

Cybersecurity among University Students from Generation Z: A Comparative Study of the Undergraduate Programs in Administration and Public Accounting in two Mexican Universities

Adán López Mendoza¹, Ramón Ventura Roque Hernández¹,
Ma. Teresa Prieto Quezada², Rolando Salazar Hernández¹

¹*Autonomous University of Tamaulipas, Av. de la Republica SN Nuevo Laredo, Tamaulipas, C.P. 88275, Mexico*

²*University of Guadalajara, Periférico Norte N° 799, Núcleo Universitario Los Belenes, C.P. 45100, Zapopan, Jalisco, Mexico*

Abstract—The present study aimed to differentiate cybersecurity habits among Generation Z university undergraduate students of Public Accounting and Administration at two Mexican public universities and to identify relationships between the study participants' self-perceived level of computer knowledge and cybersecurity habits. Data were collected using a questionnaire, which was administered to 321 and 242 students from Tamaulipas and Jalisco respectively. The results showed that students from Jalisco scored higher in knowledge regarding cybersecurity and risky practices. Similarly, weak relationships were found between participants' habits/routines and self-perceived knowledge about cybersecurity. Our study highlights the importance of providing curricular and extracurricular cybersecurity-related training.

Keywords: Computer security, Students, Higher Education, Awareness, Cybersecurity.

DOI: 10.18421/TEM121-60

<https://doi.org/10.18421/TEM121-60>

Corresponding author: Adán López Mendoza,
Autonomous University of Tamaulipas, Av. de la Republica SN Nuevo Laredo, Tamaulipas, C.P. 88275, Mexico


Email: aLopez@uat.edu.mx

Received: 03 November 2022.

Revised: 11 February 2023.

Accepted: 15 February 2023.

Published: 24 February 2023.

 © 2023 Adán López Mendoza, Ramón Ventura Roque Hernández, Ma. Teresa Prieto Quezada, Rolando Salazar Hernández; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

1. Introduction

Cybersecurity has increased in importance in recent years. Long considered a corporate issue, cybersecurity now involves dealing with vulnerabilities that anyone can expose to untrustworthy actors simply by using electronic devices.

Cybersecurity research conducted among university students has revealed various risky practices and routines. Most often, students lack any formal education regarding this subject and therefore may engage in activities that compromise their personal or business devices and data. Furthermore, at work, they may compromise their organization's resources.

This article presents the results of a study examining the students of undergraduate programs in Public Accounting and Administration in two Higher Education Institutions (HEIs): the Faculty of Commerce, Administration and Social Sciences (*Facultad de Comercio, Administración y Ciencias Sociales – FCACS*), Nuevo Laredo, Autonomous University of Tamaulipas (*Universidad Autónoma de Tamaulipas – UAT*) and the University Center for Economic and Administrative Sciences (*Centro Universitario de Ciencias Económico Administrativas – CUCEA*) of the University of Guadalajara (*Universidad de Guadalajara – UdeG*).

The research questions were

1) What differences in computer security-related habits, perceptions, and routines exist between Generation Z university undergraduate students of public accounting and administration at UAT and UdeG?

2) Are computer security habits and routines related to the self-perceived computer knowledge of these students?

The present study had the following objectives:

- 1) To determine differences in computer security-related perceptions/habits/routines between Generation Z university students of public accounting and administration based on academic major and institution; and 2) to identify any relationships between the self-perceived computer knowledge and the computer security habits/routines of these university students.

Generation Z

The currently available literature on generations of people who live and coexist within different areas of society is vast. In the context of the present study, we focused on Generation Z university students of Public Accounting and Administration. These young students have started to enter the labor market in recent years [1]. The birth years of each generation can vary based on research authors’ criteria. The classification proposed by [6] was used in this study (see Table 1).

Table 1. Chronological classification by generation

Generation	Chronological classification
Traditionalist	1900–1945
Baby Boomer	1946–1964
X	1965–1979
Y	1980–1994
Z	1995.....

Source: [2]

The term “generation” describes a group of people who have been born and have grown up in the same period and, therefore, share certain characteristics in technological, economic, and cultural terms [3]. Thus, based on their birth year, individuals can be easily related to one of the existing generations.

Several studies have researched Generation Z as well as its predecessors to detect any similarities and differences between them—albeit, more often, this generation has been compared with Generation Y rather than Generation X [4], [5]. These “Zennials” are also known as “children of the internet,” “digital generation,” “digital natives,” “media generation,” “post-millennials,” “iGen,” “Gen Zers,” or even “.com generation” [2], [6].

The term “digital natives” describes individuals who grew up with technology rather than becoming accustomed to using it—as was the case with Generations X and Y [1] or some previous generations. Technological advancement is the most distinctive feature of this generation.

In fact, these young people tend to be classified as technology addicts.

Cybersecurity

Blažič, B. J. [7], has defined cybersecurity as an organization of resources, processes, and structures for protecting cyberspace and cyberspace-enabled systems from events that violate property rights. This definition clarifies that cybersecurity involves the protection of information and devices, more specifically their confidentiality, integrity, and availability.

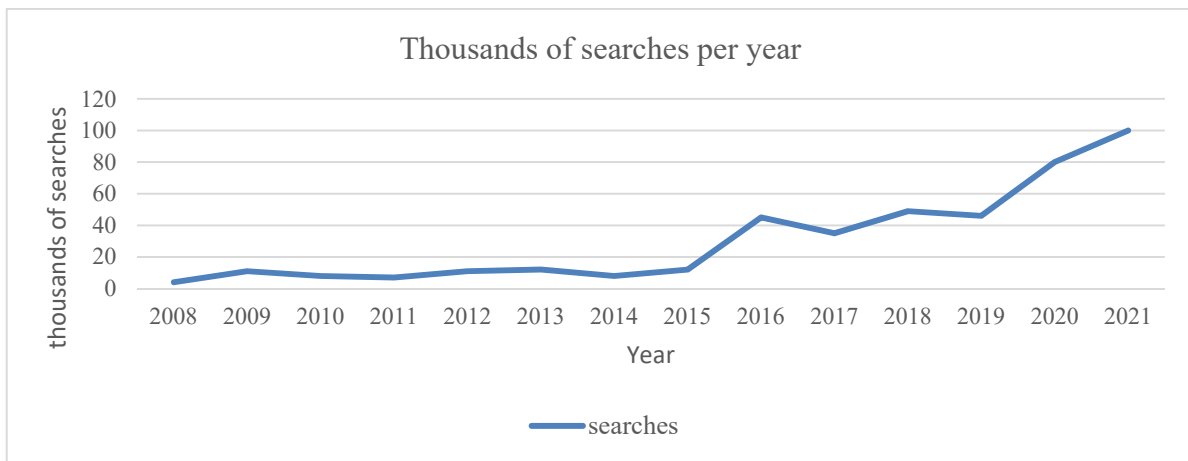
Concerns about computer security have increased considerably in recent years because most people tend to spend long periods in front of electronic devices. Some studies have mentioned that people spend more than half a day using such devices [4]. Analyzing cybersecurity is important because most people (ranging from children younger than 6 years to people older than 80 years) are now using electronic devices in their daily lives.

Technology has changed our work, academic, entertainment, and leisure activities and even how we sleep and wake up. Given these considerations, greater use of technological devices in daily activities predicts a greater risk of falling victim to cyberattacks. In Mexico, according to the National Guard (*Guardia Nacional – GN*), 2,898 cybercrime complaints were filed in 2020 [8]. This reports double the number of incidents recorded in 2019.

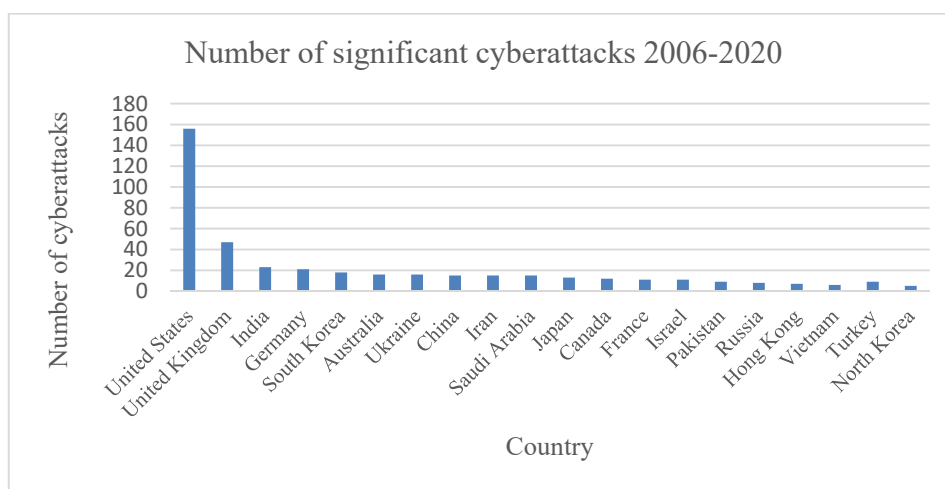
In recent years, we have witnessed different cyberattacks against financial, government, health, and airline organizations among others [9]. This author showed that young graduates of European Union (EU) universities often lack the professional knowledge and skills necessary for addressing cybersecurity activities in any organization. Similarly, the findings of Chychkan, I. V., Spasiteleva, S. O., and Zhdanova, Y. D. [9] flagged certain deficiencies in the academic programs of Higher Education Institutions (HEIs), which should reformulate their contents.

According to them, until recently, cybersecurity was regarded as a challenge to be dealt with by the technology departments of organizations and not as a business risk. Highlighting the importance of this topic, Graph 1 shows the increase in the number of Google searches for the term “cybersecurity” in recent years.

Several studies have mentioned that people form the weakest link in cybersecurity or the first line of defense [10]. As such, those without the necessary and sufficient knowledge for facing these situations tend to be more vulnerable.



Graph 1 Evolution of searches for the term “cybersecurity”
Source: The authors with data from [11]



Graph 2 Number of significant cyberattacks 2006–2020
Source: The authors with data from [11]

Graph 2 shows that the United States is the most cyber-attacked country with 156 attacks, followed by the United Kingdom with 47. In short, the United States receives approximately thrice the cyberattacks perpetrated in the United Kingdom.

The financial amounts lost to cyberattacks are incalculable. In the United States, the “Internet Crime Complaint Center” (IC3) reported that, from its creation in 2000 till 2020, 5,679,259 complaints were generated. In the last five years, 440,000 complaints have been filed per year on average. From 2016 to 2020, 2,211,396 complaints were reported, accounting for losses approaching \$13.3 billion [12].

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., and Koshutanski, H. [13], say that modern states must create a secure cyberspace by coordinating the activities of international organizations and individual states.

Scientists and academics must focus on developing new approaches for ensuring cyberspace security and the analysis of modern threats and cybercrimes that can destabilize technological systems.

These authors propose using blockchain technology to counter cyberattacks. This type of technology involves a multifunctional and multilevel digital system consisting of separate distributed ledgers in which all transactions are tracked continuously [13].

Cybersecurity and higher education

Cybersecurity has become a major issue. Teaching students to utilize basic cybersecurity concepts such as encryption protocols is challenging but critical for protecting personal and national security [14]. This problem must be approached from different angles. HEIs must update their study plans and academic programs by including current cybersecurity-related content to ensure that students develop the necessary knowledge and skills for working in the production sector.

However, organizational training departments must address the problem by updating their Information Technology (IT) staff, especially those related to cybersecurity. This area of the job market, however, is so broad that a single educational program cannot prepare students to fill any cybersecurity position.

The current generation (Z) students are digital natives; they have grown up in a technological environment that has often involved video games. According to [14], students' interest can be directed toward cybersecurity through playful activities—for instance, through systems that can involve young people in aspects such as cryptography, which aims to safeguard information and communications by using codes and is the current basis of secure network infrastructures. Cryptography is also a core research area in data security and a crucial element of information assurance. For these reasons, the teaching and learning of cryptography, whose key concepts are encryption, decryption, and cryptanalysis, must be included in all data security courses.

Kovacevic, A., Putnik, N., and Toskovic, O. [15], highlighted the importance of keeping abreast with cybersecurity issues because this area has become an essential part of the life cycle of organizations, especially those related to critical infrastructure operations. The abovementioned study combined process security models and pedagogical methods that promote skills development. Their approach is based on Bloom's taxonomy. Initially, the instructor prepares the program for professional cybersecurity certification. Then, the students receive the information and are continuously evaluated as they move upward through the training levels—that is, as they transition from the most basic to the most advanced levels, as in the layers of Bloom's taxonomy.

López Mendoza, A., Roque Hernández, R. V., Prieto Quezada, Ma. T., and Salazar Hernández, R. [16] and Magano, J., Silva, C., Figueiredo, C., Vitória, A., Nogueira, T., and Pimenta Dinis, M. A. [17] state that, considering increasing Internet availability and the continuously growing number of internet-connected devices, the cybersecurity of HEIs must be ensured. These institutions are key cells in the growth of a network that involves most of those who conduct some academic activities (e.g., professors, students, and administrators). In their study, the authors [16] & [17] mention that teaching-learning processes could be obstructed if certain services, particularly “electronic university” services, are affected, thereby breaching the contract with users when charging fees for any service. Furthermore, obstructing such processes could cause material and moral damage. Thus, data security and cybersecurity must be ensured in HEIs [17].

Mendivil Caldentey, J., Sanz Urquijo, B., and Gutierrez Almazor, M. [18] proposed a network learning model that could enable virtualization, the use of cloud technologies, and the use of mobile applications. This model was intended to provide students with specialized and professional data security and cybersecurity-related knowledge and skills. Accordingly, a proposal for the step-by-step creation of a learning environment for academic disciplines such as “Data Security,” “Data Protection,” and “Cybersecurity,” for example, was set forth at the Taras Shevchenko National University of Kyiv (*Київський національний університет імені Тараса Шевченка – KNU*), Ukraine, and at the Borys Hrinchenko Kyiv Metropolitan (*Київський столичний університет імені Бориса Грінченка – KUBG*) University. This learning environment was developed because of a growing current demand for professionals having solid security and cybersecurity-related knowledge.

The authors of this study previously addressed the subject of cybersecurity when analyzing other academic majors—mainly information technology and administration—and the generations preceding Generation Z [19], [20] and [21].

Cybersecurity during the pandemic

In 2020, the world faced a pandemic that forced society and companies to take restrictive measures during lockdowns. This situation necessitated the implementation of overnight emergency measures to allow essential industries' activities to continue [22]. Students had to continue their school activities by using online educational platforms, which most of them had never used before. Consequently, students faced some disadvantages because of online learning.

In other sectors of society, many people were forced to use technology, either for work (home office), online shopping, or communication with family and friends, thus exposing themselves to the risks of malicious attacks or identity theft.

Computer security habits and knowledge

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., and Blignaut, R. J. [23], analyzed the different factors that can influence university students' cybersecurity behaviors after considering sociodemographic data, cybersecurity perceptions, prior cybersecurity breaches, use of IT, and level of knowledge on the topic, among other aspects. The authors found that knowledge had the greatest influence with regard to cybersecurity behaviors and that, students—even though they were digital natives—felt unsafe and lacked security or adequate knowledge to protect themselves in cyberspace.

In other way [24] addressed factors related to risk-taking preferences, demographic styles, and personality traits. The authors found that financial and rational decision-making and gender were good predictors for safety behaviors and that gender was associated with password strength—with men generating stronger passwords than women.

2. Material and methods

The following section summarizes the research methodological details presented in this work.

Participants

The present study participants were students from two Mexican public universities, one situated in the northern part of the country, FCACS-UAT, and the other situated in the central part of the country, CUCEA-UdeG.

FCACS-UAT had a population of 2,574 students with five academic programs during the summer of

2019, whereas CUCEA-UdeG had a population of 19,319 students in its 14 academic majors [25].

Table 2 presents the sample of this study.

Table 2 Convenience sample characterized by Institution and Academic Major

Institution	Public Accounting	Administration	Total
UAT	177	144	321
UdeG	172	123	242
Total	349	267	563

At the time of the study, the participating students, all born after 1995, were majoring in Administration and Public Accounting. All the students were enrolled in the summer term of 2019 and give their informed consent.

Instrument

The items of this study’s utilized instrument are outlined in Table 3.

Table 3 Data collection instrument

No.	Question	Score
1	How much do you know about computers?	0 to 10
2	How much do you know about computer security?	0 to 10
3	How much do you know about computer viruses?	0 to 10
4	How likely are you to install malware on your computer?	0 to 10
5	How many times have you been a victim of identity theft in the last twelve months?	0 to 10
6	How concerned are you that your personal information could be stolen when using the Internet?	0 to 10
7	How many movies have you watched online in the last 30 days?	0 to 10
8	How many backups of personal information have you performed in the last 30 days?	0 to 10
9	How many times have you visited an institution specializing in personal data protection in the last 12 months?	0 to 10
10	How often have you consulted the knowledge of someone specialised in systems to advise you on computer security in the last twelve months?	0 to 10
11	How many active email accounts do you check daily?	0 to 10
12	How likely are you to include important dates, such as birthdays or anniversaries, in a password?	0 to 10
13	How likely are you to share any of your passwords with someone else?	0 to 10
14	How many total characters (length) is the password for the email account you use the most?	0 to 20
15	How many special characters does the password of the email account that you use the most have? (special characters include, for example, ;'#\$%&/()=?_!@~*)	0 to 20
16	How likely are you to use the same password on two or more web pages?	0 to 10
17	How likely are you to change your email password once a month?	0 to 10
18	How respectful are you of the rules of the information systems of your institution and/or workplace?	0 to 10

This instrument has been used in previous studies, and it has been prepared and refined by specialists in technology and education [19] and [20].

Program coordinators helped administer the questionnaire, and they helped the researchers by accompanying them to the classrooms to request responses from the students. The questionnaire was distributed in the form of printouts. The students' participation was voluntary and anonymous, and they received no incentives or rewards for filling out the questionnaire.

Data analysis techniques

The study data were analyzed using the statistical packages SPSS 24 and Jamovi 2.2.5. First, in SPSS, the data were captured to conduct an exploratory

analysis. Subsequently, in Jamovi, the descriptive statistics were calculated. Shapiro-Wilk normality tests were also performed, and their result indicated a non-normal response distribution. For this reason, robust ANOVA tests were performed in the Walrus package. In these tests, the effects of academic majors and institutions, as well as the simultaneous effects of both, on the participants' responses were deemed significant based on the corresponding p-values. Spearman's rank correlation coefficients were determined to identify correlations between the self-perceived knowledge and computer security habits of all the participants. In all the cases, a 95% confidence level was used, so p-values lower than 0.05 indicated significant effects.

Results

The mean, median, standard deviation, and interquartile range of the different responses to the questionnaire are outlined in Table 4.

Table 4. Descriptive statistics of the responses

Question	Mean	Median	Standard deviation	IQ Range
Q1	6.028	6.00	2.07	3.00
Q2	4.952	5.00	2.31	4.00
Q3	4.693	5.00	2.33	3.00
Q4	5.407	6.00	3.05	5.00
Q5	0.536	0.00	1.60	0.00
Q6	6.734	8.00	3.01	5.00
Q7	4.487	4.00	3.51	5.00
Q8	2.815	2.00	2.99	4.00
Q9	0.405	0.00	1.31	0.00
Q10	1.806	0.00	2.62	3.00
Q11	2.466	2.00	1.85	2.00
Q12	3.208	2.00	3.56	5.50
Q13	1.840	1.00	2.53	3.00
Q14	10.678	10.00	3.62	3.00
Q15	2.062	0.00	3.60	2.00
Q16	5.806	6.00	3.59	7.00
Q17	1.881	1.00	2.74	3.00
Q18	7.030	8.00	2.93	5.00

Table 5 presents the results that showed significant differences attributable to academic majors, institutions, or the interaction between both.

Table 5 Significant differences according to the Robust ANOVA test

Question	Between academic majors (PA and LA)	Between institutions (UdeG and UAT)	Combined interaction effects between academic majors and institutions
Q1	p=0.038 PA(M=6.5, SD=1.8) AD(M=6.3, SD=1.7)	p=0.001 UdeG (M=6.4, SD=1.8) UAT (M=5.7, SD=2.1)	
Q2		p=0.002 UdeG(M=5.1, SD=2) UAT (M=4.6, SD=2.4)	
Q4		p<0.001 UdeG (M=5.8, SD=2.8) UAT (M=5, SD=3.1)	
Q8			p=0.01 UdeG, LA (M=3.5 SD=3.1). UAT, LA (M=2.1, SD=2.5)
Q14		p=0.041 UdeG (M=11.1, SD=3.1) UAT (M=10.3, SD=3.9)	
Q16		p=0.010 UdeG (M=6.2, SD=3.6) UAT (M=5.4, SD=3.5)	
Q18	p=0.039 PA (M=7, SD=2.8) AD (M=7.5, SD=2.8)		

Note. M=Mean, SD= Standard deviation, p=p-value, PA=Public Accounting, AD=Administration, UAT=University of Tamaulipas, UdeG=University of Guadalajara

Table 6 outlines the main correlations found in this study.

Table 6 Significant Spearman's rank correlations between questions and self-perceived computer knowledge.

	Q1 - Computer knowledge		Q2 - Knowledge on computer security		Q3 - Knowledge on computer viruses	
Q6	0.125	**	0.161	***	0.169	***
Q8	0.197	***	0.242	***	0.145	***
Q21			-0.091	*		
Q14	0.112	**	0.109	*		
Q17	0.113	**	0.159	***	0.119	**
Q18	0.144	***	0.149	***	0.147	***

Note. N= 563, * p < 0.05, ** p < 0.01, *** p < 0.001

The table outlines Spearman's Rho values (asterisks indicate the p-value).

Overview of computer security-related knowledge among the participants

3. Discussion

In this section, we will discuss the implications of our findings, suggestions, potential limitations, and avenues for future research.

The university students assessed their own computer knowledge with a 6/10 score, on average; this shows that they acknowledged having some degree of ignorance regarding the subject.

This self-awareness increased in their responses to Questions 2 (How much do you know about computer security?) and 3 (How much do you know about computer viruses?). The average score for these two questions did not reach 5/10. Another noteworthy piece of information was provided by the responses for Question 4 (How likely are you to install malware on your computer?); the responses indicated, on average, a probability higher than 50%. This result indicates that students are more likely to be exposed to vulnerabilities caused by malware. Nevertheless, they expressed concern (6.7/10) that their information would be stolen when connected to the Internet. In answering the question regarding the number of characters in their email password (Question 14), the students indicated an average of 10.6 characters. This number suggests that their passwords generally have medium strength. Last, the participants stated that they were moderately respectful of the rules of the information systems of their institution or workplace (7/10).

Differences in computer security

The main differences regarding computer security awareness were found between institutions because UdeG students scored higher than UAT students. For example, they reported a higher self-perceived knowledge regarding cybersecurity than UAT students. However, the high scores of UdeG students do not necessarily imply an advantage because two of the questions referred to risky practices, namely Questions 4 (How likely are you to install malware on your computer?) and 16 (How likely are you to use the same password on two or more web pages?).

Correlation between self-perceived computer knowledge and computer security habits/routines

When examining students' self-perceived computer knowledge and its association with computer security habits and routines, several correlations were significant, though they were all weak or very weak.

Practical implications and suggestions

The cybersecurity knowledge field is constantly evolving. Accordingly, HEIs must periodically update the contents of their study plans and curricula to include current relevant cybersecurity aspects in their academic majors. Similarly, extracurricular activities and continuous institutional communication may help students strengthen their computer security levels.

Limitations

This study had some limitations. The research was conducted in only two faculties of two public universities and was limited to only two of their economics and administration majors—namely, public accounting and administration.

Moreover, this study utilized a convenience sample, and results could not be generalized.

Comparing the present study's results with the literature

Our results differ from those of [23] because our study did not find any strong relationship between cybersecurity knowledge and cybersecurity behaviors. Similarly, our findings differed from those reported by [24] because these authors did not find any significant gender differences in terms of password strength.

4. Conclusions

This article presents the results of a research study conducted in two HEIs in the Mexican Republic, namely UAT and UdeG. This study's analyzed academic majors were Public Accounting and Administration. The findings revealed a wide range of opportunities for universities to raise computer security levels among their students. Our research highlights the importance of providing students with curricular and extracurricular cybersecurity-related training and conducting research in this area.

Future Lines of Research

Further future research should examine more academic majors and institutions and utilize probabilistic sampling. Future studies should also address more cybersecurity dimensions in their objectives and conduct a more in-depth analysis of the relationships between various computer security habits.

Acknowledgments

Authors would like to thank UAT and UDG for their support in the development of this research.

References

- [1]. Younis, Y. A., & Alghamdi, M. Y. (2021). The use of computer games for teaching and learning cybersecurity in higher education institutions. *Journal of Engineering Research (Kuwait)*, 9(3A), 143–152.
- [2]. Alzahrani, L. (2021). Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. *International Journal of Advanced Computer Science and Applications*, 12(11), 630–637.

- [3]. Antonyan, E. A., & Rybakova, O. S. (2020). Blockchain technologies for security against cyber attacks. *Bulletin of National Academy of Sciences of The Republic of Kazakhstan*, 4(386), 21–26.
- [4]. Asociación de Internet MX. (2021, June 12). *Estudio de Ciberseguridad en empresas, usuarios de internet y padres de familia en México 2021*. Asociación de Internet Mx. Retrieved from: <https://irp.cdn-website.com/81280eda/files/uploaded/Estudio%20de%20Ciberseguridad%20AIMX%202021%20%28Pu%CC%81blica%29%2020210614.pdf> [accessed: 12 August 2022]
- [5]. Benítez-Márquez, M. D., Sánchez-Teba, E. M., Bermúdez-González, G., & Núñez-Rydman, E. S. (2022). Generation Z Within the Workforce and in the Workplace: A Bibliometric Analysis. *Frontiers in Psychology*, 12, 736820.
- [6]. Berkup, S. B. (2014). Working with generations X and Y In generation Z period: Management of different generations in business life. *Mediterranean Journal of Social Sciences*, 5(19), 218.
- [7]. Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*.
- [8]. Campbell, W. K., Campbell, S. M., Siedor, L. E., & Twenge, J. M. (2015). Generational differences are real and useful. *Industrial and Organizational Psychology*, 8(3), 324–331.
- [9]. Chychkan, I. v, Spasiteleva, S. O., & Zhdanova, Y. D. (2021). The educational environment for forming secure base behavior in cyberspace of future professionals in economics and management. *Information Technologies and Learning Tools*, 84(4), 354–375.
- [10]. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21.
- [11]. FBI. (2020, May 27). *2020 Internet Crime Report*. Internet Crime Complaint Center IC3. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [accessed: 20 August 2022].
- [12]. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358.
- [13]. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern aspects of cybersecurity training and continuous adaptation of programmes to trainees. *Applied Sciences*, 10(16), 5702.
- [14]. Klopota, I., Aleksić, A., & Vinković, N. (2020). Do Business Ethics and Ethical Decision Making Still Matter: Perspective of Different Generational Cohorts. *Business Systems Research: International Journal of the Society for Advancing Innovation and Research in Economy*, 11(1), 31–43.
- [15]. Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, 8, 125140–125148.
- [16]. López Mendoza, A., Roque Hernández, R. V., Prieto Quezada, Ma. T., & Salazar Hernández, R. (2022). Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y, Z: Un estudio comparativo de dos universidades públicas en México. *Dilemas Contemporáneos: Educación, Política y Valores*, IX(3), Artículo no. 26.
- [17]. Magano, J., Silva, C., Figueiredo, C., Vitória, A., Nogueira, T., & Pimenta Dinis, M. A. (2020). Generation Z: Fitting project management soft skills competencies—A mixed-method approach. *Education Sciences*, 10(7), 187.
- [18]. Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit Revista de Medios y Educación*, 1(63), 197–225.
- [19]. Nashynets-Naumova, A. Y., Buriachok, V. L., Korshun, N., Zhylytsov, O. B., Skladannyi, P., & Kuzmenko, L. (2020). Technology for information and cyber security in higher education institutions of Ukraine. *Information Technologies and Learning Tools*, 77(3), 337–354.
- [20]. Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education*, 32(2), 134–149.
- [21]. Roque, R. v., & López, A. (2019). IT Security Perceptions and Practice in X, Y and Z Generations. In Fondo Editorial Universitario (Eds.), *Liderazgo y producción de Cuerpos Académicos: Vol. I* (343–353). Universidad de Guadalajara.
- [22]. Roque Hernández, R., López Mendoza, A., & Villarreal Álvarez, M. (2019). La seguridad Informática en estudiantes universitarios de la Licenciatura en Administración nativos de la generación Z. *Vinculatégica EFAN*, 373–382.
- [23]. Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics*, 10(22), 2865.
- [24]. Universidad de Guadalajara, C. U. de C. E. A. (2020). *Primer informe de actividades 2019-2020 Mtro. Luis Gustavo Padilla Montes. Rector*. Universidad de Guadalajara. Retrieved from: <https://cucea.udg.mx/informe-2019-2020/> [accessed: 02 September 2022].
- [25]. World Economic Forum & Mclennan, M. (2021). *The Global Risks Report 2021 16th Edition Strategic Partners*. Retrieved from: <http://wef.ch/risks2021> [accessed: 23 September 2022].