International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 14, No. 1, April 2025, pp. 122~131
ISSN: 2252-8776, DOI: 10.11591/ijict.v14i1.pp122-131

Managing cyber resilience literacy for consumers

Tatiana Antipova[1,2], Simona Riurean[3]
[1]Institute of Cited Scientists, Agia Napa, Cyprus
[2]Comprehensive Science, Coal Township, United States
[3]Department of Computers, Automation and Electrical Engineering, Faculty of Electrical and Mechanical Engineering, University of Petrosani, Petrosani, Romania

Article Info

Article history:

Received Apr 22, 2024
Revised Sep 9, 2024
Accepted Nov 22, 2024

Keywords:

Cyber hygiene
Cyber resilience
Cybersecurity
Passwords
Two-factor authentication
Zero-trust

ABSTRACT

It seems inevitable that digitalization will have a profound and irreversible impact on our lives, and it seems reasonable to suppose that our world will never be the same again. Objectives of this study is to gain insight into consumers' understanding of cyber security threats and their willingness to enhance their cyber resilience. To achieve this, a survey was conducted using AI tools such as Open ChatGPT, Copilot and PI. The survey was distributed selectively among consumers via Google Form. The results of the survey conducted during the study indicated that the majority of respondents (72%) expressed interest in attending online interactive seminars to gain more knowledge about managing cybersecurity threats. However, respondents with the lowest cyber resilience knowledge did not express the same level of interest. With technology becoming an increasingly important aspect in our everyday lives, it is becoming ever clearer that cybersecurity posture relies on the behavior consumers and organizations. Based on the rule that 'never trust, always verify' we designed 'cybersecurity zero-trust framework model' for consumers that allows them to protect themselves against cybersecurity threats. In an ever-shifting landscape of cybersecurity, it is important to recognize the value of continuous education as a necessity, not just an option.

Corresponding Author:

Tatiana Antipova
Institute of Cited Scientists
Agia Napa, Cyprus
Email: antipovatatianav@gmail.com

1. INTRODUCTION

Cybersecurity is the method of shielding computer systems, and data from digital cybercriminals, damage, or illegal access. It involves the application of technical controls, such as firewalls, intrusion detection, and encryption; security policies and best practices, like managing password, and data backup; training and awareness programs, aimed at minimizing the risk of cyber attacks and ensuring the integrity, confidentiality, and availability of information. Cybersecurity is an essential component of digital security, essential for protecting individuals, organizations, and critical infrastructures from cybercrime and cyber espionage [1], [2]. It's fascinating to see how cybersecurity involves not just technology, but also human behavior, processes, and practices. These various components work together to safeguard the cyber environment, from technical tools and risk management techniques to best practices, training, and guidelines. By acknowledging the complex landscape of cybersecurity, organizations and individuals can adopt a holistic approach regarding security, minimizing vulnerabilities and maximizing their ability to mitigate cyber threats. With digital technology continuing to influence every aspect of our lives, it is vital to recognize the importance of prioritizing education and training for the population.

A number of authors developed various strategies, that can help consumers to enhance their cognitive capabilities and situational awareness and strengthening their overall cybersecurity knowledge and awarness [3]. Firch [4] 98%, the cyber attacks involve diffrent forms of social engineering where human errors are the greatest threat in cybersecurity.

The consumers (aka end-users or individuals) are seen as the weakest link within any organization security chain [5], therefore their early and constant education regarding threats and good practices online become compulsory nowadays since cybersecurity has become ubiquitous with an exponential growth of consumers' applications and IoT devices. Cybersecurity is a shared responsibility. By safeguarding assets and minimizing liabilities, consumers contribute to a safer digital ecosystem [6].

The consumers' assets cover own data privacy, personal devices' security, their own credentials and digital identity, as well as personal financial resources. Data privacy refers to the individuals' personal information, their financial records, and sensitive data.

Individuals' own devices can be anything from the smart phone, desktop, laptop to IoT smart devices that need to be protected. Credentials refer to own usernames, passwords, and authentication tokens. The digital identity is defined by the users' online presence, reputation, and social media profiles and the financiar resoruces can be digital wallets, credit cards, and/or online banking accounts. Protecting these all ensures the own consumers' privacy, prevents misus, and allow a responsible management that maintains trust and credibility online [7].

There are still a number of consumers' liabilities with the regard of cybersecurity. The lack of awarness (high ignorance about cybersecurity risks), unsafe practices (clicking on suspicious links, using weak passwords, sharing sensitive information recklessly, failure of updates (neglecting software updates exposes vulnerabilities) social engineering vulnerability (falling for phishing scams or divulging personal details to impostors) and access unprotected any insecure network (connecting to unsecured Wi-Fi networks or public hotspots) are all common liabilities today [8].

Consumer cyber resilience refers to an individual's ability to anticipate, resist, recuperate from, and adapt to difficult conditions, tensions, attacks, or concessions necessary to make, related to cyber resources. Cyber resilience means that consumers need to be able to proactively anticipate attacks, to defend, and efficiently respond to a security incident [9]. In essence, a consumer's cyber resilience is their ability to continue using digital services and protecting their data despite experiencing challenging cyber events, such as cyberattacks. It's about being prepared, being able to respond effectively, and recovering swiftly from any IT security incident. By 2030, about 60% of all IoT connected devices will be consumer-oriented [10], thus, managing cyber resilience literacy of consumers is a contemporary compulsory topic and mandatory concern for the cybersecurity responsible authorities worldwide.

This work aims to test the consumers' basic knowledge regarding cybersecurity thereats online and their willingness to become cyber resilients. Consumer cyber resilience is a critical concept in today's rapidly evolving cybersecurity landscape. As technology becomes an essential part of our everyday life, so cyber resilience becomes increasingly dependent on the behavior and choices of people and society.

2. RESEARCH METHOD

Chronologically, the present study is built on the results of previous works [11]-[13]. There was designed a logical scheme/technique that present how to stop cyber attacks to an organization website [11]. The method presented can help responsibles and IT-specialists to optimize Cyber Security System in consumers' organization to avoid cyberattacks in the nearest future. Also, this work details how to identify the "malicious" IP and find its location. The result of this study can be implemented by other business website users [11]. In conclusion of previous work has noted, that it is still important to understand information security investments in terms of compliance and risk, given that the cost of compliance is rising [12]. In addition, previous work took a broad overview of malicious attacks during 2022, the results of these attacks, and the preventive measures to avoid unwanted situations and their undesirable results following cyber-attacks [13].

In most of the situations, individuals are responsible of exposeing themselves to vulnerabilities due to lack of education, insufficient, or inadequate preparation regarding the cybersecurity awareness and threats. Therefore, the consumers are considered as the weakest links in the security chain, despite continuous education and sustained efforts and security procedures. Much of the scientific literature on the human factor in security emphasizes raising awareness, training, and education. A sad reality of cybersecurity is that human error is often the weakest link in the chain. Despite the best efforts in education and enforcement, mistakes happen, whether through ignorance, negligence, or even malice. It's a sobering reminder that cybersecurity is not just about technology, but about human behavior as well. It's a constant struggle, requiring constant vigilance and awareness to identify and mitigate potential vulnerabilities, while also

understanding that even the most robust systems and protocols can be undermined by simple errors or deliberate actions [14].

This work investigates the consumers' cyber resilience and their level of cybersecurity awarness againts threats and emphasizes the importance of building a proper cyber hygiene culture for consumer to become cyber resilients. The cyber hygiene aims to educate consumers about basic technical skills regarding password management, recognize unsecure websites, and, in order to enhance the security, use multi-factor authentication (MFA) [15].

Cybersecurity awarness covers the phishing awareness that educate customers to be cautious of unsolicited emails and verify sender legitimacy, avoid sensitive transactions on public Wi-Fi networks by being extra cautios when using public Wi-Fi networks, and learn to recognize manipulated audio and video content, being able to deteck deepfake online [16].

Designing specialized cybersecurity curricula for consumers is crucial. These curricula should focus on developing skills and knowledge related to cyber resilience in the context of the internet of everything (IoE) ecosystem. By upskilling consumers, we can collectively improve societal cyber resilience [9].

3. CYBERSECURITY FRAMEWORK

Information security management is a complex and ever-evolving field that demands a comprehensive understanding of various security domains, as well as the ability to navigate the intricate web of compliance regulations and standards. By adopting a holistic approach that addresses each of these facets, consumers can effectively mitigate risks and maintain a secure digital environment.

Application security, one of the Information security management sections, focuses on identifying and remediating vulnerabilities in software applications, necessitates rigorous code reviews, vulnerability assessments, and penetration testing. Disaster recovery, on the other hand, entails developing and implementing plans to restore critical systems and data in the event of a catastrophic event, ensuring business continuity.

Compliance standards and regulations, such as general data protection regulation (GDPR) [17], health insurance portability and accountability act (HIPAA) [18], california consumer privacy act (CCPA) or payment card industry security standards council (PCI DSS) [19], or security of networks and information systems (NIS) [20] add another layer of complexity to information security management [21]. GDPR is the regulation in EU 2016/679 related to the persons' protection regarding ways and methods to process and store personal data. It took full effect in May 2018 [17].

HIPAA, and its privacy rule, sets forth a robust framework for protecting sensitive health information, including who can access it, how it can be used and disclosed, and what rights individuals have over their personal health data. HIPAA is an important part of cybersecurity in healthcare, as the unauthorized access or expose of health information can bring serious consequences for individuals [18].

California's CCPA, amended and expanded by the california for consumer privacy (CPRA) became enforceable on July 1, 2020. Its main concern is to regulate the sale of individuals' personal data [20]. PCI DSS applies to Azure, Dynamics 365, Office 365 and other online services [19].

NIS is the EU directive of the European Parliament 2016/1148 that define rules for networks' and IT systems' high level of security in the European Union being imposed on 6 July 2016. All these requirements mandate specific security controls and safeguards to protect sensitive data, thus any failure to act following the rules has consequences with severe penalties [20].

The cybersecurity framework published by the National Institute of Standards and Technology (NIST) in the United States (SP 800-53:2020) [22] comprises five cores of interacting components: identify, protect, detect, respond, and Recover (IPDRR). NIST special publication 800-207, also known as "zero trust architecture (ZTA)," is a foundational document for organizations and individuals seeking to implement zero trust strategies [23]. NIST's principles for zero trust are broken down into three key areas: the identification of the resources that need protection, the principles and models for securing those resources, and the components and capabilities needed to implement the principles. ZTA represents a revolutionary change in cybersecurity philosophy. By shifting the focus from network-centric controls to identity-based security policies, ZTA can better address the dynamic and complex threats that organizations face in today's digital landscape. This approach relies on verifying the identity of every user, device, or application attempting to access a network resource, rather than relying on perimeter-based defenses that have proven inadequate against modern cyberattacks.

The zero-trust concept (ZTC), initially adopted by organizations to enhance their security posture, can also serve as an effective approach for consumers willing to protect themselves against cybersecurity threats. ZTC is based on the principle of "*never trust, always verify*" which requires consumers to verify their own identity and devices' security before accessing applications, data, or networks.

As seen in Figure 1, applying ZTC in a personal framework involves several key aspects as consumer's own good practices. Implementing MFA for all accounts forces consumers to proceed with two or more identification steps before accessing their own accounts, thus an additional layer of security is added. Regular software updates ensure that devices, applications, and operating systems are updated promptly to help protect against known vulnerabilities that cyberattackers could exploit. Using strong, unique passwords for each online account minimizes the risk of a cybercriminal gaining access to multiple accounts in case one account is compromised already. Enabling device encryption prevents unauthorized access to sensitive personal information, even if the device is stolen or lost. Enabling encryption on devices prevents unauthorized access to sensitive personal information, even in case that the device is stolen or lost.

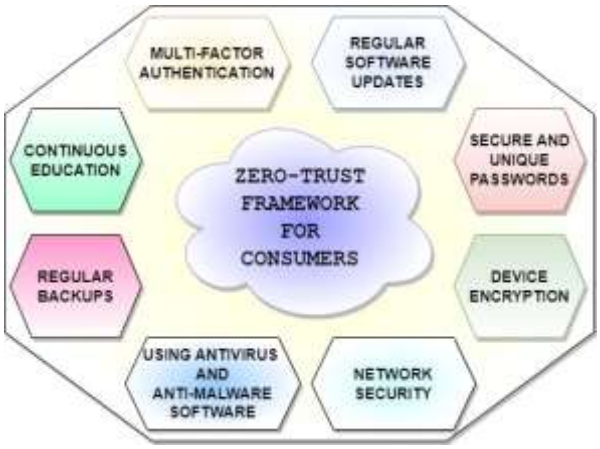

Figure 1. Cybersecurity zero-trust framework for consumers

Using secure and encrypted internet connections, such as virtual private networks (VPNs) or HTTPS websites, helps protect personal data transmitted over networks. The Wi-Fi network must be secure and use encryption, such as WPA2 or WPA3. The public Wi-Fi networks without encryption, are more vulnerable to cyberattacks therefore the personal device must be disabled to automatically connects to Wi-Fi networks within range, prevent the device from connecting to potentially malicious networks without users' knowledge.

Updated, reliable anti-virus and anti-malware application helps protect users' devices from malware and other cyber threats. Performing regular backups of sensitive data ensures that it can be restored in the event of a cyberattack or data loss. Knowledge is power when it comes to cybersecurity. As the saying goes, "forewarned is forearmed." By keeping up-to-date on the latest cybersecurity threats and trends, individuals can take proactive steps to protect themselves and theyr own personal and sensitive data from potential attacks. This includes staying informed about new types of malwares, phishing schemes, and other tactics employed by cybercriminals. Being cautious of suspicious emails or messages that ask for sensitive information or contain suspicious links or attachments, even if they appear to be from a legitimate source.

By adopting a ZT approach to personal cybersecurity, individuals can significantly reduce their exposure to potential threats and minimize the impact of cyberattacks. This proactive strategy, combined with ongoing education and vigilance, empowers individuals to protect their digital security and protect their sensitive data in an increasingly interconnected world [24].

Zero Trust is all about "trust nothing, verify everything," and this applies equally well to personal cybersecurity. When it comes to consumers online accounts and devices, past trustworthiness doesn't necessarily guarantee future trustworthiness. That's because cyber threats are constantly evolving, and the online accounts and devices you use can become compromised without your knowledge. Some security priciples of this approach refere to educate consumers to verify clearly, use the minimum privilege access, assume breach and adapt to modern environment. The conventional cybersecurity paradigm treats the network perimeter as a 'moat' that protects the 'castle' or organization, with everything inside the perimeter assumed to be trustworthy. However, with the advent of mobile workforces, cloud computing, and the increasing sophistication of cyberattacks, the castle and moat approach has been rendered obsolete. The ZT model, assumes that any user or device, could be compromised and, therefore, must be continuously verified before granting access.

4. LITERACY FRAMEWORK

The consumers' cybersecurity literacy framework must be focused on the cyber resilience that emphasizes the the core necesity of consumers' continuous education about various aspects of cybersecurity and providing them with the knowledge and skills they need to protect themselves in today's digital world. Some key components of such a framework refer to understanding cyber resilience, refering to NIST cybersecurity framework, define thematic areas, develop basic technical skills, educate consumers about they own cyber hygiene, inform consumers about IoT and IoE security and possible cyber theraths, and regulatory frameworks. Consumers should understand what cyber resilience is, i.e., a wide range of measures, including robust security controls, effective incident response plans, and the ability to adapt and learn from cyber incidents. In essence, cyber resilience is about building the capacity to not only defend against cyber threats but also to recover and even grow stronger from them.

NIST cybersecurity framework areas should be considered when building consumers' competencies. These areas are IPDRR. While cybersecurity risk management plays a critical role in addressing privacy risks associated with data breaches, confidentiality, integrity, and availability, privacy risks can arise from various other sources as data collection and processing, data sharing, lack of transparency, data retention, inadequate access controls, data misuse and regulatory compliance.

Privacy risks can arise from the collection and handling of personal information. Consumers must ensure that organizations collect only the necessary data and process it according to legal and ethical standards. Inappropriate sharing of personal data with third parties or unauthorized entities can lead to privacy violations. Failing to inform consumers regarding the way their data is collected, processed, used, stored, and shared can result in a loss of trust, and potential privacy violations.

Retaining personal data beyond its necessary lifespan can be a potential privacy risk, as is failing to securely dispose of it. Access controls are also critical, as improper implementation can lead to unauthorized access and the potential for sensitive data to fall into the wrong hands. Using personal data for purposes other than those consented in the firt place by the user, to can undermine trust in the organization and lead to legal consequences. Compliance with data protection regulations is also crucial, not only to avoid penalties but also to maintain consumer trust and confidence.

With the increasing use of IoT and IoE, consumers should be aware of the potential threats these devices can bring into their homes. With our daily dependence on digital technologies and online services, all individuals must have the necessary knowledge and skills to protect themselves against any possible cyber attack. This includes basic skills, such as creating passwords by the rules (unique and strong), using MFA, being aware of phishing scams, and understanding the importance of application updates and antivirus software. This can be achieved through specialized cybersecurity curricula. Consumers should be taught about cyber hygiene, which includes good practices like regularly updating applications (operating systems, software used), using solid passwords, and being aware of suspicious emails or links.

Consumers should also be aware of the regulatory frameworks in place that aim to strengthen their capacity to prevent incidents and ensure swift recovery after information communication technologies (ICT) related disruptions [25]. This framework aims to upskill individuals and improve the cyber resilience level across society. It's important to bare in mind that cyber resilience is not just about technology, but also about people and processes [26]. Therefore, consumer education plays a crucial role in enhancing overall societal cyber resilience.

5. RESULTS AND DISCUSSION

During this study was conducted a survey using such artificial intelligence tools as open ChatGPT, Copilot and PI by formulating the questions of this survey. Survey was distributed among consumers via Google Form in March-April 2024. This survey was conducted in two languages: English and Romanian with eight questions related to consumers' basic cybersecurity knowledge. Most of survey questions were formulated when using such artificial intelligence tools as Open ChatGPT, Copilot, and PI.

Survey was distributed among consumers via Google Form. Some questions have had multiple choices for answers. We also encouraged our respondents to answer all questions, honestly. The results were anonymous and solely designated to analyze the consumers' cybersecurity knowledge.

We have received 122 answers for the quiz in Romanian language and 58 answers for the quiz conducted in Enghlish language. Analyzing the answers of the 175 respondents in both languages as a single dataset can deliver valuable insights and help in the evaluation of the quiz, thus, for a better understanding of the quiz results, the total of 180 respondents' answers in both languages, are considered as one.

We have had 164 respondents from Romania (meaning 90,5%) (of which 42 took the test in the English language) and 17 respondents (meaning 9,4%) from abroad (6 from Cyprus, 2 from Moldavia, 1 from Nigeria, 1 from the Netherlands, 2 from Kazakhstan, 3 from Greece, 1 from Colombia and 1 from

Russia). The respondents' age varies from under 15 (2 responders, meaning 1,1%) to over 65 (7 responders, meaning 4%) as seen in the graph in Figure 2.

The most active and willing to learn more about cyber resilience are respondents with age between 36 and 49 years old (71 responders, meaning 40,4%), followed by respondents with age between 16 and 25 years old (47 responders, meaning 25,9%), age between 50 and 64 years old (34 responders, meaning 19,4%), and the age between 26 and 35 years old are the least interested responders by the active working age category (16 responders, meaning 9,1%).

The highest level of education (already graduated) counting by the number of respondents (x axis) is presented in Figure 3. Most of our respondents (124 of them, meaning 70,85 %) graduated a form of university level education (Barchelor, Master), and higher (Ph.D. and Doctor) and the rest of them (29,14) graduated elementary school and high school. We can assume that currently 26 respondents are high school students and 25 follow courses in university.

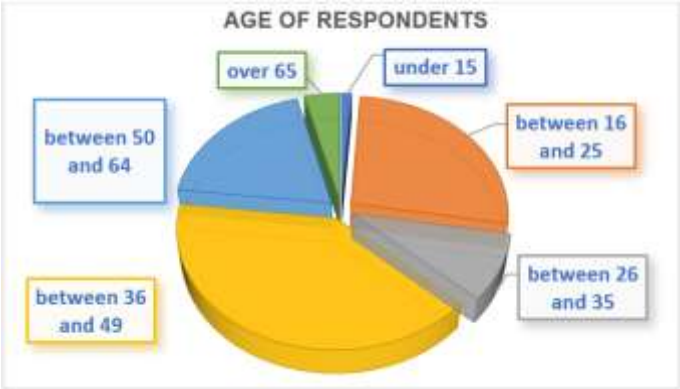

Figure 2. Age of respondents

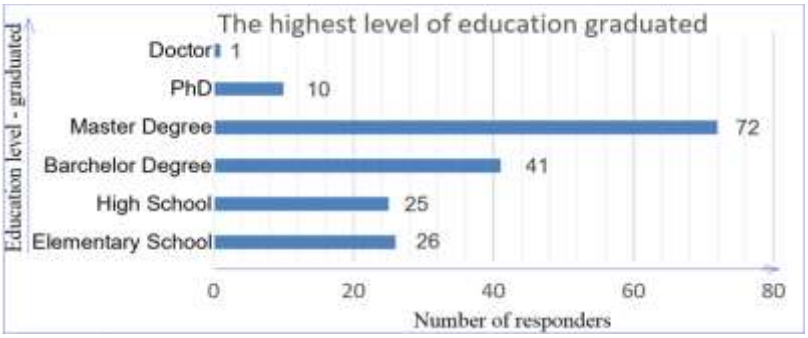

Figure 3. No of responders (axis X) with the highest level of education (axis Y) already graduated

A following question reflected the digital proficiency of our responders as seen in Figure 4. Therefore, most of our respondents (92 of them) use a computer and/or a smart phone between 6 and 16 years, 61 of them between 17 and 27 years, 16 of them more than 28 years and 6 of them (3,43%) for less than 5 years. It is also worth noting that people born after the year 2000 (so called Z generation) have been using smartphones since the age of a year or two.

For the first question '*What is the best way to create strong passwords for your online accounts*' (with two correct answers out of 4) most of the respondents (127 of them, meaning 70,56%) considered that using a combination of numbers letters, and special characters is the best answer, and only 34 of them answered that using a sentence they can remember with special characters in it, is a correct answer. Both answers are correct.

Fifteen respondents answered that using personal information like their name or birthdate is a correct answer and 24 considered that using the same password for all accounts is the best way to create strong passwords for their online accounts. Thus, less than 20 % of our responders (18,88% exactly) knew which are the best ways to create strong passwords for their online accounts.

The second question '*How does two-factor authentication (2FA) help protect your accounts?*' (a question with one corect answer out of four) received 131 correct answers (72,78%). However, a number of respondents considered that 2FA creates a backup of their passwords (8,57%), it automatically blocks suspicious websites (10,28%). The rest of the responders (11 of them) answerd that 2FA creates a backup of my account.

The third question, '*What should you do if you receive an email with a suspicious link or attachment?*' (a question with two correct answers out of 4 options) received 149 answers that avoiding clicking on the link or attachment and deleting the email is the best way to act, and 66 of the responders considered that is necessary to pay attention to any warning signs in the email, such as poor grammar or spelling errors, urgent requests for personal data or offers that are too good to be true. Only 47 of them (26,11%) marked both answers as correct. One responder would click on the link to verify its authenticity and none of them would forward the email to his/her friends for advice.

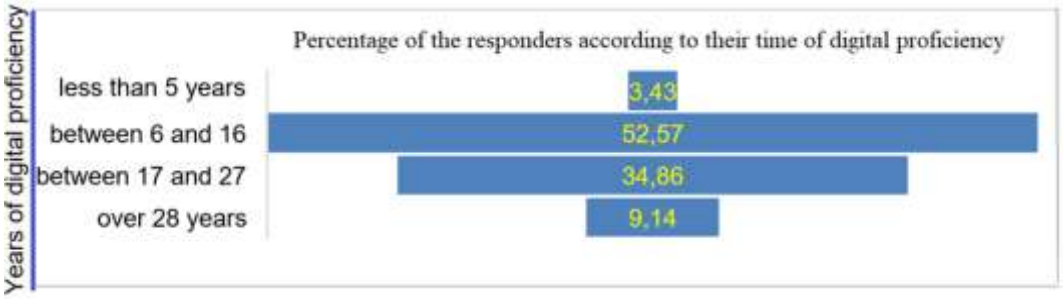

Figure 4. Durtion of responders of digital proficiency

For the fourth question '*How can you protect your devices from malware and other cyber threats?*' (a question with one correct answer out of three) 170 responders chose the correct answer (94,44% of them), saying they would install reputable antivirus and anti-malware software, 4 of them would disable software updates and 1 would use public Wi-Fi networks for sensitive activities.

The next question '*Which of the following is a good practice for securing your home Wi-Fi network?*' (a question with one correct answer out of 3) received the correct answer (enabling encryption and changing the default password) from 114 responders (63,33% out of all). However, 61 of them (34,85 %) considered that using the default password provided by my internet service provider is the correct answer and, none of them would disable the firewall.

For the sixth question, '*How can you minimize the impact of a potential cyberattack on your personal data?*' (a question with four correct answers out of 6), most of the respondents (124, meaning 70,85 %) would educate themselves and their family members about common cyber threats and how to recognize them, 93 of them would protect their home Wi-Fi network with a strong password and encryption, 88 of them would regularly review their bank statements, credit reports, and online accounts for any suspicious activity, and 69 of them would periodically backup their important data. As a general result, only 30,00% of them (54 responders) would take all the correct above necessary measures to minimize the impact of a potential cyberattack on their personal data. However, some responders would ignore any software updates (4 of them) and even share personal information on social media platforms (2 of them).

The seventh question, '*What should you do if you become a victim of identity theft?*' (a question with three correct answers out of 3) received only 61 correct answers (33,89%) (all 3 correct answers). However, 146 respondents would report the incident to the relevant authorities, 102 of them would contact their financial institutions and credit card companies, and 99 of the respondents would change their passwords and enhance the security of their accounts.

The last question of the basic knowledge in personal cybersecurity hygiene '*You find a USB drive lying unattended in a public place what do you do?*' (a question with one correct answer out of 3) received from 166 respondents (92,22 %) the correct answer that they would leave it untouched and report it to the appropriate authorities. Still, 4 of the responders would plug it into their device to see what's on it out of curiosity and 3 of the responders would take it with them and connect it to their computer to check its content later. The general results, as a percentage of the total number of responders giving correct answers are presented in Figure 5.

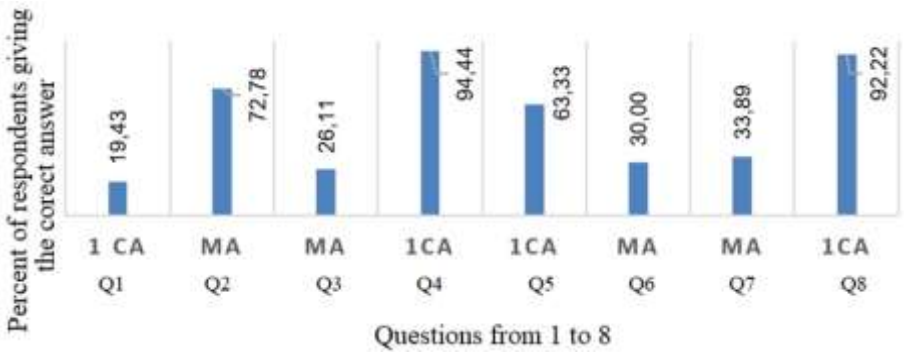

Figure 5. The results for the 8 questions (Q1 the first question on the left and Q8 the last on the right 1CA – one correct answer and MA – multiple answers)

We left the most important question regarding the consumers willing to become cyber resilient '*Would you attend online interactive seminars to know more about managing cybersecurity threats?*' (a question with Yes or No as answer) at the end of the quiz as shown in Figure 6 and the answers were really surprising. 131 of the respondents answered Yes and 49 No. The result was unexpected because the respondents with the lowest cyber resilience knowledge did not want to know more about managing cybersecurity threats.

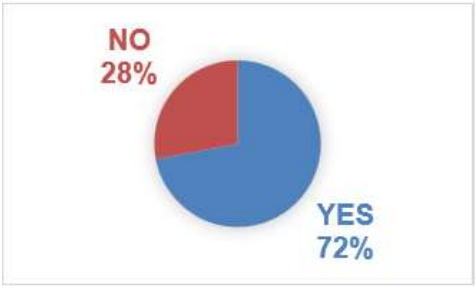

Figure 6. The consumers' willingness to become cyber-resilient

6. CONCLUSION

The arms race between cybercriminals and cybersecurity experts is an ever-changing landscape. New technologies and vulnerabilities are constantly emerging, creating fresh opportunities for cybercriminals to exploit. As such, staying vigilant and informed is crucial for consumers to safeguard their digital identities and assets. Regularly updating software, avoiding suspicious links and attachments, being mindful of privacy settings, and using strong passwords are just some of the basic best practices that consumers should adopt to protect themselves.

Since the main goal of this work was to test the consumers' basic knowledge regarding cybersecurity thereats online and their willingness to become cyber resilient we conduct a survey among internet users selectively. As a result of this survey conducted during the study, we reached to the conclusion that most of the respondents (72%) agree to attend to online interactive seminars to know more about managing cybersecurity threats but the respondents with the lowest cyber resilience knowledge do not want to attend these.

In the ever-evolving landscape of cybersecurity, continuous education is not just an option but a necessity. In addition, as digital technology continues to flood every aspect of our lives, the need to prioritize education, and training for the population becomes increasingly crucial. Digitalization is rapidly and irrevocably changing our lives and the world will no longer be the same.

By continuously learning and updating their knowledge, consumers can develop a strong foundation in cybersecurity principles and cultivate a security-conscious mindset. This includes understanding the importance of strong passwords, recognizing all kinds of social engineering attacks, keeping software and devices up-to-date, and being aware of the potential risks associated with different online activities. By fostering a culture of cybersecurity awareness and training, a safer and more secure digital environment can

be created for all of us. Empowering consumers with knowledge, skills, and vigilance contributes to a more resilient digital society.

Due to Authors' experience and knowledge we advice the following to manage cybersecurity posture: consumers should keep their devices and apps up-to-date, use device management tools, be aware of the attack vectors, restart the device before particularly private comms, do not use device as a repository for docs and important chats, not to integrate all of their devices, control retention timeframes and deploy a dedicated/isolated secure comms service. The topic for the authors' future study is the question of how to teach users most effectively to improve their posture of cybersecurity.

REFERENCES

[1] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[2] T. Vagoun and G. O. Strawn, "Implementing the federal cybersecurity R&D strategy," *Computer*, vol. 48, no. 4, pp. 45–55, Apr. 2015, doi: 10.1109/MC.2015.111.

[3] A. A. Moustafa, A. Bello, and A. Maurushat, "The role of user behaviour in improving cyber security management," *Frontiers in Psychology*, vol. 12, Jun. 2021, doi: 10.3389/fpsyg.2021.561011.

[4] J. Firch, "10 cybersecurity trends you can't ignore in 2024," 2024. https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering.

[5] M. Carlton and Y. Levy, "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals," in *Conference Proceedings - IEEE SOUTHEASTCON*, Apr. 2015, vol. 2015-June, no. June, pp. 1–6, doi: 10.1109/SECON.2015.7132932.

[6] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers and Security*, vol. 24, no. 2, pp. 124–133, Mar. 2005, doi: 10.1016/j.cose.2004.07.001.

[7] M. Sturdee, L. Thornton, B. Wimalasiri, and S. Patil, "A visual exploration of cybersecurity concepts," in *ACM International Conference Proceeding Series*, Jun. 2021, pp. 1–10, doi: 10.1145/3450741.3465252.

[8] F. Pescador and S. P. Mohanty, "Novel cybersecurity paradigms for consumer technology," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 72–73, Jan. 2020, doi: 10.1109/mce.2020.3032206.

[9] E. Stavrou, "Guidelines to develop consumers cyber resilience capabilities in the IoE ecosystem," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 458 LNICST, 2023, pp. 18–28.

[10] A. Parrish *et al.*, "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, Jul. 2018, pp. 36–54, doi: 10.1145/3293881.3295778.

[11] T. Antipova, "Cyberattacks on business website: case study," in *Lecture Notes in Networks and Systems*, vol. 381 LNNS, 2022, pp. 505–512.

[12] C. Griffy-Brown, M. Chun, H. Miller, and D. Lazarikos, "How do we optimize risk in enterprise architecture when deploying emerging technologies?," *Journal of Digital Science*, vol. 3, no. 1, pp. 3–13, Jun. 2021, doi: 10.33847/2686-8296.3.1_1.

[13] D. Moldovan and S. Riurean, "Cyber-security attacks, prevention and malware detection application," *Journal of Digital Science*, vol. 4, no. 2, pp. 3–19, Dec. 2022, doi: 10.33847/2686-8296.4.2_1.

[14] J. C. Martínez, "The human factor in information security," *Isaca*, vol. 5, pp. 1–7, 2019, [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security.

[15] A. Vishwanath *et al.*, "Cyber hygiene: The concept, its measure, and its initial tests," *Decision Support Systems*, vol. 128, p. 113160, Jan. 2020, doi: 10.1016/j.dss.2019.113160.

[16] "Cyber Hygiene - cum să te aperi de cele mai întîlnite amenințări de securitate cibernetică," 2019, [Online]. Available: https://dnsc.ro/citeste/cyber-hygiene-awareness-cert-ro-microsoft-politia.

[17] A. S. D'Amico, "The DMA's consent moment and its relationship with the GDPR," *European Journal of Risk Regulation*, pp. 1–14, Jun. 2024, doi: 10.1017/err.2024.38.

[18] F. Elkourdi, C. Wei, L. Xiao, Z. YU, and O. Asan, "Exploring current practices and challenges of HIPAA compliance in software engineering: scoping review," *IEEE Open Journal of Systems Engineering*, vol. 2, pp. 94–104, 2024, doi: 10.1109/ojse.2024.3392691.

[19] J. Seaman, "PCI DSS applicability," in *Pci Dss*, Berkeley, CA: Apress, 2020, pp. 195–211.

[20] S. Schmitz-Berndt, "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive," *Journal of Cybersecurity*, vol. 9, no. 1, Jan. 2023, doi: 10.1093/cybsec/tyad009.

[21] S. C. Wingreen and A. Samandari, *Information Technology Security and Risk Management: Inductive Cases for Information Security*. New York: CRC Press, 2024.

[22] R. M. Abubakar, M. S. Ahmad, S. N. Kapita, and A. Fuad, "Implementation framework national institute of standards and technology (Nist) evidence digital in the forensic process social media," *Technium: Romanian Journal of Applied Sciences and Technology*, vol. 17, pp. 249–254, Nov. 2023, doi: 10.47577/technium.v17i.10084.

[23] L. O. Mailloux, M. A. McEvilley, S. Khou, and J. M. Pecarina, "Putting the 'systems' in security engineering: an examination of NIST special publication 800-160," *IEEE Security and Privacy*, vol. 14, no. 4, pp. 76–80, Jul. 2016, doi: 10.1109/MSP.2016.77.

[24] A. Pasias, T. Kotsiopoulos, G. Lazaridis, A. Drosou, D. Tzovaras, and P. Sarigiannidis, "Enabling cyber-attack mitigation techniques in a software defined network," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Jul. 2021, pp. 497–502, doi: 10.1109/CSR51186.2021.9527932.

[25] A. Panda and A. Bower, "Cyber security and the disaster resilience framework," *International Journal of Disaster Resilience in the Built Environment*, vol. 11, no. 4, pp. 507–518, Apr. 2020, doi: 10.1108/IJDRBE-07-2019-0046.

[26] I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: introduction and overview," in *Cyber Resilience of Systems and Networks*, Cham: Springer International Publishing, 2019, pp. 1–25.

BIOGRAPHIES OF AUTHORS

Tatiana Antipova is an associate professor of finance and hold a D.Sc. in Economics, Ph.D. in Accounting, Auditing and Statistics, M.Sc. in Engineering of Optical-Electronic Devices. She has published above 160 works, among them journal papers, text books, edited research books and monographs, conference papers, book chapters, edited conference proceeding in the area of information technology in management science, information technology in public administration, information technology in business and finance, computer-assisted techniques, blockchain and logistic technology, intelligent technologies and robotics, wireless communication, optical wireless technologies, data engineering, computational intelligence, and artificial intelligence. She is a member of IEEE. She can be contacted at email: antipovatatianav@gmail.com.

Simona Riurean is an associated professor at the University of Petrosani, Department of Computers, Automation and Electrical Engineering, Romania. In 1991 she graduated with an electro-mechanical specialization at the University of Petrosani, in engineering. In 2000 she gained the first Ph.D. degree in Mechanical Engineering at the University of Petrosani, awarded by the Ministry of Education, Romania. In 2012 graduated from, 1 Decembrie 1918' University in Alba Iulia, Romania, earning a diploma and a Bachelor degree in Informatics, followed by a Master degree in Advanced Programming and Database, and in 2019 received a second Ph.D. degree in System Control Engineering in Romania. She is the author of more than 12 books, over 70 publications in international conference proceedings and journals. She can be contacted at email: sriurean@yahoo.com.