verifying the authenticity of documents and messages. A digital signature also ensures that the data (documents, messages, etc.) originates from a specific user and has not been altered in transit (or proves that someone did alter them), similar to the wax seal in the past.

A digital signature (its encryption mechanism) consists of two components:

- **a private key** which is secret and known only to the user,
- **a public key** which is publicly available, but at the same time paired with the user's private key.

Example: Alice would like to digitally and securely sign her message, which she can do by encrypting it with her private (secret) key. Bob (or anyone else) wishing to read the message can use Alice's public key (paired with her private key) to verify that the message comes from Alice. As the private key is only known to Alice, nobody else can sign the document the way she can, so Bob can be sure that the message originates from Alice and that nobody has altered it in transit.

Naturally, this also works the other way around. If Bob encrypts his message using Alice's public key, only Alice will be able to open and read the message. This ensures that only these two individuals know the contents of the message and that nobody intercepted or altered their communication in transit.

This mathematical scheme is closely related to so-called asymmetric encryption—Explanatory video 1, Explanatory video 2.

Are we going to vote online in the future?

One of area still resisting digitalisation is the voting process. Even though, at first glance, it may appear a clear candidate for online implementation, the possible advantages in the form of higher voter turnout or an "easier" voting process entail several serious risks due to which the paper-based alternative still remains the safer option.

Physical voting is transparent, free and secret at the same time. The voter has to visit a polling station near their home, pick or fill-in a ballot behind a divider/in a voting booth and put it in a ballot box. All the key acts are performed by the voter under the supervision of an election committee, but still concealed in a voting booth so nobody can see which party or candidate they chose. In case of doubt, the votes can be recounted to verify the correctness of the results.

Electronic voting would have to ensure all these properties (free, secret, verifiable), which so far remains an unsolved problem. For example, without the supervision of the election committee it is difficult to ensure that the vote was cast freely, secretly and not under duress. If the voter casts their vote at home or somewhere in public, someone else can influence them.

Without the supervision of the election committee it is also difficult to verify under what conditions and in what condition the person has voted. For example, they could be under the influence of a psychoactive substance. This does not disqualify them from voting, however, having to register with an election committee at a polling station may act as a psychological barrier to prevent such behaviour.

Online voting using computers, mobile phones and tablets is no guarantee of equal treatment for all voters as not every voter owns a device with internet access allowing them to use the voting system.

Another issue can be the level of voters' trust in an online voting system. Many voters don't understand digital systems and can be led to believe that the results can be manipulated by the "IT staff" who created and administer such systems.

We also need to remember that the safety of electronic voting can be at risk from digital attacks. There are multiple parties interested in manipulating election results, such as foreign actors, various domestic actors (oligarchs, the mafia, etc.), as well as ordinary criminals. They can focus on the vulnerabilities of the voting equipment/servers used to collect and count votes and either try to render them unusable or tip the results in favour of a specific candidate/party. There is a risk of election manipulation with paper-based voting as well, but this risk is localised. It can be easier to physically attack a single polling station than a centralised IT system, however, by attacking a centralised system the attacker can influence a much bigger portion of the results.

	Advantages	Disadvantages
Paper-based voting	• transparency of the act of voting • votes are cast secretly • votes are cast freely • simple and comprehensible rules • verifiable results	• high costs • problematic accessibility to voters who are unable to travel, voters with disabilities or voters who live abroad • time consuming and physically demanding to manually count votes, which may be prone to error
Electronic voting	• (presumably) higher voter turnout • lower cost to organise the elections • better accessibility to voters • quick and error-free counting of votes	• accessibility of necessary polling equipment and software to all social classes • potential interference with the freedom and secrecy of voting • possible cyberattacks on IT systems • intentional manipulation of results in IT systems

Multiple countries have already introduced electronic voting with all its advantages and disadvantages. Some of them, such as India and Brazil, use specialised voting equipment connected to the internet, however they still require that the voter to be personally present at the polling place. In multiple cases, professionals have confirmed that these devices have vulnerabilities and security issues.

Estonia has gone one step further and introduced remote internet voting: the first country in the world to do so. The voter needs to register using their electronic ID and confirm their identity multiple times. For more information about electronic voting systems in selected countries, refer to this Wikipedia page.

Electronic voting is becoming a viable alternative especially following the global coronavirus pandemic, because it allows elections to be held despite strict social distancing rules. The U.S. Department of Homeland Security, however, has strongly advised against internet voting and urged states to avoid this form of voting or limit it only to those who are unable to cast their votes otherwise.

Online, not everyone is who they seem to be

online identity | identity verification | fake account | fake profile

Issues covered in this section:

Who is who on the internet? How can you verify someone's identity on the internet?

Who is who on the internet?

"On the internet, nobody knows you're a dog". This well-known cartoon by Peter Steiner, published in the American weekly The New Yorker, very aptly depicts one of the issues the internet is facing—identity verification.

If you get to know someone online, you often have to rely on the information provided by the other party in one of their profiles or during direct communication. However, it can be extremely difficult, if not impossible, to verify their identity.

Let's look at an example: On the internet, Olivia123 has added me as her friend. She claims to be 18, likes to read and snowboard and loves movies and TV shows. In reality, the profile was created by a 30-year old unemployed man who does not read books and spends most of his time on the computer.

In the real world one could immediately see the person and identify that some of their claims are untrue, but on the internet, things are more complicated. Besides that, a malicious individual can easily create a new profile with a different photograph downloaded from the internet and make up a new name or hobbies. And they can repeat this endlessly. They can also use such fake accounts for malicious or illegal purposes.

How can you verify someone's identity on the internet?

If someone attempts to get in touch with you, you can try to verify their identity in several ways:

First, you can use the available name and look them up using Google search. Some of the results may let you know where that person lives, where they go to school, or whether they work in the area or region they have provided in their profile.

If Google finds profiles with a matching name on a social network, you should check the information provided by that person. Some external signs of the account may also suggest that the account is fake—e.g. very few friends, no photographs or just selfies with no other people in them.

You should also be careful if their profile contains content which looks too good to be true. You should carefully examine the photographs, focusing on all details in the background.

Equally useful is the user's email address tied to their accounts on social networks, such as TikTok, Snapchat, Instagram, Facebook, Twitter, Reddit, and others. If the impostor is not careful about such details, they may specify different or even contradictory information on individual sites.

Some services, however, will reveal the username only once you friend them or otherwise contact them. If you have already added the person as your "friend", carefully inspect their profile. Notice when the profile was created, whether the provided information matches what the person claims and what they have shared in the past, what language they have used and how they have interacted with other users.

Browser security

cookies | dark web | deep web | browsing history | incognito mode | surface web | safe browsing | man-in-the-browser

Issues covered in this chapter:

How can you increase browser security?

What is browsing history?

Are you browsing anonymously when in incognito mode?

How can you spot fake or dangerous websites?

What should you do if you open a dangerous website?

What are the most frequent forms of browser attack?

Which part of the web can you find using a search engine?

How can you increase browser security?

One of the first things you can do to increase your security is to use a recognised and updated browser. You should bear in mind that multiple browsers can be installed on a computer and that you should update each of them before using them.

Several popular browsers offer a "safe browsing" option which protects the user from phishing attacks (fraudulent attempts to steal user names, passwords and other sensitive information) and warns them if they attempt to visit suspicious sites or sites known to spread malware. If possible, you should turn the safe browsing option on under the "settings".

What is browsing history?

Once installed, browsers automatically collect your browsing history. This is a useful feature if you want to go back to a website you have previously visited but don't remember its name. On the other hand, it is also a source of information about the user's habits, which are of value both to the browser manufacturer and to the digital giants, such as Facebook and Google. Also, if such information ends up in the wrong hands it can be sold or misused for other nefarious purposes (such as extortion, in case inappropriate websites have been visited).

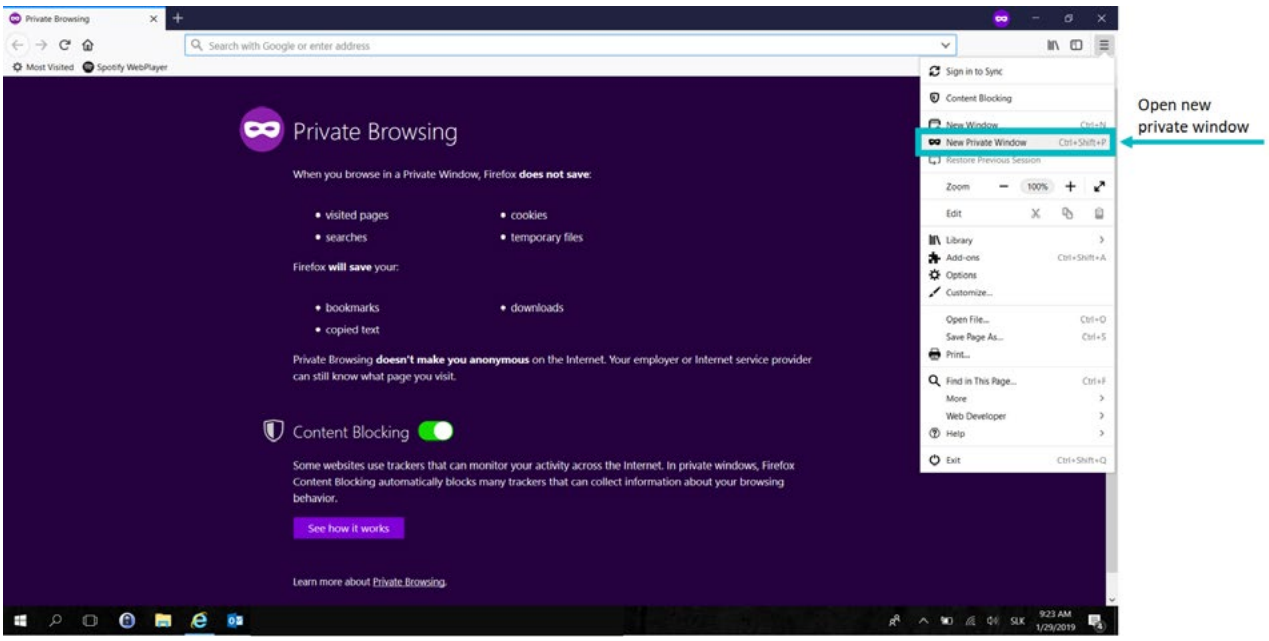
Does incognito mode mean you browse the web anonymously?

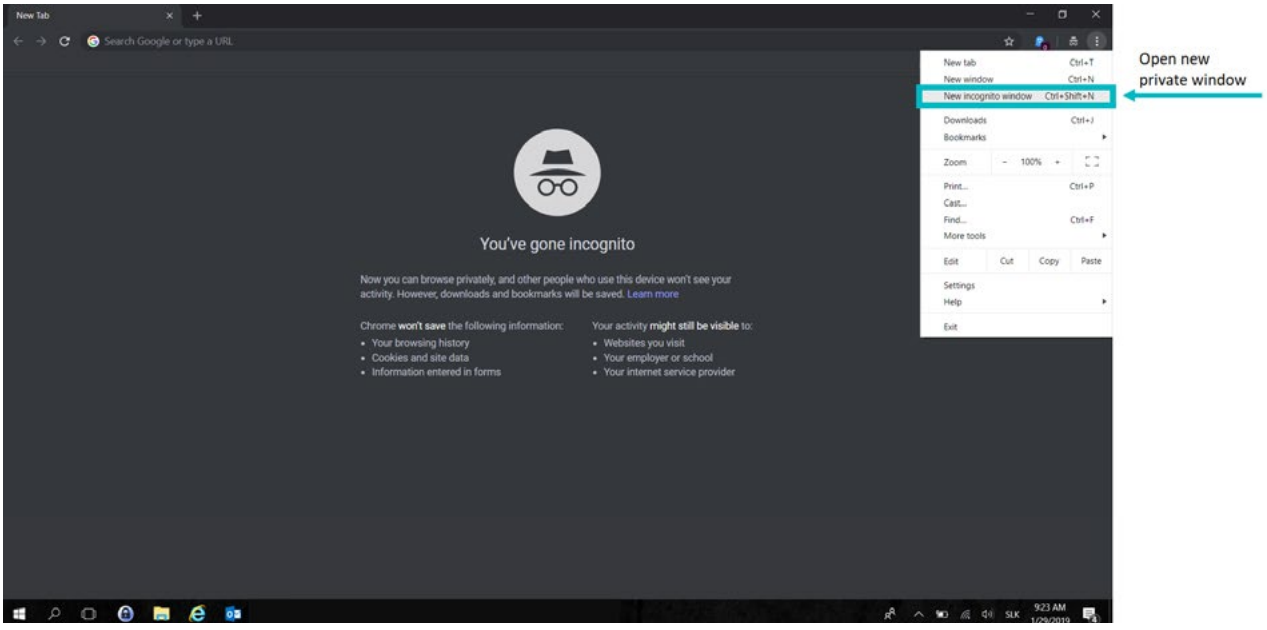
If you visit/use websites containing sensitive data (e.g. email, social networks, or, at an older age, internet banking) you should use the so-called "incognito mode". Once enabled, the browsing history stops collecting some of the user's online data.

IMPORTANT TO NOTE:

Incognito mode does not mean you are completely anonymous on the internet, it just limits the amount of data your browser collects. The information about your visits to individual websites can be collected by the browser manufacturer or connection provider and used to identify your habits and preferences based on which they can adjust the ads or content that will later be presented to you.

To put it simply, we could say that incognito mode hides the websites you visit from anyone using the same device after you. The data, however, is still digitally recorded and stored in other places, such as the browser servers or online service servers (social networks, search engines, etc.), and is thus potentially available to others, e.g. government authorities.





How can you identify an (un)safe website?

- **https://**
  First and foremost, you should pay attention to whether your communication with the given website is encrypted. You can find out by looking at the URL address, which should start with https://. The lower-case "s" at the end means "secure", i.e. a secure version of the http protocol. This is also confirmed in the URL address line by a small padlock symbol.

  If the URL address starts with http:// and there is no padlock symbol, your communication is not secure and is unencrypted. Any information you enter on such a website is sent without any kind of protection, allowing a potential attacker to intercept, read and steal it.

  For advanced users: After clicking the green padlock icon, you can view additional information about the site, such as the validity of its digital certificate, the issuer of the certificate, or the list of allowed and blocked cookies.

  Cookies are small text files a website stores on your device. Using cookies, the website temporarily stores selected information about your activity and preferences (e.g. the username, language, font size, etc.) to reuse during your next visit. Cookies can be cleared from the web browser's cache but this will make using the website less convenient as information such as credentials and preferences provided by the user in the past will be removed.

- **Website language**
  To make their fake and/or malicious websites look trustworthy, attackers often just copy another legitimate website's design and translate its content using free translators (e.g. Google Translate). This often leads to loss of meaning, mistakes in grammar or typos. Such flaws are easily identifiable at first sight and should prompt the user to leave the website immediately. **Site owner's contact information**

  Suspicious websites usually don't care for contact with users. That is why there is typically no contact information or just an anonymous form or a general email address which offers no guarantee that someone will actually get back to you. You should also check who has registered the given site, which could point to its fraudulent nature. Such data is usually available from services such as lookup.icann.org or whois.com.

  You should be careful in particular if the site was only registered recently by someone with a random name, such as John Smith or John Smith Industries Inc.

- **Suspicious content**
  If a site requires you to enter a lot of sensitive information before you even know what goods or services it offers, you should be careful. If you encounter a similar case, the chances are high that fraud is involved. This also holds true when the website author tries to scare or otherwise manipulate the user into quickly registering and entering personal data. Before registering with a new service, younger users (under 13 or 16 years of age) should also consult their parents, because the General Data Protection Regulation does not allow them to provide their data without their parents' consent.

What should you do if you open a dangerous website?

If you accidentally get to a suspicious looking website, you should avoid clicking on any of the objects on the page (buttons, images, links) and close it as quickly as possible. For additional safety, you can scan your device—computer or Android-based mobile device—using reputable security software which should detect, eliminate and remove any threats which the user may have downloaded when visiting such a website.

What are the most frequent forms of browser attack?

In your browser you can most frequently encounter phishing attacks, social engineering and malware infections.

Social engineering (in case of browser attacks) is the psychological manipulation of the victim into opening a dangerous or fake website where the attacker can extract sensitive information from them, or frighten them into installing an unwanted/unsafe application or malicious code.

Phishing is used by attackers posing as a trustworthy website or organisation to collect sensitive information. The attacker's email (message) or website can look almost identical to the messages/websites of a social network, email service or online banking website, or they can pretend to be a reputable e-shop. For examples and tests in which students can find out whether they can differentiate between real and fake sites, see the handbook of suggested "Activities".

A browser can also be a gateway to download malware (in other words, malicious code). It can spread in different ways, which we deal with in more detail in the following chapters. When the infection is introduced through a browser, it most frequently happens through:

1. **Malicious browser extensions** which the user has installed without knowing of its malicious intent, after being pressured into doing so by an attacker or out of ignorance (the app pretends to offer an interesting functionality or offers certain functionality for free).

2. **By visiting a malicious website.** You can get to a malicious website after clicking a link received in an email, instant message, in a document, on another website, or after clicking a fake advertising banner. You can get infected even without doing anything else: malicious code can be automatically downloaded when you visit such a website and be installed on your device. It can also scan your device and/or automatically download other malware.

3. **A so-called man-in-the-browser (MITB) attack.** During MITB, the victim's device is already infected with malware which then allows the attacker to access the vulnerable browser. The malware can intercept data entered by the user on different websites, modify it or extract sensitive information (credit card number, date of birth, login name, password, etc.) and forward it to the attacker. The victim does not suspect anything, because both the browser and the websites function as expected.

Surface web, deep web, dark web

dark web | deep web | surface web

Issues covered in this section:

What is surface web? What is deep web? What is dark web? Are the deeper parts of the web used for only for illegal activities? How do different layers of the web work?

Surface web

The surface web consists of publicly accessible websites which users can find by using internet search engines such as Google, DuckDuckGo or Bing. This is the smallest portion of the web, figuratively speaking "the tip of the iceberg".

Deep web

This is the portion of the internet "hidden under the surface", or to use the iceberg metaphor again—the part of the iceberg below the water. It is estimated that the dark web contains up to 96% of the entirety of online content. It is called the deep web because these are sites and contents not accessible to random users. To look them up or gain access, the user needs special software, tools or access privileges. A large portion of the deep web is legal and legitimate. This can be, for example, electronic report books, educational content intended for a specific class, but also the paid sections of news portals, internal systems of companies and public institutions only accessible to their employees or individual users.

Dark web

This represents a subset of the deep web and the part of the iceberg that is the furthest under the surface. It is not indexed by search engines and runs on the dark net, i.e. an infrastructure providing anonymity to the operators and users of the dark web. To connect to the dark web, a user needs to install special software, e.g. TOR or the I2P service (Invisible Internet Project).

As the dark web is hidden and anonymous, it protects people who in their countries are persecuted for their work (e.g. journalists), or for their religious or political beliefs, and lets them safely communicate with other like-minded groups or individuals. Unfortunately, this anonymity is also misused by (cyber) criminals, e.g. to sell malware and trade in illegal weapons, drugs or services.

Illegal downloads

Copyright | peer-to-peer service | stream | streaming site | torrent

Issues covered in this section:

What is considered illegally downloaded content? What threats are associated with illegally downloading content?

What is considered illegally downloaded content?

As we already mentioned in the chapter devoted to digital identity, every user actively or passively leaves footprints on the internet which show what they were doing. This also applies to downloaded files or watched videos. Downloading and watching illegal copies of a TV series is a very popular activity among current internet users. Most frequently, users can find them on streaming websites[4] full of ads. They can either download them from free storage servers or share them with others via so-called peer-to-peer services.

Most of these activities violate the copyright of the creators of the given work and consequently also the laws of different countries. When downloading or watching such content, the user can also be exposed to digital risks such as malware attacks or damage or loss of personal data.

What threats are associated with illegally downloaded content?

1. When downloading movies/TV shows from storage servers or when sharing them with a large group of unknown people (peer-to-peer services, a.k.a. torrents), it is very easy to download something you didn't want. The file may, for example, be named like one of the popular TV shows, movies or games, but instead contain malware.

2. You can also get infected by malicious code or end up on a dangerous website when watching TV shows and movies using free streaming services. Those are mostly known for having a huge number of ads, some of which may contain links to malicious websites or code. One wrong click is all it takes to download malware onto your device.

3. Downloading illegal content also has legal repercussions. If a user is caught downloading or using an illegal copy, they may face punishment. The punishment varies from country to country, but in some cases it may involve severe fines and sometimes even time in prison.

4 Not to be mistaken for paid streaming services, such as Netflix or HBO GO.

Online games

fake application | game client | netiquette | online games | multiplayer games | game console

Issues covered in this chapter:

What are the basic rules of digital safety when playing online games?
What do multiplayer games and social networks have in common?
Do you need antivirus protection when playing games?
What are the risks when you download and install fake games?
What should you do if you encounter inappropriate behaviour in an (online) multiplayer game?
What should you do before you sell a game console/computer or another device?

What are the basic rules of digital safety when playing online games?

When playing online games, a gamer/user should follow the elementary rules of cybersecurity including use of **trustworthy and secure devices** to play, such as a home computer or their own smartphone. The device should be connected to a trustworthy network (ideally the home network) and use an updated and supported[5] operating system and applications. The device should also use a reliable and updated security solution (antivirus).

When a player uses game clients to launch games, they should ensure they are well protected with a strong password and—if possible—also use two-factor authentication[6]. The game client is a program allowing users to purchase, install and run games and which allows for communication and interaction with multiple players. Steam and Origin are just two examples of such popular services. The game client also contains payment information (e.g. the credit card which the gamer uses to pay for new games), which is a valuable target for an attacker. Similar rules also apply to game console security (e.g. Xbox, Nintendo or PlayStation).

What do multiplayer games and social networks have in common?

Thanks to fast internet connections and a massive expansion of multiplayer gaming, many gaming worlds have basically become social networks. Instead of a profile with their own photograph, the players create fictional characters who embark on quests, carry out various tasks or gather rare objects.

If the game also has a multiplayer mode, when completing quests players can connect with other users they never met and don't know them in real life. In such cases, particularly younger gamers should exercise the same level of caution as advised for social networks. Gamers should avoid sharing any sensitive data in their gamer profile or making the game character look too much like themselves. They should also avoid contact with people in the game who propose a meeting in person or request personal information.

Do you need antivirus protection when playing games?

When playing a game, players should use security software which can protect them from malicious content. An example of this is malicious links either knowingly or unknowingly sent to the player by someone else.

Attackers can also pretend that the link they have provided will take the player to a bonus item or another game benefit (e.g. a new extension pack). In many cases, however, they just try to make the victim open a page that will manipulate them into giving up their sensitive information or disabling their protection (such as antivirus) so they can then infect their device with malicious code.

5 The manufacturer provides support for the given system/application version and issues patches and updates for it.

6 For more details on this form of security, see the chapter Passwords.

What are the risks when you download and install fake games?

You should always purchase games from official and trustworthy stores. The reason for this is that attackers like to copy popular games in order to reach as many victims as possible. Most frequently, they will use one of the following techniques:

1. **Create a fake game version** which imitates the most popular games, such as Minecraft or Fortnite, but instead contains malicious code. Reliable antivirus software can block such threats. Users/gamers can encounter similar fake applications even in some official stores (e.g. Google Play). They can notice them thanks to other users' reviews, who have presumably installed the game and, after seeing it is fake, warned other users about this in their reviews.
2. **Infect the real game with malicious code** and create so-called "Trojans". Such games can most frequently be found in unofficial stores and online forums where they can be labelled as "mods" or offered as "free downloads". The price you pay for this is usually a computer infection which can have far-reaching consequences, especially if it steals your data or damages your device.

What should you do if you encounter inappropriate behaviour in an (online) multiplayer game?

Just like in any other community, you can encounter different types of group behaviour among gamers. A game gives free rein to emotions, which are further emphasised by adrenaline and gamer commitment. This often causes aggressive comments, insults, accusations, etc. This stirs up emotions which gamers often let run free in the in-game chat. If this is just a one-time occurrence, it's not an issue, however you don't have to put up with regular insults.

- The best course of action is not to react to such one-off occurrences and not take them too seriously, otherwise you will be dragged into an inappropriate communication.
- If such behaviour repeats within the group, you should consider choosing a different group of gamers.
- Just like in other groups, gamer groups are also prone to bullying and cyberhate, which you don't have to put up with. The gamer in question can also be an aggressor misusing the gaming environment to hurt others.
- Many games—just like social networks—allow gamers to report improper behaviour, problematic gamers or cheaters. Responsible reporting improves the safety of both the gamer reporting a problem and all others in the game.
- When worrisome things happen in a game or the gamer community, you should notify someone you trust.
- The same standards apply to all gamers. Users should also remember that their own behaviour and comments can be hurtful to someone. "Netiquette" should be followed even when playing games.

What should you do before selling a game console/computer or another device?

If you decide to sell or swap your gaming console, computer or another (mobile) device for a new one, you should first erase all your personal data and games, and ideally reset it to its factory defaults. This option is usually available in the gaming console or PC operating system settings. This will remove any stored contents and different online accounts and services you have used, which otherwise you would be giving to the buyer along with the device.

Malware and other malicious activities

adware | backdoor | banking malware | worm | coinminer | hybrid war | spam | distributed denial of service (DDoS) attack | downloader | dropper | exploit | kit | keylogger | cryptocurrency | cryptowallet | cyberweapon | toolbar | phising | cyber espionage malware | password stealer | potentially unwanted applications (PUA) | ransomware | scam | skimming | social engineering | spyware | Trojans | virus | advanced persistent threat (APT) | zero-day vulnerability

Issues covered in this chapter:

What is malware?
What categories of malware do we know?
What types of malware are there?
What motivates the attackers' malicious activities?
What do potentially unwanted applications (PUA) look like?
What does a common malware attack look like?
What can advanced malware, such as an APT, do?
Why don't we talk about viruses and worms anymore?
What else, besides malware, do attackers use?
What other forms of attack are there?

What is malware?

This word is an amalgamation of the words malicious and software and denotes a computer code that was created to do harm/damage. This is a more accurate name for what many people refer to as a (computer) virus, which is just one subcategory of malware.

What categories of malware do we know?

Malware can be divided into different categories. If we categorise malware according to the risk it poses, we get the following categories:

1. **Potentially unwanted applications (PUA)**
   While not malware per se, these applications belong to a grey zone as they have some unwanted properties. They may not be directly harmful to the user, but they can be annoying, misleading or eat up a device's resources and represent the first step towards truly malicious code or dangerous internet locations. Users can often install such PUAs "bundled" with other software or encounter them on dubious websites.

2. **Malware**
   Malware contains malicious code which has a clear objective—to cause harm to the user. It can, for example, steal data, login information or monitor the user or their online activity, blackmail them or steal their money. With most malware, the objective is to earn money for its creators who spread and manage the malware. Malware contains a number of subcategories, such as ransomware, spyware, Trojans, downloaders, keyloggers, backdoors, adware and many others.

3. **Advanced Persistent Threat (also known as an APT)**
   As the name suggests, these are exceptionally sophisticated types of malicious code created by groups of expert attackers who put a lot of time, energy and money into creating their malware. They usually focus on sensitive areas of public services such as the power supply, government or international institutions, or traffic control systems. APT groups and their tools can cause serious damage and even pose a threat to human life. Some of their malware is even labelled as cyberweapons (e.g. Stuxnet) or tools of cyber espionage. The average person will probably never experience an APT attack directly; however, they may experience their consequences if such an attack disables the power supply in their region or disables a service provided by a state agency.

What motivates the attackers' malicious activities?

At present, the motivations of cybercriminals are very different from those of their predecessors in the 1980s and 1990s, when the first cyberattacks began. In the past, their main objective was to show the world their abilities and build a reputation within the "hacker" community.

The main motivation today is money. Malicious code is usually made so that it can be used universally, re-sold, and reused by other attackers in exchange for significant amounts of money. The sale of malware as a service opens access to malware even to inexperienced criminals who are unable to write the code themselves, but who can effectively buy and spread it for their own benefit.

There is also a small group of very advanced attackers who write malware for targeted attacks. In this case, profit is not important, because they are funded by a contractor—usually a nation state which has sufficient resources and reasons, such as using the code as a weapon in hybrid warfare or using it for cyberespionage. Whereas the consequences of such activities can affect the real world and can cause damage, for instance to industrial equipment or critical systems, we sometimes refer to these as cyber weapons.

What do potentially unwanted applications (PUAs) look like?

One type of PUA is so-called **coinminers** which use up computer resources to mine cryptocurrencies such as bitcoin or Monero. Some of these unwanted applications use a disguise and try to persuade you to install them directly into your device, however, some can access your device's resources via the browsers as soon as the victim opens a website that contains specific coinmining code[7]. Coinminers are ranked as less dangerous as their activity stops as soon as the user closes the browser window or the browser itself.

In the past, the most common PUAs were **so-called toolbars** which the victim knowingly or unknowingly installed into their browser. These toolbars usually came bundled with other software, but did not provide the advertised functionality; instead they slowed down the browser and complicated its use.

Other examples of PUA are various **browser applications and extensions** promising to remove bugs, reduce load, or "clean up" the device and improve its performance. In most cases these are just empty promises without any actual results. The main objective of such apps is to display ads or collect information about users' behaviour.

What does a common malware attack look like?

Malware can take different forms. This overarching term includes viruses, worms, Trojans and other types of malicious code. We will discuss the individual types of malware you can encounter in more detail below.

- **Adware**
  If a device becomes infected by adware, it will show an excessive number of adverts even when you don't expect it—e.g. when the browser is not open. If you think adware is not that dangerous, you may be mistaken. Besides being a nuisance to the user, it also deploys some aggressive techniques typical of malware. For example, it can modify the device settings without the user's knowledge or install or uninstall other software. These actions may pose the threat of a secondary, much more serious infection.
- **Backdoor**
  This name is also very apt. It is a type of malware that can open a backdoor allowing the attacker to misuse such access to the user's system, to monitor them or install additional malware. The backdoor often serves as the basic tool and starting point for advanced persistent threats (APTs) described in detail below.

7 However, note that some users mine cryptocurrencies knowingly, and intentionally install similar code on their devices or websites in order to earn money.

- **Banking malware**
  Focuses primarily on theft of the victims' financial information, such as credit card numbers, bank account access, cryptowallets and other money or cryptocurrency related services. However, some banking malware families try to collect even more data and are thus often labelled infostealers.
- **Downloader/dropper**
  Following its installation, this malicious code connects to a specific website or server and downloads and installs additional malicious code selected by its criminal operators.
- **Keylogger**
  This code monitors the user's every step, or, more precisely, their every keyboard stroke and mouse move. This allows it to monitor (map) their activity in detail and can also steal data which is not stored anywhere, but merely entered by the user from time to time in a service or program login screen.
- **Password Stealer**
  In terms of malware categories, the password stealer is very similar to banking malware and infostealers. However, it focuses on files and programs which could contain passwords. Many of them, for example, try to steal passwords stored in browsers or vulnerable password managers.
- **Ransomware**
  Following a compromise, ransomware blocks the device's screen or encrypts its data. The victim has to pay a ransom to unblock/decrypt the device. The best known examples are WannaCry (2017) or CryptoLocker (2013). A ransomware named (Not)Petya (2017) was part of the most devastating cyberattack in history, causing damage in excess of 10 billion dollars.
- **Spyware**
  Malicious code which spies on the victim via their compromised device. Its objective is to stealthily collect as much data as possible, e.g. passwords, access codes and other sensitive data, and upload it to the attackers' servers. The criminals will then try to monetise the data on the "dark web"[8] or use it for other malicious activities. This means the user's sensitive data can fall in the hands of criminals who can misuse it to damage the victims, e.g. through more data theft, or by stealing their money or identity.

Naturally, this list is not exhaustive and the features of the malicious code may differ and focus, for example, on network communication, on collecting sensitive data from the device memory or on attacking the device even before the operating system is started (bootkit/rootkit). Sometimes, combinations of different types of malware can occur, consisting of multiple levels or modules with similar functionality (downloader + ransomware, downloader + banking malware + keylogger, etc.)

What can advanced malware, such as an APT, do?

The criminals behind such malware are usually seasoned software developers with years of experience working with malware. Their "products" are usually modular—comprising several parts which can be added or removed—taking advantage of known software vulnerabilities or sophisticated manipulation techniques to infiltrate the victims' systems. Chances are high that they have enough time and resources to develop their malware, so profit is not their main motivation. They mostly focus on espionage and the destructive effect of their work.

8 For more information on this topic, see the chapter Surface web, deep web, dark web.

An example of such a targeted attack was one on energy distributors in Ukraine where the attackers targeted industrial "switches" and the computers that control them. All-in-all, only several tens of devices were affected, yet the attackers were able to cause a blackout that affected hundreds of thousands of users. The operators behind the attack gained access through infected email attachments that were opened by one of the employees at the distribution company. This access allowed them to install and run dangerous malware, specifically BlackEnergy and later Industroyer. Both managed to disconnect the power supply to households for several hours. Sophisticated malicious code was also the source of the most destructive attack in history, known under the name Petya or NotPetya. This attack disabled numerous global companies and caused damage in excess of USD 10 billion, despite being originally targeted only against Ukrainian companies.

Why don't we talk about viruses and worms anymore?

Both of these categories of malware were widespread in the past—in particular during the 1980s and 90s. Today, however, the range of malware is much greater and neither viruses nor worms rank among the most dominant, especially in comparison to PUAs, Trojans, adware or ransomware.

- **Viruses** work similarly to the flu or other viral diseases. They need a host, i.e. vulnerable programs and applications they can infect and use to spread further.
- **Worms**, unlike viruses, don't need any programs to spread and are able to replicate (multiply) on their own through the network, emails and portable media (e.g. USB flash drives).
- **Trojans** are probably the most widespread types of malware today. They use the same principle as the mythical Trojan Horse. On the outside, they pretend to have a legitimate function (such as a video player, game, chat application) or masquerade as a harmless file (document, update), however, their real objective is to cause harm. Interestingly, some Trojans provide part of the promised functionality or service, to mask their main, nefarious, objective.

What else, besides malware, do attackers use?

For the attacker to gain something, they need at least partial cooperation from the victim. If they mostly create malicious code with no access to the hard drive containing documents, to the camera, microphone or other parts of the system, there would not be much to gain.

Therefore, attackers often use **social engineering**, i.e. sophisticated techniques designed to manipulate the user into unknowingly giving them approval to control the device. You can find more information about this form of attack below.

The most advanced attackers, however, have other ways to infiltrate a device. Some are looking for hitherto unknown **zero-day vulnerabilities** in software[9], or deploy specialised tools to find them (**exploit kits**). In other cases the attackers pinpoint a legitimate piece of software (or one of its versions) and compromise it with malware. The original creators of the legitimate software have no knowledge of this and the user installing the infected version unknowingly runs the malware.

9 A zero-day vulnerability is a vulnerability not yet known to the software creator. The attacker misuses this vulnerability without anyone else knowing about it. Most frequently, attackers focus on well-known and documented vulnerabilities which had been previously made public, as this represents a cheaper and easier alternative.

What other forms of attack are there?

Cyberattacks can take different forms and malware doesn't have to be the only/final tool the attackers use. Here are a few other examples:

- **A botnet** is a network of infected devices ("bots") remotely controlled by the attacker from a server or using commands which the devices exchange. A botnet can spread spam or malware, or be used to cover the attacker's tracks or for DDoS attacks (see definition below). An existing botnet may even be leased by the attacker on the dark web to other attackers or for other purposes. A botnet can consist of millions of devices. Currently, attackers are focusing on devices that comprise the internet of things (smart devices or IoT), which are known for their inferior security.
- The objective of a **distributed denial of service (DDoS) attack** is to take down a website or an online service using the network traffic created by a botnet. A large network of infected devices can generate a huge number of access requests directed at a specific site, thus overloading the servers that host it. One of the largest DDoS attacks took place in March 2018 and targeted an undisclosed US company with 1.7 terabits per second (Tbps) of data.
- **Exploit** is an English word meaning "to use something for one's own benefit". Its negative connotation is used in the field of digital security. This is basically a piece of code or a procedure created by the attackers to take advantage of vulnerabilities and bugs in software or hardware in order to take control of it.
- **Phishing** is a fraudulent attempt to obtain sensitive information and data, where the attackers disguise themselves as a trustworthy entity, service or person. A fake link received by email will take the user to a website purporting to be from trusted parties, such as a social network, an email service or a bank. Users can come across phishing links in spam, however, they also often spread through chat forums, social networks or by SMS. Many of them can be intercepted by security software. The important thing, as always, is to check twice before you click on anything.
- **Social engineering** describes a range of non-technical attack techniques that are used by cybercriminals to manipulate victims into breaking security rules and performing harmful actions or giving up sensitive information.
- **Spam** is any unsolicited electronic mail. It can take the form of an email, an SMS message or a chat message. It may contain unwanted advertising but can also be used to spread links to other malicious content.
- **Scam** is a type of social engineering where the attacker deceives the victim or a group of victims to gain their trust, which is then exploited for the criminal's own benefit. Such elaborate deceits usually take advantage of human traits such as gullibility, compassion, irresponsibility or greed. Examples of scams are fake e-shops with cheap brand glasses, or competitions promising a giveaway of a popular device for free. In the end, the victims can lose their data or sometimes even their money.
- **Skimming** belongs to the banking attack category. A skimmer is an inconspicuous hardware device installed on an ATM to scan data from the cards inserted. This valuable data is then stored or sent to the attacker, who can then sell it or exploit it to make purchases in the name of the victim. Similar attacks also take place in the digital environment, where attackers can use malicious code to infect the payment gateway of a legitimate e-shop.

Security solution (antivirus)

antivirus | security solution | malware | fake antivirus | machine learning

Issues covered in this chapter:

What does antivirus do?
Why do you need a security solution?
What should you pay attention to when selecting a security solution?
What is the difference between a paid and a free security solution?
Do two security solutions provide better protection than one?
Why is the name "antivirus" inaccurate and why should it be replaced?

What does antivirus do?

Antivirus, or, more precisely, a security solution, is a piece of software which protects the user from threats and risks that exist in the digital environment. When a security solution detects malicious code, behaviour or activity, it notifies the user.

Why do I need a security solution?

Information in today's world is of huge value. Attackers are aware of this and misuse a number of technological and psychological tools to gain access to information, sell it, or exploit it for their own gain. Many users think they don't own any valuable information, yet the opposite is true. In addition, an infected device can also be a valuable source for middleman to continue spreading malware.

Experienced attackers, whose objective is to profit from the victim and their data, write their own malicious code, improve it, sell it and spread it. The less tech-proficient ones can buy such code or focus on devising ingenious lies with which they can manipulate victims and extract sensitive information from them, such as bank account credentials.

Naturally, there is a relatively large grey zone where both approaches mix. For more information about what forms malicious code can take, see the chapter Malware.

Users can protect themselves from a large proportion of these threats by using reputable and reliable security software (commonly referred to as antivirus). Such solutions should be able to detect threats using different techniques and offer multiple layers of protection. Threats can be detected in different places, e.g. at the network level, when entering the device, when launched, or when delivered to one's inbox pretending to be a harmless email or an "innocent" attachment.

What should you pay attention to when selecting a security solution?

A good practice when selecting a security solution is to review the results of independent tests. Here are a few examples of organisations doing such testing: VirusBulletin, AV Comparatives, AV-Test.

In their tests, users can review the different features of the security software—e.g. how much resources they use, what percentage of malicious code can they detect and block, or how many false positives they produce.

A key factor in selecting a solution should be whether the security software uses a mix of techniques which can protect the user on multiple levels. Antivirus solutions using just one dominant technique or only focusing on one type of detection are easier for attackers to bypass.

We could compare this to car security features. A vehicle equipped with assistance systems that can help the driver with loss of traction or protect them with safety belts and airbags is certainly much safer than an older model which protects its passengers with just one of these features.

It is also important to observe whether the security software selected requires the user's consent to process data in compliance with regional laws such as the GDPR in the EU, or the CCPA in California. The user should be notified prior to installation what data the solution will be collecting and for what purposes.

What is the difference between a paid and a free security solution?

Any security software is better than none. In general, there are two main categories of security solutions—paid and free.

Free security solutions provide a certain level of protection, however, the company producing them have to earn money in a different way. They can do so either by collecting and selling data about their users, by selling paid in-app features, or by displaying ads.

On average, a **paid security solution** costs a couple of tens of euros per year. In exchange for this amount, its developers can work on ensuring its operation and improving the technology while not bothering the user with advertising and only collecting information about malware. Some security programs also offer so-called trial periods during which the user can install and use them for several weeks or months free of charge.

However, you should be careful about software resembling a security solution and providing zero protection—so-called **fake antivirus**. This type of fraud can cost the victim a significant amount of money while also jeopardizing their safety. When selecting a security solution, always check whether it's a reliable and trustworthy product.

Do two security solutions provide better protection than one?

When two or more security solutions are running on a single device, this usually impairs the user experience as well as the level of protection. The reason for this is that security solutions inspect incoming and outgoing data, network communication, processes running on the device, etc., to detect and remove any malicious activities. When several security programs are granted such rights, they get in each-other's way, reducing their efficiency. It can also complicate the user's situation, as collisions between individual apps can lead to a number of false positives.

Why is the name "antivirus" inaccurate and why should it be replaced?

At present, "antivirus" and "security solution" are used as synonyms. From the manufacturers' viewpoint, however, there have been significant changes which the word "antivirus"—despite its popularity—cannot encompass. The name security software or security solution is therefore much more apt.

First of all, modern security solutions don't exclusively focus on protection from viruses, but from a much wider range of malicious code and activities which did not even exist in the era of the original antivirus solutions. To be able to do so, traditional antivirus had to evolve and add new technologies and protection layers, including machine learning—i.e. the ability of the program itself to analyse data, identify similarities or anomalies and learn from previous experience. Besides protecting users from malicious code, a modern security solution also offers other premium features such as data encryption, password management or the localisation of a lost or stolen device.

Internet connection security

hotspot | internet browser | internet of things (IoT) | smart home | smart device | virtual private network (VPN) | webcam | Wi-Fi Protected Access (WPA)

Issues covered in this section:

Which types of networks or network connections are safer? How can you recognise an (un)safe network? How can you avoid unsafe networks? What is a virtual private network (VPN)? What is the internet of things (IoT)? How does IoT impact users' online safety? Do you need to cover your webcam?

Which types of internet connections (networks) offer greater security?

Corporate networks usually offer the highest level of security, however, home network security is gradually improving as well. The lowest level of security is offered by public Wi-Fi networks with no password protection. These are typically available in city squares, cafés, mass transportation, hotels and on public premises.

The main difference between a secure and a less secure network is the use of an improved security protocol (WPA2 or ideally the upcoming WPA3) and a password which the user has to enter to be able to connect. However, neither of these traits offers a 100% guarantee that the network you connect to has not been compromised or even created by an attacker.

How can you recognise an (un)safe network? What to look for?

- **Choose the location where you connect to the internet**
  - If possible, you should only connect to networks for which you know the administrator or the security settings. These are normally school, home (in your or your friends' homes), and corporate networks. If possible, you should completely avoid public networks.
- **Name of the Wi-Fi network**
  - When selecting a Wi-Fi network, carefully study its name. One of the most widespread attack methods is to create a hotspot/network with a name that is **almost** identical to the legitimate network in that location. By using this approach, attackers improve their chances that the victim will connect through their Wi-Fi and they will then be able to monitor what data the victim is sending.

SPECIFIC EXAMPLE: A café offers a free network with the identifier *Cafe_wifi*. The attacker thus creates a similar one named *Cafe_wifi_free*, *Cafe_wifi1*. Unless you check with the staff which one is legitimate, you will never know.

- **Security protocol/password**
  - Until recently, the highest level of protection was offered by the WPA2 protocol (Wi-Fi Protected Access 2). The data sent over a network secured with this protocol is encrypted, which prevents attackers from reading it. However, researchers have found serious vulnerabilities in this protocol, which is why a new version named WPA3 is currently being rolled out.
  - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access version 1) protocols are outdated and don't offer sufficient protection for your communication. When an available Wi-Fi network still uses these protocols, it is better to avoid it.
- **Look for https://**
  - If you connect through a public Wi-Fi network that you cannot verify as being secure, you should only visit websites whose URL starts with **https://**. That means the communication with the site is encrypted and an attacker logged in to the same network will not be able to read the data you transmit.

How can you avoid unsafe networks?

Nowadays, almost everyone owns a mobile phone with a data package. Provided the data allowance is sufficient, they can create their own Wi-Fi network (so-called hotspot) and set the desired level of security (ideally WPA2 or WPA3) with a name and password. They can then use this network to connect other devices, such as a notebook, tablet or other smart devices. It is difficult for an attacker to infiltrate such a network.

What is a virtual private network (VPN)?

If you don't have the option to create your own network, as an alternative you can use a VPN (virtual private network) service which can create an encrypted tunnel between the user's device and the target site. This tunnel is virtually impenetrable to attackers. The downside is that reliable and high-quality VPN services are not free of charge. However, some browsers, such as Opera or EPIC, have this functionality built in. VPN represents a higher level of protection, which makes sense especially when the user needs to remain anonymous or needs to bypass internet connectivity limitations. Examples of such situations are journalists and civil activists persecuted or constrained by authoritarian regimes.

What is the internet of things (IoT)?

The internet of things denotes all devices collectively referred to as "smart" or "intelligent". When a device is referred to as "smart", besides meeting other conditions it also has to be connected to the internet. While in the past such devices were mostly computers and later mobile phones and tablets, today they also include many TVs, cameras, watches, refrigerators, and even cars. Internet connectivity expands the functionality of such devices, but at the same time opens a path for attackers.

How does IoT impact user online safety?

The internet of things is altering our households and it is estimated that over the coming decades entire households (so-called "smart homes") will connect to the internet. They will collect huge amounts of sensitive data about the household's occupants. This is a valuable commodity, in particular for cyber criminals who can both steal and sell such data and misuse it to track victims. The worst-case scenario is that they gain control of an entire smart home.

This is not sci-fi—vulnerabilities of this kind have been discovered in almost every device tested by cybersecurity experts. Some devices suffer from serious issues—they use a weak password or none at all, they don't encrypt the stored data—while others form the central points of smart homes and in case of a data leak or a vulnerability can pose a great risk to the privacy of their owners.

A GOOD DEMONSTRATION of what vulnerabilities can be caused is shown in the introductory scene from the popular TV show Mr. Robot (series 2, episode 1).

Do I need to cover my webcam?

Laptops, smartphones and tablets are commonly equipped with cameras. This technology adds video to phone calls and simplifies adding new photos on social networks, chat forums, or to your personal collection.

Yet this also has a downside. There is the risk that someone will misuse these technologies against the device's owner. Attackers have proven time and again that a webcam can be a useful tool for tracking victims. This effect is further multiplied by the fact that many users keep their smartphones within reach almost all the time.

Camera security seems to be the main focus for many leading tech personalities, chief among them the funder and manager of Facebook Mark Zuckerberg. It was Zuckerberg who back in 2016 posted this photograph, where in the background you can see that his computer has its camera and microphone jack taped over.

Even though not everyone has such valuable information as the CEO of Facebook, even private or intimate photographs can be valuable for attackers. They can use them to extort victims by threatening to publish them or sell them on the dark web.

This form of attack, however, requires cooperation from the victim. The attacker needs to persuade or manipulate them into installing a malicious application on their device. Such an application can then activate the camera or collect older images and send them to the attacker. In most publicised cases, the attacker even had physical access to the device and manually installed spyware on the device.

To avoid this scenario, users should:

- Cover the camera on their device. Some computers offer this functionality by default, but if they don't, it is recommended to tape the camera over with a non-transparent adhesive tape or a special cover.
- Use reliable security software which can protect the camera's security and block any attempts at camera misuse.
- Ensure that the camera is off and does not record what is going on around it. Also regularly check which apps and programs on the device have been granted permission to access the camera and images.
- When putting the device with a built-in camera aside, position it so that it doesn't show any sensitive areas of a room or apartment. The camera should not be pointed e.g. at your bed, the bathroom or other areas where intimate pictures could inadvertently be taken.
- You should also avoid taking pictures with intimate content, which could fall into the wrong hands. Teenagers should bear in mind that it is not recommended to share such images with their current partner because, should they split up, the images can end up in the wrong hands or on the internet.

When it comes to webcams (and other cybersecurity threats) teachers and parents should serve as role models and follow the rules just like students and children.

Passwords

passphrase | two-factor authentication | password | password manager | brute force attack | multi-factor authentication

Issues covered in this chapter:

What is a password?
What should a good password look like?
What can you do if you have too many passwords?
What can you use instead of a password?
What is two-/multi-factor authentication?
How do attackers steal passwords?

What is a password?

A password is a secret code, word, phrase, sentence or series of characters which is known only to the user, used in conjunction with a login name to identify the user when logging in to digital devices, systems or services.

What should a good password look like?

A good password should meet several criteria. Properties of a good password:

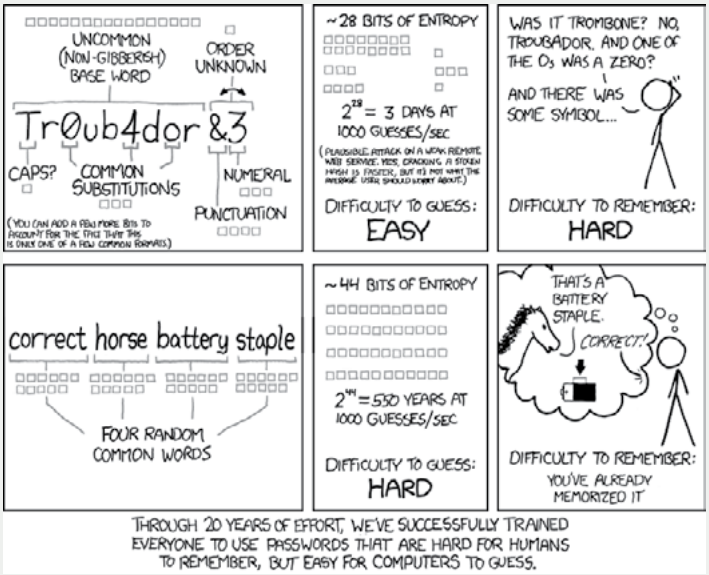
- **It's secret—**Known only to the user[10].
- **It's unique—**Each service or device should be protected by a different password so that if someone steals one of them, they don't gain access to all accounts/devices.
- **It's long—**It consists of at least 8 characters, ideally 16 or more. A good option is security phrases, as described below.
- **It's difficult to guess—**It should not include simple series of numbers such as "123456" or simple words such as "password". Attackers can also easily guess popular book or movie quotes, words from a dictionary or combinations of user data, e.g. "namesurnameyear". The data of which such a password comprises is often available on social networks, and when the user's security is not set up properly, attackers can collect them and use them to guess passwords.
- **It wasn't part of a previous leak or data breach—**This can be verified via services such as Have I Been Pwned.
- **Complexity is not necessary—**Previously, users were advised to create passwords by employing a series of numbers, lower- and upper-case letters and special characters (e.g. @, #, $, %). However, this advice has been superseded by the latest edition of password guidelines and requirements published by US National Institute of Standards and Technology (NIST).
- **It consists of a security phrase—**A sentence or a phrase (including spaces) which is easy to remember for the user and which is sufficiently long and complicated so it's impossible to guess. An example of a good security phrase is "Nobody can t8ke w#at you already ate", because it comprises 36 characters, contains spaces, lower- and upper-case letters, a number, a special character and is easy to remember[11].

BONUS TIP:
The list of the 100 worst passwords leaked on the internet is published annually by TeamID (2018, 2017, 2016, 2015, 2014).

10 In the case of young children, passwords should be shared with the child's parents or be created with their help.

11 Unfortunately, its publication in this handbook means that this pass phrase is no longer secure, because too many people will know it or can easily guess it.

This comic from https://xkcd.com/ can be used as a demonstration of a suitable procedure for creating a strong password:



What can you do if you have too many passwords and cannot remember them?

We recommend using an application called a password manager. It can store not only all of the user's passwords but protects this list with an additional password and also encrypts them. When selecting a password manager, you need to be careful of fraud and look for trustworthy brands with a good reputation and verified security—such as Sticky Password, KeePass, or LastPass. Some operating systems offer a built-in password manager—e.g. Keychain on MacOS.

What can you use instead of a password?

Passwords are now being replaced by biometric identification—e.g. scanning of the user's fingerprint or face. Should these fail, they usually use a numeric PIN code as a backup.

In general, passwords are usually secured by adding another verification/step to ensure that the password was entered by the authorized individual. This is called **two-factor** or **multi-factor authentication**. This form of verification can have multiple forms:

- **Using a different communication path**—a verification SMS is sent to the user's mobile phone.
- **Using other, previously agreed codes**—e.g. a physical card containing a code matrix, from which one is selected at random which the user must then enter on a website or in an app; or an electronic reader—a hardware device which generates a unique code for the user which the other party can verify.

- **Using a special application that creates expiring codes—**The code is usually valid for a limited period of time, e.g. 30 seconds. After the time limit expires, the code changes and the original one loses its validity. This significantly reduces the time for an attack, further improving password security. However, these apps can only be used with some online services. Two examples of a relatively universal solution are Google Authenticator and Microsoft Authenticator.

Here are some discouraging examples that the teacher can present (based on real life):

A girl was using a Facebook account with an easy-to-guess password. Besides that, when travelling abroad she logged in to an unsecured Wi-Fi network where an attacker probably intercepted her password. Using this information, he managed to hack her account and steal private photographs she was exchanging with her boyfriend. He then blackmailed her, threatening to publish the images unless she paid a ransom. When she refused, he sent the photographs to all her Messenger groups.

A victim had an email server in his company protected by a simple password. It was a publicly accessible system, and the attacker found it on the internet and broke the password. He then kept sending malicious emails and improper adverts to all the contacts in the address book.

How do attackers steal passwords?

There are several ways an attacker can obtain a victim's password:

1. **By watching them—**this may sound absurd, but attackers often get passwords by looking over their victim's shoulder or recording them on video. This applies to logging into online services as well as to devices.

    a. Illustration video: https://www.youtube.com/watch?v=e9CfWK-uN44—the code is long and complicated, but once it is published on the internet it cannot reliably protect the user any more.

2. **Social engineering—**The attacker manipulates or tricks the victim into giving them the password. To do that, they can use a fake website, a custom-made email, or a social network message where they pretend to be a trustworthy person/institution or pretend that the request originates from a bank/social network/online service.

3. **Malicious code—**The attacker infects the victim's device with malware (e.g. using a software vulnerability, social engineering, an infected website, etc.), which has been created specifically to identify, monitor and steal passwords and send them to the attacker.

4. **Network communication attack—**The attacker may intercept the victim's data at the network level. If the attacker decides to do so on a public Wi-Fi network, in most cases they have to be near the victim[12] and the Wi-Fi must run on an outdated security protocol. A similar attack can, however, also be carried out using malicious code—in this case, the attacker doesn't have to be present.

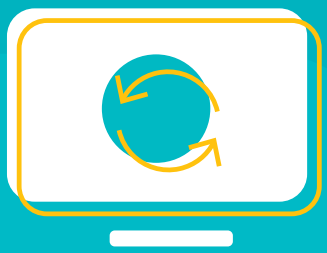
5. **Guessing (a so-called brute force attack)—**One of the most frequently used tactics. The attacker is guessing commonly used or preset passwords and uses dictionaries or known phrases. For this purpose, they use a special code or entire devices which can guess thousands of passwords in a matter of seconds. This allows them to easily and quickly hack into an account with a weak or short password. For example, a code consisting of four characters and numbers can be guessed by the attacker almost instantly.

    a. Examples of password strength calculators:

http://lastbit.com/pswcalc.asp

https://tmedweb.tulane.edu/content_open/bfcalc.php

12 In many cases, an attacker just needs to be close to the victim's home or apartment. Today's Wi-Fi access points often have a range that extends tens of metres beyond the walls of an apartment/house. Besides that, an attacker equipped with an antenna can boost the signal and further increase the range.



Updates

update | firmware | operating system | patch

Issues covered in this chapter:

What are updates and how can a user know that a piece of software needs to be updated?
Why are updates important?
Why should you not postpone updates?
Should you use automatic updates?
Which programs and parts of the device need to be regularly updated?

What are updates and how can a user know that a piece of software needs to be updated?

Updates are new versions of software or parts thereof. Updates often fix software errors and improve application security.

Sooner or later, every digital device user will come across updates. The operating system or an app will notify them of the need to update, usually using a pop-up window/notification. Once the update is completed, it may be necessary to restart the device.

Some updates are also called patches because they fix "security holes". Other updates (e.g. security software updates) only update selected databases or add new features. In English, they are mostly referred to as "updates" or "patches".

Why are updates important?

Updates may serve different purposes. From the viewpoint of security they fix vulnerabilities and improve application, user and device security. Another purpose of an update is to fix problems reported by users—e.g. malfunctioning buttons, missing features and so on—thus improving performance and user value.

Larger application or operating system updates which involve moving to a newer version often include other benefits in the form of new features, improved interface and options which make the application or operating system more attractive to users.

Why should you not postpone updates?

Pop-up windows notifying you of an update usually include an option to postpone the update by several minutes, hours or days. Unfortunately, users often opt for the longest possible delay as they don't want to be held up at that moment. The update, however, may fix a critical security or other program/device related issue and should not be postponed.

Because of cybercrime, all software should be updated as soon as possible. Attackers usually try to take advantage of known software vulnerabilities to gain control of the victim's device. The longer you postpone the update, the greater the risk of someone misusing the vulnerability.

Should you use automatic updates?

A good option to keep devices updated and up to the latest security standards is to activate automatic updates. They can, for example, always be installed at the end of the day or just before the device is being switched off. Automatic updates can usually be enabled directly in the pop-up window displayed to the user, or via the device's settings.

Which programs and parts of the device need to be regularly updated?

All operating systems need to be updated. Among the most popular are Windows, MacOS, Linux, iOS and Android.

Updates must also be installed for all applications and programs running on the device, including the internet browser, music player, graphics editors or games. In some cases it is also necessary to update the so-called firmware—e.g. the low-level software running below the operating system that ensures all the hardware components work correctly.

Glossary

This handbook contains some IT security-specific terms and expressions. For easier reference and understanding, we recommend that readers become familiar with them prior to using this handbook. In the glossary below you will also find explanations of some terms which, through their overuse in the media, have lost a part of their meaning which, in our opinion, is key.

Attacker/cybercriminal

Whereas malicious hackers only form a subset of this group, the terms attacker or cybercriminal are much more apt and that is why we use them throughout this handbook.

Cyberbullying—misuse of the internet and digital technologies to intentionally and systematically inflict harm on others.

Cyberhate—any use of electronic communication to attack others on the grounds of actual or perceived race, ethnicity, language, nationality, complexion, religious beliefs, sex, gender, sexual orientation, political affiliation, socio-economic status, age or mental or physical health, and the dissemination of hate speech.

Cyberstalking—repeated and long-term misuse of digital technologies to stalk and harass other user(s), which is usually very intimidating and deprives the victim of the feeling of security. It can include threats of physical harm, false accusations, the damaging of data or identity theft, monitoring of the victim's computer and the like. The intensity of the harassment usually increases and doesn't stop even if the attacker is prompted to stop or after the victim blocks them. From the online environment it often extends offline.

Disinhibition effect—the loss of inhibitions and restraint in the online environment due to the feeling of anonymity. As a consequence, when communicating online people are often more courageous, but also more aggressive, and they dare do things they would never do face-to-face with someone. This effect relates to cyberbullying, trolling and cyberhate.

Hacker

Among the general public, the word hacker has a negative connotation—this is not how IT security specialists perceive them, however. The word also describes an individual trying to find a new or original use for a (software/hardware) system or a part thereof which is completely different from its original intent. In general, hackers can be divided into three categories: Ethical hackers (white hat), those who operate in the grey zone (grey hat), and those with clearly malicious intentions (black hat).

In general, a hacker can also be a person who disassembles a radio and instead of receiving signals and listening to music uses it as a transmitter and signal jammer. Ethical hackers try to find weak spots in an organization's systems with the objective of notifying the owner and helping them fix the problem. This process is also called ***penetration testing.***

Hacking

Cybercriminals in the movies often just need an internet connection and in a matter of minutes (or even seconds), they can access any system—no matter whether it is an electronic door lock, an internal network of a secret service or the police, or the controls of traffic cameras. The complexity of today's systems is such that actions like these would take criminals weeks or perhaps months, because they need to become familiar with the internal workings of the system first and only then can they start working towards their original goal. Hacking is often a long-term and goal-oriented activity in which the hacker (ethical hacker or attacker) tries to find vulnerabilities in a given system and either reports (ethical) or exploits (attacker) them.

Happy slapping "slapping for fun"—a new form of ill-treatment which combines face-to-face bullying with cyberbullying. The aggressor physically attacks the victim while recording the incident on a mobile phone. The recorded video is then uploaded to the internet or disseminated to peers in messages. With happy slapping, the aggressor is often a group, not just an individual. The group members are "having fun" and encouraging one-another in harming the victim.

Malware/malicious code

The word malware is an amalgamation of the words "malicious" and "software". It literally denotes a computer code or its part that has been created to cause harm/damage. Malware is an overarching name for (computer) viruses but also many other categories of malicious code.

Social engineering

This is a category of attack that requires almost no technical knowledge. Using social engineering, an attacker tries to deceive or manipulate their victims into violating certain security rules. Their objective can be to trick the victim into opening a dangerous or fake website, to extract sensitive information from them, or to scare them into installing an unwanted/unsafe application or other malicious software. This type of attack takes advantage of human ignorance and/or weakness.

Spam and phishing

Spam is any unsolicited electronic mail, e.g. email, SMS message or chat message. **Phishing** is a fraudulent attempt to obtain sensitive information and data in which attackers disguise themselves as a trustworthy entity, service or person. A phishing attack can also take the form of an email to which the victim should reply, or a link to a website that looks like the original, e.g. the website of a social network, an email service or an internet banking service. Links to phishing sites often spread through spam email, chat, social networks or SMS. Teachers and students can have a look at the phishing tests available online. The links to these exercises can be found in part two of this handbook, titled Suggested Activities.

Outing—publishing a victim's private or intimate information on the internet without their consent.

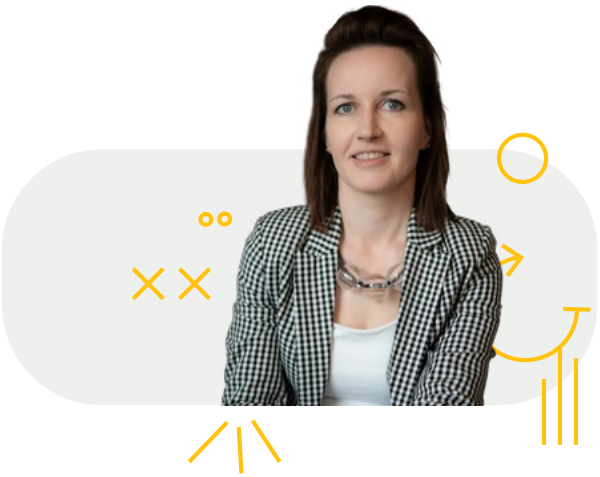
Troll—an internet user whose objective is to provoke a strong reaction from others, who deliberately disrupts or thwarts discussion and posts digressive messages.

Trolling—online communication which aims to instigate disputes and arguments, provoke, offend, lie and generally introduce chaos into communication.

Biography of the authors

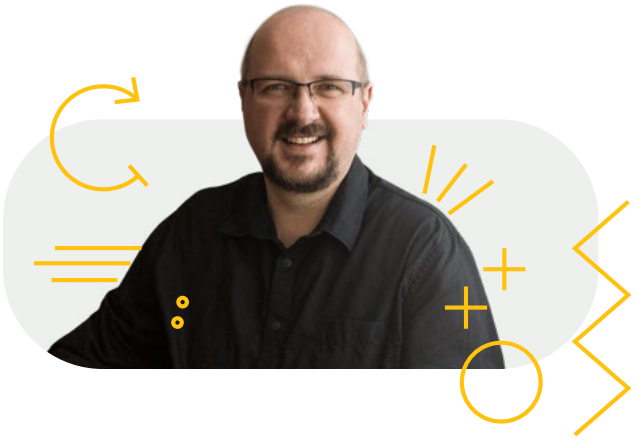
Ondrej Kubovič—Security Awareness Specialist

Ondrej has worked at ESET as a Security Awareness Specialist, which requires him to follow, write about and raise awareness of the latest cybersecurity threats. He's an expert on the subject, he also views many of the risks through the eyes of his two young nieces, who are already a part of today's digital world, via their parents' social media accounts. He is a member of the team that created materials for the project Digital Skills that offers training and information about cybersecurity to Slovak schools. Ondrej hopes thaOndrej hopes that despite all the malicious activity detected by ESET research, we will be able to make children's online experiences enjoyable and, most importantly, safe.



PhDr. Jarmila Tomková—Psychologist

Jarmila is a well-respected psychologist in Slovakia. She has worked at the Research Institute for Child Psychology and Pathopsychology, where she led research teams examining the opportunities and risks of child internet use. She coordinated the Slovak team of EU Kids Online, a multinational research network. She has also worked as a school psychologist, where she designed and implemented several development and preventative programs, such as Students against Bullying. Jarmila continues to work as a consultant for organisations and schools in the prevention of, and intervention in, negative behaviour such as bullying and hate speech. She also founded and leads the civic association ViaSua, dedicated to supporting the mental health and personal growth of individuals, families and society in general. This is achieved by counselling, awareness-raising and the destigmatisation of mental health issues. She considers language and discourse to be crucial and always favours a participative and peer-to-peer approach.



Peter Kučera—Computer Science Teacher

Peter is a computer science teacher at 1. Sukromne Gymnazium v Bratislave (1st Private High School in Bratislava) and the author of several textbooks. He cares about the quality of education on the subject not only at the school where he teaches but in all sections of society. He also gives practical lessons for students in the computer science teaching field of study at the Faculty of Mathematics, Physics and Informatics of Comenius University in Bratislava.

He created a series of textbooks called Creating with Python which include teacher's guides, and implements Python training courses for teachers. Peter founded and leads the Club of Computer Science Teachers, which functions as a platform for sharing experiences and introducing new topics. The community of teachers in the club responds together to current developments in the field of digital technologies and brings new topics and suggestions from professionals for teachers and students.

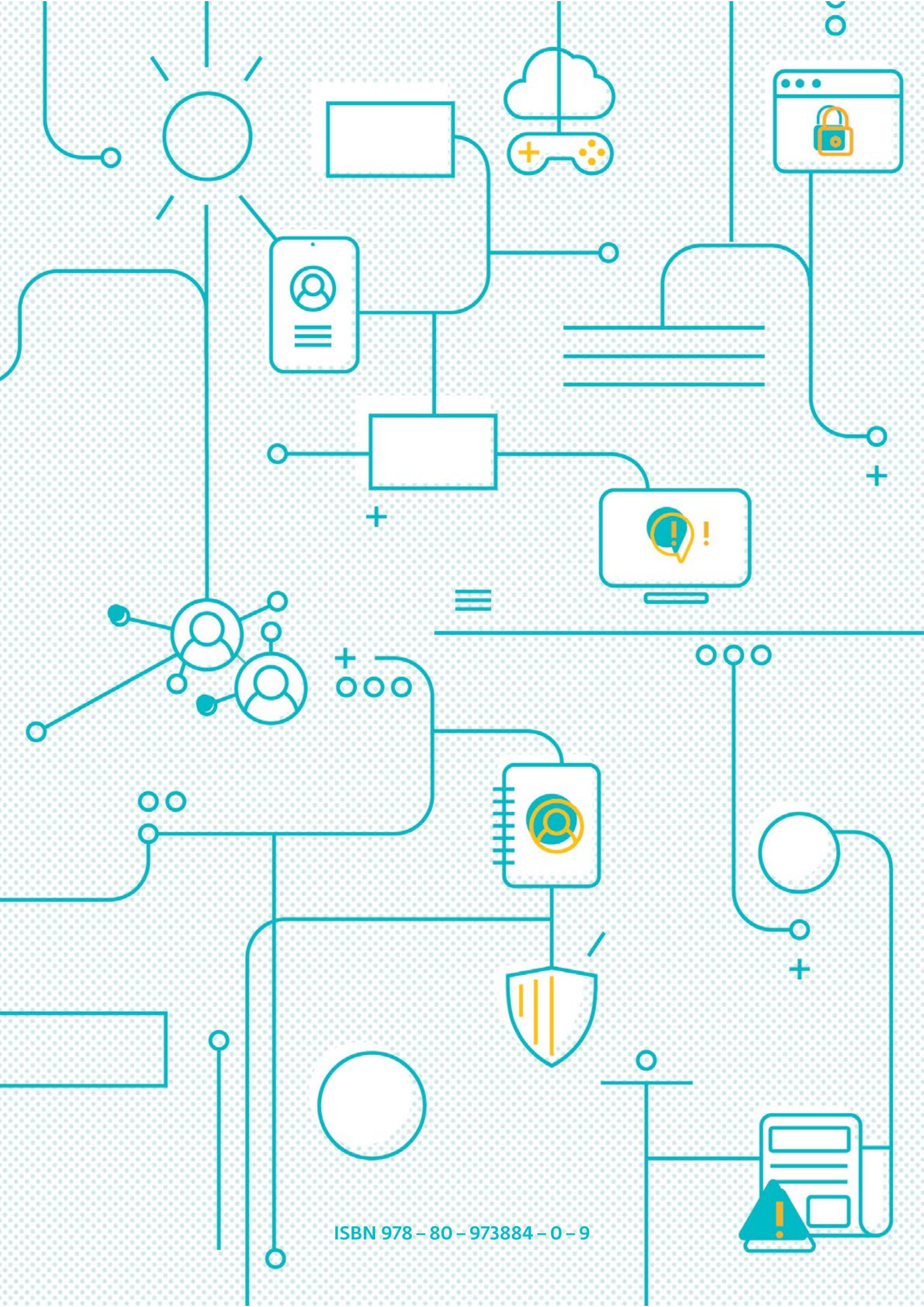
He considers digital security to be a key topic in today's online era. With the rapid development of technology, it is difficult to monitor changes and respond to them with sufficient flexibility. Therefore, it is important to help teachers and students with education and training in this area.

Jakub Daubner—Head of Internal Systems

Jakub enjoyed the natural sciences since his childhood, so he decided to study theoretical computer science and applied computer science. In parallel with his studies, he joined ESET, where he managed to build a department of 45 developers over the course of 10 years. His team focuses mainly on the development of internal tools and automatic systems. The workshop has also produced a detection module based on machine learning and artificial intelligence. In addition, he runs a pupil programming group at a primary school and also collaborates with Ondrej Kubovič on the Digital Skills project, in which they produce educational materials and train teachers.

saferkidsonline by ESET®

ISBN 978 – 80 – 973884 – 0 – 9



ISBN 978 – 80 – 973884 – 0 – 9