All organizations that dispose of your personal data in accordance with the General Data Protection Regulation (Articles 24, 25 and 35) are obliged to take all appropriate technical and organizational measures in order to adequately protect the personal data of their employees, users, clients, in short individuals (respondents) and reduce the risk of personal data violations and misuse to a minimum.

Organizations that do not do so are exposed to serious consequences: reputational risk and high fines.

However, there are situations in which, even with all security measures taken, an attacker manages to take advantage of system vulnerabilities and gain access to your personal data.

What to do in such a case?

In cases where your personal data, such as name and surname, phone number, email, OIB, fall into the hands of criminals, you should pay special attention to the e-mails and messages you will receive, because there is a high possibility that the attacker will try to reach others as well. personal data, such as your bank card data.

After security incidents in which personal data become available to people with unknown intentions, an increase in Internet fraud such as phishing is expected. Phishing refers to Internet scams in the form of fake e-mail messages that appear to be sent by legitimate organizations (for example, a bank or online shopping site) and that trick the recipient into sharing personal, financial, or security information. In this way, fraudsters gain access to usernames, passwords or credit card information. In such emails, you are most often asked to download an attached document or click on a link.

WARNING! Do not reply to a suspicious email or open an attachment! Do not click on the link, but type the address in the browser! Do not respond to messages in which someone asks you to send them a bank pin, password or other strictly confidential personal information!

There is a whole series of internet frauds that you can find out about in Europol's information brochure:

https://www.europol.europa.eu/sites/default/files/documents/hr.pdf and on the Ministry of Interior's Fraud and computer security channel

https://m.youtube.com/playlist?list=PLVevEdFcQ-rPA5Br9TmosEMV6gZEiU75w

We also recommend changing passwords for all internet services you use.

On the link https://haveibeenpwned.com/ "Have I Been Pwned" check ALL your e-mail addresses that you use as a username to log into internet services or services, in this way you can check if they are compromised or if they are in hacker's bases.

If you find that a certain e-mail address has been compromised, we recommend the following:

– change the password for that email address to a new strong security password

– in all internet services and services where you used that email address as a login username (eg social networks, online store, etc.) create a new separate strong security password for each of those services and services. If that internet service or service offers this possibility, it would be advisable to include the double authentication option.

Cyber hygiene is basic security protection, both for individuals and for organizations (managers and processors). By this term, we mean security practices that include all internet users and services, applications and devices with the aim of protecting, security and integrity of personal data and preventing cyberattacks. Cyber (digital) hygiene includes knowledge about the effective application of security solutions, making backup copies, avoiding electronic violence, detecting fake news and concerns all stakeholders in society: from governments and states, directors of small, medium and large companies, employees to the average internet user and children. In today's digital age, cyber hygiene should be part of the value system of all individuals, organizations, small businesses and large companies.

Self-protection in the first place!

Processors/executors of processing (organizations, companies) are obliged to protect your personal data and dispose of them in accordance with regulations on personal data protection, but you should take the first and most important step in protecting your personal data yourself.

This primarily means that you should be careful about who you give your personal data to and why. A large number of cases of misuse of personal data occur due to the carelessness of citizens when disposing of their own personal data. With careful and conscientious behavior, we can reduce the chance of becoming victims of malicious individuals.

Namely, it is less likely that your personal data will be misused if you know who you are giving it to and why. The employer, the bank of which you are a client, service providers when concluding a contract, in accordance with legal regulations, may ask you to inspect your identity card, OIB, make a copy of your identity card or ask you for some other personal information.

The greater the amount of personal data that someone requests from you via the Internet (for example, a complete copy of an ID card), the greater the possibility of illegal publication of personal data, identity theft, conclusion of false subscription contracts and other misuse of personal data.

In situations where you provide personal data to unknown persons, dispose of them irresponsibly and unconscionably, do not inform yourself about the purpose and reason why and to whom you give them, it is completely uncertain for what purpose they will be (mis)used! WHEN SOMETHING SOUNDS TOO GOOD TO BE TRUE, IT IS MOST LIKELY A LIE! For example, you received an e-mail or a message on a social network that you are the winner of a lottery. All you need to do is provide a copy of your ID, and there have been cases where scammers have even asked for a photo of the person with their ID. Such messages are always an alarm bell and you should never reply to such messages and send your personal information.