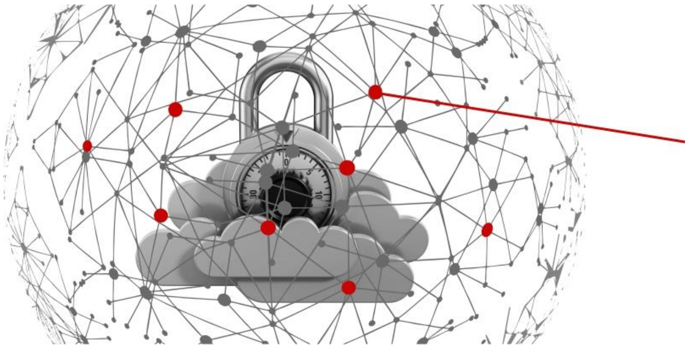
Safety on the Internet



Each year there are millions of crimes committed via the Internet. Cybercriminals use various methods to get access to our bank accounts or data which can facilitate their further illegal actions. It seems that we are just innocent victims of such crimes, however the truth is that we are often partly responsible for what happens to us. Ignoring basic Internet safety rules is like leaving the front door open or the keys in the lock overnight. On the other hand, it takes only small changes in our habits to make it much more difficult (or even impossible) for the cybercriminals to gain access to our personal data.

Currently 4.5 billion people, that is 60% of our planet's population use the Internet. Half of humanity, that is some 4 billion people, use social media and the average time spent on the Internet daily equals 6 hours 43 minutes. That is almost 30% of a day, 100 days a year!

The SARS-COV-2 epidemic, which started at the beginning of 2020, has reinforced this trend. The requirement to avoid personal contact wherever possible has forced many traditional businesses to move online and conduct e-commerce and for us to engage in more online entertainment options.

DATA THAT NEVER SLEEPS!
CLICK HERE

Another factor which has contributed to the process of digitalization is the expansion of mobile devices. At the moment we already spend more than 50% of our time on the Internet using smartphones that we carry with us everywhere. AppAnnie reports show that we spend 10 out of every 11 minutes on our smartphones using mobile applications, such as various communicators, social media, entertainment, video players, games, shopping, banking or music applications, maps and navigations or dating applications. According to the Ericsson Company, Internet users consume 50 billion gigabytes annually with their mobile devices, 60% of which is used on streaming video content.

The figures quoted above may be surprising, although we are aware that while reading this text they are most probably no longer accurate, as the statistics we refer to are constantly and rapidly growing. This process is promoted by powerful corporations and start-ups that produce and distribute devices and software so that as well as an increasing accessibility to the Internet in the world, the users themselves are keen to search unlimited Internet resources every day.

The biggest players in the virtual market, such as Google or Facebook, provide us with services and applications facilitating or in many cases enabling work and communication. They provide entertainment, offer easier access to knowledge, create possibilities to explore and search global scientific resources. We willingly access such possibilities because they are free of charge. But are they really free? Indeed, there are various applications and software that do not need to be paid with cash or a bank transfer. However, this does not mean that they are not paid for at all. The digital world values not only money, it values our data even more, personal data that we share when downloading 'free' software, films, games, surfing

in social media, shopping in virtual shops, information concerning devices that we use, our location and behaviour – both on the Internet and in the real world. Information on our appearance, family, friends, hobbies, activities, job, finances, dreams, plans etc.

CYBERCRIMES IN REAL TIME
CLICK HERE and HERE

At the beginning of the 21st century the very suggestion of placing an identification chip for example in an identification document caused controversy and resistance. It was regarded as an unauthorized interference with privacy and personal dignity. Nowadays, we are ready to voluntarily share much more than just our personal data.

However, there is a positive aspect of such behaviour. Gathering big data bases enables us to gather statistics such as those quoted above. Researchers from around the world can work together and use one another's research results as well as independently developed methods and scientific models.

TOP 5 MOST NOTORIOUS CYBERATTACKS
CLICK HERE

Big data has many benefits for all mankind, but also offers an ocean of possibilities for cyber pirates. Data that is so willingly and frequently sent out into the world, can become the source of serious troubles once it is stolen. Anything can be attacked: passwords to banking systems, private pictures or website login history. Such attacks happen every day and cybercrime statistics prove how serious this problem has become.

Let's see how many cybercrimes were committed in one 24-hour period (as of May 2020):

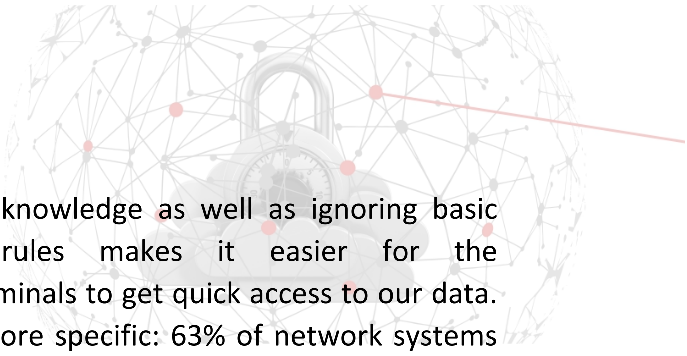
- **about 62.4 million system hackings**
- **hacker attack every 39 seconds**
- **6.4 million false e-mails sent**
- **4 ,739 websites hacked over 100 times**
- **over 1200 complaints on hacking personal computers in the USA alone**

Reports and statistics also show that within a 3-month period last year 232,292 individual users were infected by malware. At the same time, there were 260,000 successful phishing attacks by those masquerading as trusted entities. Losing data leads to consequences of both a social and economic nature. Ransomware (blocking access to the computer unless a ransom is paid) resulted in financial losses of 3.5 billion dollars last year. In 2019 there were 52.7 million attacks on cryptocurrency.

Why are there so many attacks on personal data? There are certainly cybercriminals to be blamed as they are interested in stealing our data and they constantly improve their hacking abilities. They use innovative methods in order to get access to Internet users and their devices in order to steal the information they need. Unfortunately, the increasing number of cybercrimes doesn't appear to have resulted in increased awareness of such dangers and the ability to prevent them.

HOW SECURE IS YOUR PASSWORD?
CLICK HERE

PASSWORD MANAGER PROTECTS YOUR DATA
CLICK HERE



Lack of knowledge as well as ignoring basic safety rules makes it easier for the cybercriminals to get quick access to our data. To be more specific: 63% of network systems hacking happens as a result of the breaking of passwords and usernames, which is due to the fact that most of the passwords are simple combinations of signs. We are often not aware of how easy it is to find our data and use it for illegal or undesirable purposes. Personal information that we willingly share with social media users can be easily captured by hackers. In 2019 some 849 million personal data leaks via one popular social media service only (Facebook) were noted.

We present the Internet safety rules below. By following them we can protect ourselves and our data against cybercriminal attacks.

How to use the Internet safely?

1. ALWAYS CHOOSE STRONG PASSWORDS.

Password containing your name, date of birth, login or anything that easily associates with you is neither good, nor strong. Strong passwords combine small and capital letters, numbers and special characters. How can we make our password stronger in just few seconds? If our password is 'ersmusproject2020' we can simply add some capital letters and special characters: 'Er@mu_pro!ect_2020'.

2. DO NOT SAVE PASSWORDS AUTOMATICALLY.

Remember that you should choose different passwords for each account -no repetitions are acceptable. Do not save the passwords automatically. Have you created a strong password and are you afraid of forgetting it? Password manager software can help you to manage your multiple passwords and log-in data. It is a safe storage place, where you can keep all the keys to your digital life..

3. ALWAYS VERIFY A SENDER.

A phishing attack is based on disguising oneself as a trustworthy entity, that is why you should always pay attention to the address of a sender and never open links before checking (the address can be checked by hovering a mouse cursor over a link). Check carefully if the letters are in the correct order and the sender's domain – a sender disguising themselves as a service provider would use a different country code from a top-level domain or simply create a new, fake one.

4. MAKE SURE YOU UNDERSTAND THE MESSAGE AND DO NOT REACT EMOTIONALLY.

Phishing attackers try to manipulate their victims' emotions. Remember: your e-mail address cannot be deactivated overnight, neither can your bank account nor telephone number be instantly blocked. How can you recognize a false message? Pay attention to the grammatical and syntactic correctness, rearranged letters and the time you are given to react – cybercriminals often expect you to act immediately otherwise the consequences will be enacted (eg. you bank account will be blocked). They do not ask – they make demands.

5. DO NOT PLACE PICTURES OR SCANS OF YOUR DOCUMENTS IN THE INTERNET.

Cybercriminals will be able to capture your scanned ID personal data and take out a loan on your behalf, leaving you paying it off for years.

6. KEEP YOUR PRIVACY SETTINGS ON WHILE USING SOCIAL MEDIA.

Do not share too much personal information with social media users, remember that everything which appears on the Internet stays there forever. Think twice before putting any information on the Internet.

7. ENCRYPT DATA.

EFFICIENT DATA ENCRYPTION
CLICK HERE!

You can make it difficult or even impossible for a cybercriminal to read your data even if he manages to steal it. You can encrypt your devices (hard drive, pendrive, and all types of data carriers), your files, as well as your e-mails.

8. CREATE BACK-UP COPIES.

In order not to lose important information, create back-up copies regularly. You can use external and internal media and network location. For further information see: https://support.microsoft.com/pl-pl/help/971759/how-to-back-up-or-transfer-your-data-on-a-windows-based-computer .

9. DO NOT CONNECT TO PUBLIC WI-FI.

Connecting to an unsecured, public Wi-Fi hotspot is very risky. If it seems unavoidable, remember some basic safety rules: turn off data sharing, avoid automatic connection to the Wi-Fi network, use VPN, turn on firewall. For more detailed information on how to avoid an attack while connecting to public Wi-Fi please check https://www.binance.vision/pl/security/why-public-wifi-is-insecure .

10. BEFORE YOU LOG IN TO YOUR BANK CHECK FOR A CLOSED PADLOCK ICON.

On the left side of the search bar there is a padlock icon. You can click it to display web-page details. There you can check if it is safe and has SSL certificate (it encrypts the data that is being transmitted). If yes – there is no need to worry, the transmitted data cannot be used by unauthorized persons. Remember: the padlock must be closed, if it is open, the site is unprotected.

11. DO NOT DOWNLOAD FILES FROM A SITE YOU DO NOT TRUST.

Always download free software from the producer’s website. If you download an application from the site that you do not trust, there is a risk of installing a malware too.

12. READ TWICE BEFORE ACCEPTING ANYTHING ON THE INTERNET.

Careless reading often leads to unconscious sharing of your personal data with unauthorized people or signing a contract which you do not really want to sign. The number of spam messages in your post-box results from accepting automatically all optional points in different regulations and agreements. Remember that while accepting server or website regulations, only obligatory fields must be checked. If you read without paying close attention to detail, you also risk paying money to the frauds, who try to convince you that by having registered with a certain website, you will have a chance to win a new iPhone.

These 12 simple rules of how to use the Internet safely are not difficult to follow. However, we often break many of them. We tend to use the same password or allow it to be remembered automatically. We often accept regulations without even skimming them – looking forward to downloading an application, completing a purchase or creating a new account. To feel more secure on the Internet we need to give up our old, bad habits and adopt new ones. Here is how Brian Tracy, guru of personal development and a motivational speaker, describes such a process:

Good habits are the source of your success and happiness, while analogically bad habits are responsible for most of your problems and failures. However, bad habits are also learned and therefore they can be unlearned and replaced by the good ones (B. Tracy: Million Dollar Habits).

Changing one's old habits is never easy, but it is certainly worth the effort.