SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Cybersecurity Knowledge Deterioration and the role of Gamification Intervention

Fatokun Faith Boluwatife[1,*], Zalizah Awang Long[1], Suraya Hamid[2], Fatokun Johnson O[3], Azah Norman[2]

[1] Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia
[2] Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, Malaysia
[3] Department of Mathematical Sciences, Faculty of Science, Anchor University, Lagos, Nigeria

ARTICLE INFO

Article history:
Received 15 August 2023
Received in revised form 22 September 2023
Accepted 24 October 2023
Available online 8 April 2024

Keywords:
Cybersecurity; Cybersecurity Knowledge; Cybersecurity Gamification; Gamification; Cybersecurity Awareness

ABSTRACT

Cybersecurity is becoming an overly critical issue in contemporary times. Cyberspace safety is declining, covering all sphere of humanity. Deterioration in cybersecurity knowledge and awareness has resulted to more cybercrime victimisation. The more novel security systems are being developed, the higher the innovativeness of cybercriminals techniques to attack cyber-users. Thus, investigating the stance of cybersecurity knowledge among general IT (Information Technology) users, especially in the 21st century is paramount. This paper designed a cybersecurity quiz based on adaptations from literature and past cybersecurity quizzes and conducted investigations to test the knowledge of random cyber-users. Results from investigations are instructive, thus serving as a propelling motivation to develop a cybersecurity game. Findings reveal that most cyber-users lack knowledge about network security. Also, respondents lacked knowledge on social engineering. Thus, it is important for upcoming innovations to consider aspects of network security, social engineering when designing cybersecurity gamification approaches. Gamification has been used as teaching aids for diverse learning fields, however its application in cybersecurity is still understudied. The result of this quiz is intended to further boost the development of a cybersecurity game, which can be age centric, thus developing suitable cybersecurity games for specific user groups. Interestingly, though females were not regular game players, however they were highly interested in playing a cybersecurity game, as majority of cyber-users (males inclusive), believed that a cybersecurity knowledge gamification approach can help enhance their cybersecurity knowledge and awareness. Conclusively, it is obvious that both the young and old still lack basic cybersecurity knowledge, thereby making them easy prey for cyberattacks. Gamification if applied properly into cybersecurity, could be an interactive learning platform that is both enjoyable, produces a high spirit of learning as well as help serve as a strong awareness tool that can boost cybersecurity user's knowledge.

[*] *Corresponding author.*
E-mail address: evangfatoks@gmail.com

https://doi.org/10.37934/araset.43.1.6694

1. Introduction

Cybersecurity simply refers to cyberspace protection, alongside the protection of cyberspace supporting ICTs, as well as cyberspace users in diverse capacities (either individual, societal, and even national), with the inclusion of individual interest, whether it be intangible or tangible, that pose risks to being attacked in the cyberspace [1, 2]. Thus, cybersecurity is not limited to the protection of information systems and the resources of an organization or individual. Cybersecurity also covers protecting the users of cyber-environment resources alongside other several assets [3, 4], with the inclusion of those that belong to the society that are vulnerable because of ICT (Information, Communication, and Technology) usage.

Regardless of how training programmes and security awareness are paramount, there is still a huge concern with the human aspect of cybersecurity, as this poses a challenge of a secure and safe cyberspace either offline or online, thereby the revealing of confidential data being paramount in digital systems [5, 6]. Moreover, there are extensive consequences, both individual and economic of cyber victimization for internet users, coupled with negative repercussions for cyber-infrastructure and economies, respectively. Therefore, the rise in online threats and cyber fraud remains a crucial concern. It is paramount to note that the design of contemporary systems is focused on the general audience, not preferencing user personality variations. Thus, it was suggested by Halevi, et al. [7] that individual differences should be put into consideration when developing 21st-century applications and innovative system designs. Particularly, comprehending contributing factors to secure online behaviour is paramount in the creation of such targeted systems of defence.

Cybersecurity knowledge does not really have a fixed definition in literature, however there are some suggestions as to what it connotes. Therefore, cybersecurity knowledge comprises the familiarization, experience, know-hows, and assimilation or understanding of individuals with regards to cybersecurity practices and cyber-threats, with the aim of ensuring cybersecurity assurance [8]. Thus, it is shocking yet imperative to state that majority of small-scale technology-inclined businesses, are vulnerable to cyberattacks and most times lack the adequate knowledge of cybersecurity alongside dedicated cybersecurity personnel and financial capacity to tackle such menace [9, 10]. Thence, the demand for acquiring cybersecurity knowledge is of paramount inevitability for all cyber-users. As a result of limited cybersecurity knowledge and awareness, a lot of persons become targets of cyber-crime victimizations. Moreover, hackers, scammers, criminals, and persons with harmful tendencies are in the search for novel attacking techniques [11]. Even though, in recent times, the government is getting interested in cybersecurity issues as it is affective to government systems too, thus leading to the organising of Capture the Flag (CFT) competitions [12], cyber-awareness events, as well as disbursing grants to encourage institutions in carrying out cybersecurity intervention research, there is still little success recorded. Consequently, a lot of events have been ongoing with a central aim of providing cybersecurity awareness most especially among students.

The idea of utilizing games in teaching is not rarely new however, it has been established to be one of the most superlative approaches for teaching and learning, respectively [12, 13]. Thus, incorporating gamification into learning is an effective approach. If a learning platform integrates competitive elements alongside fun, it results to enjoyability as well as boost learning spirit of the course. Gamification, if properly integrated, has the tendencies of achieving massive results. A lot of research is ongoing recently on the effectiveness of gamification. Therefore, it is established that gamification most times produces remarkable results [14]. In the field of cybersecurity, gamification is still at the conceptual stage. As a result of online service pervasiveness in the 21st century, comprising social media and internet banking, it is paramount for cyber-users to be knowledgeable in fundamental security measures that can help protect them in the cyber-space. Nevertheless, a lot of cyber-users lack the knowledge of techniques that can promote secure cyber interactions, thus signifying a need for research in this field. Gamification therefore is getting popular in contemporary times and has been utilized in teaching diverse subjects [8, 15, 16].

Gamification is an advancing trend, wherein elements and design principles of a game are being leveraged in non-gaming applications for the purpose of enhancing motivation alongside the engagement of users [17]. Thus, it comprises the integration of popular gamely elements such as badges, leaderboard, and points into a non-gaming application's normal process. Initially, gamified applications were employed mostly in the marketing domain [18]. However, as time progressed, gamification has gained popularity in diverse fields such as health, education and military, wellbeing, and business, respectively. Thence, gamification tools used for educational purposes helped in course delivery via the utilization of properly established principles of game design to boost the development of skills, self-testing, as well as enhance routine practices [19]. More so, developing effectual as well as diverse programs that promote security awareness is still the most substantial approach to boost cybersecurity knowledge. A lot of techniques have been utilised to intensify and enhance cybersecurity behaviour and knowledge among cyber-users. Nonetheless, the effectuality of the numerous interventions remains unaddressed. Gamification concepts are now trending of recent and are being used in teaching variety of topics, yet such applications are still lacking in cybersecurity.

The application of gamification in a world centric with software gives a presentation of innovative techniques that can be used in propelling users of all background and ages in engaging in serious game training [20-22]. As indicated by research, productivity of participants is enhanced by a gamified reward system incentive [2, 23]. Moreover, game design elements can represent important building blocks that can help in development of cognitive performance of users for educational purposes [16, 24]. Corroboratively, Qusa and Tarazi [25] asserts that gamification benefits can lead to increased satisfaction as well as motivation of users, as progress is being visualised by the incessant journaling of an individual's personal behaviour. This further facilitates the individual in deriving personal goals that are achievable, as well as offer instant feedback which can help users in perceiving high personal performance feelings. The benefits of employing gamification as a tool to enhance cybersecurity knowledge is numerous as it can help increase accessibilities to learn cybersecurity foundations [16]. Nonetheless, an inclusive cybersecurity gamification tool can help propel all round engagement in enhanced security knowledge immersion as well as could be designed in context according to special needs, such as considering age groups, gender-based games, as well as the disabled community.

Imperatively, the higher the development of new security systems, the higher the rate of cyberattacks via novel approaches by cyber-criminals with major target on cyber-users. Thus, there is a need to investigate the stance of cybersecurity knowledge among the general IT users, especially in the 21st century. This paper designed a cybersecurity quiz based on adaptations from literature and past cybersecurity quizzes and conducted investigations to test the knowledge of random cyber-users via the cybersecurity quiz. The cybersecurity quiz was carefully designed to incorporate several aspects of cybersecurity, focusing on network security, password security, internet/website security, and social engineering (phishing). Moreover, since the idea was to develop a cybersecurity gamification tool later, this quiz was designed with some element of gamification, such as scoring, and feedback on each question asked. Whether the users got the question or not, they would still receive comprehensive feedback explaining the answer to that question. The goal was dual, first to test the knowledge of cyber-users, as well as to enhance their cybersecurity knowledge through the quiz by providing feedback of the individual cybersecurity questions. Also, the survey was able to gather some feedback from cyber-users with regards to their perceptions and willingness to use a cybersecurity gamification tool in boosting their cybersecurity knowledge. Therefore, major objectives of this research are to identify the socio-demographic factors affecting cybersecurity knowledge, investigate the cybersecurity knowledge of 21st century tertiary institution students, and assess the predictors of knowledge for gamifying cybersecurity. Consequently, the research questions are: RQ1: What socio-demographic factors affect cybersecurity knowledge? RQ2: What is the current cybersecurity knowledge of 21st century tertiary institution students? RQ3: What are the predictors of knowledge for gamifying cybersecurity?

The remainder of this paper is thus: Section 2, gives a brief overview of the literature regarding related works in cybersecurity knowledge and gamification. Section 3 presents the methodology used in conducting the research. Section 4 presents the results and findings. Section 5 presents the discussion of results, alongside study implications, limitations, and recommendations. Section 6 concludes the paper.

2. Overview of Literature

2.1 Cybersecurity Knowledge

Majority of cyber-users lack knowledge about medium level difficulty cybersecurity concepts and issues. As the world expands digitally, individual confidential data could be of more value as well as become susceptible to probable cyber attackers. In a research by Smith [26], via a survey comprising 13 cybersecurity questions, it was discovered that majority of adults only had surface knowledge about identification of strong passwords, yet they lacked substantial knowledge on technical cybersecurity issues. Though, the study was conducted in USA, it would be interesting to investigate on a different populace. Moreover, Raineri and Fudge [9] explored the sufficiency of cybersecurity knowledge among undergraduate students enrolled for entrepreneurship programs. It is paramount to note that small businesses that utilise technology are vulnerable to cyberattacks and unfortunately most times lack adequate cybersecurity knowledge, dedicated security personnel, as well as financial budgets [9]. Therefore, from their findings, it was discovered that most students obtained knowledge of strong password development via personal study efforts. Nevertheless, most of the participants lacked substantial knowledge of cyberthreats and were unable to comprehend in clear terms the concept of phishing. Research has revealed that the topic of social engineering is not knowledgeable among internet users. Moreover, physical data security is an unfamiliar topic among cyber-users. It can be established that technical knowledge of cybersecurity is lacking among internet users, thus posing a critical challenge in the world of cybersecurity. Some of the previous studies only focused on undergraduate students from programs, such as either business or computer science students, thence it will be interesting to test cybersecurity knowledge among the general populace, regardless of their specific field of study. Consequently, studies [27-29], have revealed that majority of participants learn cybersecurity via self-study; however, this has not proven to be sufficient in enhancing knowledge of cyber-users. Thus, a more promising approach, such as gamification or expert systems which could be built based on existing models and targeted to help instil lasting cybersecurity knowledge could proffer better efficiency. Due to the evolution of technology alongside the emergence of cyberthreats, it is only instructive for cybersecurity researchers to produce novel methods that could mitigate cybersecurity attacks on individuals as well as enhance adequate cybersecurity knowledge.

Consequently, based on literature review, another expansive prevalent approach used in practicing cybersecurity skills as well as instilling cybersecurity knowledge is through the informal Capture the Flag (CTF) competitions and games, usually integrated with formal education. Such events witness exercising of cybersecurity skills by small teams of participants, who engage in solving several tasks in a virtual learning scene. Thus, CTF tasks, referred to as challenges, comprises several assignments ranging from password cracking, website exploitation, to breach of unsecured networks. To achieve the goal, a successful challenge solution results into a string text referred to as a flag which is submitted online. In an analysis conducted by Švábenský, et al. [12], it was discovered that cybersecurity topics such as network security, technical knowledge and cryptography were more popular in CTF games, however, human aspects such as awareness of cybersecurity and social engineering were lacking. Thence, this immensely popular cybersecurity knowledge tool CTF is not sufficient to enhance the cybersecurity knowledge of internet users in the 21st century. The areas of more concern in the 21st century lies in the human behavioural aspect of cybersecurity as well as social engineering attacks, which needs to be tackled more when proffering any innovation to ensure cybersecurity assurance.

2.2 Cybersecurity Gamification

Attention is massively drifting towards cybersecurity behavioural aspects in contemporary times. Therefore, resultant cyberattack effects are crucially severe in most cases. Data hacks or breaches might result to a potential major economic or reputational damage, thus, further causing lack of trust in the affected firms. Moreover, there is lack of assurance of safety for personal cyber-users, thence an extensive cyberattack outcome which exposes national security to probable threats [30, 31]. A couple of approaches are explored by various researchers in the cybersecurity field. This includes but not limited to, challenge-based learning, where a couple of challenges from specific domains are being received by users [32], awareness campaigns [27], capture the flag events, as explained earlier, where files or flags are being secured by users alongside having the opportunity to capture flags of others [12], as well as table-top games [13]. Therefore, implementing serious games is another approach entirely. A serious game differs distinctively from regular games, as the main aim is not to promote only enjoyment or entertainment [22]. However, serious games are targeted at facilitation learning and immersion of knowledge amongst the participants or users, respectively [21, 22, 33].

Serious games application in cybersecurity field ranges from wargames [34] to safety and security games, a probable suitable substitution for regular cybersecurity trainings, thereby enabling users in considering diverse circumstances prior to experiencing them in their day-to-day routines [35]. As asserted by literature, cybersecurity is potentially an appropriate topic that can incorporate training via serious gaming [21]. Nevertheless, majority of studies that have explored this research line experienced limitations in sample sizes, as well as lacking an empirical form of building the gamification tool, wherein they move straight to designing and developing games without any quantitative or qualitative research backing the validation of the game. Therefore, there is still a large gap regarding serious games application in the field of cybersecurity [36]. Contemporarily, a vast amount of large and medium-sized organizations, are probed regularly based on numerous critically severe cyber-attacks. Thence, weak links in information defence mechanism is tantamount to face business data breaches. It is therefore highly essential to build cybersecurity workforce that are more enhanced as well as more prepared professionally who can lead the war front of providing unbeatable defences to IT infrastructures as well as win the prevailing cybercrime war.

The ideology backing the utilization of games in teaching is not new, however, it is one of the most sufficient techniques used in learning, teaching, and knowledge immersion [13, 37]. Gamification, thence, is an excellent approach to learning. If a platform of learning is integrated with competitive elements coupled with fun features, learning could become more enjoying, thereby leading to knowledge being highly retained by the learner. Moreover, a proper integration of gamification can lead to faster achievement of intended results as well as deep immersion of knowledge in the respective field. Several research in contemporary times has focused on effects of gamification, thus, the fact that gamification has resulted positively in most cases is established [12, 38-40]. However, with regards to the utilization of gamification in enhancing cybersecurity knowledge among cyber-users, there remains a large gap in research.

Recently, there is an escalation of the spread of cyber-attacks and cybercrime as well how the duo has negatively impacted diverse sectors, with the end-users as a major target. Targeted attacks in diverse forms are also being launched on web applications alongside IT systems daily [41]. Thence, cybersecurity is an essential issue that needs urgent attention both in public and private sectors. Unarguably, the demand for more technical experts in the cybersecurity workforce is on the high side, nonetheless, it is more important to equip the end-users with adequate cybersecurity knowledge to enable them to fight the cyberattacks faced daily on the cyberspace. Therefore, as advised by Dabrowski, et al. [42], cybersecurity awareness should not be reliant on mere technicality and security software, but should be a mix of expert mindset, alongside typical attacking techniques to be at equilibrium with the attackers. In this light, gamification is deemed the best option to tackle cybersecurity as it possesses the ability of achieving positive outcomes on most occasions. Research by Abu-Amara, et al. [43] presented a gamification classification taxonomy which was hinged on cybersecurity training resources, after which a training resources list was gathered and classified for the purpose of cybersecurity lecturing. Moreover, the goal was to use gamification to improve the learning process of students by the instructors and lecturers, respectively. The gamified approach was also targeted at raising the student's interest in the field of cybersecurity, to further reduce the lack of professionals in the field.

There is a rapid drift in the development of user-centric cybersecurity technologies. Among the challenges of a cybersecurity system that is user-centric is the diversity in cybersecurity knowledge of individuals who are interacting with the cybersecurity system. Thus, there is a continuous change in the cybersecurity threat landscape due to the emergence of new threats. Therefore, familiarity of cyberthreats might vary according to users. In recent research by Matovu, et al. [27], the authors assessed gamification effectiveness in teaching and learning cybersecurity awareness among college and university students. The findings revealed that gamification is an effective pedagogical approach that can be used in impacting the knowledge of cybersecurity awareness in a small institution. In this study, the authors made use of a gamification tool such as Kahoot and reported that its gamely elements gave a sense of achievement (such as instant rewards and leader board), thereby stating its efficiency in delivering crucial learning objectives in cybersecurity awareness. Importantly, game elements such as time were not appreciated by students as it pressured them. Gamification, consist of various constituents (entertainment, acquisition of knowledge, and winning). Among these attractive constituents, it was discovered that students have more interest in the acquisition of knowledge as compared to other aspects [2, 27]. Another recent scholarly work by Malone, et al. [44] presented cybersecurity education experiential gamified learning which was designed to provide an assimilation of needed techniques and knowledge for learners to be able to solve daily challenges whilst immersing them simultaneously in a competitive scenario. It has been discovered that students were highly engaged by gamified experiences. Therefore, integrating gamified elements into cybersecurity might help in adequate immersion of cybersecurity knowledge among cyber-users if properly incorporated with the most essential approaches.

3. Methodology

3.1 Participants and Sampling

Participants in this research comprise students from both colleges and universities across Klang Valley Malaysia. The students who participated in this study were in one of the following categories: Secondary School/High School; Diploma/Pre-Degree Program; Bachelor; master's and PhD/Doctorate. Moreover, regarding the gender, both male and females participated respectively in this study. The age group of participants was from 15 years to above 60. All participants were given a fair chance to participate in this research, thence, there was no deliberate action by the researcher to affect their cybersecurity knowledge performance in the quiz. For the sampling, the research utilized a simple random sampling approach. Here, all participants were given equal chance to be selected for the study [45].

With reference to the calculation of sample size, based on the acceptable standard in literature, about 5% margin error, 95% confidence level, and 20% response rate of a targeted population is acceptable for surveys [46]. Thus, since respondents were drawn from random institutions, thereby making it almost impossible to obtain the exact population size, a renowned sample size calculator [47] was used in determining the required number of respondents by computing 500,000 as the population size. Based on the calculation, about 150 respondents were needed to run this survey. However, about 227 persons eventually attempted the cybersecurity knowledge quiz for this study.

3.2 Procedure and Materials

This research was conducted via a quantitative approach. First, a cybersecurity quiz was designed based on adaptations from relative literature. The items of the quiz were reduced to 10 major aspects of cybersecurity to ensure briefness and allow participants answer all items in good time. Moreover, the areas covered in the quiz comprised of basic internet security, such as how to identify a secured website URL (http or https); being able to identify an example of a phishing attack; network security – where participants were prompted to differentiate between botnet, rootkit, DDOS, and operating system; website and online service security, where the participants were asked to identify a two-step authentication via an image; passwords – identifying strong passwords; encryption and decryption of personal files and data; Private browsing – where participants were asked if internet service providers can see the online activities of their subscribers when those subscribers are using private browsing; smartphone security – testing the knowledge of participants on the security risks attached to putting on a GPS (GLOBAL POSITIONING SYSTEM); Wi-Fi network security – participants were asked if they feel it is safe to use passworded public Wi-Fi networks for sensitive activities, such as online banking; Virtual Private Network (VPN) – finding out the knowledge of participants regarding the security limitations of a VPN. Moreover, a question was asked about phishing, an aspect of social engineering, where participants were asked to identify an example of a phishing attack.

The quiz was conducted via a survey which was prepared on google forms. Since the goal of this research eventually is to propose a cybersecurity knowledge gamification model, the quiz was designed with some basic gamification elements, such as including scores to questions – wherein each question was assigned 10 points, making a total of 100% for 10 questions and providing feedback to each question, thus mimicking the function of an expert system. Moreover, participants were also given an opportunity to provide feedback to the quiz, as well as declare their willingness to participate in a cybersecurity knowledge game/gamification intervention. Interestingly, this research was concerned about how well the participants enjoyed the quiz as well as find out if they gained any new cybersecurity knowledge. Table 1 presents a summary of the survey items (quiz questions) as well as corresponding literature.

Table 1
Summary of survey items (Quiz questions)

S/N	Quiz question	Cybersecurity aspect	Reference
1	What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?	Internet/Website Security	[30]
2	Which of the following is an example of a “phishing” attack?	Social engineering (Phishing)	[48]
3	A group of computers that is networked together and used by hackers to steal information is called a …	Network Security	[49]
4	Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?	Internet/Website Security	[50]
5	Which of the following four passwords is the most secure?	Password security	[51]
6	Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …	Network Security	[4, 52]
7	“Private browsing” is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?	Internet/Website Security	[53, 54]
8	Turning off the GPS function of your smartphone prevents any tracking of your phone’s location.	Network Security (Smartphone security)	[31, 35]
9	If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it safe to use that network for sensitive activities such as online banking?	Network Security	[55]
10	What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?	Internet/Website Security	[56]

Table 1 above shows how the questions selected for the quiz were scrutinised from relevant literature and were deemed essential to test the cybersecurity knowledge of internet users via a survey. The 10 questions selected are amongst crucial contemporary cybersecurity issues. Thence, it is important to assess if cyber-users are equipped with these salient cybersecurity knowledge as well as discover the lacking aspects to incorporate this in the future development of the cybersecurity knowledge game for the 21st century users.

For clearer elucidation of the detailed quiz items, all information regarding gamification elements of the quiz as well as quiz items, are reported in the Appendix section of the manuscript.

3.3 Data Collection

Data collection was conducted via online platforms, however, a QR code was created to ease collection of data at physical points. One of the researchers FF, gathered some data by prompting users to scan the QR code and try the quiz. Physical observations were made also as at some point, the researcher met with groups of people who tried the survey and asked questions, thence turning the survey into a mini cybersecurity awareness training.

3.4 Data Analysis

All data was converted from google forms to excel spreadsheet, after which coding was applied to all data in preparation for computation into the data analysis software, SPSS version 29. Data computation techniques employed coding the responses into 3 groups for better analysis. For each of the 10 quiz questions used to test cybersecurity knowledge, the correct answer was coded as 3 (CR), incorrect answer, but attempted was coded as 2 (NC), and non-attempted or unsure answer was coded as 1 (NS), respectively. The reason for this coding was to ensure a widespread in analysis as this is a quiz with multiple choices unlike the conventional Likert scale response. For the remaining questions on feedback, they were coded using a reverse order 3 Likert scaling technique, such as Yes (3), Maybe (2), and No (1), respectively. Questions in this segment comprised feedbacks on: Did you enjoy the quiz?; Did you learn something new about cybersecurity from this quiz?; Do you play games?; Would you be willing to play a cybersecurity knowledge game?; Do you think a cybersecurity knowledge gamification tool can help enhance your knowledge and awareness about cybersecurity? accordingly.

For the analysis of data properly, descriptive statistics was used in finding the mean and frequency distribution of the research variables. First, demographic descriptive analysis was conducted to provide a clear understanding of the research data characteristics. Here, the age, gender, and educational level distribution was analysed. Furthermore, series of advanced descriptive analysis were used in answering the research questions. Research question 1 was answered via Compare means and proportion function in SPSS, where the mean of socio-demographic factors was compared to see if there were differences in the sociodemographic of participants regarding cybersecurity knowledge. For research question 2, frequency statistics was used in finding out the current cybersecurity knowledge of 21st century cyber-users. All questions asked were analysed to see the percentage of performances as to finding out those who got the correct answers for each question compared to others. Moreover, it was possible to also detect which part of cybersecurity participants performed better and which aspects need urgent interventions. To answer research question 3, an inferential analysis was conducted via Multiple Linear Regression to assess the predictors of knowledge for gamifying cybersecurity. These results were used to make assertions on the investigation of cybersecurity knowledge in the 21st century.

4. Result & Findings

The results of data analysis alongside the findings are presented in this section accordingly. First, demographic data alongside the descriptive analysis for some of the feedback questions is presented, following by analysis findings conducted for each research question of this study.

4.1 Demographics

Here, the demographic distribution of the participants was analysed. This comprises gender distribution, age distribution, and education level distribution. More descriptive analysis which were not directly covered by the research questions are also presented in this section such as analysis of the feedback section of the survey.

4.1.1 Gender distribution

A total of 227 persons participated in this research study. Out of the 227, there were 92 females and 135 males, respectively. In the data analysis via SPSS, females were coded as 0 and males as 1. Male respondents were slightly higher than females in this study however, the results are interesting to interpret. Table 2 presents the Gender Frequency Statistics.

Table 2
Gender frequency statistics

Gender	Frequency	Percent
Female	92	40.5
Male	135	59.5
Total	227	100.0

4.1.2 Age distribution

For age distribution, 5 groups were used to classify the ages of participants. Since a few secondary school participants and diploma students participated, the age limit was reduced to 15 years old. Thus, the age categories are: 15-20, coded as 1; 21-30: 2; 31-40: 3; 41-50: 4; 51-60: 5; and above 60: 6, respectively. Regarding the age distribution, majority of respondents (about 46.7%) were in the 21-30 years old category. The next age group with more participants were the 15-20 years old category who were about 23.3%. There was also a fair distribution of the 31-40 years old group, as they amounted to 20.7% of the population. The least age group distribution among respondents were those above 40 years old. Hence, there was a good participation among young adults and middle age in this research. Table 3 presents the frequency distribution for age.

Table 3
Age frequency statistics

Age group	Frequency	Percent
15-20	53	23.3
21-30	106	46.7
31-40	47	20.7
41-50	15	6.6
51-60	5	2.2
Above 60	1	0.4
Total	227	100.0

4.1.3 Educational level distribution

Educational level was split into 5 categories comprising: Secondary School/High School, coded as 1 in SPSS; Diploma/Pre-Degree Program: 2; Bachelor: 3; Masters: 4; and PhD/Doctorate: 5, respectively. One interesting aspect of this study is that it studied various levels of students, as compared to majority of studies where the focus is on a particular educational level, mostly bachelor students. In this study, descriptive statistics indicated the prevalence of bachelor students as they amounted to about 58.1% of the population. This was followed by postgraduate students (Master and PhD respectively), amounting to a total of 29.9%. There were few diploma/pre-degree students and very few secondary students who participated in this study, however their data was not discarded as it may provide indication for future specific studies on that group. Table 4 presents the educational level frequency distribution.

Table 4
Educational level frequency statistics

Education level	Frequency	Percent
Secondary School/High School	9	4.0
Diploma/Pre-Degree Program	18	7.9
Bachelor	132	58.1
Masters	45	19.8
PhD/Doctorate	23	10.1
Total	227	100.0

4.2 Descriptive Analysis Quiz Feedback

Regarding the feedback of participants concerning the cybersecurity quiz used in investigating their cybersecurity knowledge, five questions were asked. The questions comprised: Did you enjoy the quiz? Did you learn something new about cybersecurity from this quiz? Do you play games? Would you be willing to play a cybersecurity knowledge game? Do you think a cybersecurity knowledge gamification tool can help enhance your knowledge and awareness about cybersecurity? The responses of participants were coded as either Yes (3), Maybe (2), and No (1) respectively. Descriptive frequency results for the response distribution of participants for the 5 questions are presented in the next subsections. Table 5 presents a summary of the descriptive frequency results for the 5 feedback questions, after which the findings are analysed accordingly.

Table 5
Descriptive frequency results for feedback questions

Feedback Questions	Stat	Yes	Maybe	No
Did you enjoy the quiz?	N	181	35	11
	%	79.7	15.4	4.8
Did you learn something new about cybersecurity from this quiz?	N %	164 72.2	45 19.8	18 7.9
Do you play games?	N	161	18	48
	%	70.9	7.9	21.1
Would you be willing to play a cybersecurity knowledge game?	N %	153 67.4	52 22.9	22 9.7
Do you think a cybersecurity knowledge gamification tool can help enhance your knowledge and awareness about cybersecurity?	N %	199 87.7	23 10.1	5 2.2

4.2.1 Did you enjoy the quiz?

For this question, as presented in Table 5, a huge majority of respondents, about 79.7% reported that they enjoyed the quiz. However, there were a few who were sceptical and unsure as to if they enjoyed the quiz or not. Moreover, a little proportion about 4.8% informed that they did not enjoy the quiz. Thus, it would be interesting to know if there were differences as to enjoyment of the quiz with regards to socio-demographic factors. This will be analysed in the research question 1.

4.2.2 Did you learn something new about cybersecurity from this quiz?

The findings in Table 5, reveals that majority of participants (72.2%) reported to have learnt something new in cybersecurity because of participating in this quiz. Thus, it shows the importance of knowledge acquisition via gamely elements. Gamification could even produce better effectiveness rate as compared to the quiz used in this study. The goal of the ongoing future research is to develop a cybersecurity knowledge behavioural gamification model. Nevertheless, there were a few who were not sure as to if they had learnt something new or not about cybersecurity from the quiz. This could be those who already have knowledge about cybersecurity. Thus, we hope to diversify in future assessment as to find out the cybersecurity/ computer skill expertise level of participants.

4.2.3 Do you play games?

Here, about 70.5% of respondents informed that they do play games, thus, it might be interesting for them to play a cybersecurity game. However, there were a fair number of participants (21.1%) who reported not to be game players. Therefore, if the cybersecurity gamification tool is interesting and has more of educative elements, they might be willing to improve their cybersecurity knowledge via such gamification medium.

4.2.4 Would you be willing to play a cybersecurity knowledge game?

Here, majority of the respondents, 67.4% reported to be willing to play a cybersecurity game that can help in enhancing their cybersecurity behaviour. However, a trend of unsureness was discovered here, as a fair proportion of the participants (22.9%) were double minded as to if they had the willingness to play a cybersecurity knowledge game. This could indicate the need for cybersecurity knowledge game to be designed in such a way that will inculcate more of knowledge, learning, and education of cybersecurity rather than entertainment as most regular games entail.

4.2.5 Do you think a cybersecurity knowledge gamification tool can help enhance your knowledge and awareness about cybersecurity?

When asked their perceptions as to if their knowledge and awareness about cybersecurity could be enhanced by a cybersecurity knowledge gamification tool based on the performances and experience with the quiz, the responses were interesting. A huge majority of the respondents, about 87.7% stated to be of a highly positive perception that a cybersecurity knowledge gamification tool will help in improving their cybersecurity knowledge and awareness. This was the highest significantly responded question from the feedback of the participants of this cybersecurity knowledge quiz in this study. This reveals the urgent need for innovative interventions to be developed that can help in curbing cybersecurity issues as well as promoting cybersecurity assurance among the populace.

4.3 Socio-demographic Factors Affecting Cybersecurity Knowledge (RQ1)

In this section, analysis was conducted on the 3 socio-demographic factors used in this research, to find out if there are differences with regards to participation in the cybersecurity quiz – further investigating if cybersecurity knowledge is affected by age, gender, and educational level differences. To achieve this, a Compare Means Test was conducted in SPSS to compare means alongside ANOVA to find the significant differences within the groups. The results are presented in accordance with the socio-demographic factors.

4.3.1 Gender differences → Cybersecurity knowledge

Among the 10 questions used in assessing cybersecurity knowledge (Please refer to Table 1), performance of Questions 3, 6, 7, and 9 were significantly different with respect to gender of respondents. This indicates that males and females performed differently for the questions. The highest significance (P=0.004) was found in question 9: If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it safe to use that network for sensitive activities such as online banking? This was a network security questions, and results indicates that male respondents (M = 2.79; SD = 0.479) answered the question more correctly than the female counterparts. Thus, this could indicate that males are more knowledgeable in network security as compared to the female counterparts. Question 7 which focused on Private browsing, an internet security question, was also well performed by males as compared to female respondents (M = 2.66; SD = 0.613, P=0.006). Corroboratively, questions 3 (P = 0.018) and 6 (P = 0.026) both network questions also indicated significant difference to gender, with males performing better. These results indicate males possessing more cybersecurity knowledge in the aspect of network security as compared to the females. Thus, there is a need to focus on both gender when organizing cybersecurity training as well as developing novel interventions that could teach network security amongst the female cyber-users. Also, there should be more opportunities for females in the cybersecurity work force and incentives that can motivate more females to join the war against cybercrime. Regarding the feedback questions, the highest significant differences among gender was found in: Willingness to Play Cybersecurity Knowledge game (P<0.001), where males (M = 2.71; SD = 0.609) were more willing to play the game as compared to females. Another significant difference was found in the question that asked if they enjoyed the quiz (P = 0.012), where males (M = 2.82; SD = 0.471) indicated to have enjoyed the quiz more than the female counterparts. Finally, the question asking if they play games also had significant differences across gender (P = 0.015), where males (M = 2.61; SD = 0.744) again reported to play games more than females. A remarkably interesting finding is in the perception of participants as to if a cybersecurity knowledge gamification tool can enhance their knowledge and awareness about cybersecurity. Though, there was no significant differences among gender as the response among both male and females were almost tallying, however, it is interesting to note that females (M = 2.87; SD = 0.339) had a slightly higher perception that their cybersecurity knowledge and awareness can be bettered by a cybersecurity knowledge gamification tool. Table 6 presents a summary of the gender differences with regards to participants’ cybersecurity knowledge based on their performance in the quiz.

Table 6
Gender differences on cybersecurity knowledge

Item	F	P-value	Male		Female	
			M	SD	M	SD
Q1	0.011	0.915	2.51	0.732	2.52	0.748
Q2	0.207	0.650	2.45	0.631	2.41	0.632
Q3	5.639	0.018*	2.19	0.839	1.91	0.860
Q4	1.952	0.164	2.50	0.609	2.39	0.573
Q5	1.448	0.230	2.87	0.395	2.80	0.474
Q6	5.007	0.026*	2.64	0.653	2.42	0.774
Q7	7.644	0.006**	2.66	0.613	2.40	0.785
Q8	0.227	0.634	2.16	0.648	2.12	0.644
Q9	8.689	0.004**	2.79	0.479	2.55	0.701
Q10	0.553	0.458	2.22	0.687	2.15	0.710
FB1	6.406	0.012**	2.82	0.471	2.64	0.604
FB2	0.220	0.639	2.66	0.648	2.62	0.590
FB3	6.054	0.015*	2.61	0.744	2.34	0.905
FB4	14.410	<0.001**	2.71	0.609	2.38	0.693
FB5	0.204	0.652	2.84	0.455	2.87	0.339

4.3.2 Age differences → Cybersecurity knowledge

Regarding age differences, results indicated that significant differences were found in Questions 3, 7, and 9 of the cybersecurity knowledge quiz. More specifically, this indicates that participants of diverse age groups performed differently for the questions. The highest significance (P=0.022) was found in question 7: Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing? Here, it was revealed that those in the age group 15-20 (M = 2.62; SD = 0.596) and 21-30 (M =2.61; SD = 0.684) were more knowledgeable about private browsing as compared to older age groups. Furthermore, question 9: a question on the safety of using public Wi-Fi network, had significant differences (P = 0.024) with age group 41-50 (M = 2.87; SD = 0.352) performing better than the other groups. However, ages 31 – 40 (M = 2.77; SD = 0.560) also performed brilliantly well for this question. More interestingly, the 3rd group of averagely excellent performers were the age 21-30 (M = 2.71; SD = 0.568). These findings infer that regarding knowledge of public Wi-Fi safety, a network security question, the middle age, and older adults were more knowledgeable as compared to younger persons. It would be interesting to find out in future analysis if age influences the cybersecurity knowledge acquisition of cyber-users. For the feedback questions, there were differences in age as well. The most significant difference in age for the feedback questions was found in FB5 on the perception of knowledge enhancement via a cybersecurity knowledge gamification tool (P <0.001). Here, the age group 21-30 (M = 2.92; SD = 0.299), representing young adults, had a higher perception as to the effectiveness of a cybersecurity knowledge gamification tool in improving their knowledge and awareness of cybersecurity. This was followed by ages 31 – 40 (M = 2.89; SD = 0.375) and 41 – 50 (M = 2.87; SD = 0.352) respectively. Consequently, question 3 on network security also revealed significant differences in age of participants (P = 0.032). The highest difference was found in ages 41-50 (M = 2.27; SD: 0.884) another indication that experience might affect knowledge in network security of cyber-users. Regarding the feedback question (FB3), asking if the play games, there were significant differences among ages (P =0.011). Here, as expected, the younger participants were regular game players as compared to the older group. Specifically, ages 21-30 (M = 2.61; SD = 0.725) played games more, followed by ages 15 – 20 (M = 2.60; SD = 0.768). Surprisingly, the ages 41 – 50 (M = 2.53; SD = 0.834) also had a considerable proportion of game players. Moreover, the feedback question, FB 4 on willingness to play cybersecurity knowledge game was also varying for the age groups (P = 0.015). Here, the middle age, 41 – 50 were more willing to play the game (M = 3.00; SD = 0.000). This was followed by ages 15-20 (M = 2.74; SD = 0.524) and ages 31-40 (M = 2.53; SD = 0.687) respectively. Table 7 presents a summary of the age differences with regards to participants cybersecurity knowledge based on their performance in the quiz.

Table 7
Age differences on cybersecurity knowledge

Item	F	P-value	15-20		21-30		31-40		41-50		51+	
			M	SD	M	SD	M	SD	M	SD	M	SD
Q1	0.530	0.753	2.49	0.750	2.49	0.746	2.62	0.677	2.60	0.737	2.20	1.095
Q2	0.816	0.539	2.40	0.599	2.43	0.569	2.49	0.748	2.53	0.743	2.00	0.707
Q3	2.488	0.032*	2.23	0.869	2.05	0.844	2.04	0.833	2.27	0.884	1.00	0.000
Q4	0.673	0.644	2.45	0.637	2.45	0.588	2.55	0.544	2.33	0.617	2.20	0.837
Q5	0.862	0.507	2.81	0.441	2.81	0.480	2.89	0.375	3.00	0.000	3.00	0.000
Q6	1.603	0.160	2.43	0.772	2.63	0.622	2.53	0.747	2.60	0.828	2.40	0.894
Q7	2.694	0.022**	2.62	0.596	2.61	0.684	2.51	0.718	2.40	0.828	1.80	0.837
Q8	0.628	0.678	2.23	0.697	2.08	0.672	2.15	0.691	2.33	0.488	2.20	0.837
Q9	2.654	0.024*	2.60	0.631	2.71	0.568	2.77	0.560	2.87	0.352	2.40	0.894
Q10	0.593	0.706	2.32	0.613	2.15	0.701	2.15	0.722	2.27	0.799	2.00	1.000
FB1	1.586	0.165	2.68	0.581	2.81	0.439	2.79	0.549	2.60	0.737	2.40	0.894
FB2	2.100	0.066	2.62	0.596	2.67	0.613	2.72	0.579	2.40	0.737	2.60	0.894
FB3	3.069	0.011*	2.60	0.768	2.61	0.725	2.19	0.970	2.53	0.834	2.00	1.000
FB4	2.907	0.015*	2.74	0.524	2.48	0.707	2.53	0.687	3.00	0.000	2.20	1.095
FB5	7.154	<0.001**	2.71	0.466	2.92	0.299	2.80	0.375	2.87	0.352	2.00	1.000

4.3.3 Educational level differences → Cybersecurity knowledge

For educational differences, surprisingly, results indicated that there are no significant differences in cybersecurity knowledge of participants as concerns their performance in the 10 cybersecurity quiz questions. This could further indicate the need for users in every level of education to have the chance of gaining cybersecurity knowledge and not just focusing on certain educational levels as recorded pervasively in literature, where most cybersecurity intervention programs are conducted on undergraduate / bachelor students, mostly among computer science or business students. Furthermore, regarding the feedback questions, significant differences was observed in FB3, where users were asked if they play games (P<0.001), it was discovered that the diploma/pre-degree students (M = 2.67; SD = 0.686) played games more than the others, this was followed by bachelor students (M= 2.62; SD = 0.737). Although, there were no significant differences among other feedback questions, however it is relevant to note that most participants in all educational levels were willing to play a cybersecurity knowledge game. Moreover, majority of the respondents regardless of educational level had a strong perception that a cybersecurity knowledge gamification tool can help in enhancing their knowledge and awareness about cybersecurity. Table 8 presents a summary of the educational level differences with regards to participants' cybersecurity knowledge based on their performance in the quiz.

Table 8
Educational level differences on cybersecurity knowledge

Item	F	P-value	High school		Diploma		Bachelor		Masters		PhD	
			M	SD	M	SD	M	SD	M	SD	M	SD
Q1	0.789	0.534	2.67	0.500	2.33	0.840	2.56	0.713	2.51	0.727	2.35	0.885
Q2	0.215	0.930	2.44	0.527	2.39	0.608	2.44	0.609	2.49	0.695	2.35	0.714
Q3	0.571	0.684	1.89	0.928	1.89	0.832	2.14	0.854	2.00	0.826	2.09	0.949
Q4	0.628	0.643	2.33	0.500	2.28	0.575	2.49	0.612	2.44	0.586	2.48	0.593
Q5	0.414	0.799	2.89	0.333	2.83	0.383	2.82	0.476	2.89	0.383	2.91	0.288
Q6	1.953	0.103	2.11	0.782	2.33	0.840	2.64	0.645	2.53	0.757	2.43	0.788
Q7	2.115	0.080	2.67	0.500	2.61	0.698	2.64	0.619	2.33	0.853	2.39	0.783
Q8	1.815	0.127	1.89	0.928	2.28	0.575	2.07	0.668	2.31	0.668	2.26	0.619
Q9	0.949	0.437	2.67	0.707	2.72	0.575	2.66	0.590	2.67	0.674	2.91	0.288
Q10	0.584	0.674	2.33	0.500	2.33	0.686	2.21	0.677	2.11	0.745	2.09	0.793
FB1	0.972	0.424	2.56	0.726	2.72	0.461	2.80	0.470	2.69	0.633	2.65	0.647
FB2	1.451	0.218	2.56	0.726	2.56	0.616	2.68	0.570	2.49	0.787	2.83	0.491
FB3	4.852	<0.001**	2.56	0.882	2.67	0.686	2.62	0.737	2.38	0.886	1.87	0.968
FB4	0.871	0.482	2.78	0.441	2.33	0.767	2.60	0.616	2.56	0.755	2.61	0.722
FB5	1.480	0.209	2.78	0.441	2.78	0.548	2.91	0.289	2.80	0.505	2.74	0.619

4.4 Cybersecurity Knowledge of 21st Century Cyber-Users (RQ2)

This question was used in measuring the current knowledge of the participants with regards to their cybersecurity knowledge as well as trying to investigate how knowledgeable cyber-users are in the 21st century. To address this issue, advanced descriptive analysis was conducted for each of the 10 cybersecurity questions attempted by participants of the quiz survey. The questions were carefully designed to cover different prevalent aspects of cybersecurity, but generally classified into two: Internet/website security (which covered general website behaviour/awareness and Identifying secure URL (Q1), two step authentication (Q4), password security (Q5), and private browsing (Q7)), and network security (covering issues on social engineering-phishing (Q2), network hacking (Q3), encryption/decryption safety and identifying ransomware scam (Q6), GPS tracking/smartphone security (Q8), Wi-Fi network privacy/safety (Q9), and VPN security (Q10)). Figure 1 depicts the performance of participants with regards to cybersecurity knowledge as revealed via the 10-question quiz.

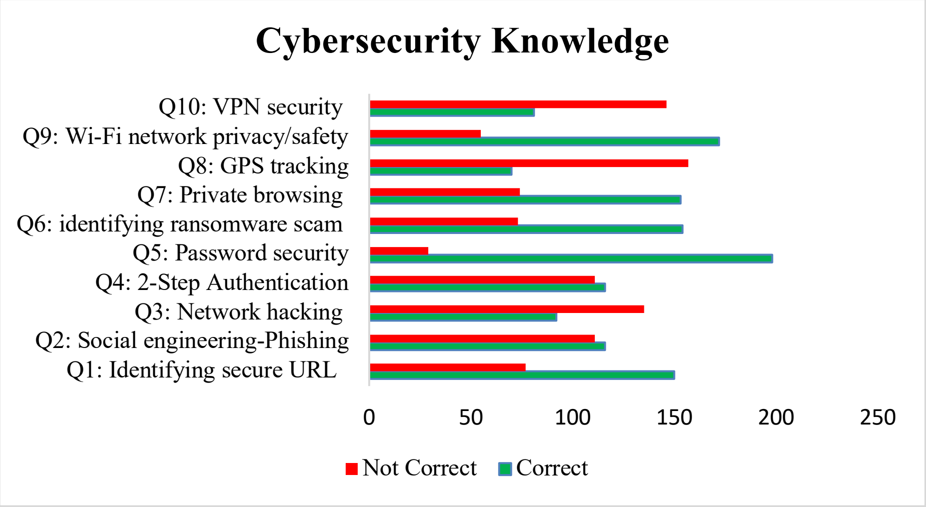


Fig. 1. Cybersecurity knowledge assessment

As depicted in Figure 1, the performance of participants is varying for various aspects of cybersecurity knowledge. For question 1, which focused on identifying secure URL, as well as assessing if participants could differentiate between https:// and http:// in a website URL, a good majority about 66.1% of participants answered the question correctly. However, a reasonable number (33.9%) based on their performance in the quiz, lacked knowledge about how to identify a secure URL. This shows that even the quite simple aspects of internet security should not be left out during cybersecurity awareness or campaign that is intended to boost knowledge of cyber-users. Also, the general cybersecurity behavioural knowledge, dealing with how to behave well on the internet should be incorporated into the cybersecurity innovative interventions for the 21st century cyber-users, such as gamification for learning cybersecurity. Consequently, question 2 was on social engineering, with focus on identifying a phishing attack. The performance of participants was fair, as only a little above average (51.1%) was able to identify a phishing attack, leaving the remaining 48.9% unknowledgeable about social engineering. Though, this is just one question and may not be able to generalise their social engineering knowledge, however this is an indication that this crucial aspect of cybersecurity lacks adequate knowledge by cyber-users. Social engineering thus, needs to be incorporated into novel cybersecurity assurance interventions, such as gamification as proposed by this research, as social engineering is one of the most common attacks targeted at engineering the behaviour of humans to be lured into falling for a fraud. Question 3 assessed the knowledge of participants on network hacking, and a considerable proportion of participants performed poorly. About 59.4% failed this question. There is a trend that network security knowledge is really lacking among the 21st century cyber-users. Unfortunately, this is an aspect of cybersecurity where most cybercriminals take advantage of the vulnerability of victims and attack via network frauds. It is therefore important to illustrate common network attacks to the general internet users and not just computer science / cybersecurity experts. In the 21st century, everyone is a potential victim and target of cyberattacks, most of which are network-based.

Furthermore, findings from question 4 revealed that only about 51.1% were knowledgeable about 2-step authentication. This is alarming as most online services use this feature for extra protection of users when trying to approve a transaction or gain access into their online portal. Most cyber-users do not take note of this opportunity to protect their accounts from unauthorised access to their personal information. It is also possible that some persons do not set the proper security controls on their social media accounts, banking accounts, among others. There is a serious need for more cybersecurity awareness and knowledge impartation among cyber-users in the 21st century. Interestingly, question 5 on password security is the most correctly answered question. A whopping 87.2% were able to choose a secure password from the choices of passwords given. This means their password security is good, however having mere knowledge of secure passwords may not be necessarily sufficient for password security but possessing an in-depth understanding about the privacy of passwords, where these passwords are/should be kept, as well as having appropriate knowledge of how hackers could gain access to the passwords via keylogging attacks. Network security in general is a core aspect that should be inculcated into cybersecurity knowledge intervention to ensure people are well informed and duly secured online. This is important as majority of high-profile cyberattacks occur via a network. Question 6 asked a question about ransomware, and a respectable number of participants, about 67.8% were able to prove their knowledge of a ransomware. However, this might not be a yardstick to prove they are cybersecure. They might understand this well due to familiarity with such instances or even past experiences of falling for such unfortunate fraud. However, a reasonable number of respondents did not get the question correctly, thence it is still essential to include such instances of network attacks by illustrating how a ransomware fraud is orchestrated into the cybersecurity knowledge gamification.

Ransomware is also a form of social engineering, where sometimes the information used to trick the user is just imaginary and targeted at weakening the mindset of the individual to pay some ransom to avoid getting their files deleted among other actions.

Question 7 was a question asked about private browsing and how to be sure while surfing the internet. Above average of the respondents answered this question correctly (67.4%), however, there are differences in the age and gender of those who proved being knowledgeable about private browsing. For instance, age-wise, those in the age bracket of 15-20 and 21-30, respectively had better knowledge of this question. This might be because of their constant surfing of the internet, thus, making them more conscious of their browsing behaviour and privacy due to the numerous sites they might be browsing for diverse purposes. Nevertheless, the more advanced in age may be more occupied with life challenges to have time for regular internet browsing and surfing of the net. Also, it is possible the younger people make use of free websites and software instead of paid ones as majority of them might not be in the working class yet or may not have a stable income. Furthermore, question 8 which focuses on location tracking via smartphone GPS, was woefully failed by the participants. This is yet another network security question which proved lack of knowledge by 21st century cyber-users. A huge majority, about 69.2% got the question incorrectly. This question falls under the mobile network security category. Majority of respondents were not aware that turning off GPS function on their smartphone cannot prevent their phone location from tracked. This was a tricky question which truly assessed the cybersecurity knowledge of users on network security. It is therefore important to propose innovative ways of integrating cybersecurity knowledge, especially focusing on network security. Emphasis should also be placed on social engineering, including phishing, identity theft, among other attacks, as many 21st century cyber-users lack adequate knowledge of these vices.

Question 9 was another well correctly answered question which was on Wi-Fi network privacy/safety. Surprisingly, huge majority of respondents, about 75.8% proved to be knowledgeable about safety of using Wi-Fi networks. This proves their subconsciousness in being sceptical of public Wi-Fi networks. Despite using a password to access, most cyber-users knew it is not still safe to use such network for sensitive activities, for example, online banking. However, a fair portion still failed this question. More so, there were differences in age and gender regarding the knowledge of Wi-Fi security. For instance, middle-aged persons in the age range of 41-50 correctly answered this question more than other age groups. Also, 31-40 young adults performed well. However, the younger persons proved lack of knowledge in Wi-Fi safety. This calls for training and interventions to be designed and prepared for more younger generation to learn proper cybersecurity practices and be equipped with adequate knowledge of cybersecurity. Finally, question 10 which was focused on VPN security, yet another network security question, was poorly performed by participants. About 64.7% lacked knowledge of the kind of cybersecurity risks that can be minimized via the use of a virtual private network (VPN). This reveals that despite the availability of security systems to curb cybercrimes, a lot of persons still fall victim of cyberattacks due to lack of knowledge about the use and importance of such security systems.

4.5 Predictors of Knowledge for Gamifying Cybersecurity? (RQ3)

To find the knowledge predictors for cybersecurity gamification, multiple linear regression analysis was conducted on each of the feedback questions – targeted at the quiz performance and gamification, and the cybersecurity questions. Since each question was part of a cybersecurity sub-topic, to make a more generalised assertion, the cybersecurity questions were split into two parts, namely, internet/website security and network security as described in previous sections of this paper. From the findings, only two feedback questions related to gamifying attained significance in the regression analysis. They are, enjoyment, and willingness to play cybersecurity game. The result for regression analysis for enjoyment → cybersecurity knowledge (internet/website security, network security) is presented in Table 9 below.

Table 9
Regression analysis for enjoyment → cybersecurity knowledge

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. error	Beta		
1	(Constant)	1.578	.247		6.388	<.001
	Internet website security	.438	.111	.300	3.941	<.001
	Network security	.029	.097	.023	.305	.761

a. Dependent variable: Did you enjoy the quiz?

From the regression analysis in Table 9, there is a significance in cybersecurity knowledge of internet / website security on the enjoyment of users in the cybersecurity quiz. This asserts that questions on internet/website security (t = 3.941, P<.001) predicts the enjoyment of users in a cybersecurity knowledge quiz. Moreover, it can be inferred that cyber-users / general internet users will enjoy a cybersecurity gamification that has more of internet/website security as compared to network security. The reason behind this could be due to difficulty in network security which is seen as an expert field even among security professionals. Nevertheless, it is instructive to design the network security gamification questions in a more illustrative way to ensure general cyber-users can gain some knowledge about network attacks. Moreover, a knowledge-based intervention for cybersecurity knowledge enhancement should not only be focused on enjoyment but the impartation of knowledge, learning combined with a glimpse of enjoyment to achieve the goal of immersing adequate cybersecurity knowledge in the users. Table 10 presents the regression analysis for willingness to play a cybersecurity game → cybersecurity knowledge (internet/website security, network security).

Table 10
Regression analysis for willingness to play a cybersecurity game → cybersecurity knowledge

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. error	Beta		
1	(Constant)	1.575	.314		5.012	<.001
	Internet website Ssecurity	.418	.141	.231	2.958	.003
	Network security	-.021	.123	-.013	-.168	.867

a. Dependent variable: Would you be willing to play a cybersecurity knowledge game?

Regression analysis result in Table 10, reveals that the participants were willing to play a cybersecurity knowledge game if it had more of the internet/website security component. Thus, internet/website security (t = 2.958, P = .003) predicted the willingness to play a cybersecurity knowledge game. Therefore, this result aligns with the findings on enjoyment, as cyber-users perceive they will enjoy a cybersecurity game that is more internet/website security based as compared to those with network security. So, if they will enjoy internet/website security inclined game, then they will also be willing to play such category of a cybersecurity game. This finding is interesting and instructive at the same time as it is a revelation for cybersecurity gamification researchers to consider the interest of cyber-users in the design of cybersecurity games. However, since this intervention via gamification is not just for entertainment purposes as it is a serious game, it must be balanced. Though, there is a likely relationship between internet security and network security as internet is also a comprehensive network. Thence, network security knowledge could be incorporated in a seamless manner where network frauds that are common to general users via mobile network, websites, emails, and other internet/online security avenues are properly illustrated and should be considered in the innovative interventions, for example via gamification to ensure a profitable learning process for cyber users. The next section gives a brief discussion on the key vital findings from the results presented.

5. Discussion

In this section, a brief discussion is presented on the result findings already presented comprehensively in the previous sections. The implication of the findings, as well as recommendations, limitations and future work will be also discussed here. The key findings are split into 3, namely: gender disparity and experience in cybersecurity knowledge; lack of network security knowledge in the 21st century, and knowledge components for gamifying cybersecurity.

5.1 Gender Disparity & Experience in Cybersecurity Knowledge

From the findings in the investigation conducted by this study, it was revealed that there were differences in gender and experience according to age on cybersecurity knowledge. This is very imperative to note and consider as the issue of gender equality is paramount in various fields. In the information technology field in general, there is a lack of female professionals, as the job title is more predominant among males. Specifically, in cybersecurity, the proportion of females is even lower or almost insignificant. Majority of females lack the interest to either study or work in a cybersecurity profession. Formidably, females are victims of a lot of cybercrimes as some studies has proven [31, 57, 58]. These findings also tally with the result of this study as females were most lacking in cybersecurity knowledge in both internet/website security and network security accordingly. There is a need therefore to promote female participation in cybersecurity awareness campaigns, trainings, as well as ensure more females have accessible to cybersecurity knowledge intervention programs and innovations such as the gamification of cybersecurity. Surprisingly, there was no gender differences in the knowledge of identifying phishing, a component of social engineering. This was in corroboration with a study where there was no strong correlation among demographics and susceptibility to phishing [59], although there are other studies that discovered some differences [60, 61], however, the trend is changing as cybercriminals tend to be more creative in finding ways of luring their victims to fall for social engineering scams of which both gender regardless of experience can be captured, hence the need for innovative knowledge intervention programs such as gamification that can help immerse cybersecurity knowledge for all categories of users and expertise.

5.2 Lack of Network Security Knowledge in the 21st Century

The major findings from result of the investigation of cybersecurity knowledge in the 21st century as addressed by this study is the lack of network security knowledge. It is quite alarming that most internet users lack basic network security knowledge, in fact, as observed from the latter findings of this study, there is a great lack of interest in network security among the general populace. Though, network security might be seen as a more expertise field, it is also important that general cyber-users are aware and well knowledgeable of the way these network attacks occur. If they are well knowledgeable, they can be able to make careful decisions when communicating over the network and detect network frauds, popular ones of which are botnet attacks, phishing, amongst others. Though, the findings of this research showed that users had a quite impressive knowledge of strong passwords, however it is not enough as they were unable to detect that strong passwords could also be cracked by hackers if the necessary authentication are not put in place. It is therefore instructive that institutions begin to illustrate network security attacks to the general student population as well as enlighten people on the danger level of such attacks. High profile frauds are because of network attacks [49, 62] and there is a large effect of attacks on network. As a matter for immediate action, cybercriminals are beginning to shift from conventional system network attacks to mobile network attacks [63, 64], whereof every mobile device user is a potential victim.

5.3 Knowledge Components for Gamifying Cybersecurity

As advised by the results of this research, as well as alignments with existing literature, the components of knowledge that should be included in gamifying cybersecurity are narrowly focused yet should be comprehensive. Most studies that developed cybersecurity games or interventions were focused on just one aspect of cybersecurity such as Password security [12, 51, 65, 66], Phishing experiments [59, 61, 67-71], of which phishing is paramount in literature. However, other aspects of social engineering are still lacking in the gamification of cybersecurity, such as identity theft, fraud detection, fake actors/scammers, amongst others. Gamification of such should include real world scenario that can teach several aspects of social engineering. Another area that is lacking from literature which is important for gamifying cybersecurity is good cybersecurity behaviour. As simple as it may seem, literature has revealed that most of the security errors made by humans are because of lack of good cybersecurity behaviours [3, 72]. Therefore, issues such as how to identify scammers easily, avoiding fake actors, social media security, ignoring fake links, ignoring fake friend requests, maintain good cybersecurity practices, avoiding get rich schemes, ignoring too good to be true rewards, how to chat with strangers, and protecting computing devices (both offline and online), should be incorporated into the gamification of cybersecurity to ensure users are equipped with a comprehensive and balanced knowledge of cybersecurity.

5.4 Study Implications & Recommendations

This study has a couple of implications and recommendations for stakeholders, institutions as well as the general users. For stakeholders, this study findings reveals the current situation of the lack of cybersecurity knowledge among 21st century cyber-users. Moreover, it could help in planning out strategic security measures as well as setting policies that could foster better acquisition of cybersecurity knowledge. Furthermore, security developers can have a clearer insight of the core cybersecurity constituents to be included when designing cybersecurity intervention programs and software. It is obvious that network security knowledge is lacking and should be incorporated in the design mechanisms of novel and emerging security mediating platforms. Consequently, the findings from this study can be useful for various educational institutions to tighten their security awareness approaches to include comprehensive aspects of cybersecurity. Also, the results can propel institutions to carry out more effective cybersecurity trainings for security personnel as well as the general community. These cybersecurity training should include social engineering tactics in the 21st century, network security, as well as general internet/mobile security.

5.5 Study Limitations & Future Work

Despite the very insightful findings from the investigation conducted by this study, there are some limitations which could be improved in future research works. First, the cybersecurity knowledge in this study was assessed by a quiz of 10 cybersecurity questions which focused on internet/website security and network security, respectively. Though, the authors carefully selected questions based on literature recommendations believed to be present day cybersecurity issues, it is possible that cybersecurity knowledge may be better assessed via a more comprehensive quiz. Future work can increase the number of questions to spread across more emerging areas of cybersecurity, such as having more questions of practical social engineering applications, identity theft, fraud detection, etc. Also, instead of just a quiz like question, future research can use existing systems such as Kahoot which is more of a gamification environment to test the cybersecurity knowledge of users to as to improve engagement and enjoyment, as the end goal of our research is to propose a cybersecurity gamification model which will be published soon. Moreover, gamified elements can be used to describe some of the questions via illustrations, especially the aspect of network security, it could increase enjoyment of participants in network security related questions. Consequently, the questions used in assessing the cybersecurity knowledge of cyber-users should be updated to latest cybersecurity issues depending on the period of conducting the research and issues related to a particular location. Finally, the knowledge of cyber-users can be assessed geographically, that is to find out if location or nationality of a person affects their knowledge of cybersecurity.

6. Conclusion

In conclusion, this research has been able to first, identify the socio-demographic factors affecting cybersecurity knowledge, investigate the cybersecurity knowledge of 21st century cyber-users, and assess the predictors of knowledge for gamifying cybersecurity. The findings are quite interesting and insightful in developing innovative interventions to enhance cybersecurity knowledge in the 21st century. Network security knowledge is lacking among cyber-users in the 21st century and should be incorporated into emerging knowledge intervention programs, one of which is gamification to ensure enhancement of cybersecurity knowledge to combat the unrelenting cybercrime forces and attackers. Female participation in cybersecurity should be encouraged and educational incentives should be provided to motivate females in enrolling for cybersecurity courses at higher institutions. Also, the cybersecurity workforce should ensure gender unbiases in recruiting cybersecurity professionals to balance the professional stance of the cybersecurity field. Summarily, this paper has revealed a deep insight to the current state of cybersecurity knowledge in the 21st century.

Data Availability

The data gathered and analysed in this study are not available publicly. However, materials and other resources used during this research are available upon reasonable request.

Conflict of Interest

The authors declare they have no conflict of interest.

Acknowledgement

This research was funded by a grant from Universiti Kuala Lumpur, Malaysia under the UniKL Excellent Research Grant Scheme (UERGS Grant UniKL/CoRI/UER22008).

References

[1] Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." *computers & security* 38 (2013): 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[2] van Steen, Tommy, and Julia RA Deeleman. "Successful gamification of cybersecurity training." *Cyberpsychology, Behavior, and Social Networking* 24, no. 9 (2021): 593-598. https://doi.org/10.1089/cyber.2020.0526

[3] Hadlington, Lee. "The "human factor" in cybersecurity: Exploring the accidental insider." In *Research anthology on artificial intelligence applications in security*, pp. 1960-1977. IGI Global, 2021. https://doi.org/10.4018/978-1-5225-4053-3.ch003

[4] Kelley, Timothy, Mary J. Amon, and Bennett I. Bertenthal. "Statistical models for predicting threat detection from human behavior." *Frontiers in psychology* 9 (2018): 466. https://doi.org/10.3389/fpsyg.2018.00466

[5] Kearney, Wayne D., and Hennie A. Kruger. "Can perceptual differences account for enigmatic information security behaviour in an organisation?." *computers & security* 61 (2016): 46-58. https://doi.org/10.1016/j.cose.2016.05.006

[6] Yan, Zheng, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen, and Ethan Sprissler. "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?." *Computers in Human Behavior* 84 (2018): 375-382. https://doi.org/10.1016/j.chb.2018.02.019

[7] Halevi, Tzipora, Nasir Memon, James Lewis, Ponnurangam Kumaraguru, Sumit Arora, Nikita Dagar, Fadi Aloul, and Jay Chen. "Cultural and psychological factors in cyber-security." In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*, pp. 318-324. 2016. https://doi.org/10.1145/3011141.3011165

[8] Faith, B. Fatokun, Zalizah Awang Long, Suraya Hamid, O. Fatokun Johnson, Christopher Ifeanyi Eke, and Azah Norman. "An intelligent gamification tool to boost young kids cybersecurity knowledge on fb messenger." In *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pp. 1-8. IEEE, 2022. https://doi.org/10.1109/IMCOM53663.2022.9721733

[9] Raineri, Ellen M., and Tamara Fudge. "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs." *Journal of Higher Education Theory & Practice* 19, no. 4 (2019). https://doi.org/10.33423/jhetp.v19i4.2203

[10] Shibgatullah AS, Othman I. S., Basari A. S. H., and Noh Z. A. M. "The Awareness of Security Breach among IT Users in Kolej PolyTech MARA, Batu Pahat." *Journal of Advanced Research in Computing and Applications* 5, no. 1 (2016): 1-10.

[11] Taib A. M., and Azman N. N. K. A. "Experimental Analysis of Trojan Horse and Worm Attacks in Windows Environment." *Journal of Advanced Research in Computing and Applications* 13, no. 1 (2018): 1-9.

[12] Švábenský, Valdemar, Pavel Čeleda, Jan Vykopal, and Silvia Brišáková. "Cybersecurity knowledge and skills taught in capture the flag challenges." *Computers & Security* 102 (2021): 102154. https://doi.org/10.1016/j.cose.2020.102154

[13] Thompson, Lily, Nicholas Melendez, Justin Hempson-Jones, and Francesca Salvi. "Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning." In *European Conference on Games Based Learning*, vol. 16, no. 1, pp. 562-569. 2022. https://doi.org/10.34190/ecgbl.16.1.504

[14] Coenraad, Merijke, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David Weintrop. "Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games." *Simulation & Gaming* 51, no. 5 (2020): 586-611. https://doi.org/10.1177/1046878120933312

[15] Scholefield, Sam, and Lynsay A. Shepherd. "Gamification techniques for raising cyber security awareness." In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, pp. 191-203. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-22351-9_13

[16] Boopathi, K., S. Sreejith, and A. Bithin. "Learning cyber security through gamification." *Indian Journal of Science and Technology* 8, no. 7 (2015): 642-649. https://doi.org/10.17485/ijst/2015/v8i7/67760

[17] Jelo, Martin, and Pavol Helebrandt. "Gamification of cyber ranges in cybersecurity education." In *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 280-285. IEEE, 2022. https://doi.org/10.1109/ICETA57911.2022.9974714

[18] Huotari, Kai, and Juho Hamari. "Defining gamification: a service marketing perspective." In *Proceeding of the 16th international academic MindTrek conference*, pp. 17-22. 2012. https://doi.org/10.1145/2393132.2393137

[19] Demmese, Fikirte, Xiaohong Yuan, and Darina Dicheva. "Evaluating the Effectiveness of Gamification on Students' Performance in a Cybersecurity Course." In *Journal of the Colloquium for Information System Security Education*, vol. 8, no. 1. 2020.

[20] Le Compte, Alexis, David Elizondo, and Tim Watson. "A renewed approach to serious games for cyber security." In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 203-216. IEEE, 2015. https://doi.org/10.1109/CYCON.2015.7158478

[21] Hendrix, Maurice, Ali Al-Sherbaz, and Bloom Victoria. "Game based cyber security training: are serious games suitable for cyber security training?." *International Journal of Serious Games* 3, no. 1 (2016): 53-61. https://doi.org/10.17083/ijsg.v3i1.107

[22] Hare, Ryan, and Ying Tang. "Player modeling and adaptation methods within adaptive serious games." *IEEE Transactions on Computational Social Systems* (2022). ttps://doi.org/10.1109/ICCSI53130.2021.9736213

[23] Das, Sanchari. "SoK: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review." In *Proceedings of the workshop on usable security and privacy (USEC)*. 2022.

[24] Sharif, Karzan H., and Siddeeq Y. Ameen. "A review of security awareness approaches with special emphasis on gamification." In *2020 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 151-156. IEEE, 2020. https://doi.org/10.1109/ICOASE51841.2020.9436595

[25] Qusa, Hani, and Jumana Tarazi. "Cyber-hero: A gamification framework for cyber security awareness for high schools students." In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0677-0682. IEEE, 2021. https://doi.org/10.1109/CCWC51732.2021.9375847

[26] Smith, Aaron. "What the public knows about cybersecurity." (2017).

[27] Matovu, Richard, Joshua C. Nwokeji, Terry Holmes, and Tajmilur Rahman. "Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges." In *2022 IEEE Frontiers in Education Conference (FIE)*, pp. 1-9. IEEE, 2022. https://doi.org/10.1109/FIE56618.2022.9962519

[28] Kennison, Shelia M., and Eric Chan-Tin. "Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors." *Frontiers in Psychology* 11 (2020): 546546. https://doi.org/10.3389/fpsyg.2020.546546

[29] Tirumala, Sreenivas Sremath, Abdolhossein Sarrafzadeh, and Paul Pang. "A survey on internet usage and cybersecurity awareness in students." In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pp. 223-228. IEEE, 2016. ttps://doi.org/10.1109/PST.2016.7906931

[30] Shehzad, Rohail, Zulqurnan Aslam, Nadeem Ahmad, and Muhammad Waseem Iqbal. "Web Usability and User Trust on E-commerce Websites in Pakistan." *International Journal of Advanced Computer Science and Applications* 8, no. 12 (2017): 509-517. ttps://doi.org/10.14569/IJACSA.2017.081267

[31] Ameen, Nisreen, Ali Tarhini, Mahmood Hussain Shah, and Nnamdi O. Madichie. "Employees' behavioural intention to smartphone security: A gender-based, cross-national study." *Computers in Human Behavior* 104 (2020): 106184. https://doi.org/10.1016/j.chb.2019.106184

[32] Agaku, Israel T., Akinyele O. Adisa, Olalekan A. Ayo-Yusuf, and Gregory N. Connolly. "Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers." *Journal of the American Medical Informatics Association* 21, no. 2 (2014): 374-378. https://doi.org/10.1136/amiajnl-2013-002079

[33] Rohan, Rohani, Debajyoti Pal, Suree Funilkul, Wichian Chutimaskul, and Wichai Eamsinvattana. "How gamification leads to continued usage of MOOCs? A theoretical perspective." *IEEE Access* 9 (2021): 108144-108161. https://doi.org/10.1109/ACCESS.2021.3102293

[34] Amran, Ammar, Zarul Fitri Zaaba, Manmeet Mahinderjit Singh, and Abdalla Wasef Marashdih. "Usable security: revealing end-users comprehensions on security warnings." *Procedia Computer Science* 124 (2017): 624-631. https://doi.org/10.1016/j.procs.2017.12.198

[35] Breitinger, Frank, Ryan Tully-Doyle, and Courtney Hassenfeldt. "A survey on smartphone user's security choices, awareness and education." *Computers & Security* 88 (2020): 101647. https://doi.org/10.1016/j.cose.2019.101647

[36] Mystakidis, Stylianos, Jeries Besharat, George Papantzikos, Athanasios Christopoulos, Chrysostomos Stylios, Spiros Agorgianitis, and Dimitrios Tselentis. "Design, development, and evaluation of a virtual reality serious game for school fire preparedness training." *Education Sciences* 12, no. 4 (2022): 281. https://doi.org/10.3390/educsci12040281

[37] Yasin, Affan, Lin Liu, Tong Li, Jianmin Wang, and Didar Zowghi. "Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG)." *Information and Software Technology* 95 (2018): 179-200. https://doi.org/10.1016/j.infsof.2017.12.002

[38] Alqahtani, Hamed, Manolya Kavakli-Thorne, and Majed Alrowaily. "The impact of gamification factor in the acceptance of cybersecurity awareness augmented reality game (CybAR)." In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pp. 16-31. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-50309-3_2

[39] Jin, Ge, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. "Game based cybersecurity training for high school students." In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, pp. 68-73. 2018. https://doi.org/10.1145/3159450.3159591

[40] DeCusatis, C., B. Gormanly, E. Alvarico, O. Dirahoui, J. McDonough, B. Sprague, M. Maloney, D. Avitable, and B. Mah. "A cybersecurity awareness escape room using gamification design principles." In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0765-0770. IEEE, 2022. https://doi.org/10.1109/CCWC54503.2022.9720748

[41] Rohan, Rohani, Debajyoti Pal, Jari Hautamäki, Suree Funilkul, Wichian Chutimaskul, and Himanshu Thapliyal. "A systematic literature review of cybersecurity scales assessing information security awareness." *Heliyon* (2023). https://doi.org/10.1016/j.heliyon.2023.e14234

[42] Dabrowski, Adrian, Johanna Ullrich, and Edgar R. Weippl. "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well." In *Proceedings of the 33rd Annual Computer Security Applications Conference*, pp. 303-314. 2017. https://doi.org/10.1145/3134600.3134639

[43] Abu-Amara, Fadi, Reem Almansoori, Safa Alharbi, Marwah Alharbi, and Asma Alshehhi. "A novel SETA-based gamification framework to raise cybersecurity awareness." *International Journal of Information Technology* 13, no. 6 (2021): 2371-2380. https://doi.org/10.1007/s41870-021-00760-5

[44] Malone, Mac, Yicheng Wang, Kedrian James, Murray Anderegg, Jan Werner, and Fabian Monrose. "To gamify or not? on leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention." In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, pp. 1135-1141. 2021. https://doi.org/10.1145/3408877.3432544

[45] Patten, Mildred L. *Understanding research methods: An overview of the essentials*. Routledge, 2016. https://doi.org/10.4324/9781315213033

[46] McCall, Chester Hayden. "Sampling and statistics handbook for research." *(No Title)* (1982).

[47] Qualtrics. "Calculating Sample Population Size " https://www.qualtrics.com/blog/calculating-sample-size/ (accessed.

[48] Hatfield, Joseph M. "Social engineering in cybersecurity: The evolution of a concept." *Computers & Security* 73 (2018): 102-113. https://doi.org/10.1016/j.cose.2017.10.008

[49] Ben-Asher, Noam, and Cleotilde Gonzalez. "Effects of cyber security knowledge on attack detection." *Computers in Human Behavior* 48 (2015): 51-61. https://doi.org/10.1016/j.chb.2015.01.039

[50] Kim, Semin, Hyung-Jin Mun, and Sunghyuck Hong. "Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal." *Applied Sciences* 12, no. 5 (2022): 2301. https://doi.org/10.3390/app12052301

[51] Hartwig, Katrin, and Christian Reuter. "Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations." *Behaviour & Information Technology* 41, no. 7 (2022): 1357-1380. https://doi.org/10.1080/0144929X.2021.1876167

[52] Grubbs, Paul, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed, and Thomas Ristenpart. "Leakage-abuse attacks against order-revealing encryption." In *2017 IEEE symposium on security and privacy (SP)*, pp. 655-672. IEEE, 2017. https://doi.org/10.1109/SP.2017.44

[53] Thompson, Christopher, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt. "The web's identity crisis: understanding the effectiveness of website identity indicators." In *28th USENIX Security Symposium (USENIX Security 19)*, pp. 1715-1732. 2019.

[54] Abu-Salma, Ruba, and Benjamin Livshits. "Evaluating the end-user experience of private browsing mode." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-12. 2020. https://doi.org/10.1145/3313831.3376440

[55] Ramezanpour, Keyvan, Jithin Jagannath, and Anu Jagannath. "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective." *Computer Networks* 221 (2023): 109515. https://doi.org/10.1016/j.comnet.2022.109515

[56] Gaur, Anubha. "VPN: Problem relates with security of data in tunneling process and requirements." *ACADEMICIA: An International Multidisciplinary Research Journal* 12, no. 4 (2022): 633-639. https://doi.org/10.5958/2249-7137.2022.00356.1

[57] Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. "Correlating human traits and cyber security behavior intentions." *computers & security* 73 (2018): 345-358. https://doi.org/10.1016/j.cose.2017.11.015

[58] Mohamed, Norshidah, and Ili Hawa Ahmad. "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia." *Computers in human behavior* 28, no. 6 (2012): 2366-2375. https://doi.org/10.1016/j.chb.2012.07.008

[59] Mohebzada, Jamshaid G., Ahmed El Zarka, Arsalan H. BHojani, and Ali Darwish. "Phishing in a university community: Two large scale phishing experiments." In *2012 international conference on innovations in information technology (IIT)*, pp. 249-254. IEEE, 2012. https://doi.org/10.1109/INNOVATIONS.2012.6207742

[60] Rajivan, Prashanth, Pablo Moriano, Timothy Kelley, and L. Jean Camp. "Factors in an end user security expertise instrument." *Information & Computer Security* 25, no. 2 (2017): 190-205. https://doi.org/10.1108/ICS-04-2017-0020

[61] Arachchilage, Nalin Asanka Gamagedara, Steve Love, and Konstantin Beznosov. "Phishing threat avoidance behaviour: An empirical investigation." *Computers in Human Behavior* 60 (2016): 185-197. https://doi.org/10.1016/j.chb.2016.02.065

[62] Brun, Olivier, Yonghua Yin, Erol Gelenbe, Y. Murat Kadioglu, Javier Augusto-Gonzalez, and Manuel Ramos. "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments." In *Security in Computer and Information Sciences: First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers 1*, pp. 79-89. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-95189-8_8

[63] Liébana-Cabanillas, Francisco, Francisco Muñoz-Leiva, and Juan Sánchez-Fernández. "A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment." *Service Business* 12 (2018): 25-64. ttps://doi.org/10.1007/s11628-017-0336-7

[64] Eustace, Ken, Rafiqul Islam, Philip Tsang, and Geoff Fellows. "Human factors, self-awareness and intervention approaches in cyber security when using mobile devices and social networks." In *Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13*, pp. 166-181. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-78816-6_13

[65] Aytes, Kregg, and Terry Connolly. "Computer security and risky computing practices: A rational choice perspective." In *Advanced Topics in End User Computing, Volume 4*, pp. 257-279. Igi Global, 2005. https://doi.org/10.4018/978-1-59140-474-3.ch013

[66] Whitty, Monica, James Doodson, Sadie Creese, and Duncan Hodges. "Individual differences in cyber security behaviors: an examination of who is sharing passwords." *Cyberpsychology, Behavior, and Social Networking* 18, no. 1 (2015): 3-7. https://doi.org/10.1089/cyber.2014.0179

[67] Sheng, Steve, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions." In *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 373-382. 2010. https://doi.org/10.1145/1753326.1753383

[68] Rocha Flores, Waldo, Hannes Holm, Gustav Svensson, and Göran Ericsson. "Using phishing experiments and scenario-based surveys to understand security behaviours in practice." *Information Management & Computer Security* 22, no. 4 (2014): 393-406. https://doi.org/10.1108/IMCS-11-2013-0083

[69] Arachchilage, Nalin Asanka Gamagedara, and Steve Love. "Security awareness of computer users: A phishing threat avoidance perspective." *Computers in human behavior* 38 (2014): 304-312. https://doi.org/10.1016/j.chb.2014.05.046

[70] Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." *Computers & Security* 68 (2017): 160-196. ttps://doi.org/10.1016/j.cose.2017.04.006

[71] Arachchilage, Nalin Asanka Gamagedara, and Steve Love. "A game design framework for avoiding phishing attacks." *Computers in Human Behavior* 29, no. 3 (2013): 706-714. https://doi.org/10.1016/j.chb.2012.12.018

[72] Fatokun, F. B., S. Hamid, A. Norman, and J. O. Fatokun. "The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities." In *Journal of Physics: Conference Series*, vol. 1339, no. 1, p. 012098. IOP Publishing, 2019. https://doi.org/10.1088/1742-6596/1339/1/012098

APPENDICES

In this section, all information regarding the questions items and gamification elements of the quiz are provided.

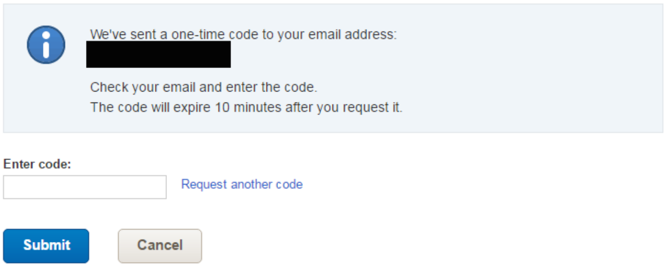
APPENDIX 1
QUIZ ITEMS AND GAMIFICATION ELEMENTS

1. What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?
(a) That the site has special high definition
(b) That information entered into the site is encrypted
(c) That the site is the newest version available
(d) That the site is not accessible to certain computers
(e) None of the above
(f) Not sure

2. Which of the following is an example of a “phishing” attack?
(a) Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows.
(b) Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information
(c) Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
(d) All of the above
(e) Not sure

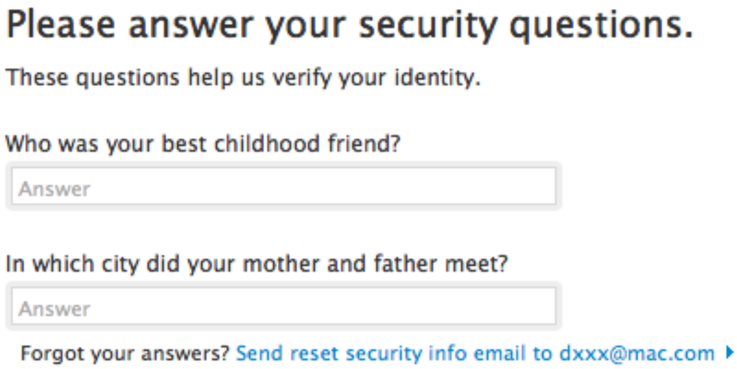
3. A group of computers that is networked together and used by hackers to steal information is called a …
(a) Botnet
(b) Rootkit
(c) DDOS
(d) Operating System
(e) Not sure

4. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?
(a)



We've sent a one-time code to your email address:
[redacted]
Check your email and enter the code.
The code will expire 10 minutes after you request it.

Enter code:



Please answer your security questions.

These questions help us verify your identity.

Who was your best childhood friend?

Answer

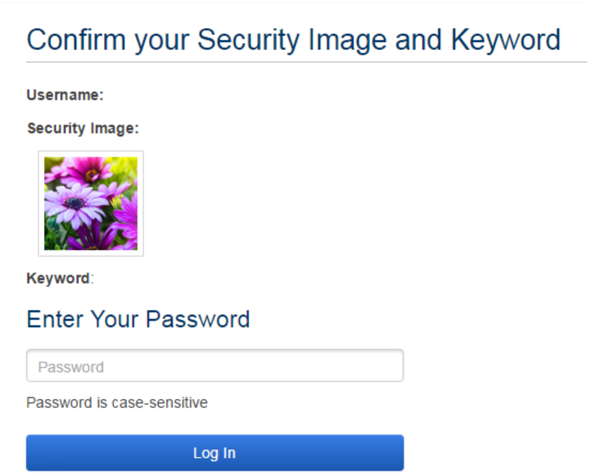
In which city did your mother and father meet?

Answer

Forgot your answers? Send reset security info email to dxxx@mac.com ▸

(b)

(c)



Confirm your Security Image and Keyword

Username:

Security Image:

Keyword:

Enter Your Password

Password

Password is case-sensitive

(d) None of these
(e) Not sure

5. Which of the following four passwords is the most secure?
(a) Boat123
(b) WTh!5Z
(c) intro*48
(d) 123456
(e) Not sure

6. Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …
(a) Botnet
(b) Ransomware
(c) Driving
(d) Spam
(e) None of the above
(f) Not sure

7. "Private browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?
(a) Yes
(b) No
(c) Not sure

8. Turning off the GPS function of your smartphone prevents any tracking of your phone's location.
(a) True
(b) False
(c) Not sure

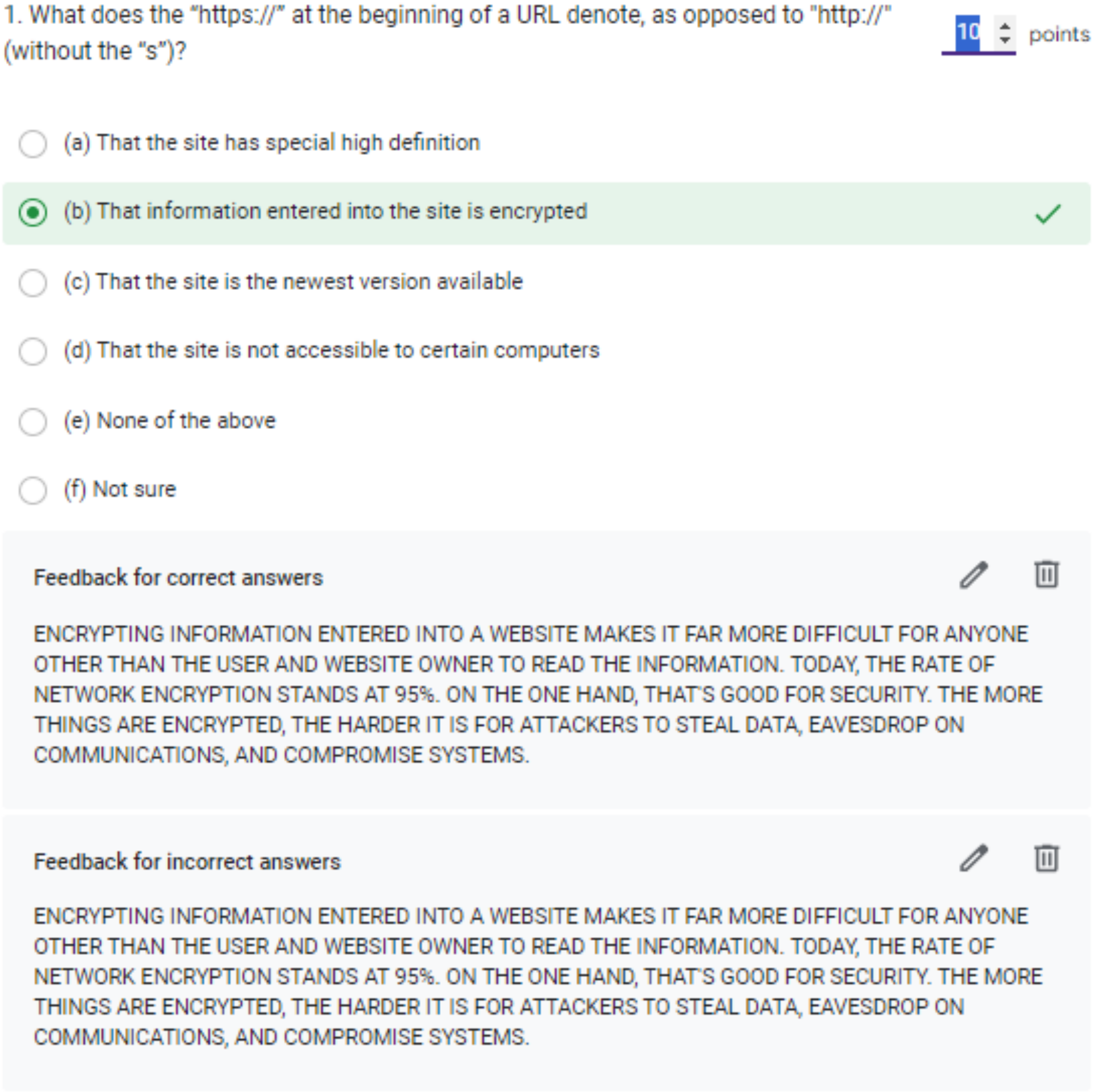
9. If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?
(a) Yes, it is safe
(b) No, it's not safe
(c) Not sure

10. What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?
(a) Use of insecure Wi-Fi networks
(b) Key-logging
(c) De-anonymization by network operators
(d) Phishing attacks

(e) Not sure

APPENDIX 2

As indicated in section 3 of the text, "The quiz was designed with some basic gamification elements, such as including scores to questions – wherein each question was assigned 10 points, making a total of 100% for 10 questions and providing feedback to each question." Figure 2 below depicts the Quiz design with point and feedback provided for each question, thus inculcating basic gamification elements.



1. What does the "https://" at the beginning of a URL denote, as opposed to "http://" (without the "s")?

10 points

○ (a) That the site has special high definition

● (b) That information entered into the site is encrypted ✓

○ (c) That the site is the newest version available

○ (d) That the site is not accessible to certain computers

○ (e) None of the above

○ (f) Not sure

Feedback for correct answers

ENCRYPTING INFORMATION ENTERED INTO A WEBSITE MAKES IT FAR MORE DIFFICULT FOR ANYONE OTHER THAN THE USER AND WEBSITE OWNER TO READ THE INFORMATION. TODAY, THE RATE OF NETWORK ENCRYPTION STANDS AT 95%. ON THE ONE HAND, THAT'S GOOD FOR SECURITY. THE MORE THINGS ARE ENCRYPTED, THE HARDER IT IS FOR ATTACKERS TO STEAL DATA, EAVESDROP ON COMMUNICATIONS, AND COMPROMISE SYSTEMS.

Feedback for incorrect answers

ENCRYPTING INFORMATION ENTERED INTO A WEBSITE MAKES IT FAR MORE DIFFICULT FOR ANYONE OTHER THAN THE USER AND WEBSITE OWNER TO READ THE INFORMATION. TODAY, THE RATE OF NETWORK ENCRYPTION STANDS AT 95%. ON THE ONE HAND, THAT'S GOOD FOR SECURITY. THE MORE THINGS ARE ENCRYPTED, THE HARDER IT IS FOR ATTACKERS TO STEAL DATA, EAVESDROP ON COMMUNICATIONS, AND COMPROMISE SYSTEMS.

Fig. 2. Gamification Elements such as Point and Feedback in Quiz Design