***Multidisciplinary Research Academic Journal* (MDRAJ)**
Vol 8. Issue 2, September 2023, pp 41-50
ISSN: l-2467-4699
ISSN: e-2467-4834
https://www.openlu.org/research/

End User Security Awareness and Usage of Mobile Devices among University Students of Bugema University

Muwanga Erasto Kosea[1] & Oloo Stephen Nyanjwa[2]

Abstract

The survey aimed to investigate End User Security Awareness and usage of Mobile Devices among University Students at Bugema University. The survey found that the students had social network accounts and were using mobile devices, laptops, Smartphones, or tablets. Despite being able to research and use the internet, students needed to be made aware of how to protect their data from various security risks. The university minimally sensitizes and disseminates knowledge about end-user security awareness and how the students can protect their data from potential misuse or unauthorized access. Therefore, there is a need for the university to put in place a policy for end-user security as well as create awareness among the students.

Keywords: End User Security, Awareness, Usage of Mobile Devices, University students.

Résumé

L'enquête visait à étudier la sensibilisation à la sécurité des utilisateurs finaux et l'utilisation des appareils mobiles parmi les étudiants universitaires à l'Université de Bugema. Les personnes interrogées ont découvert que les étudiants disposaient de comptes de réseaux sociaux et utilisaient un appareil mobile, un ordinateur portable, un smartphone et/ou une tablette. Même s'ils étaient capables de rechercher et d'utiliser Internet, les étudiants ne savaient pas vraiment comment protéger leurs données contre divers risques de sécurité. L'université sensibilise et diffuse de manière minimale des connaissances sur la sensibilisation à la sécurité des utilisateurs finaux et sur la manière dont les étudiants peuvent protéger leurs données contre une utilisation abusive potentielle ou un accès non autorisé. Par conséquent, il est nécessaire que l'université mette en place une politique de sécurité des utilisateurs finaux et sensibilise les étudiants.

[1] *Muwanga Erasto Kosea is the Head of the Department of Software engineering, Bugema university Kampala, Uganda*
[2] *Dr. Oloo Stephen Nyanjwa is the Head of the Department of Social Science at Bugema University, Kampala, Uganda. Email: oloosteven9@gmail.com*

Mots clés : sécurité des utilisateurs finaux, sensibilisation, utilisation des appareils mobiles, étudiants universitaires.

Introduction

Given the new global age, countless unfolded opportunities may touch every aspect of life (Mai & Tick, 2021). Today, it is not easy to imagine life without information technology. Students currently utilize the Internet to find data and gain general knowledge, hence becoming a data super highway where they propel their ideas and social experiences. Society has increasingly relied on the Internet for studying, communication, banking, and e-commerce (Scholefield & Shepherd, 2019). Users browse the web but do not note the many ways they may place themselves at risk. This is because cybercrime has increased steadily as technology advances, varying from robbery, identity theft, ransom, spying, and deception.

Cyber-attacks and exploits are conducted daily, exploiting miscellaneous vulnerabilities on different devices. The growing trend to protect user identities is to enforce Multi-Factor Authentication (MFA). Hence, increased adoption is the callback feature, where the user initially authenticates using their credentials (username and password), and receives a call to enter their PIN. To guarantee optimum levels of information security is a challenging task. As technology keeps advancing, continuous monitoring is essential, and defensive mechanisms are also being innovated to cope with the rapid pace. (Diogenes & Ozkaya, 2019). Users are expected to have, at least, basic knowledge of security risks and privacy policies and security awareness that plays a pivotal role in our daily life of technology. When it comes to maintaining a robust cyber security approach, the user's attitude toward protecting themselves from cyber-attacks is a critical factor (Young et al., 2018). Smartphone technology has increased end-user accessibility to internet resources since its usage extends beyond and covers applications with minimum required security (Koyuncu & Pusatli, 2019).

Although smartphones can contain valuable information, they are prone to becoming targets from attackers for hardware and software. These vulnerabilities may cause catastrophic results for the owner of the devices. These attacks and vulnerabilities may include interacting with poorly coded and unsecured websites, creating weak passwords, and downloading data containing malicious files. Hence, there is a need to assess the end-user security awareness for the students using mobile devices for the Internet to browse and use the e-learning management system platform. Therefore, this study analyzes the end-user security awareness and usage of Mobile Devices among University Students of Bugema University.

Literature Review

Security awareness is not a training. The purpose of awareness presentations is to focus attention on security. Awareness presentations are intended to allow individuals to recognize Information Technology security concerns and respond accordingly. The number of cyber-attacks has grown tremendously in the last few years and is likely to increase. According to PricewaterhouseCoopers, there were 42.8 million security incidents in 2016, which was a rise of 48% compared to 2019. Larger organizations spend almost 35% of their annual security budget on end-user security training and awareness. With the wide-scale adoption of information technologies in recent decades, the average information technology user is not necessarily technically educated and is unlikely to have studied cybersecurity in his/her previous education. Hence, an organization needs to invest in the security awareness of

employees in order to inform or control its systems. The most frequent reasons for cyber security incidents are naïve behavior and accidental mistakes of computer users. Unaware employees may share sensitive information with unauthorized persons or, inadvertently install malware, create weak passwords, or be the victim of phishing attacks (Kovaˇcevi & Radenkovi, 2020).

Kirwan, Fullwood, & Rooney (2018) conducted a study to understand how students of a Malaysian university were aware of the risks imposed by social networking sites, revealing that about 33.3% of the students had been victims of some social networking scams. Another study by Hossain and Zhang (2015) in the realm of social networking was conducted among 377 Facebook, Twitter, and LinkedIn users, where 41% showed concern about online privacy and 44% lacked the mechanisms of social networking privacy policy.

Senthilkumar & Easwaramoorthy, (2017) performed an online survey for 500 Tamil Nadu college students regarding miscellaneous cyber security threats. The results revealed that 70% of the participants were fully aware of security practices to prevent virus attacks and had been using up-to-date antivirus software. On the other hand, the remaining 30% of participants were reported to be using obsolete antivirus software, and 11% of them were not even using antivirus at all. It might be observed that most of the studies highlighted that most participants do not have the sufficient awareness of cyber security practices and principles, revealing much personal information that exposes their privacy to considerable security risks without them noticing. Moreover, the issue does not emerge from not having enough security awareness and knowledge but from applying that knowledge when it comes to cyber-related routine, which is tremendously challenging.

The widespread increase in dependence on information technology in the daily work activities of employees and students in organizations makes keeping this technology secure more of a challenge since the vital human factor is considered the weakest link in an organization's line of defense in the Information technology (Alotaibi & Alfehaid, 2018). Security awareness involves activities that have been designed to change an employee's behavior so that it falls within the information security boundary.

Users often need help finding the creation and retention of solid and secure passwords problematic, and several studies have been conducted to address the issue of security awareness regarding passwords. A standard method of raising password security awareness involves using password meters, typically placed next to forms on a web page, to give users a general indication of password strength (Scholefield & Shepherd, 2019). Several cyber security-based games have previously been developed to educate users. Many of these games have been aimed primarily at children and young people, such as the Webonauts Internet Academy, an online game designed to educate children about online etiquette where users travel around space, visiting different planets, learning to deal with different behaviors exhibited on each of them. These skills are synonymous with behavior on the Internet.

Information and knowledge society in the "digital society" has generated enormous challenges to universities and academic institutions regarding the digitalization in the education system, such as the comprehensive integration of digital, online, and e-learning educational forms, the exploration of industrial and business academic programs (Mai & Tick, 2021). Cyber security risks can threaten confidential identity, identity, and privacy. Hence, the existence of cyber risks also emerges, which are explicitly cybersex, pornography, personal information exposure, cyber addiction, online fraud, and addiction to gaming and

gambling, which have adverse effects on adults and children. Most internet users still need more awareness of various internet threats/ cyber hazards.

Smartphone data can be easily breached and stolen, which raises security risks and causes severe threats to its users. The Bring Your Own Device "BYOD" culture weakens the security of organizations' networks (Taha & Dahabiyeh, 2020). The advent of mobile learning needs educational institutions to be vigilant to the risks that cyber security problems might cause. Universities are the main targets of security threats because of the large volume of personal data they have, and hence, students become more vulnerable to these threats. There is an increased dependence on digital educational systems and free Wi-Fi for students to connect to the university network via smartphones.

Methodology

The survey employed a descriptive design that involved the use of online questionnaires delivered through Google Forms. Simple Random Sampling was the method used for choosing the respondents. A questionnaire consisting of three sections was developed; the first section was about demographic information related to the faculty of the participants. The second section was about computer usage behavior, and the last was about computer security awareness and training. This questionnaire was the main tool for data collection, and 49 students participated in the survey.

Results and Discussions

The survey looked at respondents from different schools of Bugema University and whether they have social network accounts. The findings reveal that 77.6% of the participants who belonged to the School of Sciences and Technology have a social network account, followed by 6.1% who belonged to the School of Health and Allied Sciences, whereas 4.1% from the School of Business had an active social network account and 2% was from School of Education, Humanities and Social Sciences as compared to 2% in School of Business. The findings imply that students have social network accounts at Bugema University, irrespective of the school. On the other hand, participants from the School of Sciences and Technology have a higher probability of having a social network account than those of the School of Business. Thus, a social network account is a crucial issue among students since most have one. Although students from the School of Sciences and Technology were the majority in the survey, there is a clear indication that in all schools, students have a social network account for various reasons.

Table 1. *Social network account*

		Do you have social network account		Total
		No	Yes	
which school do you belong to	School of Business	1	2	3
	School of Education, Humanities & Social Sciences	0	1	1
	School of Health and Allied Sciences	0	3	3

	School of Science and Technology	4	38	42
Total		5	44	49

The survey further looked at mobile devices used to access the internet and social network accounts. The findings show that the majority, 44.9% of the participants were using a laptop and Smartphone and had a social network account, followed by 18.4% who used Smartphone and had a social network account, 14.3% were using Laptop and had a social network account, another 6.1% were using Laptop, Smartphone and or Tablet. In line with the findings, the most typical mobile devices used to access the internet were Laptop-Smart phones, Smartphones, and Laptops, which were vital in having a social network account. Therefore, access to the internet plays a role in promoting having a social network account among Bugema University students. This means that smartphones and laptops have been vital for students, and some desktops are being used to access the internet. In line with the findings, a good percentage of students have access to mobile devices for internet access, but this needs to be further surveyed to determine the security of each category. The mobile devices used to access the internet and whether students have a social network account can be represented as shown in the Bar chart.

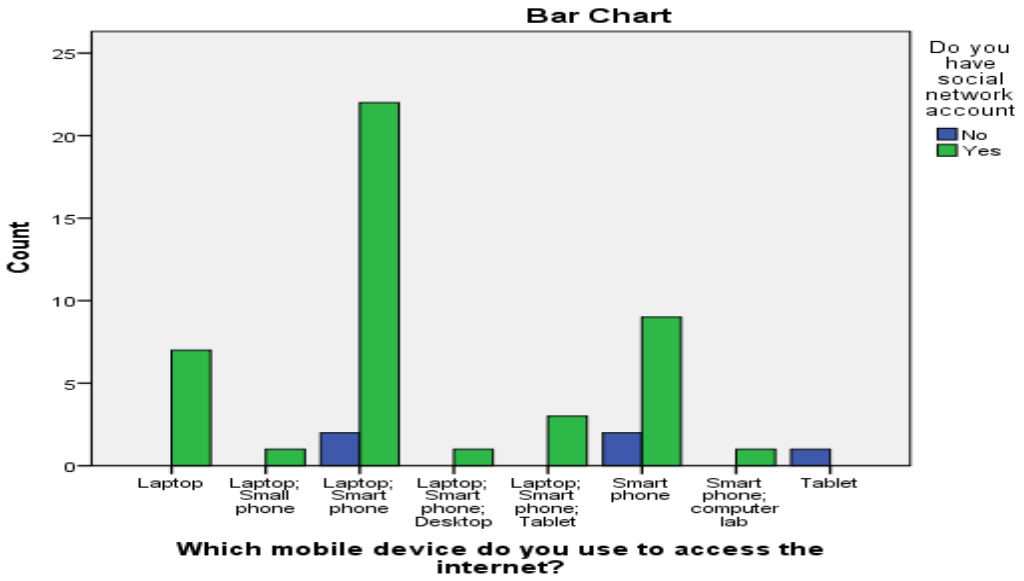

Figure 1: ***Mobile devices used in accessing internet***

The survey further looked at the possibility of participants doing research online about whether they have a computer network usage policy at the university. The findings indicated that 53.1% of the participants did not use it whether they were doing research online and whether Bugema University had a computer usage policy, whereas 26.5% accepted that they do research online. The university has a computer network usage policy, while 16.3% said no to research online, and Bugema University has a computer network usage policy. In these cases, the number of students doing research online was moderate, and the university lacked a computer network usage policy. This can be because the participants were undergraduates unaware of the computer network usage policy or the institution's failure to create awareness among the students on the same fact. Implementing user experience principles to improve

usability remains an open issue with implementing CIS in organizations. While security is user-focused, users still actively avoid hard-to-use security mechanisms and make mistakes that undermine security. About keeping data, systems, and devices safe for vulnerable groups, it was said that security can be a barrier to usability.

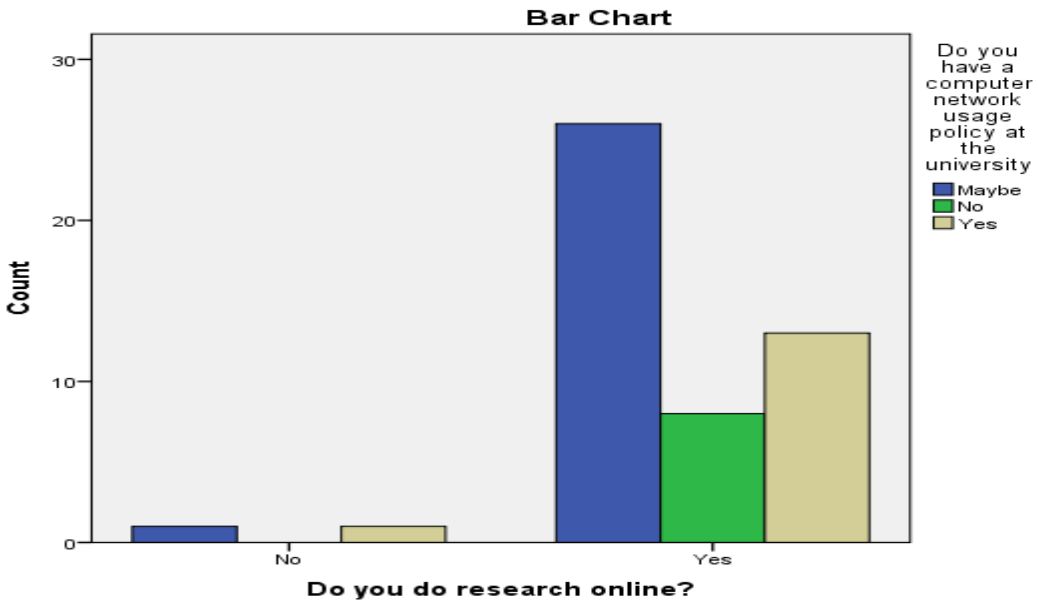

Figure 2. ***Research online***

The survey assessed whether while participants are doing research online, they use paid or free VPNs on mobile devices, and the result reveals that 57.1% of the respondents agreed that they use paid or free VPNs on their mobile devices compared to 38.8% who said no. Students enjoy using free VPNs on their mobile devices while researching online. Therefore, students know what they can access and how to access it while researching online.

Security awareness

Regarding whether participants accept cookies offered by websites visited and whether they use accessible Wi-Fire networks, the findings indicate that 61.2% accept cookies provided by websites when using the internet and also use accessible Wi-Fire networks. Free Wi-Fire is standard within the university, which allows them to use it without paying.

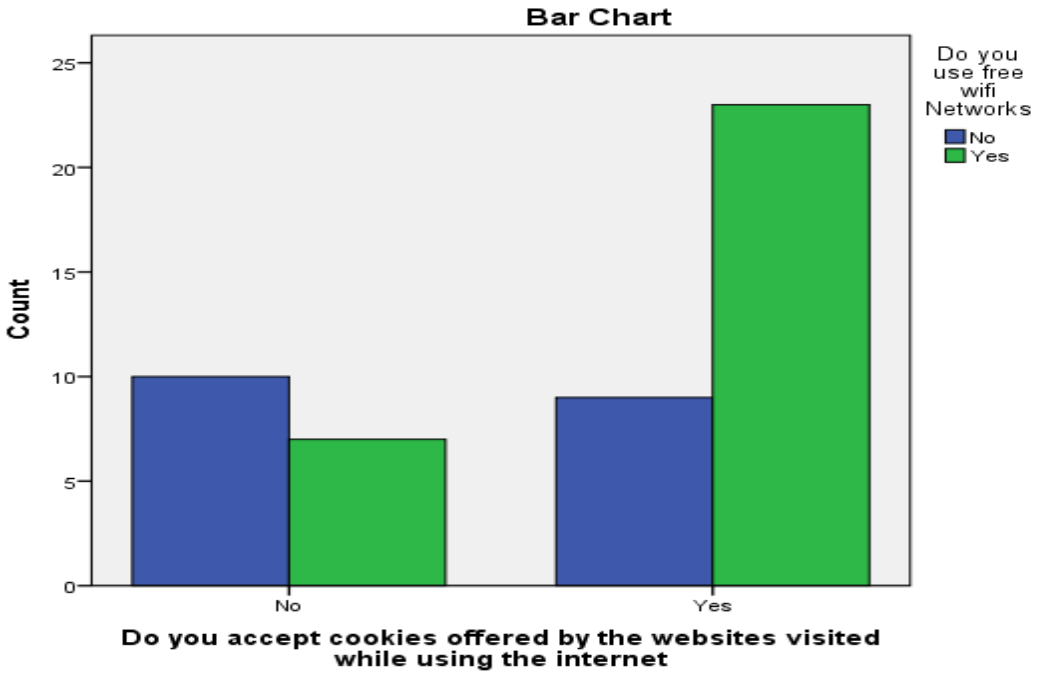

Figure 3. ***Accepting cookies***

The survey further inquired whether participants accept cookies offered by the websites visited while using the internet and whether they use paid or free VPNs on their mobile devices. The findings show that 61.2% agreed that they accept cookies offered by websites and use free VPNs on their mobile devices, compared to 38.8% who said no. This means that students accept cookies provided by websites visited on the internet and use paid and free VPNs on their mobile devices. The use of paid internet is based on the fact that students with Smartphones buy their data to use and also due to the access to the internet on campus, which they pay for.

Whether participants have had computer security awareness training at the university and accept cookies offered by the websites visited, the findings indicate that 65.3% of the respondents agreed, compared to 34.7% who disagreed. This means that students have had an opportunity to a computer security awareness training at the university. This may be why they accept cookies offered by the websites visited. Therefore, security awareness is vital for students to be aware of security threats and ways to ensure the security of their mobile devices rather than exposing them to threats of different kinds. Security threats and social attacks have increased dramatically, increasing organizations' efforts to mitigate or prevent these threats. The quality of interrelated influences between components of the human factors system may affect overall human performance and actions. Poor management practices, poorly written rules, and unclear procedures can have many adverse effects. Today's college generation faces an emerging risk of reputational harm or financial loss, much more so than prior generations, since social media is their primary form of communication. According to Moallem (2018), "users' understanding of risks and how to protect themselves from cyber-attacks is therefore fundamental in modern life" (p. 80)."

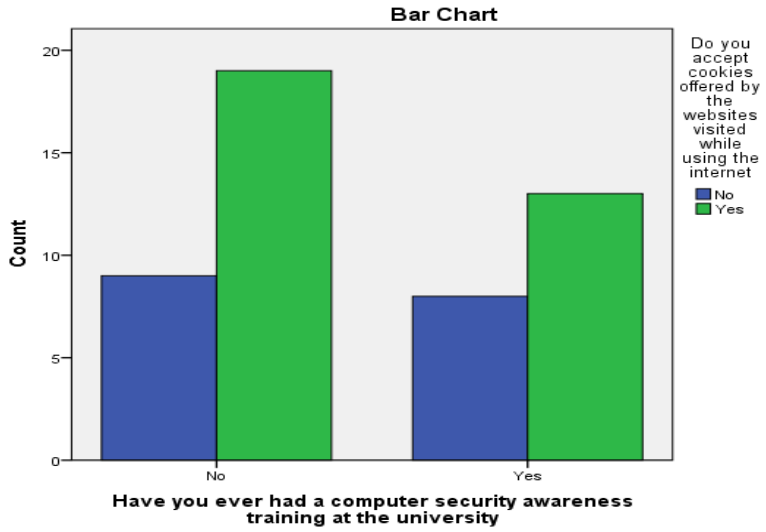

Figure 4. ***Security awareness***

Furthermore, the survey looked at whether students have had computer security awareness training at the university and clicked pop-ups or advertisements that arise on their screen while using the internet. In light of the findings, it was found that 61.2% of the participants disagreed with clicking the pop-ups or advertisements that arise on their screen while using the internet, whereas 38.8% agreed that they click on the pop-ups or ads that occur on the screen while using the internet. Therefore, through security awareness training, most participants rarely click on pop-ups or advertisements that arise on their screens while using the internet. Some pop-ups contain threats that affect the Laptop or Smartphone operations; hence, many students have learned to refrain from clicking them to avoid the risks. This calls for university training to ensure that students are aware and ensure security features are followed or used accordingly.

Conclusions and Implications

There is an urgent need to avail end-user security policy that the students can follow to become security conscious. Security awareness policy targets and goals can be achieved when students" behavior is based on the best practice that they are advised to follow during information security policy dissemination and the awareness programs conducted by the university Information Technology support team. Therefore, information security awareness is a preventive measure, and many international standards, such as ISO 27005 COBIT, have referred to it as a prerequisite. Thus, if organizations aspire to a certification form of those standards, they must initially implement information security awareness plans. Password meters are typically placed next to forms on a web page to give users a general indication of password strength.

Therefore, raising students' awareness of security, threats, and risks enhances students' references to action when confronting cybercrime to protect information and technology assets. It also motivates students to participate in security training that helps them build their

expertise in information security. In addition, preparing them to enter the labor market with sufficient security awareness is vital.

This survey has uniquely contributed to information system education by addressing a current gap. There is no formal structure to assess and develop privacy/cyber security awareness training for university students. This study proposes a maturity model that will develop students beyond simple security settings to active management of their online identity and personal brand.

An opportunity within academia lies in helping students understand the importance of reading and understanding the privacy policies of the sites they visit or applications they use. One of the future directions is a study of the reality of privacy practice and its relationship to crime among different age groups among university students. The second direction is comparing the security awareness level of Computers College students with those of other colleges. The third direction is knowing the factors that enhance security awareness among university students in Saudi Arabia and provide a platform for cyber security awareness and correct practices to confront cyber threats in each university, with the addition of incentives for students such as a certificate of attendance that increases the student's CV, also to make sure that the student has acquired sufficient awareness of security, through his assessment or a test.

References

Alotaibi, M., & Alfehaid, W. (2018). nformation Security Awareness: A Review of Methods, Challenges and Solutions. *Infonomics Society*.

Diogenes, Y., & Ozkaya, D. E. (2019). *Cybersecurity – Attack and Defense Strategies.* Packt Publishing Ltd.

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity Attack and Defense Strategies.* Packt Publishing Ltd.

Fedor, O. (2023, february 05). *93 Must-Know Ransomware Statistics [2022]*. Retrieved from Antivirus Guide: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=CjwKCAiAxP2eBhBiEiwA5puhNSyuWvD8HKjhbHRmDfmZ6Q46ySlm61j8PPbVhMe4Vmc_IagGP7ZYFxoC2PYQAvD_BwE

Hossain, A. A., & Zhang, W. (2015). Privacy and Security Concern of Online Social Networks from User Perspective. *1st International Conference on Information Systems Security and Privacy (ICISSP-2015)* (pp. 246-253). SCITEPRESS (Science and Technology Publications, Lda.

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. *CYBERPSYCHOLOGY, BEHAVIOR, AND S OCIAL N ETWORKING*.

Kovaˇcevi, A., & Radenkovi, S. D. (2020). SAWIT—Security Awareness Improvement Tool in the Workplace. *applied sciences*.

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Hindawi*.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytechnica Hungarica* .

Scholefield, S., & Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. *1st International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019*.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering.

Taha, N., & Dahabiyeh, L. (2020). College students information security awareness: a comparison between smartphones and computers. *Springer Science+Business Media, LLC*.

Young, H., Vliet, T. v., Ven, J. v., Jol, S., & Broekman, C. (2018). Understanding Human Factors in Cyber Security. *Springer International Publishing* .