Advanced Engineering Days

aed.mersin.edu.tr

The role of education in cyber hygiene

Albina Basholli*[1], Besjana Mema [2], Fatmir Basholli [2], Dolantina Hyka [3], Denisa Salillari [1]

[1]Polytechnic University of Tirana, Faculty of Mathematics Engineering and Physics Engineering, Tirana, Albania, a.basholli@fimif.edu.al / albinabasholli@yahoo.com, d.salillari@fimif.edu.al
[2]Albanian University, Department of Engineering, Tirana, Albania, b.mema@albanianuniversity.edu.al; fatmir.basholli@albanianuniversity.edu.al
[3]Mediterranean University of Albania, Department of Information Technology, Albania, dolantina.hyka@umsh.edu.al

Cite this study: Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. Advanced engineering Days, 7, 178-181

Keywords
Cyber hygiene
Education
Identification
Prevention
Cooperation

Abstract

In recent years, societies around the world have made great strides in the field of information and communication technology. Albania ranks among the countries where the development of technology, access to the Internet and the computerization of society progresses very quickly. Today, the e-albania government portal offers 1225 online services for citizens and businesses. In this framework, information security is paramount in modern cyber defense and an important factor related to the reduction of security breaches influenced by people by being included under a new concept, "cyber hygiene". This concept focuses on how we can protect ourselves from online risks and threats and how we can use technology in a safe and sensible way. Using a combination of available resources and a review of field studies, this article addresses and defines the importance of proper preparation and awareness of users to deal with risks and threats in their online operations. The results of this analysis will be based on the processing of surveys carried out in three public university faculties and two engineering departments in private universities, from which we conclude that education in cyber hygiene is the basis for promoting the safe and reasonable use of technology, improving in the continuation of the curricula of courses with object from the sciences of information technology.

Introduction

While attacks and data leaks are present, the increase in human or financial resources allocated to cyber security and the prosecution of computer crimes has not definitively prevented these interventions. According to some observations that we organized in the first five months of this year, it is observed that this uncertainty is due to deficiencies in cyber education and that human error is the main cause for violations of personal data and secure information [1]. In this article we will talk about the increasing use of technology and the importance of cyber hygiene as a current challenge in the modern world and we will give a general concern about internet security and the impact on our daily lives. By analyzing some of the most common risks and threats on the Internet, such as virus attacks, malware, phishing and data leaks, we aim to show users how these threats can cause damage and, most importantly, how to prevent them [2]. To examine the importance of cyber hygiene education, where there are several "human factors" that increase or decrease the likelihood of being a victim of a cyber attack, hack or data breach, and even being victimized multiple times, we will emphasize the advantages of a responsible and genuine education in the security and protection of personal data. Successful cyber hygiene education methods and strategies include interventions by responsible government structures, educational institutions, non-governmental organizations and the community at large. The treatment will contain recommendations for elements such as suitable curricula, specialized training for Internet users, awareness campaigns and the increase of public-private partnership. Next steps and challenges in cyber hygiene education will include recommendations for the development of education and training programs, as well as for the creation of policies and legislation that promote Internet safety [3]. Cyber hygiene is certainly important in maintaining cyber security, but it is not necessarily synonymous with cyber security. While cyber security is the

objective measurement of behaviors taken to maintain security and strengthen defenses against cyber-attacks, cyber hygiene relates to internet security knowledge and practices related to further enhancing cyber security. In conclusion, to improve cyber security, we need to improve cyber education.

Material and Methods

The material and methods are based on an analysis of available and specialized sources in cyber security such as the National Authority for Electronic Certification and Cyber Security (AKCESK) and the observation of teaching programs, curricula, literature to identify important data and the latest in the field of education and cyber hygiene in several public and private engineering departments and faculties.

a) Detection of cyber intrusions

From the monitoring of several state institutions and Internet Service Providers (ISPs) operating in Albania, which generate malware with a source in Albania and destination in different countries, the following data extracted from this monitoring are evident [4-6]. Below are the corresponding tables and graphs for two institutions and for four ISPs, identifying them with institution 1 and institution 2, as well as the ISPs, with ISP-1 to ISP-4.

Table 1. The number of malwares generated in the months of May-June 2021

The year 2021	Number of Malware		Number of Malware			
Months	Institution-1	Institution-2	ISP-1	ISP-2	ISP-3	ISP-4
May	882	1286	17109	85759	15494	73210
June	1155	1078	21256	89745	15135	1792
July	334	1771	19358	87572	7171	114
August	109	115	11200	50322	3785	326
September	135	261	11154	38159	416	410
October	178	193	16516	54494	60	796
November	100	250	15431	47861	51	912
December	148	267	15360	38613	52	892

b) Penalties for computer crimes consist of the following aspects:

• Computer fraud - Entering, changing, deleting or removing computer data or interfering with the operation of a computer system, with the aim of providing oneself or third parties, by fraud, with an unfair economic benefit or causing them a third decrease in wealth [7- 8].
• Unauthorized computer access - Unauthorized access or in excess of authorization to access a computer system or a part of it, through the violation of security measures.
• Illegal interception of computer data - Illegal interception by technical means of non-public transmissions of computer data from/or within a computer system, including electromagnetic emissions from a computer system, which carries such computer data.
• Interference in computer data.
• Misuse of equipment - Manufacturing, keeping, selling, providing for use, distribution or any other action, for making available a device, including a computer program, a computer password, an access code or such data similar, which are designed or adapted for access to a computer system or a part thereof [9-11].

Table 2. Computer Crime and Criminal offense in the field of Information Technology

Categories of crimes	Month and year					
	January 2018	January 2019	January 2020	January 2021	December 2021	January 2022
In the field of IT	6	10	14	17	25	14
Through the computer system	7	5	8	17	30	21
Number of Cyber Crimes	13	15	22	34	55	35

c) Education in the field of Information Technology

Where we include knowledge about Information Technology, cyber security, therefore Cyber Hygiene. While online safety guidelines for students, college students, and consumers are available free of charge, it is worth considering how many users read and understand these reports and whether these safety guidelines are written in language that can be understood by the general consumer. and literate, as well as for those left behind with current technology [12]. Through the table below, we can understand the educational gap in cyber security, and the need for mandatory cyber hygiene education for all individuals, including professions that use information

technology as a basis for their work [13]. Extract from the Bachelor study program, in the Engineering Departments at the University A, B, C, D, E in Table 3.

Table 3. Extract from the Bachelor study program

Training subjects for Information Technology, which contain university curricula (Bachelor)	Credits	Amount of hours	The percentage that occupies the educational program
Engineering software	5	68	2.8 %
Architecture of control systems	5	64	2.8 %
PLC, Programmable automata	5	60	2.8 %
Informatics	5	67	2.8 %
Information and communication technology	5	45	2.8 %
Basic elements of informatics	5	61	2.8 %
Computer architecture	4	42	2.2 %
Theory of computer networks	5	60	2.8 %
Database	9	110	5.0 %
Electronic calculators	6	60	3.3 %

Results and Discussions

From the analysis of Table-1, "Discovery of cyber intrusions", Table-2 "Penalties for criminal offenses on Computer Crime" and Table-3 on "Education in the field of Information Technology" is easy to conclude in deepening our understanding of the importance of education in cyber hygiene and providing sustainable recommendations to improve existing programs, policies and practices [14]. These statistics can be used as a basis for the development of future strategies and the implementation of cyber hygiene policies at local, national and wider levels. To positively impact safety and security in the cyber world, we must invest in user education, raise awareness and promote safe practices. Only through joint efforts and continuous improvements in the field of education and cyber security, we can build a reliable and safe environment for all Internet users [15]. Our responsibility as individuals, institutions and society is to improve our awareness, build our capacities and create a culture of security and awareness in the cyber world. Internet users should understand that everyone has personal responsibility for their own online safety. They should be encouraged to learn and implement security practices, cultivate awareness, and share cyber hygiene information with others [16]. In conclusion, improving cyber hygiene education is a shared task for all. Only through broad engagement and cooperation can we build a safe and reliable cyber environment for all users. Cyber challenges know no boundaries. It is important to develop international cooperation in the fight against cyber threats and to improve education in cyber hygiene. This includes the exchange of knowledge, experiences and good practices with other countries, as well as the development of common standards and policies for cyber security [17]. It is important to develop suitable and easy-to-use educational materials for all age groups. These materials should be clear, straightforward, and address online risks and safe practices. They can be in the form of books, brochures, video tutorials and mobile applications. Education in cyber hygiene should not be a prescribed process, but should be an ongoing effort. Educational institutions, non-governmental organizations and technology companies should provide continuous education and training programs to keep users informed and up-to-date with developments in the cyber field [18].

Conclusion

- ✓ School curricula should include more information and activities related to cyber hygiene. This can be done through the creation of separate modules or through the integration of cyber hygiene into existing subjects such as informatics, control systems architecture, computer architecture and community service education.
- ✓ It is important to monitor and evaluate the effectiveness of cyber hygiene education programs. This can be done through the assessment of user knowledge and behavior, identification of new challenges and needs, as well as through the analysis of cyber security statistics and data.
- ✓ Educational institutions and non-governmental organizations can organize clubs and interest groups dedicated to cyber hygiene. These forums can provide opportunities for discussion, specialized training, exchange of experiences, and the development of joint projects that address Internet security issues.
- ✓ Technology industries have an important role to play in improving cyber hygiene. Educational institutions and organizations should collaborate with these companies to develop innovative educational materials, secure applications, technology tools and platforms that help educate users about online safety and security.
- ✓ Collaboration between the public and private sectors can strengthen cyber hygiene education efforts. Partnerships can bring added resources, different expertise and opportunities to implement joint education and awareness programs.

- ✓ The development of advanced tools and technologies can help improve cyber hygiene education. The use of technologies such as artificial intelligence, mixed reality and data analytics can improve teaching and make cyber training more engaging and effective.

References

1. Johnson, L., Smith, J., & Davis, C., (2019). The Role of Cybersecurity Education in Combating Cyber Threats. International Journal of Cybersecurity Intelligence and Cybercrime.
2. Smith, J., Johnson, A., & Brown, L. (2022). The Role of Education in Cyber Hygiene: A Systematic Review. International Journal of Cybersecurity Education, Research, and Practice
3. Martinez, R. (2021). Educational Approaches to Cyber Hygiene: A Case Study of Secondary Schools. Journal of Cybersecurity Education, Practice and Research.
4. Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. International Scientific Journal Security & Future, Publisher: Scientific Technical Union of Mechanical Engineering Industry-4.0, 5(2), 72-75
5. Basholli, F., Daberdinİ, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.
6. Thompson, E. (2020). Cyber Hygiene Education for Older Adults: A Review of Current Approaches. Computers in Human Behavior.
7. Johnson, M. (2021). The Role of Education in Cybersecurity: A Systematic Literature Review. International Journal of Cybersecurity Education, Research and Practice.
8. Smith, K., Brown, T., & Johnson, R., (2020). Promoting Cyber Hygiene in Higher Education: An Empirical Study. Journal of Information Privacy and Security.
9. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.
10. Basholli, F., Daberdini, A., (2022). Security in telecommunication networks and systems. International Interdisciplinary Conference "The role of Technology in the Shaping of Society", 72
11. Basholli, F., (2022). Cyber warfare, a new aspect of modern warfare. Confsec 2022, VI International Scientific Conference, 52-54
12. Jones, S. (2018). Promoting Cybersecurity Education in K-12 Schools: Challenges and Opportunities. Journal of Educational Technology.
13. Pajaziti, A., Basholli, F., & Zhaveli, Y. (2023). Identification and classification of fruits through robotic system by using artificial intelligence. Engineering Applications, 2(2), 154-163.
14. Williams, L. & Smith, M. (2017). Cybersecurity Education in Higher Education: Current Challenges and Strategies. Computers & Security.
15. Brown, D. (2016). Enhancing Cybersecurity Education through Experiential Learning. Journal of Information Systems Education.
16. Balfe, N., Sharples, S., & Wilson, J. R. (2018). Understanding is key: An analysis of factors pertaining to trust in a real-world automation system. Human factors, 60(4), 477-495.
17. Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors. Journal of Cybersecurity Education, Research and Practice, 2017(1), 1-17.
18. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.