SECURITY DIMENSIONS
ISSN 2353–7000
NO. 26; 2018 (173–186)
DOI 10.5604/01.3001.0012.7249

Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population

Ing. Peter Lošonczi, Ph.D. MBA MSc.
University of Security Management in Košice, SLOVAKIA

ABSTRACT

This article deals with the importance of focusing seniors' attention on cybercrime and cybersecurity. We should perceive cybersecurity as a key component of state security. Technological development has brought new forms of crime in this area. The people above 55 belong to the most vulnerable group in terms of cybersecurity threats and consequently they become a common target for cyber criminals. Prevention in this area is therefore of the utmost importance. Information and communication technologies make our lives easier. They speed up communication and information access and as well as access to various services on one hand. But in case of insufficient security, an increasing dependency of the public and private sector on these technologies is increasing the threat of a cybercrime. This makes cybersecurity one of the biggest challenges that need to be properly addressed by the state.

ARTICLE INFO

Article history
Received: 29.05.2018 Accepted 20.06.2018

Key words
Cybersecurity, cyber threats, cybercrime, prevention, senior

Introduction

The internet has penetrated into many areas of the older generation´s life. The internet has long been a space for younger generations. More and more people above 55 years of age go online and enjoy the internet´s

endless possibilities such as they younger relatives do. The people older than 55 use the internet for fun, mutual communication, financial operations, interaction with public or private institutions and so on. Lack of knowledge in terms of computing, data processing and the internet threats is the basis for security risks and their occurrence is just the matter of time. Nowadays, senior citizens belong to the most vulnerable group in terms of cybersecurity and therefore they often become an attractive target for cyber criminals. The online activities have an increasing influence on our everyday lives. This applies to the youth as well as to seniors.

We should consider the attributes which differentiate seniors from a common student or internet user. For these people, the internet is just a means for communication, searching information, services and fun. Seniors do not have space, possibilities and knowledge to educate themselves through various websites and online publications, which are often complicated even for an experienced user.

The term cyber security dates from the invention of first computers. The problems related to cyber security got even more serious with the internet connection. The most serious problems, threats and cyber risks on the internet posse illegal software, malware, tracking software, malicious software and viruses, fraudulent emails, spread of "hoaxes" a non-existent threats, financial loss due to theft of financial account information, fraudulent ads, ill-considered sharing of private information, emails with infected links, theft of personal data, photos, and then consequent blackmailing or bullying, and so on[1]. These risks can not be completely eliminated, but with greater knowledge and the right form of prevention, they can be minimized to an acceptable level[2].

1. Cybersecurity and cybercrime

Cyber security plays an important role to secure the people who use internet via different electronic devices in their daily life. Some causes occurred all over world that people face problems when they connect their devices and system via internet. There are some highly sensitive data like biotechnology and military assets which are highly threatened by the hackers;

[1] T. Petrowski, *Bezpečí na internetu. Pro všechny*, Dialog, Liberec 2014, p. 248.

[2] S. Križovský, M. Kelemen, M. Blišťanová, *Analýza prostredia ako základný predpoklad účinnej prevencie*, „Procedia Engineering: 24th DAAAM International Symposium on Intelligent Manufacturing and Automation" 2014, vol. 69, p. 1529–1533.

cyber security plays a vital role in securing such data. Misusing the internet becomes a current issue in different sectors of life especially in social media, universities and government organizations[3].

Rapid spread of information and communication technologies results into increasing speed and quality of information process, but in the same time, it is necessary to focus on data protection in information systems. Hackers are constantly looking for new ways of attacking the information systems with the intention to change, decrease or only enter the systems. This relates to a new crime phenomenon and anti-social behaviours called cybercrime. This endangers not only credibility, integrity or accessibility of the computer systems but also security of the crucial state infrastructures. Technological development provides space to criminal activities in this field among others.

Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space[4].

Computers, however represent huge risks. These risks are data protection, technology misuse for terrorist purposes, critical mistakes and their influence on people´s lives and many more to mention. One of the key issues in terms of the computer systems is the question of data and system security which the particular system contains. What would be the outcome of people scanning through confidential information such as medical reports, birth number and criminal records or further such data of other people? Therefore, we have to protect the data against the unauthorised users. Hackers are trying to obtain classified information through different means. Their tool is the computer with its imperfections or mistakes the user has made. For examples, banks use computers for majority of their work and they of-

[3] M. Kashif at al., *A Systematic Review of Cyber Security and Classification of Attacks in Networks*, „International journal of advanced computer science and applications" 2018, vol. 9, issue 6, p. 201–207.

[4] Cyber Security Concept of the Slovak Republic for 2015–2020, http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015–2020-A4.pdf.

ten become victims of hacker attacks. There is no organization which would willingly disclose information about such attacks, especially when the organization is a key player on the market, which could possibly raise doubts and cause lack of confidence of its customers and clients.

Cybercrime is currently in the agenda of National Security Authority and it is covered by the Act on Cybersecurity n. 68/2018 Coll.

The strategic goal of cyber security in the Slovak Republic is to achieve an open, secure, and protected national cyber space, i.e. building trust in the reliability and security of, above all, critical information and communication infrastructure, as well as building of certainty that this will perform its functions and serve national interests also in cases of cyber-attacks. Basing on the current situation in cyber security in the Slovak Republic, the goal of the Concept is to achieve a state where:

– protection of national cyber space is a system operating conceptually, in a coordinated manner, efficiently, effectively, and on a legal basis,
– security awareness of all components of society is systematically increasing,
– the private and academic sectors as well as civil society actively participate in the formulation and implementation of the policy of the Slovak Republic in the area of cyber security,
– efficient collaboration is provided for both at national and international levels,
– the adopted measures are adequate and respect the protection of privacy and basic human rights and freedoms[5].

In terms of statistics of the Ministry of the Interiors, criminality in this field is defined differently. For example, blackmailing and extortion fall under the violent crime, trafficking in human beings falls under crimes against morality, fraud is a part of economic crime etc. We lack the statistics, where the victims have been persons of 55 years of age and above and the criminal act was committed via the internet. We can state, that number of persons in this age group, who start using the internet, has increased recently which increases the number of the potential victims.

The investigators, prosecutors and judges fighting this type of crime face many forensic problems. This is partly because digital processes developed in connection with the intangible and transient character of digital evidence. In addition, effective investigation and prosecution of cybercrime

[5] Ibidem.

often requires monitoring of criminal activities and their consequences through a number of different internet providers, in some cases outside the borders of the state, which can lead to complex issues of jurisdiction and sovereignty[6].

The Slovak Republic must be prepared to react to a wide spectre of existing and potential threats. At the same time, it is aware of the fact that threats and attacks emerging in cyber space may escalate up to a level that would require collaboration of the allies within the North Atlantic Treaty Organization.

Thus, cybersecurity also needs to be perceived as a subsystem of national security and cyber space as its new operational domain. The Slovak Republic intends to cooperate with all relevant state and private cyber space actors, which respect identical values and do not restrict the freedom and security of the use of cyber space[7].

2. Overview of studies

Dealing with this issue, it is necessary to look at the examples of real incidents on the internet which seniors above 55 years of age have to face. We can understand an incident as a diversion from an expected and standard interaction with the internet environment, for example online identity theft, financial frauds, hacking, cyber bullying, email spoofing, software piracy and forgery and intellectual property crime. Each activity performed by seniors above 55 is connected with a threat or incident as mentioned above. Therefore, we present definitions of certain threats, that most often endanger seniors on the internet.

Spam can be defined as sending unsolicited electronic messages. The messages are typically send to a large number of users. If the device used for the internet connection is not protected properly, after being infected by a virus it can send out spam without the user´s conscience. Most of the spam contain malware – a malicious code, which can "steal" personal data from the computer[8].

---

[6] J. Požár, *Vybrané hrozby informační bezpečnosti organizace*, [in:] *Kybernetická bezpečnost: sborník příspěvků z bezpečnostního semináře 2011,* Policejní akademii ČR v Praze 2011, https://www.cybersecurity.cz/data/srib.pdfhttps://www.cybersecurity.cz/data/srib.pdf.

[7] Cyber…

[8] A.M. Al-Zoubi at al., *Evolving Support Vector Machines using Whale Optimization Algorithm for spam profiles detection on online social networks in different lingual contexts*, „Knowledge-Based Systems" 2018, vol. 153, p. 91–104.

Hoax is fake news or a falsehood. It is often an email message which for example warns of a non-existing threat, computer viruses, asks for help etc. It often asks the receiver to forward the message to the friends, family, relatives and so on. Based on this request we can identify the hoax.

Phishing is a fraudulent technique that uses information and communication technology to obtain sensitive data – login information, passwords, credit card numbers, and so on. Although phishing is a form of cybercrime that internet users get confronted with rather frequently, many people still get deceived by these practices[9]. The whole principle is based on a faithful imitation of the request from e.g. a bank, a mailbox or social network operator etc., so the user is forced to enter his/her login information. These messages, applications are most often emailed to you. These emails include links to web pages on which the user clicks, but they do not redirect them to the original page, e.g. a bank website, but to a fraudulent website that is very similar to the original one. By entering your login information on such a false page, the user will provide his / her personal information to the attacker. Nowadays, these fraudulent sites – "imitations" – are so incredibly realistic that even an experienced internet user may have a problem to find out[10].

Pharming, unlike phishing, is a more sophisticated and much more dangerous form. It uses fraudulent techniques for obtaining sensitive personal data as the previous one. However, the principle is to attack the DNS server and rewriting the IP address. This means that if you want to log in, for example, to www.vsbm.sk page, after typing in this site into the search engine, the infected DNS server does not direct the user to the original website but to a fraudulent copy with the attacker's IP address, this website looks unrecognizable from the original website.

Malware (malicious software, computer viruses, worms, Trojans, spyware, adware, keyloggers, etc.) is a computer program or any piece of program code created for attacking or intrusion into the system, that is to say, infecting for purposes of its destruction, data aft, user tracking, etc.[11]

[9] L. De Kimpe at al., *You've got mail! Explaining individual differences in becoming a phishing target*, „Telematics and Informatics" 2018, vol. 35, issue 5, p. 1277–1287.

[10] M. Alsharnouby, F. Alaca, S. Chiasson, *Why phishing still works: User strategies for combating phishing attacks*, „International journal of human-computer studies" 2015, vol. 82, p. 69–82.

[11] T. Lee at al., *Automatic malware mutant detection and group classification based on the n-gram and clustering coefficient*, „Journal of supercomputing" 2018, vol. 74, issue 8, p. 3489–3503.

Ransomware is also worth mentioning as a threat to the older generation. It is a type of malware which encrypts selected files in the infected system and the user is then extorted by paying the ransom. Ransomware spreads like a worm or a Trojan horse[12].

Cyberbullying is a type of bullying that uses information and communication technologies (computers, tablets, mobile phones, social networks, emails, etc.) to hurt others – bullying, harassment, threats, intimidation[13].

The above-mentioned and described threats are among the most common ones encountered by the older generation using the internet. It is therefore necessary to educate and inform this generation in this field to make their activities on the internet secure.

Information Technology has grown tremendously during the last two decades and became the main source of knowledge. The latest information and the current technology are available through the Internet making it the most valuable source of information to almost all people from the novice to the expert in all fields of knowledge[14]. The Internet has penetrated life of the older generation as well. According to a survey conducted by Kaspersky Lab in cooperation with B2B International, up to 90% of seniors above 55 years of age use the internet for shopping in various online stores or electronic banking. The survey, which contained 12 546 internet users from around the world, shows that the oldest generation of users is becoming an increasingly popular target for cyber criminals. People above the age of 55 often use the internet for shopping, banking or communication with their closest people. They often fail to protect themselves and what is most valuable to them against the threats of cyber criminals[15].

According to a survey by Kaspersky Lab and B2B International, up to 84% of users above the age of 55 are now joining the internet at home several

[12] Q.G. Miao at al., *Malware detection using bilayer behavior abstraction and improved one-class support vector machines*, „International journal of information security" 2016, vol. 15, issue 4, p. 361–379.

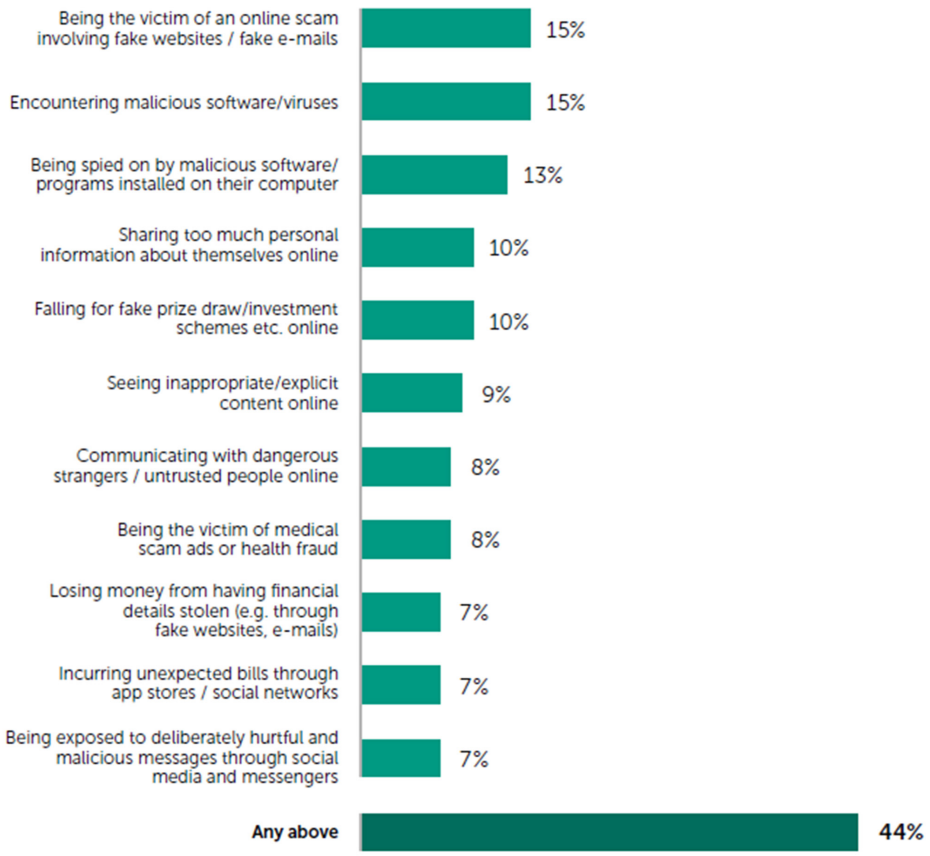
[13] I.K. Peter, F. Petermann, *Cyberbullying: A concept analysis of defining attributes and additional influencing factors*, „Computers in human behavior" 2018, vol. 86, p. 350–366.

[14] A.R. Mathew at al., *Cyber Crimes: Threats and Protection*, „International conference on networking and information technology (ICNIT)" 2010, p. 16–18.

[15] Kaspersky Lab, *Not logging on, but living on. Consumer Security Risks Survey 2018*, https://media.kasperskycontenthub.com/wpcontent/uploads/sites/100/2017/11/10083912/4114_B2C_Report_2017_WEB.pdf.

times a day, with 44% are online at least 20 hours a week. According to data from the second half of 2017, this age group owned up to 4 devices with access to the internet, mostly including 2 computers and 2 mobile devices. More than half (60%) of respondents in the survey acknowledge that they are concerned about the security of their older family members, with 44% reporting that they have already encountered an internet threat with their senior relatives as victims – 15% have been victims of online scams, 15% were affected by malware or other virus infections, 13% were again tracked by illegal malicious software, and so on. (Figure 1)[16].

Fig. 1. The threats faced by older relatives in 2017



Source: Kaspersky Lab, *Research 2017 Consumer Security Risks Survey: Not logging on, but living on*.

[16] Ibidem.

Another survey that we would like to mention in this study is "Seniors go online" which was realized by Seznam.cz and Centre for the Prevention of Risky Virtual Communication of the Pedagogical Faculty of the Palacky University in Olomouc. 1072 respondents were surveyed in 2017. According to this research, the most active spammers on the internet are people aged 65 and above. Often, unsolicited emails are also spread with a variety of fake news, "Hoaxes" or disinformation. Research has shown that 35% of people aged 55–64 years and 47% of respondents above the age of 65 spread e-mails containing a warning of non-existing danger. According to this research, the older generation uses the internet in different ways. The most widespread is the use of emails by 97% of respondents, the search for information by 95% of respondents and internet banking by 64% of respondents. According to the survey, the older generation does shopping at least once a month via the internet[17].

3. Prevention measures against cybercrime in people over 55 years of age

One of the most important thing in targeting computer crime is prevention. Computer crime in many forms, for example, online identity theft, financial fraud, extortion, cyber-bullying, hacking, email spoofing, information piracy, forgery and intellectual property-related crimes can, in the best case, cause serious inconveniences and complications in the lives of victims. In the worst case scenario, computer crime can lead to a financial crisis and potentially jeopardize the reputation of the victim and personal security.

Preventive measures for the older generation, which is nowadays the most vulnerable group on the internet, are very important and also justified. These preventive measures could be implemented as interactive lectures, which would be in a form of a structured interview, further in a form of leaflets, posters, brochures dealing with this issue and prevention itself. Furthermore, it is very important to inform seniors on the most common threats and to teach them how to use the internet. Thus, security education in this area for this age group is very important[18].

[17] Výskum „Starci na netu". Seznam.cz a Centrum prevencie rizikovej virtuálnej komunikácie Pedagogické fakulty Univerzity Palackého v Olomouci, https://www.novinky.cz/internet-a-pc/463392-spamy-na-internetu-nejcasteji-siri-seniori.html.

[18] L. Kováčová, M. Vacková, *Applying Innovative Trends in the Process of Higher Education Security Personnel in Order to Increase Efficiency*, "Proceedings of 5th world confer-

With the increasing time people spend online and the increasing number of cyber-related risks, it is essential to have protection against current threats as well. The first step should be to install truly effective security patches, an effective antivirus program that protects all devices, including smartphones or other mobile devices. This is the minimum we can do to protect our senior relatives and friends against the threats of the current digital world.

Older internet users can be very easily influenced and consequently they influence their friends or their surroundings by emails. Therefore, it is very important to teach the older internet users to distinguish true and false (hoax) information, learn how to critically work with information, teach them to search for primary and trusted resources and point out the strategies the authors of hoaxes use.

Senior are often give computers from their children who are not interested what they do with it anymore. Prevention is therefore crucial. With regard to prevention in this area, it may be necessary to constantly remind and teach seniors the basic rules for using the internet. Among such rules, we can include:

– when buying a new computer, first of all it is important to install an effective antivirus program and update it regularly,
– no storing of personal data, information or passwords on the internet browsers or other programs connected to the internet,
– in the case of a correspondence via the internet it is necessary to remember that we never know who is on the other side and not everything written is true,
– always tell your relatives or closed ones about the meetings you appointed via the internet,
– passwords for different internet services should not be the same,
– before any confirmation, it is necessary to read carefully all the conditions,
– no sharing of photos of family members, they can be misused,
– no sharing of any personal information,
– no sharing of email addresses online,

ence on learning, teaching and educational leadership. Procedia Social and Behavioral Sciences" 2015, vol. 186, p. 120–125.

– spam messages should be never opened; if possible, report this message and change it, in any case, do not click on any link or button in this message,
– emails from unknown users should not be opened as well, you should not read emails from unknown users at all,
– neither the bank nor any similar institution ever asks for a login, certificate renewal, verification or change of login data by e-mail; in this case, if something happens, it is necessary to verify and report the sender, do not click on the inserted link and do not enter any login information,
– when using Internet banking it is necessary to be cautious, it is necessary to monitor whether the user is on the correct web site and whether it is connected via a secure connection.

These are just a few rules – advice that every senior should know before starting to use the internet. Prevention is of utmost importance, because the consequences can be serious. Computer crime prevention in people aged 55 and above is indeed well-founded.

Conclusion

The dependency of today's society on information and communication technologies increases every day; over the past decade, these have changed and impacted almost every aspect of our lives. Human activities are slowly but surely shifting, to a large extent, from physical space to cyberspace. On the one hand, information and communication technologies make our lives easier, speeding up communication and access to information and services. On the other hand, however, the increasing dependency of the public and private sectors on these technologies, if insufficiently protected, renders them more vulnerable, making cyber security one of the most important challenges the state has to face today[19].

This study deals with seniors' dealing with of cybersecurity and cyber criminality. The subject group are people of 55 year of age and above with an interaction in working, social, public and family environment. This interaction also creates a need to use the internet for obtaining various information, communication, social networking, internet banking, e-government, fun etc. However, we can see lack of systematic educa-

[19] Cyber…

tion and knowledge in the field in this age group, unless the seniors came in contact with it during their working lives. Their knowledge in this area is partial, mostly intuitive or based on the trial and error approach. But up to certain extent, they are expected to handle information technology in its basic operations.

People of 55 years of age and above are constantly exposed to a certain kind of threat using their computers or smartphones. The threat is everywhere around them. It may be suspicious websites, hacker attacks, malicious software or something else. We should not forget about the cyber criminals who are trying to gain money or obtain personal data from the users. The internet related threats are nowadays so complex that a regular user may not be familiar with all of them. For people who start using the internet, everything is even more complicated and dangerous. Therefore it is important to protect seniors against threats and dangers which they can encounter using the internet.

References

1. Alsharnouby M., Alaca F., Chiasson S., *Why phishing still works: User strategies for combating phishing attacks*, „International journal of human-computer studies" 2015, vol. 82.
2. Al-Zoubi A.M. at al., *Evolving Support Vector Machines using Whale Optimization Algorithm for spam profiles detection on online social networks in different lingual contexts*, „Knowledge-Based Systems" 2018, vol. 153.
3. Cyber Security Concept of the Slovak Republic for 2015–2020, http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015–2020-A4.pdf.
4. De Kimpe L. at al., *You've got mail! Explaining individual differences in becoming a phishing target*, „Telematics and Informatics" 2018, vol. 35, issue 5.
5. Kashif M. at al., *A Systematic Review of Cyber Security and Classification of Attacks in Networks*, „International journal of advanced computer sci ence and applications" 2018, vol. 9, issue 6.
6. Kaspersky Lab, *Not logging on, but living on. Consumer Security Risks Survey 2018*, https://media.kasperskycontenthub.com/wpcontent/uploads/sites/100/2017/11/10083912/4114_B2C_Report_2017_WEB.pdf.

7. Kováčová L., Vacková M., *Applying Innovative Trends in the Process of Higher Education Security Personnel in Order to Increase Efficiency*, "Proceedings of 5th world conference on learning, teaching and educational leadership. Procedia Social and Behavioral Sciences" 2015, vol. 186.
8. Križovský S., Kelemen M., Blišťanová M., *Analýza prostredia ako základný predpoklad účinnej prevencie*, „Procedia Engineering: 24th DAAAM International Symposium on Intelligent Manufacturing and Automation" 2014, vol. 69.
9. Lee T. at al., *Automatic malware mutant detection and group classification based on the n-gram and clustering coefficient*, „Journal of supercomputing" 2018, vol. 74, issue 8.
10. Mathew at al. A.R., *Cyber Crimes: Threats and Protection*, „International conference on networking and information technology (ICNIT)" 2010.
11. Miao Q.G. at al., *Malware detection using bilayer behavior abstraction and improved one-class support vector machines*, „International journal of information security" 2016, vol. 15, issue 4.
12. Peter I.K., Petermann F., *Cyberbullying: A concept analysis of defining attributes and additional influencing factors*, „Computers in human behavior" 2018, vol. 86,
13. Petrowski T., *Bezpečí na internetu. Pro všechny*, Dialog, Liberec 2014.
14. Požár J., *Vybrané hrozby informační bezpečnosti organizace*, [in:] *Kybernetická bezpečnost: sborník příspěvků z bezpečnostního semináře 2011,* Policejní akademii ČR v Praze 2011, https://www.cybersecurity.cz/data/srib.pdfhttps://www.cybersecurity.cz/data/srib.pdf.
15. Výskum „Starci na netu". Seznam.cz a Centrum prevencie rizikovej virtuálnej komunikácie Pedagogické fakulty Univerzity Palackého v Olomouci, https://www.novinky.cz/internet-a-pc/463392-spamy-na-internetu-nejcasteji-siri-seniori.html.

Author

Peter Lošonczi – has long been engaged in the research on the Protection of Persons and Property. He is an author of many scientific publications and researcher in various scientific projects in the field of cybersecurity, rescue services and private security services. He works at the University of Security Management since its establishment.

Cite this article as:

P. Lošonczi, *Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population*, "Security Dimensions", 2018, no 26, p. 173–186, DOI 10.5604/01.3001.0012.7249.