Mérnöki Szimpózium a Bánkiban
(ESB 2020)
http://bgk.uni-obuda.hu/esb/2020

Security awareness in the education system

Andras Pallagi[1][0000-0002-6466-2631]

[1] *Obuda University Doctoral School on Safety and Security Sciences, Budapest, Hungary*
pallagi.andras@phd.uni-obuda.hu

Abstract.
In my paper, I present the threats related to information security and, in this context, the possible solution for the development of a security awareness approach and its integration into the education system. I present the opportunities offered by gamification and octal as a potential educational methodology for teaching security awareness. During the research, I surveyed the safety awareness of the previous two generations, Y and Z.

Keywords: Security Awareness, Education, ICT.

1 Introduction

Today, almost 5 billion people actively use the Internet. [1] This number is growing rapidly, as is the amount of data created by humanity. However, in most cases, the growth of user-generated and managed data is not followed by measures to protect the integrity of the data. Cyber attacks against various data centers and server parks are almost commonplace. Unfortunately, as a simple user, there is not much we can do against these since we do not retain most of the data.

With a few simple methods built into our data management process, we can increase the security of the data we create and manage. With this, we can make it harder to acquire, and they can access it to do, or they can just harder to get our data and our increasingly look for easier targets. However, we also need to be aware that if the attacker (s) need our data, they are almost not deterred by anything.

There is a price to protect our data, and we have to give up some of the convenience features. For example, if we do not use a code, pattern, or biometric identifier to unlock our mobile phone, the data stored on it will not be appropriately protected.

For this reason, I find it necessary to set complicated passwords or identifiers to protect our information. Don't follow those who still believe that the top three passwords are 123456, password, or 12345678 are the best choice. [2]

Utilizing information security solutions that are improperly or not at all can harm users. Due to poorly chosen virus scanners, there have been blackmail attacks in recent years that have made the contents of your computer's hard drive inaccessible and only resolved after payment of the ransom.

With poorly protected data, identity theft can be carried out, and new contracts can be made on behalf of the victims. The Insurance Information Institute (USA) has been collecting statistics on the effects and results of this attack method for several years. It showed that in 2018 more than 40% of the abusers entered into new credit agreements on behalf of the victims.[3] However, the attacks did not necessarily obtain personal or financial information directed. Their potential goal is to use the free resources of computers to perform a task/attack that requires more computing power.

In many cases, large companies and organizations have not even applied adequate security

systems to protect information. Think of the privacy issues of Facebook-Cambridge Analytica, or Julian Assange-Wikileaks, or recent hacking attacks. The latest known example made the entire server park of the Hungarian Development Center unusable.[4]

As a user must pay attention to better protect the data and media devices there, you need to know the dangers and care that should be drawn to them. By doing so, you can increase your own and our security awareness.

Information security threats can be brought to the attention of the education system from the very beginning. Most of the Alpha generation starting their studies started using ICT tools at an early stage [5] but are not aware of the dangers involved.

During my research, I sought a solution to introduce them, the members of the Alpha Generation, to the threats to their data, their devices, and the possible security measures. My goal is to integrate safety awareness into their daily lives and not see the bad in it.

2 Implementing and raising awareness of security culture

Not only the Alphas but also members of the previous generations Y and Z are already using info communication (ICT) tools, which is why there is an urgent need to develop an appropriate information security culture. I think it is essential to have proper guidelines for the safe use and storage of their personal data and devices.

In my research, I have taken into account the nine principles formulated by the Organization for Economic Co-operation and Development (OECD) in the field of developing a culture of information security. These principles apply equally to different users, students, teachers, with appropriate responsibilities for their role. All users benefit from awareness, education, information sharing, and training, which can result in a better understanding of security and better security practices.

The first of these is the principle of awareness. This includes knowledge of our environment. Everyone should know how the information system is structured, its benefits, and its risks and dangers. Students should be introduced to the other side of the coin, with possible consequences and outcomes. There are many examples of security risks ranging from blackmail to personality theft.

In the United States, The Federal Trade Commission follow up complaints about abuses of consumer fraud and identity theft that were filed in the federal, state, and local law enforcement bodies and private organizations. Between 2015 and 2018, approximately 3 million registered fraud cases were committed each year, with an average of 15% of identity thefts (Fig. 1.).

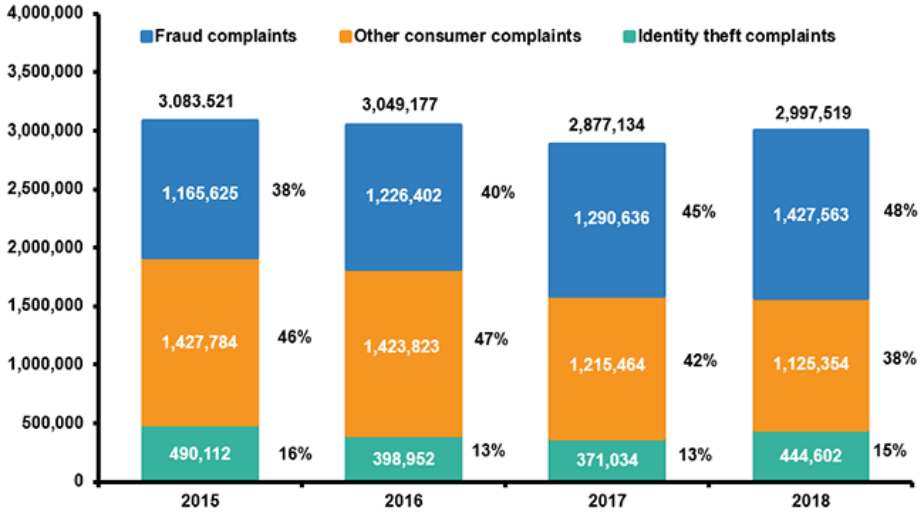

Figure 10. Identity Theft And Fraud Reports, 2015-2018

In many countries, it has happened that somebody has received too much negative attention in social media, for that reason, commit himself to do the wrong things (school shooting, suicide). Let us be aware of the power of information and pass on this thought to future generations.

The second principle is the principle of responsibility. Each user, operator, developer, or owner of an ICT System is responsible for the security of the network in different areas and to different degrees. In order to maintain safety, each actor must be aware of his or her own responsibilities.

The basic principle of response measures consists of two main parts. The first is to detect, prevent, and respond to unexpected security incidents in a timely manner. The second main part is the continuous exchange of information on detected vulnerabilities and threats.

The ethical principle to respect the legitimate interests of others and to be aware of the impact our actions, or even lack thereof, may have on other users.

The principle of democracy states that information security solutions must be in line with the values of a democratic society and support the free flow of ideas and ideas. Furthermore, there should be no restrictions on the protection, transparency, and openness of personal data.

The principle of risk assessment is that when designing our security systems, we must first and foremost assess the actual external and internal risks. From the assessed risks, the threats, vulnerabilities, and their effects on our own organization and on others must be identified. It is also an important step to determine the level of tolerated / tolerable risk.

Based on the principle of security planning and implementation, all elements of the information network must be designed with optimal security in mind. The plan must consider minimizing potential hazards and risks and minimizing impacts. In determining the level of protection should be sought proportionality of risk, observing the principles described above.

The security management principle is that all our organizational tasks must be based on risk assessment and follow our dynamically changing security status. We need to investigate future threats and disruptions. Security management shall include the ongoing review and maintenance of information security components, policies and regulations.

The ninth and last principle is the principle of reassessment. This principle essentially summarizes the previous eight principles. In our changing security environment, we need to

continually review and reassess the security of information systems and networks and make appropriate changes to security policies, practices, measures, and procedures. More and more threats and vulnerabilities are emerging that need to be addressed.

The adoption of these nine directives and comply with the instructions provided to promote the formation and development of a safety culture in the society. Our information security environment is continually changing, and newer and newer risks are emerging. Security awareness plays an essential role in the development of a safety culture. Dr. Kornélia Lazányi, in her article "The Security Culture," said:

"So, in addition to knowledge and competences, awareness and intentionality are a necessary element of a safety culture. Security awareness is an individual's sense of danger that extends not only to personal but also to organizational security. "[7]

In my opinion, the broader interpretation of the organization here can be applied to society. From this point of view, the knowledge needed to develop a safety culture could be passed on to students in the education system. This is the first opportunity to introduce information security threats and the measures needed to counteract them. The following chapter describes these hazards, their effects, and the methods of protection against them.

3 Threats to, and impact on, and appropriate management of ITC users

Unauthorized access to data is considered when an unauthorized person (s) access or modify our data. This usually includes obtaining a user ID and the associated password but includes obtaining a personal identification badge. Its impact can be multifaceted, ranging from simple data access to classified information security incidents. You can protect against this by using hard-to-guess passwords and by setting up risk-based security systems.

In recent years, there have been several major international examples (Facebook, Uber, AOL, etc.) of getting or cracking passwords [8]. The ordinary user will continue to use 123456 as a password or any personal information that may be associated with it, such as birth date, pet name, etc. If an attacker is explicitly seeking to gain access to our data, he will use a brute force program that first attempts to log on to the system using passwords generated from data associated with us. It is possible to protect your passwords from getting and deciphering by using a well-formed combination of lowercase-uppercase-number-special character.

Viruses are tiny little malware whose purpose is to accomplish a specific task, be it destruction or extortion. In most cases, they come from some bootable files on our ICT device. By starting the application, the virus is already activating itself and performing a specific task or a command. Mobile phone viruses have also proliferated in recent years, mostly on Android devices, thanks to open source. To protect against them, it is possible to have an up-to-date database antivirus application. At the same time, I would like to emphasize that we do not allow the installation of programs from unknown sources in a security-conscious manner.

Worms are malicious software that exploits and spreads malfunctions in our devices or network security settings. Their primary goals range from deleting files to building a zombie network (botnet). For example, the Conficker worm forced the French Air Force on its knees because they could not send flight planes to fighter jets. [9] You can defend against this by constantly updating your security software on the network and ICT tools.

Trojan horses are seemingly useful programs that, in addition to their visible function, also perform dangerous functions. They typically come to our devices from infected websites or emails.

Their most important task is to acquire data and build botnet networks. The best-known of these trojans was Zeus, which used it to collect bank access information between 2007 and 2011, causing $ 70 million damage [10]. You can protect yourself with an up-to-date antivirus program.

Spyware and malware, like the previous ones, are designed to obtain a user's personal or banking information. A variant of these is the recent appearance of "ransomware". Its impact can range from "simple" data theft to infecting government-owned computers. Protect yourself against them is difficult due to continuous development, use of up-to-date antivirus and anti-malware applications are recommended.

Other threats include junk mail (spam), hoaxes, and adware. A common feature of these is that they "bombard" the user with messages based on the email address or downloaded utility provided on an infected website. These have the greatest impact on resources and comfort. The only way to protect against this is to only register on a trusted website.

Phishing pages are created in most cases by copying Internet banking pages linked to financial institutions. In a received email, the user is asked to log in to their Internet bank and change their password because of a security incident. A link to the password reset page is placed in the email, leading the unsuspecting user to a page that is hauntingly identical to the original page, where he enters the requested information and delivers it to attackers. The basis of defense against this fraud is alertness and caution.

If you feel that a problem has occurred, please contact your system administrator, ICT Service Provider, or authority, depending on the magnitude of the impact of the information security incident.

4 Direct threats related to information security

Shoulder surfing is one of the most prominent immediate threats. Many people still store their passwords on paper sticking to their monitor or area, but it is not uncommon for a credit card to have a PIN on it. Abusing our passwords or identifiers can cause others to act on our behalf, which can have serious consequences. You can create or modify documents and make financial transactions. The defense against this is straightforward, do not write down your passwords and identifiers right next to the user interface or remember them. [11]

The next danger is fraudulent fraud or social engineering. In this case, the attackers manipulate their victim by various psychological methods and force them to enter their password and ID. Typically, a request for information reconciliation over the telephone is made about an information security incident. However, phishing emails may also be included. The effect of the acquired ID-password can be varied depending on the pair. It is easy to protect against it; do not give us your passwords or IDs.

It is also important to point out the dangers of stealing and scrapping IT assets. In many cases, the loss of negligently managed assets causes a major privacy problem. A lot of data can be recovered from the memory or storage of improperly managed scrap computers, phones. Sensitive organizations, therefore, typically do not dispose of device mass storage devices, but physically destroy them.

The last two common threats to information security, dumpster diving, and the inappropriate use of social networks. The former provides the necessary information from the trashed paper. In the latter, the user shares personal or official information on social networks, and from this information, many conclusions can be drawn. For example, an apartment may be empty or robbed during a long vacation.

The most obvious (and most cost-effective) solution to preventing the threats listed above is to raise awareness of the dangers. The following chapter summarizes this.

5 Awareness, gamification

Through (security) awareness, users are prepared for the dangers they face and are presented with the right information management behaviors. This method allows them to manage their ICT tools responsibly and aware of the risks they are aware of in their daily lives. The knowledge provided by the well-formulated awareness method is embedded in the basic behavioral standard, thereby reinforcing the previously defined security culture.

Numerous studies have been conducted in several countries around the world on how the two "digital generations", Z and Alpha, could more effectively communicate information within the education system. In an inverted classroom concept created by Guy Retta and Marquis Gerald [12], students were taught with video lessons and podcasts (audio) instead of personal performance. It was found that the students so educated outperformed the traditional classroom students, finding the actual class in the classroom to initiate more interaction. However, there were still problems during the adaptation period of this research.

Researchers say that playful learning activities allow students to acquire knowledge, develop skills, and promote positive traits through games specifically designed for learning. In other words, this type of teaching, gamification, is a student-centered process. It can be used from primary school to higher education and even in adult education.

In the Z and Alpha generations, the most appropriate learning and teaching scenario are no longer teacher-centered but instead focuses on active student activity and interaction. Recent years

The spread of the e-learning method is also an excellent example of this and the ever-popular Kahoot! too. In the latter's online interface, students are able to respond promptly to questions asked in the context of education. The system evaluates the answers and gives feedback to the student and the teacher immediately.

Gamification, as an educational methodology, is a new approach to training. Students born in the digital age can be reached through new channels that are more accessible to them. The essence of this teaching method is that instead of direct channels, the lecturer and the student interact with each other through digital or online interfaces. Individual and group challenges, rewards, points and levels have also emerged as incentives. The teaching and assessment method is more personalized and differentiated according to their own abilities. [13]

Research clearly shows that gamification has had a positive impact on learning outcomes in various forms, such as lesson enjoyment, commitment, motivation, effectiveness, satisfaction, and a better attitude to learning materials. [14]

In the gamification toolbox, students are most motivated by achievable and reward points, leaderboards, digital badges and challenges [15]. Research shows that these four elements (reward, leaderboard, digital badge, and challenge) are essential if you want to create effective learning activities. These elements should be considered as closely linked and used together to support learning activities.

Experience has shown that in order to achieve a larger goal (points, badges), groups were formed and solved the challenges together. This increased their communication and created their first group roles.

Ranking as a tool has played an essential role in the teaching method, as the results seen there move forward and also motivate students to hold the position when they are on top, while others are more motivated to reach and chase on top. Besides, they are happy to share their achievements online.

Summing up the results of the gamification make students more active and motivated in learning, allowing them to achieve the best performance of the evaluation of learning. It follows that

such an educational methodology can catalyze commitment and motivation (internal and external) that are essential to creating quality learning.

5.1 Octalysis, the new wave

This teaching method is continually evolving, refining, and adapting to the expectations of the age. One direction of development is the learner-centered framework created by Yu-Kai Chou [16], octalysis, which identifies the eight basic motivational forces that energize and "keep in play" students. This human (learner-centered) design recognizes that people have emotions, uncertainties, and reasons for wanting or not wanting to do things, and therefore optimize their feelings, motivations, and commitment as opposed to industrial systems in everyday life.

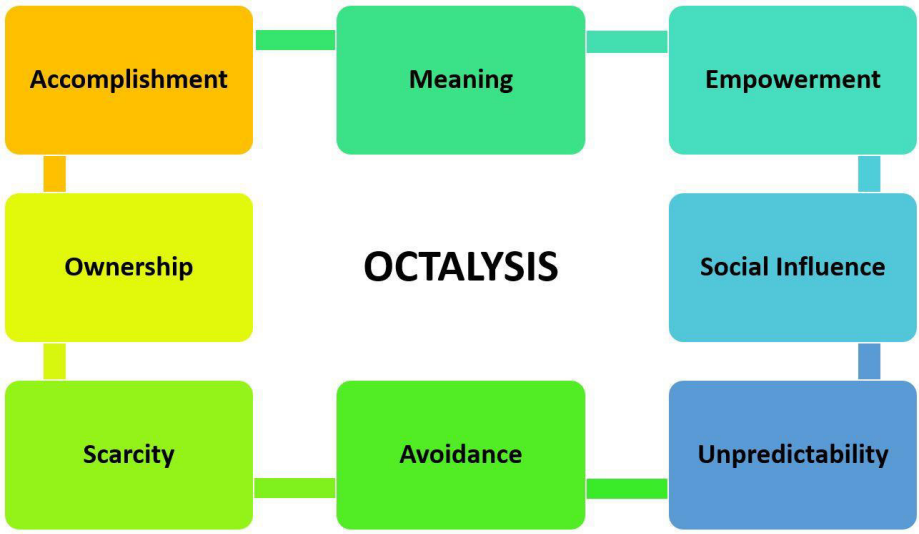

Figure 2. Octalysis framework with the eight core drives

Core drivers:

1: Epic Meaning: Volunteering for the community, not with external recognition, but with an internal reward.

2: Development and accomplishment: The inner driving force for progress, skill development, mastery, and finally overcoming challenges. However, it is important to recognize the challenge. A victory without struggle does not motivate. Scores, badges, and leaderboards are the most characteristic of this motivating force.

3: Empowerment of creativity and feedback: This feeling develops when students engage in a creative process, discover new things, and try different combinations, but they need to see the results and get feedback. A simple example is the Facebook Like button.

4: Ownership and possession: The need for ownership and the resulting comparability is a motivating force. The human desire to accumulate wealth and the overvaluation of physical and virtual objects (Facebook profile, number of Instagram followers) also belong.

5: Social influence and relatedness: This incentive power encompasses all the social elements that motivate people, including mentoring, social acceptance, company, and even competition and envy.

6: Scarcity and impatience: the fundamental drivers of something you desire, simply because it is extremely rare, exclusive, or inaccessible. Many people play with builder games where you have to wait for hours or days (torture breaks) to complete a building (but if you pay, you don't need to wait).

7: Unpredictability and curiosity: the main driver of ongoing commitment because it is not known what will happen next. When something is abnormal, our brains start to work wildly and pay attention to unexpected events. This is also the primary driver of gambling addiction.

8: Loss and avoidance: It motivates us to avoid something negative. Temporary, short-term opportunities make the most of this significant power because people feel that if they don't act right away, they lose the chance to act forever.

The octalysis-based education does not have much experience at the moment, but it seems to be a right direction. An outstanding feature of the system is the transparency and systematic nature of the curriculum. [17] Both gamification and octalysis can, in my opinion, provide a reasonable basis for developing a safety culture-building curriculum that raises security awareness.

6 Security Awareness Survey

In my research, I surveyed the safety awareness of these members of Generation Y and Z with 250 respondents from several regions of Hungary. Respondents were required to complete the following questionnaire.

Q1: Do you have a smartphone?

Q2: Do you use a password, pattern, biometric ID to unlock your phone screen?

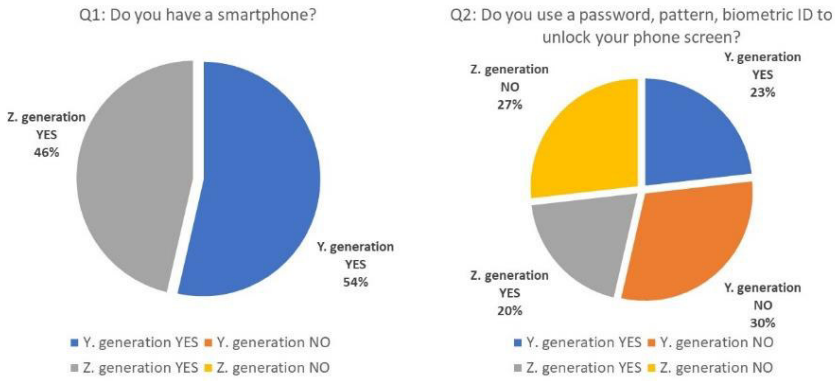

Figure 3. Evaluated safety awareness questionnaire responses (source: author's own)

Q3: Have you changed your unlock password or pattern over the past two months?

Q4: Have you changed your email inbox password in the last two months?

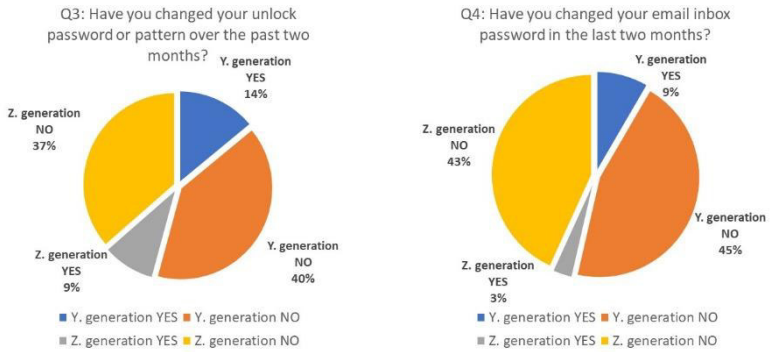

Figure 4. Evaluated safety awareness questionnaire responses (source: author's own)

Q5: Do you use the same password multiple times?
Q6: Did you give this password to someone?

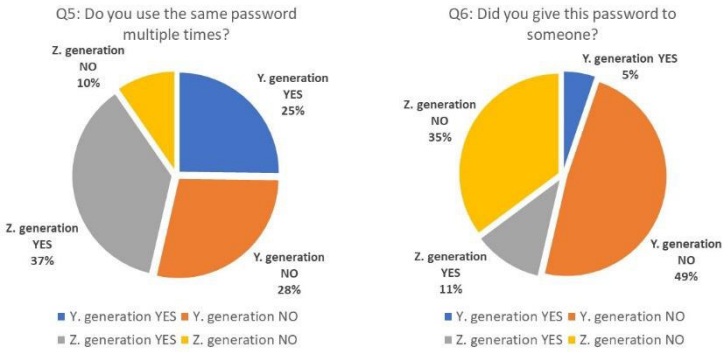

Figure 5. Evaluated safety awareness questionnaire responses (source: author's own)

Q7: Is your antivirus software up to date?
Q8: Do you store your personal information on your computer?

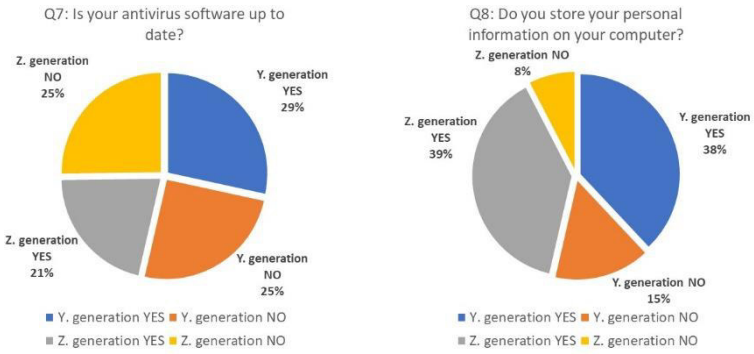

Figure 6. Evaluated safety awareness questionnaire responses (source: author's own)

Q9: Have you made a backup of them in the last two months?
Q10: Do you use IT tools at work for private purposes?

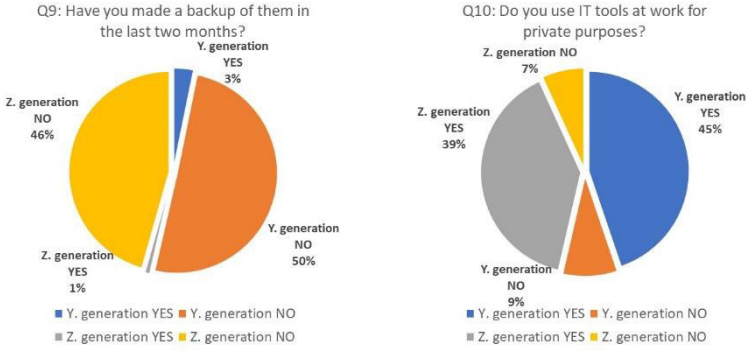

Figure 7. Evaluated safety awareness questionnaire responses (source: author's own)

As a result of the questionnaire, I made the following statements:

1. All respondents have a smartphone, but more than half (56-58%) do not properly protect their devices.

2. 74% and 79%, respectively, who have not changed their phone security solution in the last two months.

3. Over the past two months, 15% of Generation Y members have changed their mailbox password, which is used by 47% of users elsewhere. The same for Generation Z respondents, 7% and 80%.

4. 10% and 24% of the surveyed Y and Z generation users have already given this password to others.

5. 47% and 54% of the respondents, respectively, do not have an up-to-date antivirus system.
6. 71% and 84% of users store their personal data on a computer, but a small percentage (1-6%) of them have backed up in the last two months.
7. More than 83% of respondents also use corporate ICT tools for private purposes.

7 Summary, conclusions

During my research, I have found that most members of Generation Z and Generation Y do not adequately protect your personal information. However, nowadays, almost every movement we make, whether or not we communicate, with our consent or not, can impact our lives. I think the time has come to prioritize the security of our data over the convenience features. In my opinion, this process should be started from the ground up with members of the Alpha generation newly entering the education system, taking into account the needs of the digital age. Gamification and octalysis are the appropriate teaching methods.

In this topic, I plan to conduct further research on the relationship between smart cities and education, and the importance of adequate protection of biometrics.

8 References

[1] https://www.internetworldstats.com/stats.htm (Downloaded on 02/11/2020)
[2] https://www.welivesecurity.com/2018/12/17/most-popular-passwords-2018-revealed/ (download date: 7/30/2019)
[3] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (download date: 02/07/2018)
[4] https://168ora.hu/itthon/magyar-fejlesztés-kozpont-hacker-tamadas-adat- lose-kiss-antal-kkm-172356 (download date: 7/2/2019)
[5] http://subscribe.ofi.hu/uj-kozneveles/what-tap previous-s-kulul-az-alfa-generacio-az-iskolaba (download date: 21/09/2019)
[6] OECD Guidelines for the Security of Information Systems and Networks: Towards a Security Culture (http://www.oecd.org/sti/ieconomy/15582292.pdf) (download date: 02/07/2019)
[7] Dr. Kornélia Lazányi: Security Culture, Taylor: Journal of Business and Organizational Sciences: Publications of the Virtual Institute for Central Europe Research 7: (1-2) pp. 398-405.
[8] https://hostingtribunal.com/blog/biggest-data-breach-statistics/ (download date: 21/07/2019)
[9] https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (download date: 21/07/2019)
[10] https://usa.kaspersky.com/resource-center/threats/zeus-virus (download date: 21/07/2019)
[11] Gergely Horváth, Krisztián, CISA CISM: UNDERSTANDING (NOT ONLY) ON IT SECURITY, 2013 (https://kifu.gov.hu/sites/default/files/IT_brosura_v7.pdf) (download date: 02/07/2018)
[12] Guy, Retta; Marquis, Gerald (2016). The Flipped Classroom: A Comparison of Student Performance Using Instructional Videos and Podcasts Versus the Lecture-Based Model of Instruction. Issues in Informing Science & Information Technology. 13: 001-013. doi: 10.28945 / 3461st ISSN 1547-5840 (download date: 7/29/2018)

[13] Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". Proceedings of the MindTrek '11. doi: 10.1145 / 2181037.2181040
[14] Richards Fromann, Andrei Damsa: Motivational Toolkit for Gamification in Education, New Pedagogical Review, 2016, http://viroiratok.ofi.hu/uj-pedagogiai-memle/a-gamifikacio-jatekositas-motivacios-eszkoztara -in-tutorial # main-content (download date: 07/07/2018)
[15] Mohd Hishamuddin Abdul Rahman, Ismail @ Ismail Yusuf Panessai, Noor Anida Zaria Mohd Noor and Nor Syazwani Mat Salleh - Gamification Elements and Their Impact on Teaching and Learning, International Journal of Multimedia & Its Applications (IJMA) Vol.10, No.6, December 2018, DOI: 10.5121 / ijma.2018.10604 (download date: 02/07/2019)
[16] Yu-kai Chou: Actionable Gamification, Beyond Points, Badges, and Leaderboards, 2015, ISBN-10: 1511744049, ISBN-13: 978-1511744041
[17] Róbert Korényi: Why does gameplay work for the Y and Z generations? Applying Motivation Theories in the Gameplay Process, Generation (s) Studies on Generations, 2017, ISBN: 978-963-269-688-1

9 Figure index