IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Validation of cyber security behaviour among adolescents at Malaysia university: Revisiting gender as a role

Tin Tin Ting[1*], Kar Man Cheah[2], Jie Xin Khiew[3], Yung Chin Lee[4], Jun Kit Chaw[5], Chong Keat Teoh[6]

[1]Faculty of Data Science and Information Technology, INTI International University, Negeri Sembilan, Malaysia.
[2,3,4]Faculty of Computing and Information Technology, Tunku Abdul Rahman University of Management and Technology, Kuala Lumpur, Malaysia.
[5]Institute of Visual Informatics, Universiti Kebangsaan Malaysia, Bangi, Malaysia.
[6]Artificial Intelligence Research and Computational Optimization Laboratory, DigiPen Institute of Technology Singapore.

Corresponding author: Tin Tin Ting (*Email: tintin.ting@newinti.edu.my*)

Abstract

Cyber-attacks and crimes are still a problem in Malaysia. COVID-19 has pushed Malaysians into the digital world more quickly. These cyberattacks may rise and affect more people. Thus, the aim of this study is to find out if there is a significant difference in the level of cyber security behaviour between males and females in the aspects of malware, password usage, phishing, social engineering and online scamming in Malaysia. An online questionnaire survey was used to gather data from Malaysia and received 207 total responses. Cronbach's alpha is used to measure questionnaire items' reliability. A t-test is used to determine the differences between male and female cyber security behaviour. The results show that there is no significant difference between males and females in four aspects out of five, which are malware, password usage, phishing and social engineering. There is a significant difference between males and females in the aspect of online scams. This research helps those who formulate education policies by determining that there is no noticeable gender difference. Men should get the same level of education and training as women. The findings also demonstrate that women's awareness of technology is increasing.

Keywords: Cyber security behaviour, Cyber security threat, Gender, Malware, Password Usage, Phishing, Scam, Security awareness, Social engineering, Young generation, Cybercrime.

DOI: 10.53894/ijirss.v7i1.2544
Funding: This study received no specific financial support.
History: Received: 20 February 2023/**Revised:** 13 October 2023/**Accepted:** 19 December 2023/**Published:** 10 January 2024

Authors' Contributions: Conceptualization, T.T.T., K.M.C., J.X.K., Y.C.L., J.K.C., C.K.T.; methodology, T.T.T., K.M.C., J.X.K., Y.C.L., J.K.C., C.K.T.; validation, T.T.T., K.M.C., J.X.K., Y.C.L., J.K.C., C.K.T.; formal analysis, T.T.T., K.M.C., J.X.K., Y.C.L.; investigation, K.M.C., J.X.K., Y.C.L.; resources, T.T.T.; data curation, T.T.T., K.M.C., J.X.K., Y.C.L.; writing—original draft preparation, T.T.T., K.M.C., J.X.K., Y.C.L.; writing—review and editing, T.T.T.; visualization, T.T.T.; supervision, T.T.T.; project administration, T.T.T.; funding acquisition, T.T.T., J.K.C., C.K.T. All authors have read and agreed to the published version of the manuscript.
Competing Interests: The authors declare that they have no competing interests.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Institutional Review Board Statement: The Ethical Committee of the INTI International University, Malaysia has granted approval for this study (Ref. No. INTI-FDSIT-13-03-2022).
Publisher: Innovative Research Publishing

1. Introduction

Cyber Security is the protection of systems that are connected to the internet against unauthorized access to data centres and other computers. These attacks can come in many different forms and it is difficult to keep up with cyber security [1]. According to the Malaysia Communications and Multimedia Commission (MCMC), phishing and scams are among the main concerns about online harm in the country. The Internet Service Provider (ISP) plays an important role in taking proactive action [2]. However, reducing online damages also depends on end users being aware of cyber security risks. Another report from MCMC discovered that online fraud is increasing and 70% of the cyber security reports received from the public involve online fraud [3]. In the Kaspersky report, Malaysia is found to be one of the top Southeast Asian countries facing social engineering with 45% of respondents reporting as victims [4]. Therefore, it is important to identify the characteristics of potential victims to protect against such threats.

This study focuses on five common types of cyber assaults which are malware, password usage, phishing, social engineering and internet scams. Malware is an abbreviation for malicious software which is any script or binary code that conducts some destructive behaviour. Meanwhile, using weak passwords increases the risk of hacking which can result in financial losses and even have negative effects on one's physical and emotional well-being. Phishing is a type of deception in which an attacker copies a trustworthy entity to get sensitive information from a victim. On the other hand, social engineering fraud involves criminals exploiting a friend’s trust to gain confidential data to perform a crime. Online or internet scams are those that use mass communication technologies to deceive people.

Albladi and Weir [5] claimed that females are more likely to be victims of cyber threats. According to different research, women are more likely to depend on social media companies to protect their personal data [6]. However, this study did not take geography into consideration. Thus, the purpose of this study is to determine whether gender differences present in Malaysian cyber security behaviour are related to malware, password use, phishing, social engineering and online scams.

2. Literature Review

2.1. Security Behaviour in the Aspect of Malware

Malware has been defined in several ways. For example, Christodorescu and Jha [7] defined malware as software with a harmful goal [7]. McGraw and Morrisett define malicious code as "any code added, modified or removed from a software system with the intent to intentionally cause harm or interfere with the intended operation of the system" [8]. According to Vasudevan and Yerraballi, malware is “a broad term that combines viruses, trojans, spyware and other intrusive software” Vasudevan and Yerraballi [9]. Or-Meir, et al. [10] use the terms “malicious binary code”, “malicious script” or “malicious executable” in the study refer to malware, since malware can be delivered in a variety of ways including executables, binary shell code, scripts and firmware. Viruses, worms and trojan horses are all classic instances of malware. This classification necessitates a more in-depth examination of the malware.

Malware spreads through the internet and corrupts operating systems. Malware exploits data through malicious code by exploiting weaknesses in computer applications and operating systems. Additionally, it uses social engineering to persuade users to execute malicious software by presenting them with appealing tools and applications. The dynamic nature of malware and its growing sophistication need the modification of protection techniques accordingly. Focusing on proactive protection is one strategy to handle these developments. An early warning system for malware attacks needs to assess the risk level in order to be proactive [11]. Cybercriminals are increasingly using several types of revenue-generating techniques such as targeted ransomware assaults and banking fraud focusing on certain user groups and regions of the world. It is possible that hackers are targeting certain groups to optimize success and money in the same way that internet advertising campaigns are now targeting specific groups using profile information based on computer usage behaviour.

Lévesque, et al. [12] research showed that gender was a key factor linked to malware exposures. In particular, the possibility of being a male was noted as a risk factor. Malware was 1.40 times more common in males than in females. In addition, there was a noticeable relationship between male and eight different categories of malware: ransomware, info stealer, virus, cracks, exploit, bot and rootkit. In contrast, this study revealed that there was no relationship between gender and protection against adware showing that females were somewhat more vulnerable to this particular kind of malware. A study conducted by Ameen, et al. [13] discovered that there are notable gender disparities in smartphone security behaviour whether working for international companies in a developed country that is regarded as advanced in cyber security defense or a developing country that is regarded as behind in the field [13]. In the United States and the United Arab Emirates, there are considerable gender inequalities in terms of the severity and certainty of punishment. Furthermore, there are considerable gender differences in terms of the influence of their stated national cultural values on the behavioural goal of Bring Your Own Device (BYOD) security Ameen, et al. [13].

McGill and Thompson [14] showed that there are significant differences between the genders in three of the six particular security behaviours and women show less security behaviours than men. Females have stronger security perceptions and a higher level of severity in security concerns than males. However, females belong to vulnerable groups that may contribute to lower overall security behaviour. Finally, there are gender differences in social norms with females being more likely to believe that other people implement security measures although they did not differ in perceptions of whether other people may want them to take security measures. The following hypothesis is proposed based on this literature:

H_1: There is a significant difference in the level of cyber security behaviour between males and females in the aspect of malware.

2.2. Security Behaviour in the Aspect of Password Usage

Password-protected accounts are commonly used for online services such as instant messaging, email, online banking and online retail purchases. Systems would expect users to create passwords that are exceptionally safe considering the importance of the data kept in these accounts and the possibility of misuse and exploitation by others. This has not been demonstrated to be true as the users tend to ignore the strong password guidelines. In addition, service providers do not warn users that their chosen passwords are not secure [15].

Despite the development of increasingly advanced authentication techniques such as biometrics, hardware tokens and 2-factor authentication, passwords, PINs and solving a visual puzzle are still the most widely used authentication methods. Passwords protect people's personal data against unauthorized access. Many systems rely significantly on text-based passwords to verify valid users. However, passwords are a critical cyber security risk factor due to their vulnerability to attacks. This vulnerability is caused by user actions and habits rather than the password system itself. A survey conducted by Jain, et al. [16] depicted that 42% of respondents share online passwords with family and friends [16]. Furthermore, a study conducted by Pearman, et al. suggested that once a user needs to manage a larger number of passwords, they cope by partially and exactly reusing passwords across most of their accounts [17]. The main issue is memorability which leads to other password problems. Some people choose to use easy passwords to remember them ignoring security risks. Furthermore, some users use the same or weak password for many company or personal accounts [18-20]. Furthermore, another study conducted by Bakas, et al. [18] indicated that 67% of participants in an online survey revealed that when altering their previous passwords to their new ones, 30% of respondents capitalized a letter as the most frequent alteration [21]. However, self-reports show that periodic password changes do not appear to result in weaker passwords. 82% of the participants in their study agreed that frequently changing passwords protects accounts against unauthorized users.

Some studies have been conducted to investigate gender differences in password behaviour. In a survey conducted by Juozapavičius et al., there were some gender differences in password creation. For all age categories, males had passwords that were significantly stronger than females [22]. Password complexity decreased with age equally for both genders. Very poor password hygiene was detected; 72% of users relied on words as their passwords or just used a set of numbers and over 39% of users' passwords were discovered in word lists of previous breaches. Gender and cultural differences were also investigated in another study through an online survey of users in China, Turkey and the United Kingdom. The results revealed some differences in both cultures and genders [23]. The survey discovered a significant difference in the length of passwords between men and women. Women reported 15.4 character passwords compared to 12.2 character passwords for males. There was also a significant gender difference with women mentioning cryptic sequences more frequently than men. The study found a significant difference between men and women when it came to remembering passwords with men having more difficulty than women. Additionally, a study conducted by Helkala and Hoddø Bakås [24] revealed that men trust their memory more than females when it comes to password remembering. Females often use a reset option (remember all passwords) more than men. They also found that males reuse fewer passwords than females [24]. The following hypothesis is proposed based on this literature:

H_2: There is a significant difference in the level of cyber security behaviour between males and females in the aspect of password usage.

2.3. Security Behaviour in the Aspect of Phishing

Phishing is a form of social engineering in which the attacker attempts to induce the target to provide personal information such as a login, password, email address or financial information by using a variety of techniques [25]. For example, a system may be theoretically safe against password theft; ignorant end users may leak their passwords if an attacker requests that they change their credentials over a specific Hypertext Transfer Protocol (HTTP) link posing a danger to the system's overall security. Furthermore, technological flaws like Domain Name System (DNS) cache poisoning may be used by attackers to create considerably more persuasive socially engineered messages. As a result, phishing attempts are a multi-layered problem and successful prevention would include addressing both technological and human difficulties.

Generic "lures" are commonly used in phishing attempts. For example, a phisher posing as a well-known online auction site or major financial institution will have a respectable return despite the fact that they don't know anything about the recipient. Phishing threats are becoming more widespread all around the world. In 2008, 51,401 phishing websites were identified by the anti- phishing workgroup [26]. During 2018, there was a 350% increase in ransomware attacks, a 250% increase in spoofing or business email compromise attacks and a 70% increase in spear-phishing attacks in companies [27]. Service providers are investing more in technological, instructional and legal countermeasures as they become more conscious of the problem. Phishers are evolving in sophistication in order to overcome these systems and increase competition in organizations. This tendency may be seen in both social and technological ways: better spelling, the use of subdomains and cousin domains to fool users and enhanced psychological design of the request are all instances of the former. The latter includes the use of DNS changes to prevent takedown and the usage of keyboard loggers to collect data. Research on the deception component of phishing or its social components is not as advanced as that of technology.

Therefore, the next wave of phishing may probably take a more deceptive approach. Thus, this study aims to find out if gender plays a role in understanding the danger of phishing to avoid the increasing cases of phishing.

Furthermore, phishing scams are becoming more deceptive with attacks that can manipulate end-users. For example, attacks can be made through fake phone calls and targeted emails [28]. Personal computer clients are victims of phishing attacks for five primary reasons: (1) Users do not have a basic understanding of Uniform Resource Locators (URLs). (2) They do not know which pages can be trusted. (3) They do not know the precise location of the page due to redirection or hidden URLs. (4) The URL has many alternative possibilities or some pages are unintentionally typed and (5) they do not know how to distinguish a phishing website page from a valid one [29].

Phishing emails are commonly used by cybercriminals as a method to spread dangerous links and files or steal personal information from users [30]. The reason for this is that both individuals and corporations are increasingly relying on email for communication. It was discovered that some sectors such as the healthcare industry had a greater rate of phishing scams or ransomware that resulted from phishing emails [31]. According to a study by Gordon, et al. [32], 1 in 7 healthcare employees were prone to respond to phishing emails. On the other hand, phishing emails frequently help to persuade and lure the victim by offering a wealth of information about a company or person. For instance, a cybercriminal might send phishing emails to a targeted client (i.e., victim) making it appear like the email is from the victim's own bank (for instance, Hong Kong and Shanghai Banking Corporation, HSBC), by imitating the email address, subject line, salutation and email signature in a single email and requiring bank information from those victims.

Das et al. carried out a user study and found an overconfidence bias in self-detection among participants regardless of their technical background Das, et al. [33]. Li, et al. [34] found that age significantly affects phishing email content and repeated exposure to phishing exploits. On the other hand, men are more likely to click on financial email when considering the gender click behaviour according to email content [34]. Meanwhile, Ngwane's study revealed that there is a significant relationship between gender and awareness of phishing attacks. Males are more likely to be aware of phishing attacks than their female counterparts [35]. However, research conducted in Thailand found that gender plays a role in cyber security awareness as the Thai female employees in the financial services company in this study had a higher level of cyber security awareness than the male employees [36]. In another review study, 24 papers out of 35 were studied in which the accuracy of males and females in detecting phishing and legitimate emails was compared. However, meta-analysis results showed that males do perform better than females [37]. The following hypothesis is proposed based on this literature:

H5: There is a significant difference in the level of cyber security behaviour between males and females in the aspect of phishing.

2.4. Security Behaviour in the Aspect of Social Engineering

Social engineering is a term used to describe a type of attack in which the attacker takes advantage of human weaknesses to gain access to sensitive data, hack computer systems and networks, gain unauthorized access to secured areas or violate the security objectives (such as confidentiality, integrity, availability, controllability and auditability) of cyberspace elements (such as infrastructure, data, resource, user and operation) [38]. Technical defenses are frequently ineffective in the face of such an attack. Furthermore, most people feel that they can detect such attacks.

Social engineering attacks are currently the biggest threats facing cyber security not only focused on individuals but also on the lack of cooperation in cyber security [39]. The attackers examine the psychological behaviours of the victims about their online security practices including password storage locations and attitudes towards security ranking. Victims are taken advantage of by social engineers to get sensitive information that can be used for specific purposes or sold on illegal platforms such as the black market and dark web. These collections of data can be sold on a huge scale in today's market [40]. Several research studies show that attacks by social engineering are most successful when combined with other methods such as phishing [41]. A study was carried out in Malaysia and found that Malaysians could have a high chance of becoming victims [42] but they did not differentiate in detail a specific characteristic of users. Thus, this study aims to find out if gender plays a role in understanding the dangers of social engineering.

According to a data breach report by International Business Machines Corporation (IBM) and the Ponemon Institute, the cost of a data breach in 2021 is US$ 4.24 million, this is a 10% rise from the average cost in 2019 which was $3.86 million. This also suggests that the number of security breaches is still increasing. Using advanced and sophisticated deception methods to manipulate victims to access sensitive information is the essence of social engineering. The number of social engineering attacks that exploit human vulnerabilities dramatically increased over the year examined [43]. Thus, identifying the characteristics that make them vulnerable to social engineering is a major step towards protecting against such threats [5]. Identifying the weak point helps raise awareness in an effort to reduce the possibility that they will be victims.

Notable factors include network engagement such as the use of social networks that have millions of active users who share and express their thoughts, photos and locations with others. This attracts cybercriminals who find social networks to be a rich platform for their illegal activities [5]. The individual's level of network engagement can be determined by several factors such as time spent in the network. High levels of social media usage have been found to make users more exposed to online threats in knowledge exchange networks [44]. In addition to network engagement, relying on social community companies to protect privacy and safety from cyber criminals is a common mindset among customers. These customers also tend to expose their sensitive information online without being aware of potential exploitation [5]. This research is not commonly found in Malaysia. However, a study claims that Malaysians lack knowledge about social engineering attacks [42].

A study has been conducted to show that gender does not affect awareness of cyber security in aspects of social engineering [5]. Nevertheless, more recent studies have also proven that women are more vulnerable to victimization [43]. Furthermore, a study conducted by Ngwane [35] found significant relationships between gender and receiving and responding to online pop-up messages that seemed to be social engineering attacks confirming that male students are more susceptible to online pop-up messages. Males are more curious which suggests that they are likely to respond to the online pop-up messages that appear while they are browsing the internet. According to these studies, it was found that the behaviour of university students had changed within two years. Females are more open to social media usage and are more likely to reply to junk advertisements. Moreover, females tend to trust social network providers to protect members' private information which causes them to be more willing to share their photos on the network [6]. Changes in behaviour can be found in Malaysia and other countries. The following hypothesis is proposed based on this literature:

H_4: There is a significant difference in the level of cyber security behaviour between males and females in the aspect of social engineering.

2.5. Security Behaviour in the Aspect of Online Scams

Online scams are defined as "a type of identity theft that uses a bogus email to try to steal private data such as online bank account information" [45]. The internet has facilitated the spread of cyber scams which are generously defined as any fraud that uses mass communication technology to defraud people. The UK National Fraud Authority (NFA) has issued a paper on scam typologies and victims which shows how victims are picked, approach techniques and victim profiles [46]. This paper cites several research publications that show that many schemes target individual vulnerability to scams. For example, using time-limited replies restricts thought. Additional personality traits associated with scam victim characteristics include risk-taking and a lack of self-control. The survey also dispels the assumption that elderly people are more likely to be victims (although they are more likely to experience scams than theft or robbery). Lower levels of reporting may be more noticeable among elderly victims regardless of whether they were aware of the scam. Those who blame themselves are also less likely to complain. Active social networks promoted reporting. However, there are fewer of them in certain elderly groups [46].

Overseas lotteries, sweepstakes and romance are all examples of scams [47]. One of the most prevalent kinds of internet fraud is the buying scam in which scammers obtain credit card numbers and Personal Identification Numbers (PINs) from internet users which they use to take money from the victim's bank account. Scammers use a variety of strategies to obtain victims' sensitive information and deceive them into making financial payments in order to defraud them [48]. Another kind of scam involves thieves creating bogus websites to lure victims with material that appears to be authentic and trustworthy.

Popular studies on online scam have mostly focused on the persuasion power of the fraudster's scam message or the potential victim's understanding of scams Harrison, et al. [49]. On the other hand, Judges, et al. [50] discovered the characteristics linked to individual psychological variations that make people more susceptible to being deceived by deceptive communication. Research by Modic and colleagues has highlighted individual differences in scam compliance from the standpoint of persuasiveness susceptibility and wider theoretical connections with social influence Modic, et al. [51]. Xu, et al. [52] found that males had a scam rate of 17.32% while females had a rate of 13.19% in a university. As a result, there is a significant difference between males and females. Meanwhile, Whitty [53] revealed that women were more likely to be victims of consumer scams but males were more evenly scattered among schemes. Women were also far more likely than males to fall victim to a consumer scam while men were far more likely to fall victim to an investment hoax [53]. A study conducted by Onaolapo, et al. [54] show that hackers arrange their assaults differently for online accounts belonging to adults, teens, men and women. According to this research, male accounts received less friend requests than female ones (126 vs. 31). The reason may be found in earlier studies that showed fraudsters performing romance scams frequently pretended to be older men and targeted women [55]. Additionally, they discovered that male accounts saw greater search traffic than female ones. Previous studies revealed that hackers frequently go through stolen accounts for sensitive data that may help them conduct future attacks (e.g., financial information).

Jusoh and Nizar [56] discovered that scams on the internet are also becoming common in Malaysia [56]. Furthermore, individuals are not permitted to go out and buy products during the Movement Control Order (MCO). Customers have a strong desire for shopping on the internet. Moreover, many victims have lost a significant amount of money because of internet scams involving more than a million Ringgit Malaysia. Thus, this study wants to find out if gender plays a role in understanding the danger of online scams. The following hypothesis is proposed based on this literature:

H_5: There is a significant difference in the level of cyber security behaviour between males and females in the aspect of online scams.

3. Research Methodology

The questionnaire was used to collect data related to cyber security behaviour among Malaysians. The questionnaire is designed and structured using Google Forms. The questionnaire was distributed to young generations in Malaysia on 23 February 2022 and data was collected from respondents after two weeks. The questionnaire was distributed through social media such as WeChat, WhatsApp, Instagram and emails.

Table 1.
Questionnaire items.

Malware	Q1. You are willing to open email attachments from strangers. Q2. You think that an interesting subject line causes you to open an email attachment. Q3. You are very sure of the status of the anti-virus software on your personal computer. Q4. You are interested in opening attachments with multiple extensions. Q5. You feel something is wrong if the computer runs extremely slowly. Q6. You can download freeware on the internet. Q7. You scan removable drives prior to using them on your personal computer. Q8. You installed anti-virus software, firewall software and anti-spyware software. Q9. You are willing to download materials from unsecure sites. Q10. You apply security patches as soon as possible.
Password usage	Q1. Your password doesn’t follow the keyboard pattern. Q2. You share your password with other people. Q3. You create different passwords for different applications. Q4. Your password consists of lowercase, uppercase, numbers, and special characters. Q5. Your password is longer than 8 characters. Q6. Your passwords were created based on personal information. Q7. You never change your password. Q8. You use the “Remember my password” option. Q9. You always write down your password. Q10. You never use ‘hint’ to recover a forgotten password.
Phishing	Q1. You upgrade your phishing knowledge by reading phishing materials. Q2. Do you think that the young generation will not become a target of phishing attacks? Q3. You are willing to provide confidential information to any type of email. Q4. You are willing to click hyperlinks in email messages. Q5. You will trust any email messages announcing contests or prizes. Q6. You ensure that the URL must be “https” if you are transmitting confidential information. Q7. You do think that the existence of the padlock symbol is to transmit sensitive information. Q8. You prefer to type URL in the new browser rather than clicking on hyperlinks. Q9. Receiving a suspicious email will prompt you to contact the relevant party for verification. Q10. You check URL spelling prior to any type of transaction.
Social engineering	Q1. You are interested in reading social engineering issues. Q2. You are willing to reveal your username and password to anyone claiming to be a system administrator. Q3. You think that the young generation will not be a target of social engineering attacks? Q4. You are unwilling to respond to calls, SMS or email messages from friendly or non-threatening strangers. Q5. You are willing to follow instructions given by people who speak with authority. Q6. You are willing to provide a password to a help desk. Q7. You verify the authorization or identity of someone before talking about any issues. Q8. You don't feel intimidated by questions from someone. Q9. You would not communicate with a stranger although his or her looks warrant sympathy. Q10. You would not reveal any confidential information under any circumstances.
Online scam	Q1. You established trusted online relationships with strangers. Q2. You ignore emails from well-known organizations announcing something unusual or too good. Q3. You respond to SMS announcing contests involving huge sums of money. Q4. You never trust strangers’ identity information given on the internet. Q5. You never consider any amount of money for services offered by an online site. Q6. You are willing to deposit money requested by on-line friends. Q7. You are aware of and able to identify the latest online scams. Q8. You trust strangers’ pictures posted on the internet. Q9. You never receive parcels and gifts from Internet friend. Q10. You would not hesitate to meet face-to-face with Internet friends.

A questionnaire that assesses cyber security behaviour based on the Cyber Security Behaviour Instrument (CSBI) is adopted [42]. The questionnaire is divided into six sections. Section A assesses demographic information (2 items); section B assesses cyber security behaviour from the aspects of malware, password usage, phishing, social engineering and online scams (50 items) (see Table 1). Section A consists of 3 multiple choice questions which are about age and gender. In section B, cyber security behaviour is divided into five categories: phishing, password usage, social engineering, online scamming and malware. Each of these categories consists of 10 items. All the items in section B categories are designed with a 5-point Likert scale ranging from 5 (strongly agree) to 1 (strongly disagree). Strongly agree or agree is measured as respondents' agreement with the statement while strongly disagree or disagree is reflected as respondents' disagreement with a specific statement. A slight modification has been made to the questionnaire to ensure that the question is easy to understand and to prevent misunderstandings.

The instrument (a questionnaire) was tested in a pilot study with a group of 30 students from the same research site prior to this research. The researchers make sure that the people who take part in the pilot study will not end up taking part in the main study. The Cronbach alpha reliability coefficient was used to assess the reliability of the questionnaire. A simple random sampling method is used to sample Malaysians in the age group of 15 to 30 years old.

Participants responded to the questionnaire based on a 5-point Likert scale which divides into 5 categories (strongly agree, agree, neither agree, disagree, disagree and strongly disagree). The questions are then analysed to determine whether they are good practices or bad practices. For the question categorized under good practices, the mark is allocated accordingly based on the options (strongly agree-5, agreement-4, neither agree nor disagree-3, disagree-2, strongly disagree- 1) while for the question categorized under bad practices, the mark allocated for each option is the opposite of good practices (strongly agree-1, agree-2, neither agree nor disagree-3, disagree-4, strongly disagree-5). The scores for each question in each category are added up as a total score. Thus, the highest score obtained on the questionnaire for one category is 50 (best cyber security practices implemented) and the lowest score is 10 (worst cyber security practices implemented). The data were statistically analysed using the PSPP programme. The independent sample t-test is used to compare the means of two independent groups (males and females) to determine whether there is statistical evidence that the associated population means are significantly different. It was used to test hypotheses.

4. Results and Discussions

Cronbach's alpha reliability coefficient was used to assess the reliability of the pilot test results (see Table 2). The alpha correlation coefficients for each aspect of the questionnaire ranged from 0.79 to 0.89. Therefore, all coefficients were significant indicating that the reliability of the questionnaire falls under the category of acceptable to good.

Table 2.
Reliability measurement of questionnaire items.

Cyber security categories	Number of items	Cronbach's alpha
Malware	10	0.87
Password usage	10	0.91
Phishing	10	0.79
Social engineering	10	0.89
Online scam	10	0.80

4.1. Malware

Data in Table 3 reveals that there is no significant gender difference in level of cyber security behaviour between males (M = 33.60, SD = 5.49) and females (M = 33.57, SD = 4.76) in the aspect of malware, t (205.00) = 0.05, p = 0.963. The mean score of the male participants was slightly higher than that of the female participants (M = 33.60 vs 33.57). The difference is not significant because the sig value is greater than 0.05 (sig. = 0.963). These results suggest that both genders have nearly the same level of cyber security behaviour in the aspect of malware. The results contradict the findings of a previous study conducted by McGill and Thompson [14] which revealed that females show significantly lower overall levels of security behaviour than males and stated that there were significant differences between females and males in whether they had installed security software such as anti-malware themselves [14]. The result is also inconsistent with the previous study conducted by Ameen, et al. [13] which revealed that there are significant gender differences in smartphone security behavioural intention among employees in international companies [13]. Based on our research, both genders have quite similar behaviour to protect themselves from malware which is to install anti-virus software, firewall and anti-spyware. 74.2% of males and 75.6% of females reported that they have installed anti-virus software, a firewall and anti-spyware because all young generations nowadays in Malaysia are exposed to the same education and hence the same level of knowledge regarding cyber security which leads them to develop the same level of cyber security behaviour against malware.

Table 3.
The t-test values for differences in levels of cyber security behaviour by gender in the aspect of malware.

Gender	Group statistics			Independent sample T-test	
	Number	Mean	S.D.	t-value	Sig. (2-tailed)
Male	98	33.60	5.49	0.05	0.963
Female	109	33.57	4.76		

4.2. Password Usage

Data in Table 4 reveals that there is no significant gender difference in level of cyber security behaviour between males (M = 33.46, SD = 5.79) and females (M = 33.25, SD = 5.96) in the aspect of password usage, t (205.00) = 0.26, p = 0.796. The mean score of the male participants was slightly higher than that of the female participants (M = 33.46 vs. 33.25). The difference is not significant because the p-value is greater than 0.05 (p-value = 0.796). These results suggest that both genders have nearly equal levels of cyber-security behaviour in the aspect of password usage. The results supported the null hypothesis which opposed the findings of a previous study conducted by Juozapavičius, et al. [22] in which several gender differences were found in the behaviour of password use [22]. The result is also inconsistent with the study conducted by Petrie and Merdenyan [23] which revealed that there are some differences in password behaviour between the genders [23]. Based on our research, we discovered that 83% of male respondents and 80.6% of female respondents created their passwords with more than 8 characters. There are around 80% of both male and female respondents who reported creating their passwords with more than 8 characters. We can see that most of the respondents from both genders are practicing good habits in password creation. Therefore, proving that gender does not play a role in affecting the level of cyber security behaviour in the aspect of password usage.

Table 4.
The values of the t-test for differences in the level of cyber security behaviour by gender in the aspect of password usage.

Gender	Group statistics			Independent sample T-test	
	Number	Mean	S.D.	t-value	Sig. (2-tailed)
Male	98	33.46	5.79	0.26	0.796
Female	109	33.25	5.96		

4.3. Phishing

The data in Table 5 reveal that there is no significant gender difference in the level of cyber security behaviour between men (M = 35.66, SD = 5.40) and females (M = 35.88, SD = 5.28) in the aspect of phishing, t (205.00) = -0.29, p = 0.770. The mean score of the male participants was slightly higher than that of the female participants (M = 35.66 vs 35.88). The difference is not significant because the p-value is greater than 0.05 (p-value = 0.770). These results suggest that both genders have nearly the same level of cyber security behaviour in the aspect of phishing. The results supported the null hypothesis which contradicts the findings of a previous study by McGill and Thompson [14] revealed that women show lower overall levels of security risk behaviour than men [14] and another study by Ngwane [35] revealed that there is a significant relationship between gender and phishing attack awareness [35]. This may be tied to knowledge of cyber security. Prior exposure to phishing education is associated with less susceptibility to phishing. Based on our research, nearly 50% of the respondents responded that they upgrade their phishing knowledge by reading phishing materials and 53.1% of females agreed with the question which is higher than males (45.9%). Thus, no significant difference is found in the level of cyber security behaviour between two genders in the aspect of phishing.

Table 5.
The t-test values for differences in levels of cyber security behaviour by gender in the aspect of phishing.

Gender	Group statistics			Independent sample T-test	
	Number	Mean	S.D.	t-value	Sig. (2-tailed)
Male	98	35.66	5.40	-0.29	0.770
Female	109	35.88	5.28		

4.4. Social Engineering

Data in Table 6 reveals that there is no significant gender difference in level of cyber security behaviour between males (M = 34.28, SD = 5.27) and females (M = 34.99, SD = 4.76) in the aspect of social engineering, t (205.00) = -1.03, p = 0.306. The mean score of the male participants was slightly higher than that of the female participants (M = 34.28 vs 34.99). The difference is not significant because the p-value is greater than 0.05 (p-value = 0.306). These results suggest that both genders have nearly the same level of cyber security behaviour in the aspect of social engineering. The results supported the null hypothesis which contradicts the findings of a previous study by Ngwane [35] who found significant relationships between gender and receiving and responding to online pop-up messages that seemed to be social engineering attacks [35]. This might be due to people's experience using information and communication technologies which makes them more capable of detecting online deception on social networks [57]. For example, it has been found that the more time elapsed since joining Facebook the more capable the users is of detecting social engineering attacks [58]. A study also showed that the more experienced the users of social networks, the less vulnerable they are to victimization by social engineering [36]. It is shown that internet users in Malaysia have increased to 88.7% in 2020 and the ratio between the two genders is close to a ratio of 1 to 1 based on a survey by the Malaysian Communication and Multimedia Commission (MCMC). Thus demonstrating that the level of cyber security conduct with respect to social engineering is unaffected by gender.

Table 6.
The values of the t-test for differences in the level of cyber security behaviour by gender in the aspect of social engineering.

Gender	Group statistics			Independent sample T-test	
	Number	Mean	S.D.	t-value	Sig. (2-tailed)
Male	98	34.28	5.27	-1.02	0.306
Female	109	34.99	4.76		

4.5. Online Scam

Data in Table 7 reveals that there is a significant gender difference in level of cyber security behaviour between males (M = 35.35, SD = 5.53) and females (M = 38.08, SD = 5.98) in the aspect of online scams, t (205.00) = -3.41, p = 0.001. The mean score of female participants was significantly higher than that of male participants (M = 38.08 vs. 35.35). The difference is significant because the p-value is less than 0.05 (p-value = 0.001). These results suggest that the female has a significantly higher level of cyber security behaviour compared to the male. Results supported the alternative hypothesis which complies with the findings of the previous study by Xu, et al. [52] who found significant differences in online scam rates between males and females which females having a lower rate of being scammed online (13.19%) compared to males (17.32%) [52]. The findings also show that women have a higher level of cyber security behaviour in the aspect of online scams.

Table 7.
The t-test values for differences in levels of cyber security behaviour by gender in the aspect of online scams.

Gender	Group statistics			Independent sample T-test	
	Number	Mean	S.D.	t-value	Sig. (2-tailed)
Male	98	35.35	5.53	-3.41	0.001
Female	109	38.08	5.98		

5. Conclusion

This research focuses on the cyber security behaviour of Malaysian young generations and helps cover the gaps in understanding if there is a significant difference in the level of cyber security behaviour between the two genders, male and female with respect to different aspects. The aspects included in the research are malware, password usage, phishing, social engineering, and online scams. Data was collected from a broad range of respondents which includes all young generations aged 15 - 30 years old in Malaysia. Findings reveal no significant differences between males and females for four aspects of cyber security which are malware, password usage, phishing and social engineering. However, a significant difference is found in the aspect of online scams in which the level of cyber security behaviour of female participants is significantly higher than that of male participants. These findings contribute to the behavioural cyber security field by considering a key individual difference which is gender in the aspects of malware, password usage, phishing, social engineering and online scam. The results may be relevant when designing security education, training and awareness initiatives for the broader community.

Researchers were insistent that all internet users should be educated about the necessity of good practices. Furthermore, the younger generations are active internet users. As a result, new generations must be educated on cyber-security problems. Although education and training would not eliminate the growing cyber security incidents, internet users must be trained to improve their knowledge of these incidents so that they can take precautionary measures when necessary. Users must be educated and trained with the knowledge of cyber security to protect themselves. This is crucial to reduce cybercrime in their future workspace and to protect the company's information [59].

There are many limitations that can influence the result of this research. Participants in the current study were from both east and west Malaysia and this study included Malaysian teenagers ranging in age from 15 to 30 years old. Future research will be needed to explore cyber security behaviour in other populations such as school students, employees at companies and institutions and other generations instead of the young generation. Future research could focus on investigating the differences in the level of other categories of cyber security behaviour based on different social status, races, background, income or educational levels. Besides, future studies should split samples between west and east Malaysia or additionally break west Malaysia into states. Furthermore, it would also be advantageous to conduct an experimental study with the objective of developing a program to help people in Malaysia improve their awareness level of cyber security and their behaviour and find out which solutions work best for each type of user for these problems. Finally, it would be worthwhile investigating the factors affecting the awareness level and behaviour of Malaysians.

References

[1] P. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 7, no. 11, pp. 125-128, 2018.

[2] MCMC, "MCMC.gov.my," Retrieved: https://www.mcmc.gov.my/en/media/press-clippings/isps-need-to-be-proactive. 2021.

[3] CyberSecurity Malaysia, ""CyberSecurity Malaysia: RM10m allocation under Budget 2023 for NSRC to help in 'war' against scammers," Malay Mail," Retrieved: https://www.malaymail.com/news/malaysia/2023/02/25/cybersecurity-malaysia-rm10m-allocation-under-budget-2023-for-nsrc-to-help-in-war-against-scammers/56655. 2023.

[4] A. Asia and P. Study, ""Mapping a secure path for the future of digital payments in APAC," Retrieved: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2021/10/12113257/Digital-Payment-Report_FINAL.pdf. 2021.

[5] S. M. Albladi and G. R. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-Centric Computing and Information Sciences,* vol. 8, no. 1, pp. 1-24, 2018. https://doi.org/10.1186/s13673-018-0128-7

[6] A. D. Beldad and S. M. Hegner, "More photos from me to thee: Factors influencing the intention to continue sharing personal photos on an online social networking (OSN) site among young adults in the Netherlands," *International Journal of Human–Computer Interaction,* vol. 33, no. 5, pp. 410-422, 2017. https://doi.org/10.1080/10447318.2016.1254890

[7] M. Christodorescu and S. Jha, "Testing malware detectors," *ACM SIGSOFT Software Engineering Notes,* vol. 29, no. 4, pp. 34-44, 2004. https://doi.org/10.1145/1013886.1007518

[8] G. McGraw and G. Morrisett, "Attacking malicious code: A report to the infosec research council," *IEEE Software,* vol. 17, no. 5, pp. 33-41, 2000. https://doi.org/10.1109/52.877857

[9] A. Vasudevan and R. Yerraballi, "Cobra: Fine-grained malware analysis using stealth localized-executions," *IEEE Symposium on Security and Privacy (S&P'06),* vol. 15 p. 279, 2006. https://doi.org/10.1109/SP.2006.9

[10] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—A state of the art survey," *ACM Computing Surveys (CSUR),* vol. 52, no. 5, pp. 1-48, 2019.

[11] A. Yavneh, R. Lothan, and D. Yamin, "Co-similar malware infection patterns as a predictor of future risk," *PloS One,* vol. 16, no. 3, p. e0249273, 2021. https://doi.org/10.1371/journal.pone.0249273

[12] F. L. Lévesque, J. M. Fernandez, and D. Batchelder, "Age and gender as independent risk factors for malware victimisation," *Electronic Visualisation and the Arts (EVA 2017),* pp. 1-14, 2017. https://doi.org/10.14236/ewic/hci2017.48

[13] N. Ameen, A. Tarhini, M. H. Shah, and N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Computers in Human Behavior,* vol. 104, p. 106184, 2020. https://doi.org/10.1016/j.chb.2019.106184

[14] T. McGill and N. Thompson, "Gender differences in information security perceptions and behaviour," presented at the In 29th Australasian Conference on Information Systems, 2018.

[15] C. Pelchen, D. Jaeger, F. Cheng, and C. Meinel, "The (Persistent) threat of weak passwords: Implementation of a semi-automatic password-cracking algorithm," presented at the In International Conference on Information Security Practice and Experience, Springer, Cham, 2019.

[16] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: Comprehensive review and analysis," *Complex & Intelligent Systems,* vol. 7, no. 5, pp. 2157-2177, 2021. https://doi.org/10.1007/s40747-021-00409-7

[17] S. Pearman *et al.*, "Let's go in for a closer look: Observing passwords in their natural habitat," in *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 295-310.

[18] A. Bakas, A. Wagner, S. Johnston, S. Kennison, and E. Chan-Tin, "Impact of personality types and matching messaging on password strength," *EAI Endorsed Transactions on Security and Safety,* vol. 8, no. 28, p. 170012, 2021. https://doi.org/10.4108/eai.1-6-2021.170012

[19] J. H. Huh, H. Kim, S. S. Rayala, R. B. Bobba, and K. Beznosov, "I'm too busy to reset my LinkedIn password: On the effectiveness of password reset emails," in *In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 387-391.

[20] Verizon, "Data breach investigation report 2021," Retrieved: https://www.verizon.com/business/resources/reports/dbir/2021/masters guide/introduction/. 2021.

[21] H. Habib *et al.*, "User behaviors and attitudes under password expiration policies," in *In Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, 2018, pp. 13-30.

[22] A. Juozapavičius, A. Brilingaitė, L. Bukauskas, and R. G. Lugo, "Age and gender impact on password hygiene," *Applied Sciences*, vol. 12, no. 2, p. 894, 2022. https://doi.org/10.3390/app12020894

[23] H. Petrie and B. Merdenyan, "Cultural and gender differences in password behav-iors: Evidence from china, turkey and the uk," in *In Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, 2016.

[24] K. Helkala and T. Hoddø Bakås, "Extended results of Norwegian password security survey," *Information Management & Computer Security,* vol. 22, no. 4, pp. 346-357, 2014. https://doi.org/10.1108/imcs-10-2013-0079

[25] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet,* vol. 12, no. 10, p. 168, 2020. https://doi.org/10.3390/fi12100168

[26] K. L. Chiew, C. L. Tan, K. Wong, K. S. Yong, and W. K. Tiong, "A new hybrid ensemble feature selection framework for machine learning-based phishing detection system," *Information Sciences,* vol. 484, pp. 153-166, 2019. https://doi.org/10.1016/j.ins.2019.01.064

[27] G. Garrett, "Cyberattacks skyrocketed in 2018. Are you ready for 2019? IndustryWeek," Retrieved: https://www.industryweek.com/technology-and-iiot/article/22026828/cyberattacks-skyrocketed-in-2018-areyou-ready-for-2019. 2018.

[28] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," *arXiv preprint arXiv:1908.05897,* 2019.

[29] M. Volkamer, K. Renaud, B. Reinheimer, and A. Kunz, "User experiences of torpedo: Tooltip-powered phishing email detection," *Computers & Security,* vol. 71, pp. 100-113, 2017. https://doi.org/10.1016/j.cose.2017.02.004

[30] A. Burns, M. E. Johnson, and D. D. Caputo, "Spear phishing in a barrel: Insights from a targeted phishing campaign," *Journal of Organizational Computing and Electronic Commerce,* vol. 29, no. 1, pp. 24-39, 2019. https://doi.org/10.1080/10919392.2019.1552745

[31] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare data breaches: Implications for digital forensic readiness," *Journal of Medical Systems,* vol. 43, no. 1, pp. 1-12, 2019. https://doi.org/10.1007/s10916-018-1123-2

[32] W. J. Gordon *et al.*, "Assessment of employee susceptibility to phishing attacks at US health care institutions," *JAMA Network Open,* vol. 2, no. 3, pp. e190393-e190393, 2019. https://doi.org/10.1001/jamanetworkopen.2019.0393

[33] S. Das, C. Nippert-Eng, and L. J. Camp, "Evaluating user susceptibility to phishing attacks," *Information & Computer Security,* vol. 30, no. 1, pp. 1-18, 2022. https://doi.org/10.1108/ics-12-2020-0204

[34] W. Li, J. Lee, J. Purl, F. Greitzer, B. Yousefi, and K. Laskey, "Experimental inves-tigation of demographic factors related to phishing susceptibility," in *In Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[35] H. N. Ngwane, "Gender responses towards online social engineering attacks amongst young adult students in South Africa," Doctoral Dissertation, 2019.

[36] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks," *Education and Information Technologies,* vol. 27, no. 4, pp. 4729-4752, 2021.

[37] S. Baki and R. M. Verma, "Sixteen years of phishing user studies: What have we learnt?," *IEEE Transactions on Dependable and Secure Computing,* vol. 20, no. 2, pp. 1200-1212, 2022.

[38] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access,* vol. 9, pp. 11895-11910, 2021. https://doi.org/10.1109/access.2021.3051633

[39] M. A. Chargo, "You've been hacked: How to better incentivize corporations to protect consumers' data," *Transactions: The Tennessee Journal of Business Law*, vol. 20, no. 1, p. 115, 2018.

[40] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019. https://doi.org/10.3390/fi11040089

[41] I. A. M. Abass, "Social engineering threat and defense: A literature survey," *Journal of Information Security*, vol. 9, no. 04, pp. 257-264, 2018. https://doi.org/10.4236/jis.2018.94018

[42] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber security behaviour among higher ed-ucation students in Malaysia," *Journal of Information Assurance & Cybersecurity*, pp. 1-13, 2017. https://doi.org/10.5171/2017.800299

[43] S. M. Albladi and G. R. Weir, "Predicting individuals' vulnerability to social engineering in social networks," *Cybersecurity*, vol. 3, no. 1, pp. 1-19, 2020. https://doi.org/10.1186/s42400-020-00047-5

[44] G. Saridakis, V. Benson, J.-N. Ezingeard, and H. Tennakoon, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technological Forecasting and Social Change*, vol. 102, pp. 320-330, 2016. https://doi.org/10.1016/j.techfore.2015.08.012

[45] A. Saberi, M. Vahidi, and B. M. Bidgoli, "Learn to detect phishing scams using learning and ensemble? methods," presented at the In 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology-Workshops, IEEE, 2007.

[46] M. Button, C. Lewis, and J. Tapley, *Fraud typologies and the victims of fraud: Literature review*. London, England: National Fraud Authority, 2009.

[47] M. T. Whitty, "Predicting susceptibility to cyber-fraud victimhood," *Journal of Financial Crime*, vol. 26, no. 1, pp. 277-292, 2019. https://doi.org/10.1108/jfc-10-2017-0095

[48] H. Chen, C. E. Beaudoin, and T. Hong, "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors," *Computers in Human Behavior*, vol. 70, pp. 291-302, 2017. https://doi.org/10.1016/j.chb.2017.01.003

[49] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing," *Online Information Review*, vol. 40, no. 2, pp. 265-281, 2016. https://doi.org/10.1108/oir-04-2015-0106

[50] R. A. Judges, S. N. Gallant, L. Yang, and K. Lee, "The role of cognition, personality, and trust in fraud victimization in older adults," *Frontiers in Psychology*, vol. 8, p. 588, 2017. https://doi.org/10.3389/fpsyg.2017.00588

[51] D. Modic, R. Anderson, and J. Palomäki, "We will make you like our research: The development of a susceptibility-to-persuasion scale," *PloS One*, vol. 13, no. 3, p. e0194119, 2018.

[52] Z. Xu, X. Miao, H. Wei, J. He, and Q. Xiu, "Research on measures of prevention against network telecommunication fraud in a university," presented at the In 4th International Seminar on Edu-cation Research and Social Science (ISERSS 2021), Atlantis Press, 2022.

[53] M. T. Whitty, "Is there a scam for everyone? Psychologically profiling cyberscam victims," *European Journal on Criminal Policy and Research*, vol. 26, no. 3, pp. 399-409, 2020. https://doi.org/10.1007/s10610-020-09458-z

[54] J. Onaolapo, N. Leontiadis, D. Magka, and G. Stringhini, "{SocialHEISTing}: Understanding Stolen Facebook accounts," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 4115-4132.

[55] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "Automatically dismantling online dating fraud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1128-1137, 2019. https://doi.org/10.1109/tifs.2019.2930479

[56] W. N. H. W. Jusoh and N. M. S. Nizar, "Online scams awareness among Muslim university students in Malaysia," *Journal of Islamic*, vol. 7, no. 43, 2022.

[57] M. Tsikerdekis and S. Zeadally, "Online deception on social media," *Communications of the ACM*, vol. 57, no. 9, pp. 72-80, 2014.

[58] A. Algarni, Y. Xu, and T. Chan, "An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook," *European Journal of Information Systems*, vol. 26, no. 6, pp. 661-687, 2017. https://doi.org/10.1057/s41303-017-0057-y

[59] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks," *Information*, vol. 13, no. 413, 2022. https://doi.org/10.3390/info13090413