Cyber Security and Social Engineering

Barbora Kotkova
Tomas Bata University in Zlín
Zlin, Czech Republic
b_kotkova@utb.cz

Martin Hromada
Tomas Bata University in Zlín
Zlin, Czech Republic
hromada@utb.cz

Abstract— **Nowadays, it is quite common to use modern information technology at work, at school and in private life. Shared information can be used not only for advertising and statistics purposes. Low levels of awareness, inattention and trust can lead to the misuse of this information, using computers and smart mobile devices using the Internet. This article aims to summarize in the introduction the most common methods used to misuse information and what user behavior leads to this. Furthermore, the article then describes the purpose for which this information is misused. The conclusion then describes the methods of protection. It is necessary to constantly draw attention to this issue so that users themselves focus on information security in the environment of information and communication technologies.**

Keywords— social engineering, scamming, cyber-security, sensitive personal information, cyber attack, hazard, defense, data abuse

I. Introduction

Modern technology is one aspect of everyday life and simplifies its basic components, such as managing funds through internet banking, the ability to shop through e-shops, we can work from home or watch documentaries, movies, and series. However, there is also the disadvantage of the benefits of information and communication technologies. It consists of its negative phenomenon, the so-called computer crime. Because information systems are not perfect, they often become the target of attacks from the outside. However, these attacks are illegal and are criminal in most countries. [1] Anyone in the world has access to the Internet from anyone who has a computer or mobile device. That is, even those who intend to misuse shared information from the Internet to their advantage.

People underestimate the power of the Internet and post information, photographs, and data on social networks that so-called cyber criminals use for their fraudulent practices. Most of them are intelligent people who collect published information. These are later, at the right opportunity, abused and able to blackmail their victims. They are able to obtain access data to internet banking, access your online wallet with cryptocurrencies, the institutions in which it operates, and steal data from research or patents. Public authorities, local authorities, hospitals, schools, power plants, and petrol stations also cooperate via the Internet. An attack on these institutions can cause not only the leakage of classified information and personal data but also the cessation of electricity and gas supplies, which would already have an impact on the general public.

Attackers use a variety of methods, some of which require extensive technical knowledge, but also psychology, sociology, marketing, and more. Must have a good command of programming, planning, and preparation of attacks. In addition, they must also be able to manipulate people, some attacks are so sophisticated that they make a person who knows the area insecure.

This article serves for a general understanding of the issue, which is a well-known topic, but neglected. Most institutions, companies, and authorities are already spending some money on software security. However, the prevention of the weakest link, the human factor, is neglected. the users themselves then stick to the established security of passwords. however, they are not sufficiently secure, weak, or reused. She does not inform herself about the style of attacks on her own, they most often learn about them from newspaper articles if the attack is carried out on one of the important targets. Therefore, the article provides an overview of the most commonly used scammer techniques of social engineers. Some of them target software exploits or hardware, others take advantage of users' ignorance, and it is these that the article focuses on. Practical studies and graphs of individual research companies are mentioned, which performed an analysis of the frequency of cyber threats and attacks. The following is a list of possible approaches used. In particular, techniques applicable to a larger number of people in a short time are listed. The following are simple measures applicable to the cybersecurity of the general public on which these attacks are primarily aimed. These conclude with several practical methods of protection against these fraudulent attempts to obtain information, evaluate their effectiveness and possible advantages and disadvantages. Users who use at least one of them, preferably a combination thereof, will make it difficult for potential attackers to obtain and misuse their sensitive information. In addition to organized crime and drug distribution, cybercrime is currently ranked among the most serious forms of crime. It causes enormous damage of all kinds and is also a form of crime that is developing and improving very quickly. Attacks are carried out against the computer systems themselves, their parts, or against stored or transmitted data. [2] Therefore, this illegal activity, together with prevention and sanctions, has recently become the subject of intergovernmental negotiations and conventions. [3]

II. Cyber Criminality

Today, the vast majority of users store their private data on their computers or mobile devices. The reason is their direct acquisition with these devices or memory requirements for the necessary storage space. If the user's privacy comes first, this PC is password protected and not connected to any network. By simply connecting to the network and browsing the website, the Internet user provides data identifying directly his computer in this network (IP address, cookies, etc.) [4]

The user's perception of privacy has been shifting in recent years. People share their personal and private information primarily through websites and social networks. Here it does so in a fun way and interacts with other users. Users also often enter into unverified contracts. They also provide consent to the handling of their data without being acquainted with the

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

content of all approved documents. However, if the potential user does not agree with the agreement on the handling of personal data (or other points of the contract), he has no choice but not to use specific Internet services. [5]

Most people still live in the belief that most of the services available on the Internet are free and are paid for, for example, by advertising placed on these sites. However, they pay for several services to providers by providing some selected personal data. Every time you use the Internet, people leave traces and valuable information here. These relate to the type of site they visit, the devices they use to do so, the places they are currently located, and many other pieces of information. Based on this information, the web search engine then displays the results that are most interesting for the user. This information is also used to display and send customized ads to users. Such use of personal data for marketing purposes is the most common way of their commercial use. 6 This is not a cyber-attack or other criminal activity. [6]

A cyberattack, on the other hand, is an operation that uses a computer network to interrupt, degrade, suppress, or destroy information on computers or computer networks.36 It is an illegal act by an attacker from cyberspace that is directed against the interests of another person. This conduct does not always have to be a criminal offense, it must disrupt the victim's normal life.37 Cybercrime is therefore either directed directly against the computer, its hardware, software and networks bank fraud, industrial espionage, etc.), or the computer acts as a tool for committing a crime, or the computer network connected to the device are the environment in which such activity takes place. [7]

Computer science and technology are constantly evolving and several new types of computer attacks are being added, as well as the improvement of the technology of the existing ones.

Cybercrime can be divided into three parts according to the target of the attack:

- functionality of PC systems and electronic communication. The subject of the attacks is the functionality of computer systems and taking control of them, as well as the means of electronic communications. An attacker is trying to gain unrestricted access to these systems. Then it has full control over the system (Cybersquatting, Defacement, DoS, DDoS and DRDoS, Nigerian spam, Pharming crimeware, Phishing, Ransomware).
- content of PC systems and message transmission. Attack on the content of computer systems and messaging. This information is secretly recorded and sent to the attacker for further use. Various scanning programs, viruses, and other malicious software are used. This software is often offered for free as part of the installation of other programs. In this way, data for internet banking are obtained, as well as photographs and stored documents (Adware, Backdoor, Carding and skimming, Cracking, Hacking, Keylogger, Logical bombs, Man in the Middle, Phreaking, Spoofing Spyware and Trojan horse).
- dissemination of information and the human psyche. Frequent use of mobile phones is the cause of minimizing personal communication, which thus replaces online communication. This is directly related to the sending of various sensitive content in the form of text and photos. These are different types of general crimes (Hoax, Cybergrooming, Cyberstalking, Happy slapping, Cyberbullying). [8]

A fundamental problem in detecting evidence of criminal activity in connection with electronic media is the connection of a natural person with a given hardware device. Traces of activity are identified and recorded, not the identity of the perpetrator. Thus, the confession of the perpetrator remains the most reliable evidence of infringement in the virtual space. Another complication is that cybercrime knows no state borders. Some cyber activities are assessed differently in different countries, and what is considered criminal in the Czech Republic may not be elsewhere. [9] Last but not least, the dynamic development of modern information technologies is a problem. It may be that perpetrators of cybercrime are often more knowledgeable than criminal investigators investigating these acts. At the same time, the typology of perpetrators of this crime differs significantly from the current typology of crime. Internet offenders are not connected to other criminal elements. They are more of students or computer professionals and are unlikely to commit other crimes. Last but not least, the legislation is not able to respond with the necessary speed to technological progress in the field of information technology.

III. SOCIAL ENGINEERING

Social engineering can be defined as an attempt that can be successful or unsuccessful and is intended to influence a person to divulge information or act in a way that would, in turn, lead to unauthorized access, unauthorized use, unauthorized access to data, the network or the information system. If this attempt is successful, it is also a prerequisite for the success of the subsequent cyber attack. Social engineering is therefore a technique for influencing, persuading, or manipulating people, the aim of which is to perform a certain required action or to obtain information that the person concerned would not otherwise provide. Thus, the main intention is not to use technical approaches and tools to steal the password but to mislead the victim and reveal the password itself. [10]

Abusing human ignorance is always easier than penetrating a foreign system and also requires less technical knowledge. The weakest link in the security system is usually the lay user. Common features of social engineering, therefore, include influencing and manipulating a person who owns or has access to the required information. This is information related to information technology. The attack is usually preceded by a longer-term contact between the attacker and his victim, so building a victim's trust is also an important aspect. In the vast majority of cases, the attacker never comes into personal contact with him, however, by appropriately asking questions, he maps the victim's daily cycle and can adapt his actions to him with the intention of further building a sense of belonging.

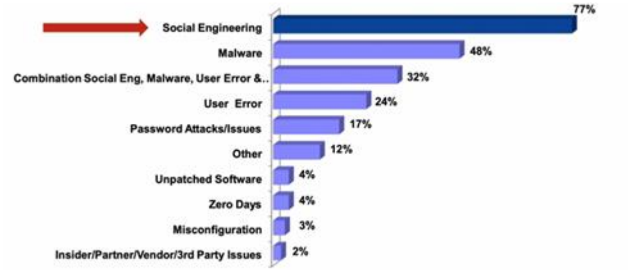


Figure 1. The main causes of network attacks that occurred during 2018 [12]

Social engineers use several types of attacks or combine them. The target can be a random victim, or a victim carefully identified. The criteria according to which the victims are selected are predetermined for selection. These can be age, gender, residence, education, and more. We currently recognize the following types of attacks:

1) *Random attacks*

A large number of users are reached without more precise targeting. This type of attack is, for example, spam. These are various offers, advertisements, e-mail messages of a personal nature (these can be written in a very bad language form to increase authenticity). They can contain an interesting story or a link to an event that is being watched en masse and current. The motive is to obtain passwords, sensitive data, bank PINs, or a payment card number. Operators are now able to block and neutralize a large number of these attacks, but some of them will still be received by users. Users should not open these messages or click on the included links. If such an email is replied to, it is a sign to the attacker that the email is real and used. Therefore, he will target another of his fraudulent emails in the future. The solution is to mark this email as spam and check the filter settings in the email. The basic technique used to filter emails includes, for example, Bayesian analysis. Its principle is that it checks the frequency of occurrence of words, which increases the probability that the incoming message is spam. It has a very good score of recognizing spam from harmless messages and it is possible to adapt it to the requirements of individual users. The more precisely the user marks a bad message from the very beginning as spam, the more this filter is improved and learns to recognize incoming spam.

Bayes' theorem:

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} = \frac{P(B|A)\,P(A)}{P(B|A)\,P(A) + P(B|\neg A)\,P(\neg A)}$$

P (A | B) - the probability that if the search word occurs here, the message is spam

P (B) - the overall probability that the message is spam

P (B | A) - the probability that the search word is contained in a message that is spam

P (¬A) - the total probability that the message is not spam

P (B | ¬A) - the probability that the search word will appear in a message that is not spam

Statistics show that the probability that the specified message is spam is 80%. [11]

2) *Selected attacks*

This type of attack is aimed at a profiled group of users with an already specific target. This uses information that victims have shared on social networks in the past and therefore usually does not affect. It can be the same residence, school studied, children or interests. It is often possible to encounter false profiles created, containing identical activities with the activities of selected victims. A relatively precise range of interests can be found, for example, from published photographs. He tries to attract attention with a targeted offer or an inquisitive question. Offers often associated with sexual overtones or money also appear.

The goal is to entice users to open a suggested link or attachment that contains malware. Detecting this type of attack is not as easy as spam. Users of the social network Facebook and LinkedIn have been facing this problem for several years. Registered profiles are usually visible here and provide a lot of information. People looking for work are an easy target for an attack, just address them with an interesting job offer. Social engineers, which can be easily identified, are often blocked by service administrators, the more sophisticated ones can only be recognized by an expert in the field.

3) *Targeted attacks*

These attacks are targeted at a specific person with a specific target. Here, a more thorough knowledge of the victim and the environment in which he moves is needed for success. Often this attack is carried out by a person from the immediate area or according to a very detailed selection. The aim is to illegally enrich the victim's property, whether by stealing access to a bank account or movable property. These can also be well-identified according to the social networks and details published on them by the victim himself. For example, holiday photos are a good indicator of the fact that the victim is currently away from home and there is no danger of her coming as a surprise. It also indicates that the act will not be detected shortly. In addition, footage of the house may reveal the existence or non-existence of security devices. [13]

IV. SOCIAL ENGENEERING ATTACKS IN 2012-2021

The Computer Security Incident Response Team has been operating in the Czech Republic since 1 January 2011 - CSIRT.CZ. Since 1 January 2015, he has also been in charge of the function of the National CERT (Computer Emergency Response Team) according to Section 17 of Act No. 181/2014 Coll., On Cyber Security 12. Both teams are operated by the CZ.NIC Association and announce the provision of services in cybersecurity. The incident handling and incident-response service is the basic service provided by CERT / CSIRTs. In the case of CSIRT.CZ is about solving and coordinating the solution of security incidents. These have their origin or destination in networks operated in the Czech Republic or affect its cyberspace.

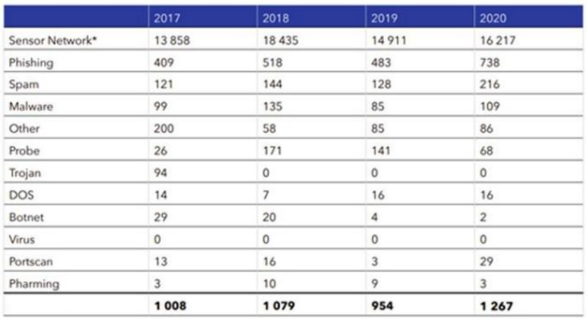
Incidents and events of the following types are reported to the CSIRT.CZ team:

- problems for which all known solutions have been exhausted but the problem persists,
- problems for which it is not easy to identify who is causing the incident or who should deal with it,
- problems that have a serious impact on infrastructure in the Czech Republic. These problems can be widespread and negatively affect other networks, services, and users, so information of this type must reach as quickly as possible those who can intervene and set, for example, appropriate methods of defense, etc.
- problems of large-scale scope, for example, computers in the botnet, devices with specific vulnerabilities, simply put, information from foreign partners concerning several networks in the Czech Republic.

On its website, CSIRT.CZ publishes the most important information about current attacks and discovered vulnerabilities for rapid dissemination. It is a sought-after source of reliable security information, not only for administrators and users. This information is also drawn by the public media, thanks to which information about new attacks is quickly spread to other potential victims, especially users. In 2020, the project Provision of Penetration Testing Services was launched, which expanded the agenda and tasks of the National Security Team CSIRT.CZ to the area of prevention. Their competence also includes the implementation of awareness-raising and training activities in the field of cybersecurity.

Incident statistics in 2020

The annual report on statistics of resolved incidents CSIRT.CZ states that a total of 1,267 incidents were resolved in the Czech Republic in 2020. This is a significant year-on-year increase not only compared to the previous year, when 954 incidents were resolved but with all previous years. This is the highest registered number of registered and resolved incidents so far. The total number of responses to incidents also increased - 17,423 were registered, which is 3,540 more than in 2019. The reason is the complexity of attacks, botnets, vulnerable devices, and compromised accounts.



	2017	2018	2019	2020
Sensor Network*	13 858	18 435	14 911	16 217
Phishing	409	518	483	738
Spam	121	144	128	216
Malware	99	135	85	109
Other	200	58	85	86
Probe	26	171	141	68
Trojan	94	0	0	0
DOS	14	7	16	16
Botnet	29	20	4	2
Virus	0	0	0	0
Portscan	13	16	3	29
Pharming	3	10	9	3
	1 008	**1 079**	**954**	**1 267**

Figure 2. Statistics of the process of solved security incidents CSIRT.CZ [14]

As can be seen from the table above, in 2020 there was a significant increase in phishing. Already in June, the number of incidents in the phishing category in previous years was exceeded. There was also an increase in the number of incidents in the category of spam, malware - especially ransomware, portscan. On the contrary, there was a decrease in incidents in the remaining categories. Graph No. 1 below shows the distribution of individual incidents according to the techniques used. It is clear that the most used techniques are phising and spam, which are the two most unused scammer techniques of fraud in the Czech Internet.

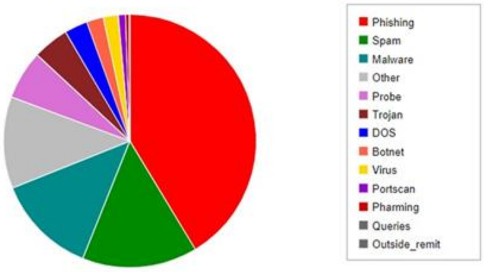


Figure 3. Total number of incidents broken down by techniques used [15]

The increase in incidents in these categories is related to the pandemic and the Covid-19 crisis. This Covid-19 pandemic naturally brought and artificially created several stimuli and currently widely monitored topics. These began to be exploited by attackers for all types of attacks. To keep the company running, at least in part, they moved employees from offices to home. This forced relocation of employees in need of access to the corporate environment has, of course, led to an increase in open ports. From a cybersecurity perspective, this solution poses major threats. The response from the attackers was therefore entirely commensurate with the increase in incidents.

Part of the solution of security incidents is also cooperation with other security teams within the scope of the Czech Republic, as well as international ones. There is also significant cooperation with the state administration and the Police of the Czech Republic on dozens of incidents - mostly abroad. The solution of security incidents also includes cooperation with a specialized workplace of the Parliament of the Czech Republic. In 2020, the CSIRT.CZ team played the role of a mediator for cooperation between the Police and members of the Fénix project in solving attacks on hospitals that took place in the spring of 2020.

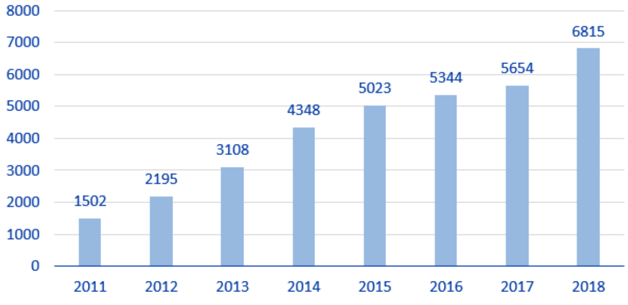


Figure 4. According to the findings of the Police of the Czech Republic, cybercrime committed on the Internet [16]

The most common registered fraudulent activities addressed in 2020 in cooperation with the Police include:

- fake e-shops
- fraudulent sites offering investments in virtual currencies
- fraudulent advertisements, especially on the social network Facebook
- fake aspects (for example, an attempt to lure funds by a US soldier on a mission in Afghanistan). [14]

V. PRINCIPLES OF PROTECTION AGAINST CYBER ATTACK

The best protection against an attack, not just a cyber attack, is prevention. The following chapter provides practical recommendations that every user should master. If these policies are followed, the chance that an attack attempt will succeed will be maximized. Attackers are usually very intelligent people who carry out an attack successfully despite following all the principles. However, it is very good to make this attack as difficult as possible for them and thus discourage them, or at least minimize possible damage. Each user also has at his disposal the NÚKIB (National Office for Cyber and Information Security) manual, which is the leading organization in the field of cybersecurity in the Czech Republic. [17]

Security of computer and mobile devices:

- Use a strong password, numeric code, fingerprint, or other available security methods to prevent misuse of the device in the event of theft.
- Never store marked credentials near the device.
- When entering login details, check your surroundings so that the details cannot be seen.
- Lock the device even when leaving it for a short time. When leaving for a longer period, close all applications and services that you need to log in to e-mail, social networks, internet banking, etc.
- Updated software to install new security measures that developers have added after a series of attacks.
- Use antivirus software.
- When using an unsecured wifi network, use VPN (virtual private network) services. It can secure ongoing communication on an unsecured network using data encryption.
- The user should encrypt his sensitive data on portable devices using available technologies.
- If you connect an unknown storage medium to your device, you need to perform a virus scan of the media.
- Prefer web pages with https security when navigating in the browser. This security is indicated by the lock logo next to the address bar.
- Do not use URLs that redirect to another unauthenticated page.
- Disable associated operating system services that monitor your location, send diagnostic data, or provide remote access to the device, and so on.

Principles of secure communication in the online environment:

- Do not disclose personal and other sensitive information about yourself, family, friends, and co-workers.
- Do not create photos and videos that can be stolen and subsequently misused to the detriment of the user.
- Verify the identity of the counterpart when communicating through information and communication technologies. If it is not possible to verify the identity of the counterparty, make a new contact from a verified number or official account.
- Do not open an attachment to a suspicious email, as this may be a phishing or other attack. If this happens, a notification to the relevant IT department should follow. Applies to any suspicious attachment, incoming to work, or private email.
- Paid services or products that are offered for free somewhere can be misused to obtain personal sensitive data and information.
- When communicating with anyone unknown, the user should be careful, not in a hurry, and think carefully. Do not work with time pressure, which the attacker can calculate.

Online account security:

- Protect access to any account with a strong password. It should consist of 12 characters, contain lowercase and uppercase letters, numbers, symbols, and other special characters.
- Use different passwords for different services.
- The user should avoid tools that check the strength of the password. When using such an online service, the entered password may be compromised and the password may be misused by an attacker.
- In the case of a large number of passwords, it is good to use the services of a password manager, which allows the user to securely store and manage passwords. Access to this manager should be provided by a strong unique password combined with multi-factor authentication.
- The user should never share their login passwords for their accounts and services.
- The user should always use all the security options offered for critical services such as internet banking or other financial or cryptocurrency management tools, private or business e-mails.
- Do not use control questions to reset your password. If this is mandatory, it is important, for example, for a question such as "What was your mother's maiden name" to choose an answer in the form of a complex password that is not based on truth. Then the attacker can't find out the fact by available means. [15]

Among the general principles of user behavior that should be followed for any environment or device is the need to constantly learn and gain a general overview of the cyber world. You can't trust everything, you have to be careful. Store the most sensitive data on devices that are not directly connected to the Internet (eg on an external HDD). Learn to share information, photos, videos, and various experiences with a slight delay, compare the authenticity of photos, eg on Google images. - Set privacy on social networks.

Do not forget about the physical security of the device (when it is stolen, you can use the option of deleting data or blocking the device remotely, thus preventing a potential thief from accessing the data stored here). When registering, it is advisable not to fill in all data, or to use a special account for registration in unknown services. Have your computer set to display all file extensions (the latter is crucial) and do not install programs from untrusted sources. In addition, you should monitor your computer for suspicious activity (such as an unusual increase in data traffic, a significant slowdown in your computer, increased hard drive activity, and so on) and, if possible, clear your browsing history regularly before shutting down. [13]

VI. Discussion

The current world can no longer be imagined without the advantages and positive advantages of cybernetics. Information and communication technologies are interconnected with the vast majority of industries, state institutions, schools and private activities. Because they make life easier for all people, it is clear that their reach will continue to grow. However, it is always necessary to keep in mind that every positive side is associated with the negative. Unfortunately, these experts still do not adequately map cyberspace. For the general public, they are then mostly confused.

Cyberspace is affected by risks and crimes transmitted to it from the real world, such as fraud, theft and misuse of sensitive data. We could follow another list of negatives in the form of cyberbullying, misleading advertising and others, which are clearly mentioned above in the article. Attackers use their technical knowledge or gaps in individual applications, human confidence and the inability to completely reliably verify all things in the online world. The creation of time constraints and the urgency of immediate decisions often play in their favor when a layman loses the opportunity to even consult with friends, let alone experts.

Users need to emphasize the need to control other people and applications, to examine their individual permissions and the information about us that we hereby allow to collect and send. Use common sense, prudence and distrust and, last but not least, further education and follow current events in the field of cybernetics. They will learn about new types of attacks, such as improved protection enhancements that prevent both property damage and possible psychological damage to the user. The public must always be aware that computers and communication devices can be used and misused without their knowledge, and the anonymity of the attacker guarantees him a minimal chance of being caught. Although the user spends some time re-verifying the information, it is certainly less than solving subsequent problems.

Not only in the Czech Republic, but in all countries of the world, there are a large number of targets that attackers focus on. At present, it can be said that the targeting of attacks has shifted from the area of private organizations also to state administration institutions and hospital facilities. There are a huge number of these institutions, along with hospitals, energy and other elements of critical infrastructure, and the cost of ensuring the security of these institutions is in the hundreds of millions. Another complication is also the time and lack of the necessary professional staff. There is no doubt that in the future, the targets of cyber attacks on schools, banks and institutions managing, for example, intellectual property, patents and others will continue to spread. We will therefore be forced to develop the possibilities of protection through artificial intelligence and the technology associated with it. Artificial intelligence is expected to dominate protection against fraudulent and hacker attacks.

It is therefore in the interest of all states, professional institutions and organizations to build and support research and the subsequent sharing of knowledge related to the protection of information and communication technologies. The plan should allocate the resources and management support needed to effectively maintain and improve incident response capabilities. [17]

The article clearly summarizes the risks involved in the misuse of cyberspace, describes the features of behavior that can initiate or facilitate an attack. It also discusses the methods of these attacks, which are the most common and how they manifest themselves. After reading the article, the attentive user will become aware of suspicious emails, applications and other ways that are no longer harmless at first glance. Finally, it summarizes at least a minimum of basic protection, such as creating strong passwords, updating devices, applications and antivirus programs, and other simple tasks. The sum of all these principles, whether part or most of them are applied, will prevent or at least make it difficult for an attacker to attack him. Only in this way will they be able to be an equal adversary to the attackers, who are also idle, and to improve their tactics. Given the paramount importance of cyber security (respectively cyber security) for the economy, society and privacy, considerable efforts are needed to create sufficiently effective educational programs, in particular a comprehensive, consistent and dynamic framework for building and improving these programs. [18]

VII. Acknowledgment

This research was based on the support of the Internal Grant Agency of Tomas Bata University in Zlín, the IGA / FAI / 2021/002 project and the Institute of Safety Engineering, Faculty of Applied Informatics.

References

[1] Where are the boundaries of ethical hacking? https://www.systemonline.cz/it-security/kde-jsou-hranice-etickeho-hackingu.htm

[2] KUCHTA, Josef. Current problems of cybercrime, including its prevention. Journal for legal science and practice. [Online]. 2016, No. 1, pp. 5-19. [feeling. 2021-05-01].

[3] Government Proposal No. 28 of the Senate of the Czech Republic of 2013 to express consent to ratification, https://www.senat.cz/xqw/xervlet/pssenat

[4] MATEJKA, Ján. The Internet as an object of law: seeking a balance between autonomy and privac, ISBN 978-80-904248-7-6.

[5] JANSA, Lukáš et al. Internet law. 1st edition Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

[6] DONÁT, Josef and Jan TOMÍŠEK. Network Law: A Guide to Internet Law. 1st ed. Prague: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

[7] JIROVSKÝ, Václav. Cybercrime: not just about hacking, cracking, viruses and Trojans without secrets. 1st ed. Prague: Grada, 2007. ISBN 978-80-247-1561-2.

[8] PĚNČÍK, Lukáš. Current trends in cybercrime and computer data security. [online]. Brno, 2020 [cit. 2021-04-30].

[9] JANSA, Lukáš et al. Internet law, 2020, Computer Press, ISBN 978-80-2514-664-4.

[10] KOLOUCH, Jan. CyberCrime, 2017, CZ.NIC, ISBN 978-80-88168-15-7.

[11] Quora. [online]. How does Bayesian spam filtering work ?. [Feeling. 02/02/2018]. Available from: https://www.quora.com/How-does-Bayesian-spam-filtering-work

[12] https://www.knowbe4.com/hubfs/SecurityAwarenessTrainingDeploymentsDeterDefeatHackers.pdf

[13] ROZMAROVA, Monika. Risks of misuse of private information in the Internet environment [online]. Brno, 2018 [cit. 2021-04-30].

[14] Statistics on resolved incidents. CSIRT [online]. Czech Republic [cit. 6/25/2020]. Available from: <https://csirt.cz/cs/o-nas/statistiky/>.

[15] NETOLIČKA, Jan. \ textit {Scamming: Techniques of obtaining sensitive data in the online environment} [online]. Brno, 2020 [cit. 2021-04-30].

[16] www.policie.cz

[17] Act No. 181/2014 Coll. Laws for people [online]. Czech Republic [cit. 6/23/2020].

[18] Roumen Trifonov, Slavcho Manolov, Georgi Tsochev, Galya Pavlova, Automation of Cyber Security Incident Handling Incident through Artificial Intelligence Methods, WSEAS Transaction on Computers, ISSN / E-ISSN: 1109-2750 / 2224-2872, ročník 18, 2019, čl. # 35, str. 274-280.

[19] Roumen Trifonov, Georgi Tsochev, Ognian Nakov, Galya Pavlova, Slavcho Manolov, Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods, Engineering World, Volume 2, 2020, pp. 145-149