Security awareness of Generation Z among university students

Klaudia Csercsa

Obuda University, Budapest, Hungary, csercsa.klaudia@phd.uni-obuda.hu

Abstract The research focuses on the cybersecurity awareness of Generation Z. This generation was born into the digital age, and the use of smart devices has been an integral part of their everyday lives since they were infants. How capable are they of making conscious decisions to properly protect their digital data? Are they aware of basic cybersecurity methods? Do they apply them? What is their level of digital security awareness? I did quantitative re-search for this. The research focuses on the following 2 hypotheses:H1: Generation Z mem-bers are not sufficiently cautious in terms of cybersecurity H2: Generation Z members do not receive adequate and relevant education on the topic of cybersecurity. Based on the re-sponses of the students involved in the research, we consider both hypotheses to be accepted. We recommend that Generation Z be educated on cybersecurity within an institutionalized framework, integrated into the curriculum, so that they pay more attention to protecting their data and live their online lives more responsibly

Keywords: Generation Z, cybersecurity, cyber protection

1 Introduction

The research examined the cybersecurity awareness of university stu-dents. The focus was on members of Generation Z, as a significant proportion of university students belong to this generation, and this is the first generation that has grown up in the digital age, and not only encountered the phenomenon of the online space that permeates their entire lives at a later stage in their lives.

The primary hypothesis of the research is that members of Generation Z are not sufficiently cautious in terms of cybersecurity. To support this assumption, I conducted a quantitative survey among university students. Participation in the research was voluntary and anonymous, using a snowball sampling method. The second hypothesis is that members of Generation Z do not receive adequate and relevant educa-tion on the topic of cybersecurity.

In the first part of the study, I clarify the emerging concepts through a critical analysis of relevant literature sources, followed by a presenta-tion of my primary research.

2 Generation Z

Different researchers categorize the members of each generation based on different years. It is not possible to draw a specific line in the years to sharply separate the main characteristics that are more charac-teristic of different generations. In my research, I consider the defini-tion of one of the most significant Hungarian generation researchers, clinical psychologist Annamária Tari, as a basis for comparison, i.e. those born between 1995 and 2009. They are preceded by Generation Y and followed by Generation Alpha. [1]

In the 21st century, the technological revolution permeates our every-day lives. The use of digital devices has become indispensable, and this is true not only for members of Generation Z, but for the vast ma-jority of people. Modern technology is present in education, the labor market, recreation, and all areas of our lives, and it even permeates our daily activities to an extent and depth never seen before. The ex-plosive development of information and communication technologies is a revolutionary change that we have not yet reached the end of. [2]

Today, we include fast, efficient, flexible and complex problem solv-ing, as well as excellent communication skills, effective information management and the ability to work in groups as basic expectations. [3]

Today's young people have a much broader range of interests than previous generations. This is thanks to the widespread, easily accessi-ble online world. The number of stimuli they encounter on a daily basis is increasing exponentially compared to previous generations. Such a turbulent pace of technological development has also had a significant impact on communication relationships [19].

“While in the lives of previous generations there was a clearly distin-guishable real and online identity, for today’s young people there is only one identity, meaning that for them offline and online existence are completely intertwined. For the young generation, these two are inseparable, and technology is only a means of expressing identity. [4]

The members of Generation Z were born into this world. They are the first global generation who listen to the same music, watch the same movies, have the same fast-food selection, and follow the same fash-ion regardless of their geographical birth. The use of digital devices is self-evident to them, and the phone is not only an accessory to their lives, but an integral part of them. They also experience their free time, social life, studies, and work on the airwaves. [1]

The attitudes and expectations of Generation Z are also completely different from those of previous generations. Their approach and rela-tionship to learning and work are completely different. They need to be motivated and valued differently than members of previous genera-tions. [5]

When Generation Z members face a problem or have a question, they expect an immediate answer. Patience and waiting for a complete, authentic answer are not their virtues. They take out their smart devic-es and search for the solution. Previous generations considered their teachers to be the main source of their knowledge. [6]

2.1 What platforms do Generation Z prefer?

Facebook was used and known specifically by young people, and then its use spread more and more widely among the older genera-tions. During a transitional period, young people slowly "erased out" from the camp of Facebook users or only left their profiles as an alter-native option (perhaps to reassure their parents), but they slowly moved their daily activities to Twitter, which is now called X, to In-stagram and later to TikTok, YouTube, and Snapchat. Using Face-book is no longer fashionable among young people. However, all the other platforms mentioned above are readily used every day.

3 Cybersecurity

Cybersecurity means the continuous and planned application of “po-litical, legal, economic, educational, awareness-raising and technical tools that can be used to manage risks arising in cyberspace.” This was discussed by, among others, Brigadier General Dr. László Ko-vács, a university professor at the Faculty of Military Science and Defence Officer Training and a cyber defense observer at the Hungar-ian Defence Forces Command, at a lecture at the Ludovika Free Uni-versity on Tuesday evening, 09.03.2022. [7]

The concept of cybersecurity does not only concern the private and corporate sectors. A country can also be exposed to a serious threat in cyberspace, i.e. the online world. In the 21st century, we no longer view aggression between countries in a purely physical sense.

Hungary considers cyber capabilities that threaten physical security or are capable of causing significant material damage as weapons, and their use as armed aggression, to which a response in the physical space is also possible (New National Security Strategy, 2020).

In United Dreams, a cyber general was appointed as early as 2008. They also declared that they might respond to a serious cyberattack with conventional missiles. [8]

An excellent example is the series of regular and very massive cyber-attacks that hit Estonia, in April and May 2007. This incident drew attention to the importance of global cooperation from a cyber defense perspective. NATO declared cyberspace an operational area in 2016, and the European Union also defined a number of tasks in this area for joint action between member states, effective information ex-change, and the protection of critical infrastructures. [9]

During the coronavirus pandemic, the digitalization of the economy and society has increased drastically all over the world. Many activi-ties could only be carried out digitally due to the quarantines that have appeared everywhere globally. Digitalization is changing our world. The effects of the rapid technological development of the fourth in-dustrial revolution pose enormous challenges to society and political decision-makers. [10] This transformation was particularly visible in higher education, where institutions and students had to rapidly adapt to online platforms and remote digital tools [17].

Remote IT solutions have become a collective and mass phenomenon in our world. From one day to the next, ordinary people have been forced to study online, work online, and shop online. The crisis has highlighted the seriousness of the (potential) dangers posed by cyberattacks.

The perpetrators of the attacks no longer posed an increased threat only to large companies, but mass threats affecting citizens have also become increasingly widespread. Jean-Baptiste Demaison, Chair of the Management Board of the European Union Agency for Cyberse-curity (ENISA), drew attention to the seriousness of the escalating situation and urged member states to identify new challenges and ad-dress them as soon as possible. [11]

More sophisticated and dangerous forms of attack appear every day, and their target may not only be large companies. Small and medium-sized companies, state institutions, critical infrastructure operators, or ordinary citizens may also fall victim.

Successful cyberattacks can result in the disclosure of business se-crets, personal and valuable information, or irreplaceable data about operations, and in addition to significant financial damage, significant loss of prestige can also be expected. Therefore, it is now very im-portant, one might say essential, to pay due attention to comprehen-sive and regular cybersecurity. [12]

Taking all these factors into account, it is necessary to create an open and secure online existence. This requires strong and up-to-date cy-bersecurity measures to ensure that citizens' security and trust in digi-tal devices and services remain intact. In Hungary, the Regulated Ac-tivities Supervisory Authority performs its official duties of certifying the cybersecurity of digital products based on EU Regulation

2019/881. The purpose of the certification activity is to guarantee compliance with the constantly evolving requirements of cybersecuri-ty in the case of info communication devices and services that can be purchased and used by citizens and businesses.

"The National Cybersecurity Strategy has defined as an important task that Hungary, through its specialized institutions, cooperation with civil, economic and scientific actors, supports activities aimed at and raising awareness of the safe use of cyberspace, as well as initia-tives promoting practical cybersecurity knowledge, paying special attention to raising awareness among individual users and small and medium-sized enterprises. Taking all this into account, one of the key goals of the SZTFH is for Hungarian citizens to use digital services safely, to know and consciously apply the procedures that will enable them to avoid or reduce the harmful effects of cyber threats" – empha-sized Dr. Balázs Bencsik, Director of Cybersecurity Certification at SZTFH. [13]

To promote cybersecurity awareness among ordinary citizens, the SZTFH has launched a podcast series called "Minden Kiberül". Here, the latest cybersecurity trends and threats are shared with the audience in plain language. The podcast aims to raise public awareness of the importance of cybersecurity and provide useful advice. [14]

3.1 Why is cybersecurity so important for ordinary citizens?

It is important to clarify from what perspective a cyberattack can af-fect the target group of Generation Z. An incident in cyberspace can cause any size problem, from a minor annoyance to the realization of a serious financial loss. As I explained earlier, this generation lives its social life primarily in the digital space. An attack on a social platform that shares personal data can have serious social consequences: em-barrassment, exclusion, depression, and in the most severe cases even suicide [18].

Even an attack on our reputation can cause very serious damage. The next level is where our data is abused. With ransomware, attackers achieve that we cannot access our personal data stored on our com-puter. Perhaps the most complex form of attack is when severe reputa-tion loss is combined with financial loss. After logging into a banking application on a public computer or using an improper password, we can also suffer serious financial losses.

The range of crimes is wide, but prevention and protection largely depend on the users. Properly managed and applied password protec-tion, two-factor authentication, keeping updates up to date, and keep-ing our passwords secret all contribute to not becoming the next vic-tim of a cyberattack. There are young people who have invested thou-sands of hours of their lives in an online game. If we consider the smallest incident to be hacking the game and not being able to log in to their own user profile, it can cause enough pain and annoyance. If untrue and malicious images of a young person are uploaded to vari-ous social platforms, they can suffer very serious, even lifelong, psy-chological abuse and even lose their friends.

4 Risk analysis on digital platforms used by Generation Z

I conducted my quantitative research using a questionnaire survey. A total of 171 responses were evaluable. I used a snowball sampling technique online. My sample is not representative.

First, I assessed which platforms are the most popular among Genera-tion Z today. Respondents could select multiple options, according to their habits.

As expected, the most popular online platforms are the following: Instagram is the most popular, which is used regularly by 88%, fol-lowed by YouTube 86%, and then in 3rd place on the podium is Tik-Tok, which represents 82% of respondents. TikTok (as expected) is more popular than Facebook.

My next study was about cybersecurity awareness. I was looking for an answer to the question of how often respondents change their passwords in general.

It is sad to see that 25% of the respondents have never changed their password, while 45% last changed it more than 6 months ago. In total, 4% change their password every month and the same number of re-spondents change their password approximately every 2 months. This generation was born into online life. They use their smart devices al-most every hour, their smartphones are constantly logged in on all password-protected platforms, perhaps with the exception of online banking, yet their user awareness falls short of the desired level. This question also clearly illustrates that more needs to be taught about cyberattacks and cybersecurity and greater emphasis needs to be placed on it during everyday life.

Finally, I closed the questionnaire with an open question, where re-spondents had the opportunity to share their personal experiences and opinions. Completing the question was not mandatory.

The vast majority of the responses (approximately 80%) were that cybersecurity is a very important and under-emphasized topic these days. More education and information should be shared on this topic and young people should be made more aware of this topic. A particu-larly interesting segment of the responses is that so many people are aware that they have shortcomings in the field of cybersecurity, but they no longer devote their free time to looking into it or getting in-formation on the issue themselves. This is also a typical characteristic of this generation. They like to get answers ready (instantly). They don't spend time on what they don't shove under their noses, even if they know that they have shortcomings in such an important and even life-defining thing.

There was also a surprising answer to this question, which I would like to quote verbatim. The answer was: “The generation before us is quite negligent in handling the data entrusted to them.” This answer could be evaluated from many aspects, which are not closely related to the topic of our research, so I will not go into it, but I found it worth mentioning.

3.1 Tips for higher cybersecurity protection based on my secondary research

- It is important to perform regular backups.
- Managing our passwords is of paramount importance. We should have separate passwords for each important platform. The password can be of mixed composition, but it is more important that it is long enough, if it needs to be quantified, in today's world it should be at least 12 characters long, but in important places it is better to have more. [15]
- Where we have the opportunity, we should use the option of two-step identification.
- We should avoid opening suspicious emails or using links in emails. If we receive an email from a friend with an unusual wording that also contains a link, we should not click on the link until we have in-formed the sender of the suspicious message. A typical example is the case of fake utility bills.
- We should use antivirus and anti-malware on our devices. The use of these programs should be essential.
- When using external data carriers, e.g. We connect a pen drive to our device, let's check it with our machine to see if it is safe to use.
- If you are not using Bluetooth, turn it off to prevent data leakage via Bluetooth devices.
- Keep your cybersecurity knowledge up to date. Take the time to inquire and get informed regularly to protect your data. Don't skimp on your resources and even seek professional help.
- Avoid using public and free Wi-Fi networks if possible. Communi-cation or file sharing may not be secure.
- If you are a victim of a cyberattack, it is important to inform as many potential victims and service providers as possible about the incident as possible. [16]

Summary

In my research, I sought to answer the question of how much mem-bers of Generation Z make conscious decisions regarding their cyber-security protection. My secondary research was followed by primary research, where I applied a quantitative method using a questionnaire and a snowball sampling procedure, focusing on the responses of Generation Z. After data cleaning, I found a total of 171 completed responses that could be evaluated. As a result of my research, it can be said that from the perspective of risk analysis, Generation Z, based on their user habits, can participate in various digital platforms with a high-risk factor. They do not make conscious decisions in order to protect their data, they do not come across preparatory materials on cybersecurity, and they do not deal with cybersecurity to a satisfactory level. Based on this, I consider the two hypotheses set out in the research, namely: members of Generation Z are not sufficiently cautious in terms of cybersecurity, and members of Generation Z do not re-ceive adequate and relevant education on the topic of cybersecurity, to be confirmed and accepted.

My suggestion is that ordinary users should meet on many more communication platforms regarding cybersecurity and protection. The importance of the security of our digital data should be better promot-ed by more educational videos, advertisements, podcasts or influenc-ers, and it should also be integrated into the National Core Curricu-lum. This research focused on Generation Z, who are currently the most active online generation, and I believe that even among them I discovered major shortcomings in this regard. Previous generations, who were not born into the digital age but had to learn about and ap-ply the excitement of being online as adults, could probably discover even greater shortcomings. This could be the subject of another re-search, but in any case, the stakes and potential sources of danger cannot be ignored.

References

[1] Tari A. (2011) Z generáció Tercium Kiadó

[2] Keszthelyi, A. L. (2015). Jelszavakról-iparági legrosszabb gyakorlatok=Passwords-worst practices in user authentication. Taylor, 7(3-4), 261-268.

[3] Cisco, Intel, Microsoft (2009): Transforming Education: Assesement and Teaching 21st Century Skills

[4] Ujhelyi, A. (2013). Digitális nemzedék–szociálpszichológiai szempontból. Lévai Dóra (szerk.) Digitális nemzedék konferencia, 9-14.

[5] Oblinger, D., Oblinger, J. et al. (2005). Educating the net generation. Brockport Bookshelf. EDUCAUSE, available electronically at www.educause.edu/educatingthenetgen/

[6] Duga, Zs. (2013). Tudomány és a fiatalok kapcsolata. Kutatási tanulmány PTE Közgazdaságtudományi kar

[7] Tasi, T. (2022). https://www.uni-nke.hu/hirek/2022/03/09/netvedelem-nelkul-semmi-sincs

[8] Coleman, K. (2008). https://www.military.com/defensetech/2008/01/02/the-new-cyber-general

[9] Hertelendi, L., & Hornyik, Z. (2022). „A kiberbiztonság jelentősége a minden-napokban”: Interjú Kovács László dandártábornokkal, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanárával. Belügyi Szemle, 70(6), 1327-1337.

[10] Rajnai, Z., & Kocsis, I. (2017, September). Labor market risks of industry 4.0, digitization, robots and AI. In 2017 IEEE 15th international symposium on intelli-gent systems and informatics (SISY) (pp. 000343-000346). IEEE.

[11] Demaison, J-B., (2020). https://www.enisa.europa.eu/sites/default/files/all_files/ENISA_Strategy_leaflet_HU.pdf

[12] 4iG (2025). Kiberbiztonság - Holisztikus szemléletű komplex kiberbiztonsági szolgáltatások és technológiák. https://www.4ig.hu/it/megoldasok/kiberbiztonsag

[13] Új állami szereplő a kiberbiztonsági palettán (2022). https://www.computertrends.hu/prcikk/uj-allami-szereplo-a-kiberbiztonsagi-palettan-320222.html

[14] Minden kiberül – kiberbiztonsági podcastet indított az SZTFH (2024). https://sztfh.hu/minden-kiberul-kiberbiztonsagi-podcastet-inditott-az-sztfh/

[15] Keszthelyi, A. (2013). A jelszavakról. Acta Polytechnica Hungarica , 10 (6), 99-118.

[16] Canteli, A. (2021). https://www.openkm.hu/hu/blog/bevalt-gyakorlatok-a-kiberbiztonsagban.html

[17] Lazányi, K., Vincze, A., & Szikora, P. (2021). The digital skills in the Hungarian higher education during the first wave of Covid-19. Higher education policies for developing digital skills to respond to the Covid-19 crisis: European and global perspectives, 4-18.

[18] Szikora, P. (2011). Döntések szerepe a vállalkozások fejlesztésében. Tanulmánykötet-Vállalkozásfejlesztés a XXI. században, 171-180.

[19] Ali, B., & Szikora, P. (2017). Az Y generáció és az internet kapcsolata. Tanulmánykötet-Vállalkozásfejlesztés a XXI. században VII., 11-23.