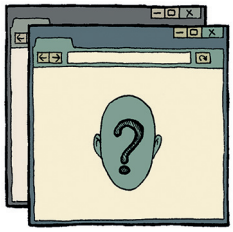
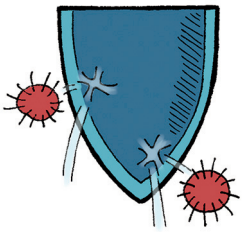
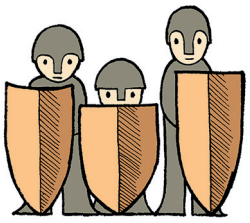


Incognito window



Antivirus

CAPTCHA

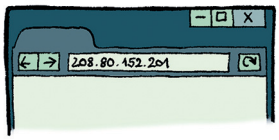


CSIRT

Digital footprint

Grooming

Hacker

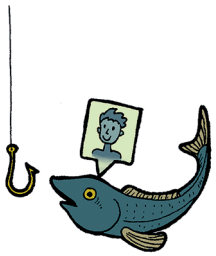


IP address

Cyberbullying

Nomophobia

Security patch



Phishing

Piracy

Ransomware

Router

Chain letter

Pexeso

Number of players: 2 and above
Age of players: 3–99 years

2 × →

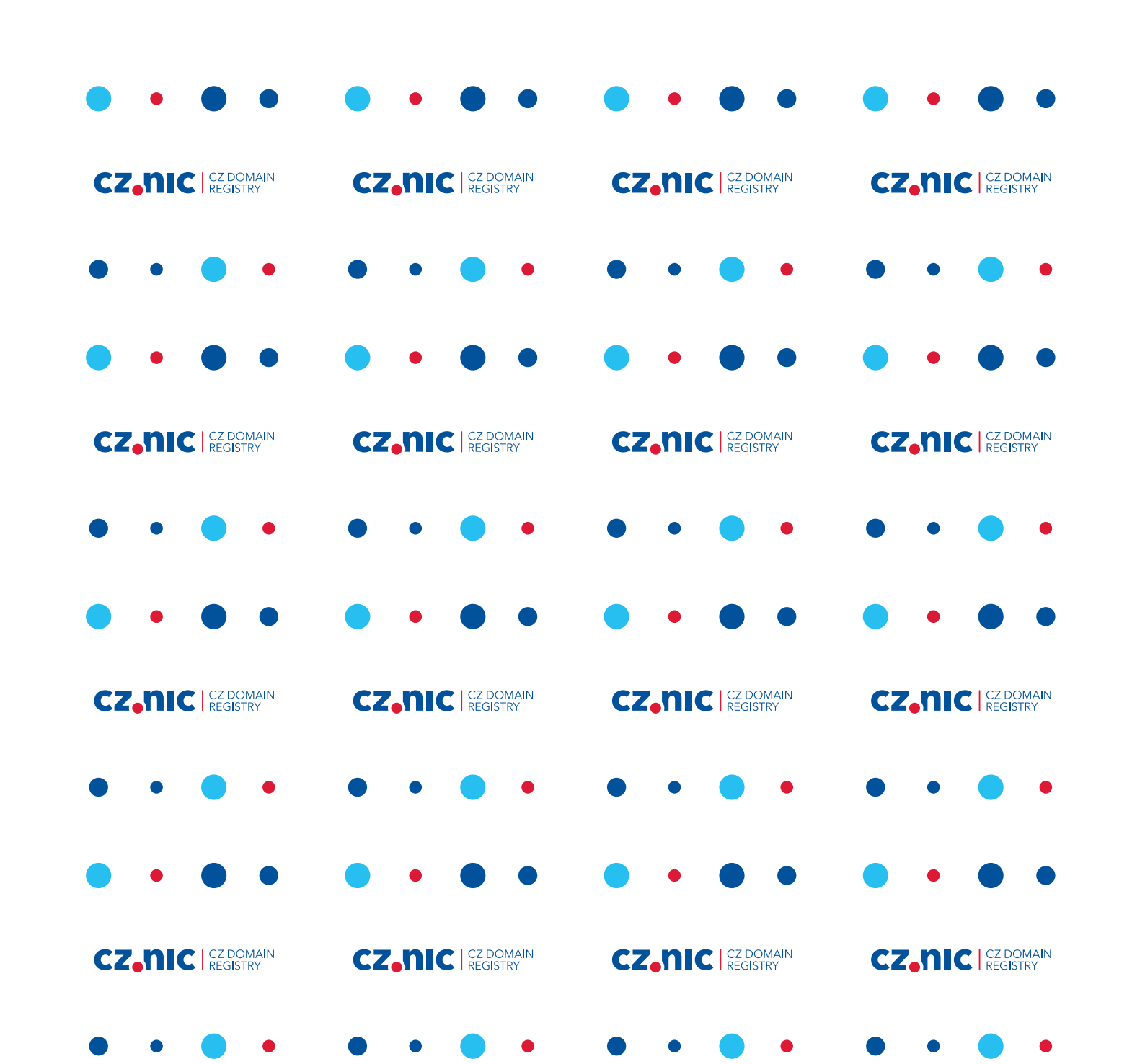
Printing: double sided (duplex)
Scale: actual size (100 %)

Rules of the game:
Mix up the cards and lay them face down so that none of the players know the layout of the cards. The players take turns to turn over a two of the cards face up, for the other players to see them as well. If the two cards match, the player takes them and turns over another pair. If the cards do not match, the player turns them back face down and another player continues. The game ends when all the cards have been matched. The winner is the player with the greatest number of matched pairs.

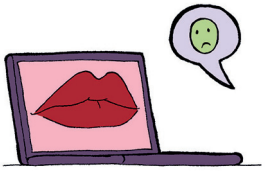
CZ.NIC | CZ DOMAIN REGISTRY

saferinternet.cz

Co-financed by the European Union
Connecting Europe Facility



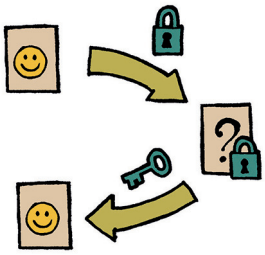
Sharing



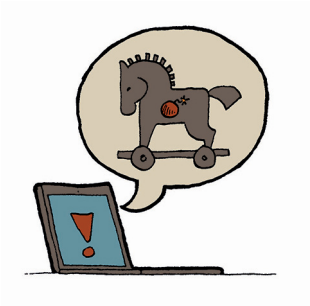
Sexting

Privacy

SPAM

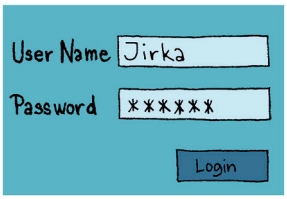


Encryption

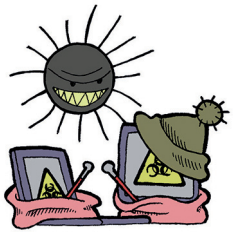


Trojan horse

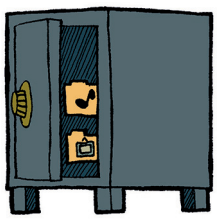
Attack



User name/password



Virus



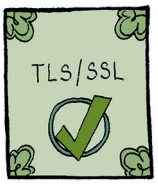
Backup

Zombie

DNSSEC

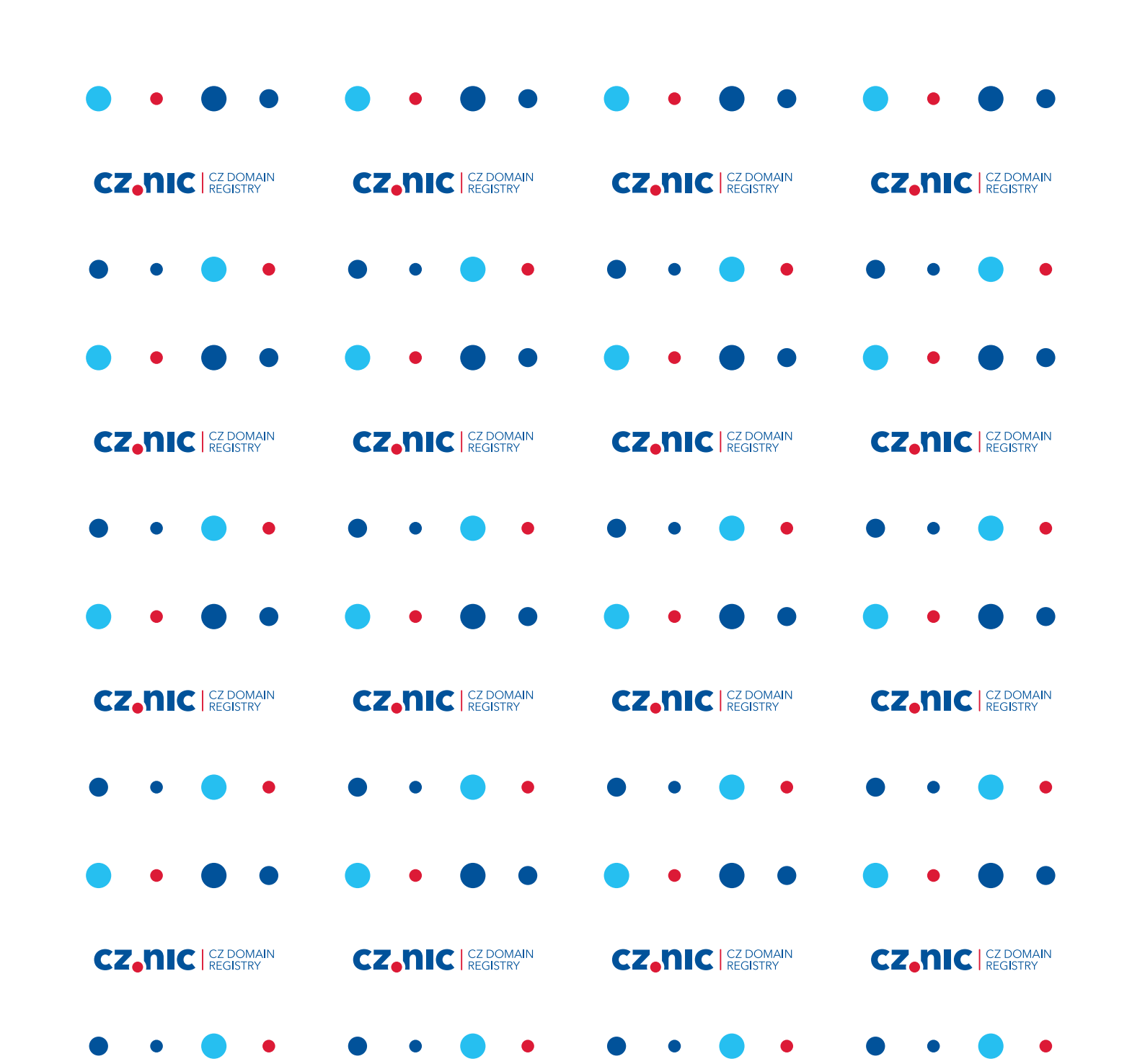
Honeypot

Cybercrime



TLS/SSL certificate

Wi-Fi



Antivirus

Computer programme working similarly to our parents trying to prevent us catching a cold. They may use one of two ways. Either they may take us to the doctor when we start coughing to determine whether we have caught a bug, or they don't let us play with a friend who they know is already sick, to not become infected too. Antivirus programmes work in a similar way. They check our computer to see whether everything is healthy and they try to prevent our PC from catching a bug from another already infected source, e.g. a game we are about to download.

Attack

Just as we regularly go for a check-up at the dentist to see whether our teeth are healthy, we should do similar check-ups with our computers, mobile phones and tablets. The repair would be just as difficult as at a dentist. If we don't install updates regularly and download software from unofficial pages, our PC can be attacked by evil hackers and used for spam forwarding, taking a system out of service, attacking the website of our school in order to steal money from bank accounts and other illegal stuff. It is very important to check the state of our devices, install updates, not to download unverified programmes and to regularly update our antivirus software.

Backup

Backup means saving information from our devices on a safe external device in case somebody starts threatening us to delete all our data (as we described in the information about ransomware). Our PC may also be attacked by a malicious virus or get broken. Online storage is best for backing up not sensitive data, e.g. Crashplan, Mozy, Dropbox, Carbonite and others that continuously upload anything we save into a selected folder, plus we may access our folders from anywhere. The files that contain our secrets should be stored on external discs only.

CAPTCHA

Hackers can create codes that try out various password combinations. These codes are called robots. Robots have many advantages over humans, but one major disadvantage. They cannot identify other than perfectly written letters. Also, they do not know what a tree, a flower or an animal really look like. People know a B is a B even if a tiny bit of it is missing or if it is written askew, they know which picture shows an animal and which is about nature, but robots cannot do that yet. The website owners use CAPTCHA to protect their users from theft of their accounts or themselves from an avalanche of spam.

Chain letter

You must know this. You are reading an interesting story and suddenly it says: "Send the story to other people or you'll be out of luck." The more we react to these stories the more often we receive them. Moreover, completely fake news is spread on the Internet in this way, for example a sick child needing help and little puppies being put to sleep without our help. If the news seems interesting to us, we first need to verify whether it is not a hoax, meaning a fully or partially invented story, which is all over the Internet. If the information is not to be found anywhere else, it is prudent not to forward it.

CSIRT

CSIRT is an acronym indicating a team that is in charge of security, similar to the police. The difference is that the CSIRT staff takes care of security in cyberspace, meaning all the computers and servers connected to the Internet. In case of an incident in cyber world, the team members must determine the cause of the incident and inform other teams whose cyber towns may be endangered, and thus prevent other incidents all over the world. Similar to policemen not standing at each zebra crossing, the CSIRT team members are not at all places all the time, therefore it is necessary to bear in mind it is mainly we ourselves who are responsible for safe movement in cyberspace.

Cyberbullying

If someone cracks our pencils and tears our T-shirt, our parents can immediately recognize it as an act of bullying and we can work on a solution together. When someone bullies us online, our parents often have no means of finding out. We may receive annoying messages on our phone at night and mischievous classmates or unknown people may hurt us via Internet by things like sending us ugly images, forcing us to do something or simply laughing at us. If we cannot find a solution alone and do not want to talk to our parents or teachers, we may ask for help totally anonymously, for example using an incognito window at a school computer, at the onlinehelpline.cz line, which offers help in these situations.

Cybercrime

It is possible to hurt other people with the help of a computer and it happens often that bad news, photos and blackmail makes people sad. PCs enable some people to steal money from other users' accounts. Each act on the Internet that harms others may be called cybercrime. Cybercrime is a behaviour that this Pexeso (memory game) will introduce to you: ransomware, viruses, Trojan horses, sexting, cyberbullying or zombie computers. It is extremely important to fight against this behaviour for example by reporting it on the www.stoponline.cz web pages.

Digital footprint

Every time we post something on the Internet, it is like we created innumerable copies and distributed them to people at an airport. The people then board different planes and fly to different countries. We will never know where the papers end up, who may read them and whether they altered them in any way. If we write our address on each of these papers, complete strangers may knock on our door and demand our attention, because they may think they know us if they received such information about us. Anything we write or add on the Internet via tablet, mobile phone or a computer, we should bear in mind it will never be erased. The information will stay there forever and even the strongest detergent your parents use for cleaning the worst stains won't help.

DNSSEC

To call our mother, we often don't know her phone number by heart. It is sufficient to type "Mum" in the contact list in our mobile, and the phone knows which number our mum has. The DNS works in a similar way. Thanks to the DNS we may type maminka.cz into a browser instead of the number 95.173.213.36. The computer will translate it into a numerical address, called IP address, and will display the requested site. During the time the DNS was created the Internet was a safe place, but with increasing number of users the security decreases. DNSSEC represents a security extension ensuring that when our PC asks what is on the maminka.cz pages, the PC does not display other, fake or infected pages that are on a different IP address.

Encryption

The word code or encryption describes the process of converting a readable text into its unreadable form. Encoded text may be decoded only in case we know the right key. We may encrypt data on a hard drive as well as portable devices, such as flash drive. We can also encode directly our entire communication, such as messages and emails. Another way of encryption is virtual private networks (VPN), which we may think of as a tunnel known only to those who use it. Encryption is used also on web pages. A page with encrypted data transfer is one whose web address starts with https instead of http and the icon of a locked lock is displayed there.

Grooming

Somebody contacts a chosen person via the Internet and after establishing a close relationship online, they will ask to meet

CZ.NIC | CZ DOMAIN REGISTRY
saferinternet.cz
Co-financed by the European Union
Connecting Europe Facility

the contacted person, for example to play computer games or to see some puppies. They may choose various reasons for a meeting. They may feel up their victim, photograph them or try to convince them to support terrorist or other extremist groups or movements, or choose a different form of manipulation with the victim. Always inform your parents, friends or other people before meeting up with someone you know only from the Internet, call them afterwards and tell them about the meeting. Never meet a person you know from social networks at a remote place or at their home.

Hacker

Hacker is often a thief who does not break into homes and banks with a gun, but into computers and servers with a programme. The ways to enter are numerous. Similar to a thief who may open the door with a fake key, enter an apartment via an open window or think up a story for you to invite them in, a hacker may use various ways to enter your PC. They employ viruses, Trojan horses, phishing pages, invented stories mailed in a text message and other modes that are classified as cybercrime. Hackers are not only bad, they may work on the good side as well. A bad hacker is professionally called a cracker.

Honeypot

When bees and wasps bother us so much we cannot even eat ice cream in peace, we may leave a pot with honey close by and thus lure the wasps and bees away. The computer honeypots work similarly. Attackers constantly invent new types of malicious codes and nice people try to protect our computers from them. Immediately after discovering new malicious code a security patch or a new version of applications are created. Honeypots serve to detect these codes and to enable us to watch possible viruses and other malicious codes.

Incognito Window

The possibility to browse the Internet privately, so that the browser does not save information about your search. In case you want to buy a present for your parent's birthday and are concerned about an ad that pops up after searching for goods, you need to click on the menu button in the top right corner (three dots or dashes, depending on which browser you are using) and select "Incognito Window". You can also use the keyboard shortcut Ctrl + Shift + N in Google Chrome and Opera, and Ctrl + Shift + P in Internet Explorer and Mozilla Firefox.

IP address

IP addresses are like phone numbers of our friends. Every person has a different one and we cannot remember them all. These numbers contain several pieces of data, for example which country our friend comes from and which provider is she using. The human memory cannot remember all these numbers and more important information for us is who is calling us and who we want to call. We do not memorise numbers by heart, but save our friends' numbers into our phone memory under their names and nicknames. These names are similar to names of web pages. For computers to recognize where to find the data and information from the requested web page, just as with a phone number they need to know the country, the operator represented by the Internet service provider and the place where the data is stored.

Nomophobia

Some people are addicted to being online on mobile phones. They are nomophobic. People addicted to mobile phones and other devices and are constantly reachable, reply immediately to our text, talk to us as long as we want when we call them and post photos and images on the web all the time. It is great to be online all the time, but these people are not there for their loved ones in the real world. People with this addiction often decline e.g. to visit the most beautiful places on Earth because they are afraid of being offline.

Phishing

The term comes from the English word fishing. The attacker is a fisherman and Internet users are fish. If we desire to eat something we have no experience with, we should first check the unknown food in detail for a hidden hook. In case we are not sure, we should ask somebody more experienced. It is important to always download only the attachments from people you really know and trust. Also we should never enter our passwords on pages that pop up randomly. Always when entering our password on the Internet, we should check whether the address in the browser corresponds to the name of the toy shop where we want to buy gifts for friends charged on our mother's credit card.

Piracy

Most of us think illegal downloading of movies and games is alright. But it isn't. Imagine drawing a picture and having the teacher tell us we can ask for a thousand Euros for it at an art exhibition next week. We are the author authorised to sell our work. Meanwhile a classmate secretly copies the picture and offers it for half the price. When we come to the exhibition, nobody wants our picture because everybody has it already. That is not right. If we don't like it, others won't either. The solution is not to download movies and games other people put online without the author's permission, meaning our permission to copy our picture and offer it to others.

Privacy

Even though it seems nobody can see inside our computer, it is not true. Our emails, photos and other data are stored on various servers where they can be viewed by other people. Protecting our privacy in a PC connected to the Internet is extremely complicated. The more hurdles hackers have to overcome the more difficult it will be to reach our private data. It is important not to save any private things on unknown storage services, to update our devices including routers and to use strong passwords. It is also vital to carefully assess what we say about ourselves on the Internet, because every time we have a public profile anyone can find out where we are, what we are doing or how we feel and can try to use the information.

Ransomware

When we enter the PIN to our mobile phone incorrectly three times, our SIM card is blocked and we have to enter a long complicated number (PUK) to unblock the SIM card. Ransomware is much worse as it can block entry to all our files in the phone, tablet or PC. We may thus lose all our messages, photos and other data. Every time we receive an online money demand or a threat to do something, that otherwise something bad will happen to us, we need to inform our parents immediately, make a screenshot of the threat and report it to the police or at www.stoponline.cz. Never try to pay anything, neither you nor your parents. It is always better to admit going to forbidden pages rather than supporting criminals.

Router

A box which allows us to connect to the Internet on our phone, tablet and PC. If we leave it without any care for a long time, it may get sick, as it is as vulnerable as our computers – which need to be helped with security patches. It is not only us who forget to care for the health of these boxes, but also their manufacturers. It is common that the boxes have holes in them, but there are no patches to be found. These boxes may be full of viruses and infect our mobiles, tablets and computers, which we take good care of. To prevent these infections we need to ask our parents to only buy routers that enable regular updates, for example Turris Omnia.

CZ.NIC | CZ DOMAIN REGISTRY
saferinternet.cz
Co-financed by the European Union
Connecting Europe Facility

Security patch
When you rip a bag, flour starts spilling from it. It goes similarly for computers. If something is "ripped", may start spilling data, meaning our passwords, photos, messages we exchange with friends and other important stuff. When that happens the computer needs a security patch as soon as possible. That means developing part of a programme which fits the space with the hole and is installed there. This process is called update. The patch is placed inside the computer on individual applications including the operating system. For the patch to reach our application as soon as possible, we need to regularly run installing updates.

Sexting
An example of digital footprint being potentially very harmful. Some people send their friends, boyfriends or girlfriends photos in which they are in underwear or even without it. These photos can never be taken back and often are shown to the entire class. Many of those sending the photos do not imagine other people could see them, too. The moment that happens, they may feel so ashamed they won't even ask for help. If you happen to make a similar mistake one day and later are harassed or humiliated for it, it is cyberbullying. Moreover, publishing our photos without our permission is illegal, so there are ways to defend oneself. The best option is to publish online only the things you would be comfortable sharing with your entire class.

Sharing
We often want to share stories of our lives. It is all right in itself, but when we share anything on the Internet, we need to be prepared that people will ask us about it. They may also laugh at us for our posts. If we don't want these situations to happen we need to share such information only with the people we really trust. We can set our posts as private and thus visible only for those we choose to be able to see them. We also may put our photos and files into a folder protected by a password and give the password only to our friends.

SPAM
A pile of useless information we receive via the Internet or text messages and which we do not want to see. We may completely lose orientation in our mail box due to spam and overlook an important message. In order for spam not to overflow us, we need to be careful every time we agree with terms and conditions or grant other approvals on the Internet. It is always important to open the terms and conditions we are about to approve, find the chapter on protection of personal data and check whether it contains a provision about your data not being given to third parties, meaning other people who could use them further.

TLS/SSL certificate
These acronyms are linked to encoding, namely encryption of web pages. You can tell a page with encrypted data transfer by looking at its address, which starts with letters https instead of http. Besides the https protocol ensuring encryption of the data you enter into an Internet form, it also enables verification whether the pages we are on really are those we wanted to go to. The TLS/SSL certificates can ward off various attacks from fishermen trying to catch us on their hooks – phishing pages. Https is also used at all times when a browser and a server exchange sensitive information, e.g. login name and password.

Trojan horse
Trojan horse was a huge wooden horse in the Greek mythology, in which were hidden soldiers about to attack the city of Troy. A similar ruse is used by mischievous people on the Internet. They try to convince us they offer something interesting, useful or a bargain, but when we download it behind the fortification of our PC, deceitful programmes which may open the gates of our computer for new and new evil attackers will download with it. To avoid foolishly downloading a Trojan horse same as the Trojan citizens did, it is necessary to always download things from official Internet pages or marketplaces and not to participate in Internet piracy.

User name/password
User name and password serve the same way as our house keys, and together they are called login. We have a range of valuable information on our accounts and they help us be in contact with our friends. It is necessary to responsibly take care of our accounts, not to be burgled. A password should always contain some letters, some numbers and a special symbol, e.g. an asterisk. It is also necessary not to write the passwords down on paper and to have different passwords for different accounts. It is not necessary to have a long and complicated password for an account where we have only photos with our classmates, as the photos are not secret and even if somebody deletes them, probably one of our classmates can send them again. It is always important to carefully consider what we store on the accounts.

Virus
When we are ill, we are glad to stay in bed, we are too tired to dress, walk or even drink. Computers are the same. When they are infected with a virus, their functions may change. They may be slower or do things we did not order them to do. PC with a virus may infect other computers and thus enable a hacker to attack some large organisations like schools, shops or pages with train timetables. Viruses are also able to send the attackers our login and anything we do on a PC, including our secret messages. To prevent getting infected it is important to install some antivirus software into a phone and a tablet as well.

Wi-Fi
In shopping malls, restaurants and cafés, but also on a bus or a train it is possible to connect to a wireless network, also called Wi-Fi. Public Wi-Fi networks must be as easy to use as possible, because they are intended for large numbers of people and devices. It is thus logical their security is not the best. A skilled hacker can read anything we do on a public Wi-Fi network, which pages we log into and can find out our login name and password. Let's thus be very careful while using public Wi-Fi networks and pay attention to where we login and which data we send to the Internet from a public Wi-Fi.

Zombie
Zombie computer differs from a normal computer by being ruled by an evil power, just like a Zombie in a movie. A hacker with evil intentions uses a virus, a Trojan horse or another way to upload a program into your PC, which may completely take over the PC. That means the attacker may send spam from our PC, use it for distributing Trojan horses, make money from adverts or login to some pages, which will completely overload the server.

CZ.NIC | CZ DOMAIN REGISTRY
saferinternet.cz
Co-financed by the European Union
Connecting Europe Facility