International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2024.5.3

Volume 10, Issue 5
May - 2024

The Effect of Training Adults on the Safe Use of Computers: An Awareness Campaign Initiative

Abrar Y. AlDekheel

The Public Authority for Applied Education and Training

Higher Institute for Telecommunication and Navigation, Computer Department

Kuwait City, Kuwait

ABSTRACT

People across different age groups worldwide use computers and smart devices with access to the Internet. This highlights the importance of educating users and making them aware of the threats to cybersecurity, hazards of the Internet, privacy and safety of personal information, and various kinds of online attacks. This study investigates the level of awareness among adults of the safe use of computers with Internet access. Data were collected by using two surveys: An initial survey was conducted to measure the users' level of awareness before they attended a lecture, training, or workshop. A follow-up survey was subsequently conducted after the lecture/training/workshop to measure its effects on the users' awareness and understanding of the safety and security of using devices connected to the Internet. This research also investigates new methods to reduce cyberattacks, and the responsiveness of users to unknown links and threats.

The findings of this study indicates that there is a positive influence on the participants after the workshop as it improves their knowledge of the privacy and security issues related to the use of social media and the use of different internet tools and increase their awareness level about the cybercrimes and different threats in the digital world. Yet, the results still show struggles in understanding the safety of their personal information and their contents in social media. Hence, a recommendation of more training in the field of applying practical privacy and security steps is still required to enhance their skills and ability to protect themselves and educate others in their communities.

Key Words: Awareness, Artificial Intelligence, Cyber security, Internet, Training.

---

1. INTRODUCTION

Computer-related skills have become essential for people of all ages in today's digital age as technology become increasingly prevalent [1, 2]. Early developers of the Internet never predicted the pace and scale of growth of the medium [3]. With the widespread integration of computers and networks on the Internet for various purposes in workplaces, businesses, education, and in people's homes [4], problems arise when users share their personal information online without appropriately considering privacy- and security-related issues.

While the Internet is a transformative innovation that has profound benefits, it also introduces risks to people's well-being [5–7] through the exposure of their personal information [8], problematic Internet use, and online fraud [9] Hackers are continually developing new ways to steal personal user information and sensitive data, and it is clearly easier to attack uneducated users than those who are skilled at using the Internet and can avoid compromising their privacy. It is thus critical for Internet users to learn the safe use of computers to protect their personal data and avoid online fraud and cyberattacks [10].

The number of Internet users in the Middle East has been steadily rising in recent years [10]. While users from the region make up only 3.2% of global Internet users, the Middle East has undergone a remarkable increase of 1825% in Internet use over the past decade compared with a global growth of 445% [11]. At the same time, the occurrence of

cybercrimes in the Middle East has risen according to local media. Such incidents include Internet scams, breaches of the security systems of financial institutions [12], and attempts to hack various websites.

The widespread use of technology and the ubiquity of the Internet have highlighted the importance of cybersecurity for both individual users and countries [13]. While these advances have significantly enhanced convenience in everyday life, the concomitant rise of cyberattacks requires preventative action [14, 15], including placing a significant emphasis on user awareness of information security, also known as cybersecurity awareness. The large number of studies on this issue, which impacts virtually every aspect of daily life, reflect its importance and the need to develop the digital skills of users [4, 16].

Defining cybersecurity awareness is essential for gaining a comprehensive understanding of the issue. Shaw et al. define it as "the degree of understanding of users about the importance of information security, and their responsibilities and actions to exercise sufficient levels of information security control to protect the organization's data and networks" [17]. [18] define cybersecurity as "the state of protection from unauthorized electronic data use and access by criminals." Cybersecurity can also be described as the process, state, or activity in which communication systems and information are protected from modification, unauthorized access, or exploitation.

As the threats to cybersecurity become widespread, the media has highlighted the different types of cyberattacks that continue to frequently occur [19]. Many reports claim that attackers apply various techniques to breach computer systems, including by embedding malware into third-party software, websites, and emails [20] as well as ransomware [21] Social engineering is a common tool used by cybercriminals to exploit the human psychology and gain unauthorized access to the personal information of users and the sensitive data of organizations [14]. Attackers use various strategies and techniques to manipulate users' private information and organizational security [22]Training users on cybersecurity can help them acquire the requisite skills to avoid cyber threats [21]

The rapid rise of Artificial Intelligence (AI) poses many challenges, especially when this highly effective tool is used by attackers online. AI is considered to be important for detecting and preventing evolving cyber threats. Cybersecurity experts are creating solutions to address the essential vulnerabilities of AI, and this underscores the need for proactive steps to ensure digital security.

Significant progress has been made to protect digital assets by integrating AI into cybersecurity. Early research in the area [23, 24] has established that intelligent systems need to adapt to the constantly changing landscape of cyber threats [25] Next-generation AI-based firewalls have been proposed for detecting, preventing, and responding to cyber threats to strengthen cybersecurity in an increasingly interconnected world, especially because traditional firewalls cannot adequately handle emerging cyber threats [26, 27]

The prevalence of AI-based tools in daily life makes it necessary to train users in this field in order to enhance their skills of ensuring security and privacy in the current digital environment.

Training and education on cybersecurity are nowadays becoming increasingly pressing [28] among users of different age groups and educational levels, and many programs and workshops tailored to each type of audience [19] have been developed to equip users with the professional and technical skills required to apply various safety- and privacy-related measures while using technology in their daily lives [29]. The past decade has witnessed a considerable amount of research on defining the content of cybersecurity training, techniques of delivery, and other essential aspects of the process. Researchers [30] have noted the negative consequences of the ignorance of security-related issues among online users. Many studies have shown that humans are invariably the weakest component of any digital system [31, 32], and users are largely unaware of threats to cybersecurity and ways to protect it. This highlights the need for training users on cybersecurity and making them aware of its importance [33, 34]. Many studies have claimed that public campaigns to raise awareness of cybersecurity and training programs for users are highly effective. [4, 20]

Most organizations focus on implementing comprehensive training and awareness programs to educate their employees on the latest techniques to defend against common social engineering-based online threats. To apply these safety procedures, they provide tailored training materials to their employees, and formulate policies for them to implement before and after attacks. Moreover, regular campaigns are held to raise awareness about information security and emphasize the importance of being alert to all types of threats [35]. Implementing cybersecurity training

DOI: 10.31695/IJASRE.2024.5.3

in various sectors faces such challenges as the need for well-trained educators who known of the latest cyber threats and have the ability to equip users with the latest tools and tips for safely browsing the Internet [36].

Cybersecurity training usually covers such threats as cyberbullying, phishing, addiction to gaming, and online pornography to create a safe environment and protect the users' privacy [4]. Trainers should emphasize the positive aspects of excessive Internet use in addition to other drawbacks [36]. At the same time, any training program requires analytical methods to identify its strengths, weaknesses, requirements, learning goals, and results to achieve the required outcomes [31].

Cybersecurity awareness initiatives are vital for fostering safe online behaviors and responsible digital citizenship from an early age. Such initiatives play an essential role in promoting safe browsing habits and responsible engagement with the digital world. Developing professional tools, awareness campaigns, and training programs are prioritized [19] to prepare users for avoiding or responding to cyberattacks [37, 38].

With growing use of the Internet and AI in Kuwait, the author and a colleague launched a community service campaign to spread awareness of cybersecurity among the public in 2016. The “Be Smart Safe” campaign aims to build a skilled online community that can safely use the Internet and attendant technological tools by introducing training sessions, lectures, and workshops for different age groups of users. In this study, we focus on the effects of training adults on cybersecurity to equip them with the tools that they need to ensure the security of their private information.

2. LITERATURE SURVEY

The digital technological revolution at the turn of the millennium has exposed users to a wide range of cyber threats. It has thus become essential to use cybersecurity awareness and training campaigns so that users can deal with various cyberattacks. We investigate the level of awareness of the safe use of computers with Internet access among adults.

Many studies have explored the importance of raising public awareness of cybersecurity in the last three decades [20]. [34] has shown that users who are the least aware of the threats to cybersecurity and the relevant solutions are also the most frequent users of digital devices. A variety of evaluations and programs have been developed in the literature to raise cybersecurity awareness among users [39–41]. Building training programs with well-defined components, such as security policies, can help achieve the desired goal [42]. [43] have suggested that there is a high correlation between users’ online behaviors and understanding in the context of threats to cybersecurity. Thus, people need to be knowledgeable in order to behave appropriately.

One study conducted a survey of students in the business department of a university in New England, Massachusetts to study their attitudes toward information security and build an effective program to improve their understanding of cybersecurity [41]. The survey’s results prove a significant correlation between students’ awareness about security hazards and the training programs applied in this field. However, there is still an obvious gap between their knowledge and applying it in their daily life due to the lack of understanding the real effect of those threats. [10] conducted a survey of students and academic staff in 2010 from three cities of UAE: Sharjah, Abu Dhabi, and Dubai, to examine their awareness of cybersecurity. While the findings lack important details, they highlight the ongoing importance of programs to raise cybersecurity awareness.The author finds that educating and training users is essential to identify different security threats and improve their skills to apply security tips practically in their daily life, with a recommendation to the governments and companies to work locally and worldwide to prevent from the cyber-attacks and build skilled team to face those hazard in business, schools and various organizations. Students and instructors at California State University were by [44], who discovered that the primary issue hindering the respondents' safe use of the Internet was not a lack of knowledge of cybersecurity, but the manner in which they applied it to their daily online activities.

Another study on students’ awareness of the possible hazards posed by social media was carried out in Malaysia by [45] Their findings showed that one-third of the participants (295 students) ended up falling victim to fraud on social media networks, which suggests that users are not sufficiently attuned to the risks associated with cyberattacks. Students in the Pacific Northwest College in the US were surveyed about their knowledge of cybersecurity [46]. The findings demonstrated that they were unable to clarify such cybersecurity-related terms as worms, phishing, Trojan

DOI: 10.31695/IJASRE.2024.5.3

horse, and malware. Students from different age groups in New Zealand were also surveyed about their knowledge of cybersecurity, and the results showed that they misunderstood many cybersecurity-related terms, such as "phishing" [47].

A survey of computer science students at Yobe State University in Nigeria sought to measure their level of awareness of cybersecurity, as they are expected to be future employees in related fields [6]. The students exhibited an adequate level of awareness of privacy and security, but still lacked the basic knowledge of certain fundamental concepts, such as phishing, securing passwords, and two-factor authentication. These researchers reported that no campaign was ongoing to raise the students' awareness of cybersecurity. Another survey [48] carried out in Bangladesh revealed variations in the degrees of users' knowledge of cybersecurity.

[49] held collaborative workshops for teachers and educators across the UK [49]with an emphasis on active involvement in discussions. They determined that the participants were enthusiastic about including various elements of cybersecurity in the curricula of their schools because they believed in the importance of knowledge of cybersecurity in daily life.

Various evaluations and surveys have been carried out with an emphasis on preventive security tools and techniques [19]. Some studies have detailed the current state of cybersecurity, while others have comprehensively considered the relevant work and evaluative methodologies. [50] investigated methods to train users to protect themselves against cyberattacks. They examined the techniques used to train users to avoid scams and phishing attempts, and proposed ways to combine or embed such training into people's everyday activities. The idea of embedded training has also been embraced in other studies [51, 52]. Researchers have focused on providing training by integrating its features into functional systems to improve users' online skills.

It is necessary to comprehensively understand the knowledge imparted by different approaches to training to enhance users' skills of online navigation [53]. Research on university students [54] has shown that developing critical thinking and comprehension is vital for ensuring cybersecurity. The relevant studies have shown that although students understand the basic principles of cybersecurity, they are still unable to apply them correctly.

To the best of our knowledge, this is the first study to conduct a survey of teachers and administrators in public and private schools in Kuwait to evaluate their knowledge of cybersecurity. Considering the worldwide interest in using AI and its huge impact in todays' education, an AI section has been added as a significant topic to be introduced through the campaign lectures and workshops. Moreover, the research reported here is distinct in that it covers all governorates of Kuwait as well as a wide range of age groups of adult users (20–50+ years of age) from different backgrounds.

3. PROBLEM DEFINITION

As the Internet has spread across the world in the last three decades [4, 6], threats to personal and organizational cybersecurity have become increasingly common [5, 7, 9]. Cyberattacks may occur in various forms, including phishing scams, malware infections, and ransomware attacks. These hazards appear in daily life and have a significant impact on users of all ages, especially children as they use digital devices for learning and entertainment. In this context, it is important to educate adults who, as parents, teachers, administrators, or caregivers, can protect their private and personal information.

We designed our lectures and workshops for the "Be Smart Safe" awareness campaign after reflecting on the knowledge and competence required to enhance cybersecurity awareness among adults and equip them with the tools and skills to protect their information without requiring advanced technical skills. A 60-minute lecture was designed to cover six topics: digital citizenship, the world of the Internet, social media networks, cyberbullying, parental control, and AI applications and security issues.

The workshop began by defining digital citizenship and the five main characteristics that users should have as digital citizens: respect, ways to evaluate information, having a worthwhile goal, balancing Internet use with real life, and being alert to any threat. We then briefly provided the audience with an account of the history of the Internet, and how it was created and spread worldwide. Following this, we explained data transmission through social media platforms

DOI: 10.31695/IJASRE.2024.5.3

in a simple manner to clarify the potential hazards to user privacy in this process. The terms of use for each application and social media platform constituted a crucial topic because most members of the audience had never read them, even though they contain critical privacy- and security-related details of each application with regard to personal user data. We introduced a hands-on exercise for members of the audience at this stage to educate them about the limitations in access to data and user content that is controlled and used by applications. We identified four steps to protect against cyberbullying, and explained how any user could easily apply them as far as they had the ability to use the device correctly without any prior technical experience. These four steps were as follows: Block the bully, inform a trusted adult, keep the evidence, and learn about the cybercrime Law in Kuwait. We provided our audience with an introduction to cybersecurity crime in Kuwait and referred them to the official account of the Electronic and Cybercrime Combatting Department of the Kuwaiti Ministry of Interior (the social media Account: @ECCCD).

While the first part of the lecture contained information and theoretical tips on cybersecurity, we started the second part by describing to members of the audience how to use the security and privacy settings in their devices and provided them with easy step-by-step procedures for different operating systems. We concluded the workshop by defining AI, summarizing the history of its development, its applications to education, and the security hazards posed by it.

We conducted pre- and post-workshop surveys from September to December of 2023 in schools in different governorates of Kuwait to measure the effectiveness of the workshop on adults' awareness of cybersecurity. Each workshop started with the introduction of the survey to the audience. We provided them with a barcode containing an online link to the survey. It targeted adults with different roles in society, including teachers, parents, trainers, administrators, and social workers ranging from 20 to older than 50 years of age. One hundred and ninety people participated in this survey, and 95 of them completed the pre- and post-workshop surveys for a response rate of 61.7%. Twenty-three of the participants were parents (24.2%), while the others were administrators, teachers, training, and caregivers (72 = 75.8%).

The surveys were designed to measure the effectiveness of training adults in improving their awareness of cybersecurity, and to assess their capabilities of applying their newly gained security skills and delivering this knowledge to their communities. Once the founders of the awareness campaign had introduced themselves and the purpose of the workshop, the audience was asked to scan a barcode that linked to a two-minute survey and answer the questions on it. This exercise was repeated at the end of the workshop. The surveys consisted of four questions on three items and two questions at the end to measure the effectiveness of the workshop. The three survey items were competence, personal attributes, and future impacts, and were taken from the ISTE standards[55]. The participants were asked to rate their responses to the questions by ticking a box on the right and were provided a five-point scale for their answer choices, ranging from 0 = "totally disagree" to 4 = "totally agree." The questions related to each survey item and the source for it are provided in Table 1.

Table 1. Survey Items and Their Resources

#	Survey Item	Supporting Literature
	Competence1	
1	I can explain to my students/children what the Internet is.	ISTE Standard 2.3a [55]
2	I can explain to my students/children how social media works.	Appendix C, Table 8(1.1.a) [56]
3	I can explain to my students/children the legal rules of my country, i.e., @ecccd	ISTE Standard 2.2c [55]
4	I can explain to my students/children how to protect themselves against cyberbullying	ISTE Standard 2.2a [55]
	Personal Attributes	

DOI: 10.31695/IJASRE.2024.5.3

5	I believe that my photos will be deleted from social media forever.	Table 5, Q31 [57]
6	I know that my personal data will not be used by any social media company.	Table 5, Q2 [57]
7	I find it difficult to update my device operating system.	Table 5, Q7 [57]
8	I know how to use the resources and search tips for the digital world.	ISTE Standard 2.2b [55] Table 1, Q 17 [58]
	Future Impacts	
9	I know that keeping my personal photos saved on my smartphone is safe because it is private.	Table 5, Q 2 [57]
10	I can protect myself from cybercrime by knowing the law.	ISTE Standard 2.2c [55] Table 1, Q48 [58]
11	I am responsible in my online behaviors, safety, and privacy.	ISTE Standard 3.1d [55]
12	I know how to evaluate online resources.	ISTE Standard 3.1c [55]

The last two questions that were used to measure the effectiveness of the workshop were as follows:

1. In this workshop, we introduced the Internet and the World Wide Web, including topics like social media, online resources, digital citizenship, cybersecurity, and parental control. In light of this, to what extent will your efforts to use this knowledge in practice will be inspired by your experiences in this workshop, and to what extent will they be inspired by other factors in your life?
2. To what extent would you say that any change in the ratings that you gave yourself before the program compared with now is the result of your experiences in this workshop, and to what extent is it a function of other factors in your life?

The participants were asked to choose their answer from among the following options:

- Uncertain
- Mostly this program
- Somewhat this program and somewhat other factors
- The workshop/lecture has not started yet.
- Mostly other factors

We ensured all the participants that their personal information would be kept confidential.

4. RESULTS AND DISCUSSION

We examined variations in the participants' responses to the 12 questions in the pre- and post-workshop/lecture surveys to measure the overall changes in their scores. The variations were evaluated by using paired-sample t-tests to focus on the upcoming workshop. A pilot study on the survey questions showed that two of them needed to be revised because the results for them were meaningless. We also decided to add two questions to further verify the effectiveness of the knowledge gained by the participants from the workshop.

DOI: 10.31695/IJASRE.2024.5.3

Table 2. Ratings of Items on the Pre- and Post-Workshop Surveys

#	Survey Item	Mean aggregates			
	Competence	**Pre-Workshop M(V)**	**Post-Workshop M(V)**	**t**	**p**
1	I can explain to my students/children what the Internet is.	3.126(0.558)	3.589(0.308)	-5.765	<0.001
2	I can explain to my students/children how social media works.	2.863(0.673)	3.536(0.378)	-7.457	<0.001
3	I can explain the legal rules of my country, i.e., @ecccd, to my students/children.	2.568(0.779)	3.505(0.486)	-10.317	<0.001
4	I can explain to my students/children how to protect themselves against cyberbullying.	2.757(0.866)	3.473(0.443)	-7.410	<0.001
	Personal Attributes				
5	I believe that my photos will be deleted from social media forever.	3.578(0.395)	3.778(0.237)	-3.098	0.001
6	I know that my personal data will not be used by any social media company.	3.042(0.615)	3.421(0.395)	-4.463	<0.001
7	I find it difficult to update my device operating system.	2.884(0.741)	3.357(1.041)	-4.439	<0.001
8	I know how to use the resources and search tips for the digital world.	2.905(0.661)	3.389(0.751)	-5.0615	<0.001
	Future Impacts				
9	I know that keeping my personal photos saved on my smartphone is safe because it is private.	3.032(0.733)	3.568(0.482)	-6.080	<0.001
10	I can protect myself from cybercrime by knowing the law.	3.378(0.556)	3.715(0.269)	-4.136	<0.001
11	I am responsible in my online behaviors, safety, and privacy.	3.412(0.606)	3.789(0.211)	-4.5351	<0.001
12	I know how to evaluate online resources.	3.221(0.621)	3.578(0.438)	-3.694	0.000
M: Mean, V: Variance					

DOI: 10.31695/IJASRE.2024.5.3

The learning indicators listed in Table 2 show that following the workshop, the respondents exhibited a better understanding of the Internet and its history, were better able to explain social media, had a general understanding of cybercrime law in Kuwait, and could better protect themselves and children in their care from cybercrime and cyberbullying. This suggests that their responses to questions under "Personal Attributes" in the survey had been positively influenced by their experience of the workshop, which had improved their knowledge of privacy- and security-related issues on social media, how their information is being used by such platforms, the importance of frequently updating their device operating system, and the how to safely access and use online resources. However, the results of the surveys also show that the participants still struggled to understand how their personal data and the content posted by them on social media were being used by these platforms. The outcomes on last four survey questions, which covered the "Future Impacts" item, also suggest that the workshop had improved the participants' awareness of the safety and privacy settings of their devices, their knowledge of cybercrime law in Kuwait as well as their digital footprint, and their capacity to evaluate online resources. The results also reveal the need for more training on ways to scrutinize and choose trusted resources.

The last two questions (13 and 14) were added to the survey to measure the impact of the workshop in terms of inspiring the participants to use the information provided in it, and whether and how it changed their level of awareness of cybersecurity. These two questions garnered responses from 83 participants after the workshop. For Question 13, only five participants (6.02%) were uncertain of the effect of the workshop in terms of inspiring them to use the information provided, 48.2% of the respondents found the workshop to be effective in this regard, 38.5% believed that the workshop and other factors were helpful to them in conjunction, while only two participants (2.4%) said that only other factors, and not this workshop, had improved their knowledge of cybersecurity. Similarly, four participants (4.82%) were uncertain about the effect of the workshop in improving their awareness of cybersecurity, 51.8% believed that it had improved their awareness, 36.14% acknowledged that other factors in conjunction with the workshop had contributed to enhancing their awareness, while only 2.41% of the participants claimed that other factors had exclusively improved their awareness. Overall, the responses to this workshop/lecture were positive.

5. CONCLUSION

The Internet and smart devices are ubiquitous in today's digital era. Nowadays, Artificial intelligence is embedded in most social media platforms and introduced as a search tool by different companies to be used by Internet users regardless of their knowledge or level of awareness of cybersecurity, which exposes them to a variety of cyber threats that compromise their personal information. This highlights the need for training users to understand the threats to cybersecurity in the form of cyberattacks. The use of the Internet has drastically risen in the Middle East in the last decade and has been accompanied by an inevitable rise in cybercrime in the region. This has prompted the "Be Smart Safe" campaign in Kuwait in 2016 to raise awareness among the public of the smart and safe use of technology.

Many studies have investigated the implications of raising awareness of cybersecurity among users by using different tools. Some researchers have focused on designing productive training programs to educate netizens. In this study, we measured the beneficial effect of training adults to enhance their awareness of cybersecurity, and examined approaches to make them more resistant to cyberattacks and breaches of their personal information. We held workshops on cybersecurity and conducted surveys of the participants before and after it to assess its impact in terms of increasing their cybersecurity awareness. The results showed that the workshop had a positive impact on the participants' knowledge and awareness. They also verified the importance of holding workshops and lectures on safe online practices for public and private school teachers, educational administrators, and parents. A course on digital awareness as part of the school curriculum is important in this regard because smart devices are widely used by children these days, and it is thus important to teach them how to safely navigate the cybersphere. This study has certain limitations as well. Many participants of our workshop did not take or complete their survey as it was being held during their classes. This affected the data collection. We recommend that the administrators of schools make sure that future workshops be appropriately scheduled to avoid such conflicts.

DOI: 10.31695/IJASRE.2024.5.3

ACKNOWLEDGMENT

I thank Dr. Hana Al-Omar, Senior Assistant Lecturer, Kuwait University, for conducting the statistical analyses of the pilot study data and sharing insights, and Dr. Zainab M. AlQenaei, Associate Professor at Kuwait University, for supervising the research.

REFERENCES

[1] James J, Morsey C, Philips J (2016) CYBERSECURITY EDUCATION: A HOLISTIC APPROACH TO TEACHING SECURITY. Issues In Information Systems 17:150–161. https://doi.org/10.48009/2_iis_2016_150-161

[2] Amankwa E (2021) Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security 12:233–249. https://doi.org/10.4236/jis.2021.124013

[3] Choucri N, Madnick S, Koepke P (2016) Institutions for Cyber Security: International Responses and Data Sharing Initiatives Institutions for Cyber Security: International Responses and Data Sharing Initiatives 2. Inf Technol Dev. https://doi.org/10.1080/02681102.2013.836699#.Unfi8eKiJO8

[4] Zukarnain ZA, Hashim MZ, Muhammad N, et al (2020) Impact of training on cybersecurity awareness. Gading Journal of Science and Technology (e-ISSN: 2637-0018) 3:114–120

[5] Mubarak AR (2015) Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region

[6] Garba A, Musa MA, Othman SH (2020) A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative. International Journal on Emerging Technologies 11:41–49

[7] Karim AA, Shah PM, Khalid F, et al (2015) The Role of Personal Learning Orientations and Goals in Students' Application of Information Skills in Malaysia. Creat Educ 06:2002–2012. https://doi.org/10.4236/ce.2015.618205

[8] Anderson G, Ktoridou D, Eteokleous N, Zahariadou A (2012) Exploring parents' and children's awareness on internet threats in relation to internet safety. Campus-Wide Information Systems 29:133–143. https://doi.org/10.1108/10650741211243157

[9] MOSALANEJAD L, DEHGHANI A, ABDOLAHIFARD K (2014) THE STUDENTS' EXPERIENCES OF ETHICS IN ONLINE SYSTEMS: A Phenomenological Study

[10] Aloul FA (2012) The Need for Effective Information Security Awareness. Journal of Advances in Information Technology 3:. https://doi.org/10.4304/jait.3.3.176-183

[11] (2010) http://www.internetworldstats.com/stats.htm. In: Miniwatts Marketing Group, 2010 Internet World Stats.

[12] Khattak ZA, Manan JA, Sulaiman S (2011) Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach. Journal of Advances in Information Technology 2:. https://doi.org/10.4304/jait.2.2.109-121

[13] Zwilling M, Klien G, Lesjak D, et al (2022) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems 62:82–97. https://doi.org/10.1080/08874417.2020.1712269

[14] Erendor ME, Yildirim M (2022) Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access 10:52319–52335. https://doi.org/10.1109/ACCESS.2022.3171829

[15] Jang-Jaccard J, Nepal S (2014) A survey of emerging threats in cybersecurity. In: Journal of Computer and System Sciences. Academic Press Inc., pp 973–993

[16] Prichard JJ, Macdonald LE (2004) Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks Executive Summary

[17] Shaw RS, Chen CC, Harris AL, Huang HJ (2009) The impact of information richness on information security awareness training effectiveness. Comput Educ 52:92–100. https://doi.org/10.1016/j.compedu.2008.06.011

[18] Trappe W, Straub J (2018) Journal of Cybersecurity and Privacy: A New Open Access Journal. Journal of Cybersecurity and Privacy 1:1–3. https://doi.org/10.3390/jcp1010001

DOI: 10.31695/IJASRE.2024.5.3

[19] Gkioulos V, Chowdhury N (2021) Cyber security training for critical infrastructure protection: A literature review. Comput Sci Rev 40:100361. https://doi.org/10.1016/j.cosrev.2021.100361
[20] Peker YK, Ray L, Silva S Da, Gibson N (2016) Raising cybersecurity awareness among college students. Journal of The Colloquium for Information System Security Education (CISSE) 4:1–17
[21] Straub J (2014) Assessment of examinations in computer science doctoral education. Computer Science Education 24:25–70. https://doi.org/10.1080/08993408.2014.890792
[22] Aldawood H, Skinner G (2019) Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet 11
[23] Gill SS, Xu M, Ottaviani C, et al (2022) AI for Next Generation Computing: Emerging Trends and Future Directions. https://doi.org/10.1016/j.iot.2022.100514
[24] Thesis M', Vihervaara J, Urama J (2022) ARTIFICIAL INTELLIGENCE IN COMPUTER NETWORKS Role of AI in Network Security
[25] Shen X, Gao J, Wu W, et al (2020) AI-assisted network-slicing based next-generation wireless networks. IEEE Open Journal of Vehicular Technology 1:45–66. https://doi.org/10.1109/OJVT.2020.2965100
[26] Zebin T, Rezvy S, Luo Y (2022) An Explainable AI-based Intrusion Detection System for DNS over HTTPS (DoH) Attacks
[27] Ahmadi S (2023) Next Generation AI-Based Firewalls: A Comparative Study. International Journal of Computer (IJC) International Journal of Computer 49:245–262
[28] Manifavas C, Fysarakis K, Rantos K, Hatzivasilis G (2014) LNCS 8533 - DSAPE – Dynamic Security Awareness Program Evaluation
[29] Hatzivasilis G, Ioannidis S, Smyrlis M, et al (2020) Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences (Switzerland) 10:. https://doi.org/10.3390/app10165702
[30] Richardson R (2008) The latest results from the longest-running project of its kind
[31] Beyer RE, Brummel BJ (2015) Implementing effective cyber security training for end users of computer networks. SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR
[32] West R (2008) THE PSYCHOLOGY OF SECURITY. Commun ACM 51:34–40
[33] McCrohan KF, Engel K, Harvey JW (2010) Influence of awareness and training on cyber security. Journal of Internet Commerce 9:23–41. https://doi.org/10.1080/15332861.2010.487415
[34] Eyong B. Kim (2013) Information Security Awareness Status of Business College: Undergraduate Students. Information Security Journal: A Global Perspective. Information Security journal 22:171–179
[35] Aldawood H, Skinner G (2019) Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet 11:. https://doi.org/10.3390/fi11030073
[36] Amankwa E (2021) Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security 12:233–249. https://doi.org/10.4236/jis.2021.124013
[37] Nagarajan A, Allbeck JM, Sood A, Janssen TL (2012) Exploring Game Design for Cybersecurity Training. IEEE
[38] Park W, Ahn S (2017) Enhancing Education Curriculum of Cyber Security Based on NICE. Comp and Comm Sys 6:2287–5891. https://doi.org/10.3745/KTCCS.2017.6.7.321
[39] Franke U, Brynielsson J (2014) Cyber situational awareness - A systematic review of the literature. Comput Secur 46:18–31
[40] Tsohou A, Kokolakis S, Karyda M, Kiountouzis E (2008) Investigating information security awareness: Research and practice gaps. Information Security Journal 17:207–227. https://doi.org/10.1080/19393550802492487
[41] Kim EB (2014) Recommendations for information security awareness training for college students. Information Management and Computer Security 22:115–126
[42] Mcdaniel EA (2013) Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness
[43] Kruger H, Drevin L, Steyn T (2010) A vocabulary test to assess information security awareness. Information Management & Computer Security 18:316–327. https://doi.org/10.1108/09685221011095236

DOI: 10.31695/IJASRE.2024.5.3

[44] Slusky L, Partow-Navid P (2012) Students Information Security Practices and Awareness. Journal of Information Privacy and Security 8:3–26. https://doi.org/10.1080/15536548.2012.10845664
[45] Kirwan GH, Fullwood C, Rooney B (2018) Risk Factors for Social Networking Site Scam Victimization among Malaysian Students. Cyberpsychol Behav Soc Netw 21:123–128. https://doi.org/10.1089/cyber.2016.0714
[46] Sarathchandra D, Haltinner K, Lichtenberg N (2016) College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. Cybersecurity Symposium : CYBERSEC
[47] Tirumala SS, Sarrafzadeh A, Pang P (2016) A survey on Internet usage and cybersecurity awareness in students
[48] Ahmed N, Kulsum U, Bin Azad MdI, et al (2017) Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective. In: 2017 IEEE Region 10 Humanitarian Technology Conference
[49] Pencheva D, Hallett J, Rashid A (2019) Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education
[50] Al-Daeef M, Basir N, Mohd M (2017) Security Awareness Training: A Review. World Congress on Engineering 1:
[51] Anderson JR, Reader LM, Herbert SA (1996) Situated learning and education1996. Educational researcher 25:5–11
[52] Kumaraguru P, Rhee Y, Sheng S, et al (2007) Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer
[53] Hautamaki J, Karjalainen M, Hakkinen P, Hamalainen T (2019) CYBER SECURITY EXERCISE – LITERATURE REVIEW TO PEDAGOGICAL METHODOLOGY. In: INTED2019 Proceedings. IATED, pp 3893–3898
[54] Scheponik T, Sherman AT, DeLatte D, et al (2016) How Students Reason about Cybersecurity Concepts2016
[55] ISTE https://iste.org/standards
[56] CERIC https://ceric.ca/wpdm-package/career-development-practice-in-canada-chapter-20-demonstrating-the-value-of-career-development-services/
[57] Sangwan A, Sangwan A, Punia P Development and Validation of an Attitude Scale towards Online Teaching and Learning for Higher Education Teachers. https://doi.org/10.1007/s11528-020-00561-w/Published
[58] Yavuz S (2005) DEVELOPING A TECHNOLOGY ATTITUDE SCALE FOR PRE-SERVICE CHEMISTRY TEACHERS

DOI: 10.31695/IJASRE.2024.5.3

APPENDIX: T-Test Results

Paired two-sample T-test for means

	1.a	*1.a*
Mean	3.126316	3.589474
Variance	0.558343	0.308399
Observations	95	95
Pearson Correlation	0.305754	
Hypothesized Mean Difference	0	
df	94	
t stat	-5.765 86	
P(T<=t) one tail	5.15 E-08	
t critical one tail	1.661 226	
P(T<=t) two tail	1.03 E-07	
t critical two tail	1.985 523	

Paired two-sample T-test for means

	1.b	*1.b*
Mean	2.863158	3.536842
Variance	0.672564	0.378947
Observations	95	95
Pearson Correlation	0.273499	
Hypothesized Mean Difference	0	
df	94	
t stat	-7.457 02	
P(T<=t) one tail	2.16 E-11	
t critical one tail	1.661 226	
P(T<=t) two tail	4.33 E-11	
t critical two tail	1.985 523	

Paired two-sample T-test for means

	1.c	*1.c*
Mean	2.568421	3.505263
Variance	0.779843	0.486674
Observations	95	95
Pearson Correlation	0.392263	
Hypothesized Mean Difference	0	
df	94	
t Stat	-10.31 79	
P(T<=t) one tail	1.94 E-17	
t critical one	1.661	

Paired two-sample T-test for means

	1.d	*1.d*
Mean	2.757895	3.473684
Variance	0.866293	0.443449
Observations	95	95
Pearson Correlation	0.341473	
Hypothesized Mean Difference	0	
df	94	
t Stat	-7.410 03	
P(T<=t) one tail	2.71 E-11	
t critical one	1.661	

DOI: 10.31695/IJASRE.2024.5.3

tail	226
P(T<=t) two tail	3.89 E-17
t critical two tail	1.985 523

tail	226
P(T<=t) two tail	5.41 E-11
t critical two tail	1.985 523

Paired two-sample T-test for means

	2.a	*2.a*
Mean	3.578 947	3.778 947
Variance	0.395 297	0.237 85
Observations	95	95
Pearson Correlation	0.387 116	
Hypothesized Mean Difference	0	
df	94	
t Stat	-3.098 73	
P(T<=t) one tail	0.001 282	
t critical one tail	1.661 226	
P(T<=t) two tail	0.002 564	
t critical two tail	1.985 523	

Paired two-sample T-test for means

	2.b	*2.b*
Mean	3.042 105	3.421 053
Variance	0.615 23	0.395 297
Observations	95	95
Pearson Correlation	0.330 393	
Hypothesized Mean Difference	0	
df	94	
t Stat	-4.463 79	
P(T<=t) one tail	1.12 E-05	
t critical one tail	1.661 226	
P(T<=t) two tail	2.24 E-05	
t critical two tail	1.985 523	

Paired two-sample T-test for means

	2.c	*2.c*
Mean	2.884 211	3.357 895
Variance	0.741 769	1.040 761
Observations	95	95
Pearson Correlation	0.398 79	
Hypothesized Mean Difference	0	
df	94	
t Stat	-	

Paired two-sample T-test for means

	2.d	*2.d*
Mean	2.905 263	3.389 474
Variance	0.661 142	0.750 952
Observations	95	95
Pearson Correlation	0.385 078	
Hypothesized Mean Difference	0	
df	94	
t Stat	-	

DOI: 10.31695/IJASRE.2024.5.3

	4.439 03
P(T<=t) one tail	1.23 E-05
t critical one tail	1.661 226
P(T<=t) two tail	2.46 E-05
t critical two tail	1.985 523

	5.061 5
P(T<=t) one tail	1.03 E-06
t critical one tail	1.661 226
P(T<=t) two tail	2.06 E-06
t critical two tail	1.985 523

Paired two-sample T-test for means

Paired two-sample T-test for means

	3.a	*3.a*
Mean	3.0315 79	3.56842 1
Variance	0.7330 35	0.48197 1
Observations	95	95
Pearson Correlation	0.3990 27	
Hypothesized Mean Difference	0	
df	94	
t Stat	-6.0799 8	
P(T<=t) one tail	1.28E-08	
t critical one tail	1.6612 26	
P(T<=t) two tail	2.56E-08	
t critical two tail	1.9855 23	

	3.b	*3.b*
Mean	3.3789 47	3.7157 89
Variance	0.5569 99	0.2694 29
Observations	95	95
Pearson Correlation	0.2535 12	
Hypothesized Mean Difference	0	
df	94	
t Stat	-4.1363 2	
P(T<=t) one tail	3.84E-05	
t critical one tail	1.6612 26	
P(T<=t) two tail	7.68E-05	
t critical two tail	1.9855 23	

Paired two-sample T-test for means

Paired two-sample T-test for means

	3.c	*3.c*
	3.41 052	3.7 894
Mean	6	74
Variance	0.60	0.2

	3.d	*3.d*
	3.22 105	3.57 894
Mean	3	7
Variance	0.62	0.43

DOI: 10.31695/IJASRE.2024.5.3

	627	105
	1	26
Observations	95	95
Pearson Correlation	0.21471	
Hypothesized Mean Difference	0	
df	94	
t Stat	-4.534818	
P(T<=t) one tail	8.49E-06	
t critical one tail	1.661226	
P(T<=t) two tail	1.7E-05	
t critical two tail	1.985523	

	082	785
	9	
Observations	95	95
Pearson Correlation	0.160013	
Hypothesized Mean Difference	0	
df	94	
t Stat	-3.69383	
P(T<=t) one tail	0.000185	
t critical one tail	1.661226	
P(T<=t) two tail	0.000371	
t critical two tail	1.985523	

DOI: 10.31695/IJASRE.2024.5.3