FACTORS AFFECTING AWARENESS OF PHISHING AMONG GENERATION Y

Nur Farhana Mohd Zaharon[1], Mazurina Mohd Ali[2*] and Suhaily Hasnan[2]

[1]KYC Operations Analyst, Citigroup Transaction Services (M) Sdn. Bhd., Kuala Lumpur, Malaysia
[2]Faculty of Accountancy,
Universiti Teknologi MARA Selangor, Puncak Alam Campus, Malaysia

ABSTRACT

The purpose of this study was to determine the factors affecting awareness of phishing among Generation Y in Malaysia. Specifically, this study identified three factors that may influence awareness of phishing by applying the Theory of Technology Threat Avoidance. The factors are social engineering, anti-phishing knowledge, and security concern. Data was collected through a questionnaire survey. This study found that all the factors significantly influenced awareness of phishing among Generation Y in Malaysia. The findings of this study provide a further understanding of the factors that affect awareness of phishing. This study would benefit the public, especially Generation Y, the government, and all types of businesses, including financial institutions, by raising awareness of phishing and reducing phishing attacks.

Keywords: phishing, Generation Y, social engineering, anti-phishing knowledge, security concern

ARTICLE INFO

Article History:
Received: 12 April 2021
Accepted: 14 July 2021
Published: 31 August 2021

* Corresponding Author: Mazurina Mohd Ali. E-mail: mazurina@uitm.edu.my

INTRODUCTION

The rapid growth in internet technology has made society dependent on it. However, its evolution has also increased cyber fraud, thus, becoming a severe problem worldwide (Kamruzzaman, Islam, Islam, Hossain, & Hakim, 2016). Cyber fraud involves usage of internet services with internet access (Zahari, Billu, & Said, 2017). Examples of cyber fraud are phishing, scam, hacking, and data breach. Due to the high dependency on the internet, people have become ignorant about transparency of their information. This ignorance allows cybercriminals to trap victims easily. Also, cybercriminals use human psychology, known as social engineering, to deceive their victims. Krombholz, Hobel, Huber, and Weippl (2014) stated that social engineering is the human psychology used to manipulate individuals to provide confidential or personal information for fraudulent purposes. Human psychology is one of the reasons why society tends to be exposed to phishing attacks.

Phishing is a cyber fraud where the fraudsters deceive individuals into providing sensitive data, such as personal information, banking and credit card details, and passwords (Katkuri, 2018). The phishers usually contact the victims via e-mail, telephone, or text messages, and it could cause financial loss. The Anti-Phishing Working Group (APWG) confirmed that the phishing attack numbers have increased to 1,220,523 cases since 2016, and it is the highest number reached since 2004 (Rao & Pais, 2019). Based on Ernst and Young's 2018 - 2019 Global Information Survey, phishing is the top cyber fraud in organizations, with 22% of the cases reported. It shows that phishing is one of the most dangerous cyber threats in the world.

Yau, Lau, Chua, Ling, Iranmanesh, and Kwa (2016) stated that the Malaysian government planned to transform Kuala Lumpur into a metropolitan and smart city compared to other states in Malaysia. The 'smart city' surrounds technological advancement and opportunities, modern transportation, communication infrastructure, high quality of life, and wise management of natural resources and overall cost. The Malaysian government also aimed to enable Greater Kuala Lumpur to become one of the top 20 most liveable cities globally and increase its gross national income per capita to more than RM 48,000 by 2020. These plans show that Kuala Lumpur has a massive exposure to communication and technology

advancements with many internet connection facilities and technical devices, such as laptops, smartphones, and desktop computers. Hence, this situation will increase the exposure to phishing attempts.

Based on the statistics from the Department of Statistics Malaysia, Kuala Lumpur's population was estimated at around 1.78 million people in 2019, consisting of 0.92 million males and 0.82 million females. From these statistics, 41% of Kuala Lumpur's population (729,800 people) were around 25 to 41 years old (Department of Statistics Malaysia, 2019). The age range of Generation Y raises many debates. However, many studies have accepted that Generation Y is the group of people born between 1978 and 1994. Therefore, as of 2020, the age of the Generation Y population is between 26 to 42 years old. Generation Y is the largest segment of Malaysia's population, comprising active internet users who are highly dependent on complex technology and willing to accept new technologies (San, Omar, & Thurasamy, 2015). Kuala Lumpur was chosen in this study to determine the factors affecting awareness of phishing among people in Generation Y due to the robust development of technology in Kuala Lumpur which can lead to a high exposure to phishing attempts, and also because a high proportion of Generation Y live in this city.

Many phishing incidents have happened in the country. For example, in November 2019, a hairdresser lost RM 14,900 through a phone call with a person who claimed that he was from the Melaka court and accused the hairdresser of being involved in money laundering. Later, the phone call was purportedly passed to a Melaka policeman before being transferred to an anti-money laundering officer (Rahim, 2019). The hairdresser claimed that he believed that the fraudster was calling from the police station as he heard people being busy at work in an office. The hairdresser also believed the fake officer because he had lost his identification card five years ago and thought that his identification card had been misused.

The scope of this study was to determine the factors affecting awareness of phishing among Generation Y. Generation Y, also known as Millennials, is the generation generally influenced by technology, social media, digital media development, and the internet (Naumovska, 2017). This influence heightens the exposure of Generation Y to phishing attacks. One factor contributing to the level of awareness of phishing among the

Generation Y in Kuala Lumpur is social engineering, which is the tactic that fraudsters use to deceive their victims by exploiting human psychology. The other factors contributing to awareness of phishing among Generation Y are anti-phishing knowledge and security concerns.

The main objectives of this study were: i) to determine the effect of social engineering influence on awareness of phishing among Generation Y in Kuala Lumpur; ii) to assess the impact of anti-phishing knowledge on awareness of phishing among Generation Y in Kuala Lumpur, and iii) to determine the effect of security concerns on awareness of phishing among Generation Y in Kuala Lumpur.

The structure of the paper is as follows. The following section is the review of literature which includes the underlying theory and research framework. The next section presents hypotheses development, research method and design, and discusses the results of this study. The final section concludes the paper.

LITERATURE REVIEW

There are many types of phishing attacks. Examples of phishing attacks are e-mail spoofing, spear phishing, and whaling. A spoofing e-mail is an e-mail message created with a bogus sender's address. The content of the e-mail tricks the victims into opening the e-mail (Gupta, Singhal, & Kapoor, 2016). E-mail spoofing usually attacks random users (Chaudhry, Chaudhry, & Rittenhouse, 2016), while spear phishing targets specific individuals or groups via e-mail. A whaling attack aims to steal money or high-level officers' sensitive data for illegal purposes via e-mail (Chaudhry et al., 2016).

The other phishing attack is SMS phishing or SMiShing, which uses short messaging services (SMS) or text messages on mobile phones. SMiShing usually attacks the victims by sending text messages that impersonate sources such as bankers, system administrators, and law enforcement agencies. They will ask their victims to give information to them (Boateng & Amanor, 2014). Other than SMiShing, vishing is a type of phishing attack via phone calls. Another phishing attack is search engine phishing, a type of phishing attack using fake web pages. The fraudster

will create fake web pages that offer cheap products and incredible deals. The web pages are very similar to the original web pages (Suganya, 2016).

Phishing attacks will harm individuals, society, and the country. One of the effects is monetary loss to individuals, society, and the economy. Besides money, financial losses also include theft of valuable and sensitive information of customers, stakeholders, and organizations (Kamruzzaman et al., 2016). In addition, phishing attacks can reduce stakeholders' and consumers' trust in online activities. They can also damage the brand reputation of an organization.

Technology Threat Avoidance Theory

Arachchilage and Love (2014) stated that the Technology Threat Avoidance theory is the theory that explains how and why individual information technology (IT) users engage to avoid technological threats (such as phishing attacks). The model in Figure 1 below describes the idea of this theory. The model shows that one behaviour of IT users that influences avoidance motivation is perceived threat. This model indicates that perceived threat is influenced by perceived severity and perceived susceptibility. In this study, perceived threat is related to social engineering as the victims are aware of any vulnerability or harm from social engineering in a phishing attack. Other than that, safeguard effectiveness refers to the IT users' efforts to protect themselves from malicious IT threats. Therefore, the results of this study can be directed to aid individuals to avoid phishing attacks by educating themselves about anti-phishing.

The model also shows that the combination of the perceived threat and safeguard effectiveness also influences IT users' avoidance motivation. Furthermore, safeguard cost is the effort and payback required in using safeguard effectiveness, which is not covered in this study. Besides, self-efficacy refers to the ability or the action of people to succeed in a specific situation. This study relates to the knowledge and confidence of IT users to avoid phishing attacks and take measures to protect themselves. Safeguard will occur when IT users are knowledgeable about anti-phishing. In this scenario, they would be more concerned about the security of their data. IT users would usually install and upgrade their anti-virus or use strong passwords to enhance security.

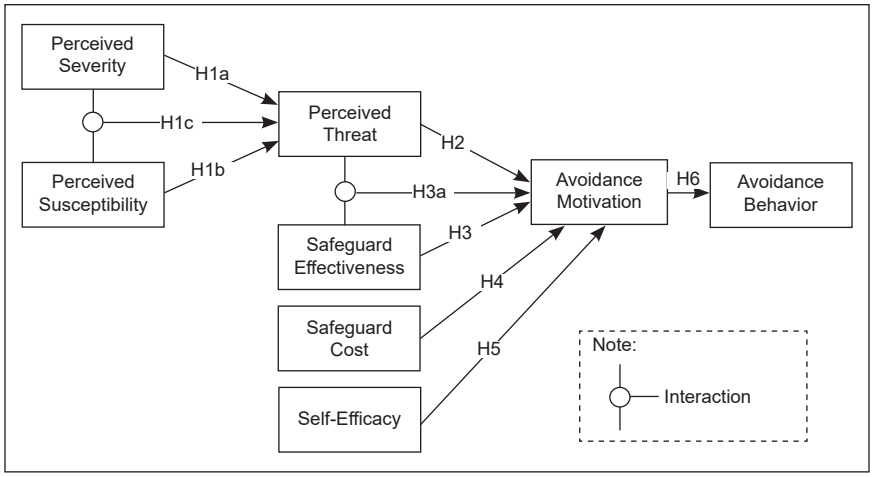

Figure 1: Technology Threat Avoidance Theory
(*Source*: Arachchilage and Love, 2014)

Research Framework

This study aimed to determine whether social engineering, anti-phishing knowledge, and security concerns influence awareness of phishing among Generation Y in Kuala Lumpur, Malaysia. Figure 2 gives a diagrammatic representation of the theoretical framework in which this empirical study was designed. This framework depicts the relationships between the dependent and independent variables. The hypotheses of this study were developed based on this research framework.

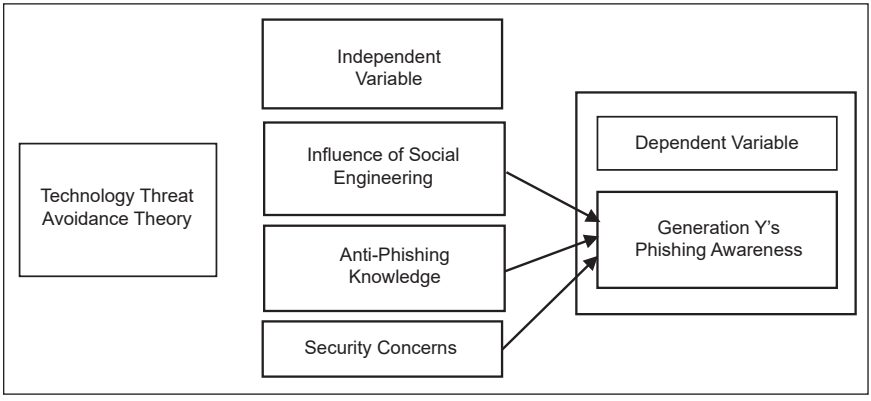

Figure 2: Research Framework

HYPOTHESES DEVELOPMENT

Social Engineering and Phishing Awareness

One of the factors affecting awareness of phishing is the influence of social engineering. Fraudsters would take this opportunity to deceive their victims by using social engineering techniques. For example, fraudsters would use human psychology and interactions to gain trust from their victims. They would convince the victims to give their personal and confidential information and money using persuasion (Ferreiraa & Telesa, 2019). 'Persuasion' is defined as a human communication process that aims to change a person's behavior, beliefs, or values towards events, ideas, objects, and other people by using spoken words, writing, or visual tools to convey information and feelings. Ferreiraa and Telesa (2019) also stated that there are five principles of persuasion in social engineering. The first principle is authority, where the fraudsters would pretend to be from authoritative agencies. In our social life, society is trained to follow the rules and not challenge and question authority. This situation gives the fraudsters a chance to pretend to be an authority. They know society would obey them and feel fear after receiving calls or messages from the authorities. The second principle is social proof. People tend to copy the actions of other people to undertake a behaviour in each situation. Fraudsters take this opportunity to convince their victims by saying other people are doing the same thing, and the victims are not solely responsible for their actions. For example, a fraud e-mail about winning attractive vacation prizes sent to the victims and e-mail would state that other people have also won the vacation prizes and enjoyed their vacation. However, the e-mail is fake, and no one has won the awards.

The third principle of persuasion in social engineering is similarity, liking, and deception. This principle is related to how people interact socially when they try to connect with others by finding more agreeable and similar characteristics. People tend to believe in what others do or say unless they suspect something is wrong or that some behaviour is wholly unexpected or manipulated. For example, the fraudsters would create a bogus shopping website and an e-mail similar to real websites and e-mails to attract victims.

The fourth principle of persuasion in social engineering is distraction. This situation happens when people are very focused on gains, losses, or needs, and there are some restrictions or limited time for the items offered. People would tend to take fewer considerations to think wisely before making decisions. For example, a bogus e-mail sent to the victims would mention that the victims had won giant lottery prizes. In this case, the victims are focused on the amount of money and would give their details, such as bank account and password, without thinking wisely. However, the lottery prizes are fake. Since the fraudsters had obtained the victims' information, they would steal the victims' money. Other than that, Lawson, Pearson, Crowson, and Mayhorn (2020), in their study, gave the example of fraudsters creating a sense of urgency, mentioning that the account would be closed within the next 24 hours to distract the victims, as shown in Figure 3.


Subject: Re-Validate Your School Mail Box

I.T HELP-DESK

----------Re-Validate-

<< Click Here>>

NOTE: That Failure to comply may result in the loss of your account within the next 24 hours.

Signed By Webmaster.
Maintained by the Technology Department. Copyright 2014.

Figure 3: Example of Phishing E-mail Utilizing the Distraction Principle

The fifth principle is commitment, integrity, and reciprocation. This principle is where people would respond as it is related to their dedication and needs. Fraudsters would take advantage of their victims' commitment and needs and make offers to attract them. For example, the fraudsters would send an e-mail about house offer prices to the victims. Since they know their victims are looking for a house to buy, they would ask their victims to lend some money to secure the house. They would deceive the victims by saying it is a limited-time offer, and the victims need to send the money immediately.

Parsons, Butavicius, Delfabbroa, and Lilliea (2019), in their study, agreed that people are heavily influenced by one of the social engineering principles, which is a distraction in the phishing e-mail. People are taking

less precautions to recognize and think wisely as the e-mail appeals for urgent actions. On the other hand, Muniandy, Muniandy, and Samsudin (2016), in their study on higher education students in Malaysia, stated that most students are not checking the authorization or identity of the person who speaks as an authority while receiving the calls. Muniandy et al. (2016) focused on the cybersecurity behaviour of Malaysian higher education students on malware, password usage, and social engineering. Moreover, Kamruzzaman et al. (2016) stated that most people were victimized by false jobs or task opportunities and trapped by monetary profits or rewards. They were too excited or attracted to the advertisement given. These studies showed that fraudsters use human psychology to deceive their victims and gain profit from it. They also showed how social engineering traps the victims in phishing attempts.

Apart from the above, fraudsters would also use human psychology to create urgency, fear, or excitement in their victims to deceive them into providing confidential information. Kennedy and Parsons (2012, 2014), Atkins and Huang (2013), Krombholz et al. (2014), Kamruzzaman et al. (2016), Muniandy et al. (2016), and Parsons et al. (2019) indicated that the influence of social engineering has a destructive impact on the level of awareness of phishing. People tending not to be influenced by fraudsters' social engineering methods shows a high level of awareness of phishing.

Based on the previous studies conducted outside Malaysia and one study conducted in Malaysia that focused on higher education students, this study focused on Generation Y because they are comfortable using digital technologies and robust technology development.

Accordingly, the study proposed the following hypothesis:

H_1: There is a negative relationship between social engineering influence and level of awareness of phishing among Generation Y in Kuala Lumpur.

Anti-phishing Knowledge and Phishing Awareness

New sophisticated phishing attacks are being developed all the time, and phishing attacks continue to rise every year. Individuals and organizations need to educate themselves and become more knowledgeable

about strategies and skills relating to computer security to minimize phishing threats (Verkijika, 2019). Most people nowadays rely more on mobile devices, such as smartphones and tablets, in daily life, giving fraudsters a chance to exploit the technological systems. Therefore, people need to know more about phishing. Arachchilage and Love (2014) discovered that anti-phishing knowledge and education positively affect computer users to mitigate phishing attacks. They would take safety measures to avoid phishing threats. It showed that a high level of computer users' knowledge would increase users' confidence in taking relevant actions to prevent phishing threats. It is also supported by Verkijika (2019), in which education on security awareness enhances users' security threat avoidance. It shows that it is essential for people to improve their knowledge of phishing. Gavett, Zhao, John, Bussell, Roberts, and Yue (2017) stated that young adults aged 18 to 44 are more susceptible to phishing than older adults. They are less suspicious of phishing attempts as they tend to trust IT security without taking self-precautions. Unlike younger adults, the older adults aged 50 years old and above have prior knowledge of phishing and personal experience of being victimized by phishing attempts, thus making them more cautious.

Previous studies had shown that many people, especially youngsters, lack awareness of gaining knowledge about phishing. Bose and Leung (2008), Arachchilage and Love (2014), Sun and Chen (2016), Gavett et al. (2017), Baral and Arachchilage (2019), Verkijika (2019), and Jampen, Gür, Sutter, and Tellenbach (2020) indicated that anti-phishing knowledge would increase the level of awareness of phishing. It is imperative to understand that phishing attempts target everyone regardless of age, gender, or background, and new phishing scams are being developed all the time. Fraudsters would enhance their skills and techniques to deceive victims. Nonetheless, many people still ignore the risks of using digital devices despite the high-risk exposure to cybercrime, especially phishing.

Accordingly, the study proposed the following hypothesis:

H_2: There is a positive relationship between anti-phishing knowledge and level of awareness of phishing among Generation Y in Kuala Lumpur.

Security Concern and Phishing Awareness

Security concern is one indicator used to examine users' attitudes on awareness of phishing. It is a condition or practice that can cause a threat, vulnerability, or loss, or the extent of the user's belief that the procedures are secured (Topaloglu, 2012). In this scenario, the application of cybersecurity safeguards, such as ensuring proper credentials, could help avoid security concerns in phishing.

Chhikara, Dahiya, Garg, and Rani (2013) and Verkijika (2019) agreed that good quality anti-virus could prevent people from being victims of phishing. Furthermore, Muniandy et al. (2016) found out that there is low awareness of protection against malware threats, where they are not scanning removable drives before using it on personal computers. Other than that, for password usage, Verkijika (2019) and Huang, Ma, and Chen (2011) stated that better password behaviors could prevent phishing attacks. However, Muniandy et al. (2016) asserted that there is low awareness of password usage among higher education students in Malaysia. Their passwords do not consist of lowercase, uppercase, numbers, and special characters, and they never change their passwords. Most of them even agreed to use their personal information in their passwords. This habit would expose them to phishing.

Previous studies have shown that many people are still ignoring the security of their information. Installing and updating anti-virus software, changing passwords regularly, and using strong passwords are very important to secure information. Using solid password credentials that consist of lowercase, uppercase, numbers, and special characters would make it complicated for fraudsters to quickly access and control digital devices (Kennedy, Chiasson, & Oorschot, 2016). Furthermore, by changing passwords regularly, fraudsters would have difficulty accessing the accounts (Kennedy et al., 2016); fraudsters would usually try to access the accounts more than once over some time. Installing and updating the anti-virus software can protect and secure the stored data, files, and the digital device. Not applying all of these security concerns gives fraudsters a high opportunity to steal information from victims.

Accordingly, the study proposed the following hypothesis:

H_3: There is a positive relationship between security concerns and level of awareness of phishing among Generation Y in Kuala Lumpur.

RESEARCH METHOD AND DESIGN

Sample Selection

This study used a non-random sampling method, where the sample units were gathered from selected people in the population. This study sample was Generation Y in Kuala Lumpur, the group of people born between 1978 and 1994 and aged around 26 to 42 years old in 2020. Generation Y is the highest population in Kuala Lumpur and is generally influenced by technology, social media, digital media development, and the internet (Naumovska, 2017). Kuala Lumpur was chosen since it is one of the smart cities in Malaysia, where all technologies are developed (Yau et al., 2016).

As discussed in Section 1, Kuala Lumpur's population in 2019 was estimated at around 1.78 million people. Forty-one percent (41%) of the population was around 26 to 42 years old in 2020. Therefore, the sampling frame for this study was 729,800 Generation Y individuals. In this study, reference was made to the Krejcie and Morgan (1970) table of sample sizes shown in Table 1 to determine the sample size. Based on the table, the sample size to be selected would be for population size (N) of between 75,000 and 1,000,000. The sample size of 384 respondents for 1,000,000 population with an error of 5% should be more than sufficient for this study. Contact details of the potential respondents whose ages were known were collected from friends, colleagues, employees, and other contacts. Since the total number of contactable individuals who met the sampling criteria came to 500, it was decided to expand the sample size to 500. According to Baruch and Holtom (2008), the average response rate for data collected from individuals is 52.7%. Therefore, the bigger sample size was also an attempt at improving the number of responses for this study to enable the results to be more generalizable to the population.

Table 1: A Sample Size of a Known Population

Table for Determining Sample Size of a Known Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

Note: N is Population Size; S is Sample Size *Source: Krejcie & Morgan, 1970*

(*Source:* Krejcie and Morgan, 1970)

Research Instrument and Measurement

This study used a questionnaire as its data collection instrument. The questionnaire was divided into five sections. The first section was the respondents' demographics, such as age, gender, marital status, and occupation. The second section was on the dependent variable, Generation Y's awareness of phishing. The third to fifth sections were for the three independent variables: influence of social engineering, anti-phishing knowledge, and security concern, respectively. These sections used the 5-point Likert scale: '1' strongly disagree, '2' disagree, '3' neutral, '4' agree, and '5' strongly agree. The variables and their measurement intervals were based on previous studies. Table 2 shows a summary of the variables and measuring scales.

Table 2: Summary of the Measurement of the Research Variables

Variable	Previous research adapted	Measurement
Dependent variable, Phishing Awareness of Generation Y in Kuala Lumpur	Muniandy et al. (2016).	Interval 5-point Likert scale. 1 - Strongly Disagree 2 - Disagree 3 - Neutral 4 - Agree 5 - Strongly Agree
First Independent Variable, Influence of Social Engineering	Muniandy et al. (2016)	Interval 5-point Likert scale. 1 - Strongly Disagree 2 - Disagree 3 - Neutral 4 - Agree 5 - Strongly Agree
Second Independent Variable, Anti-Phishing Knowledge	Muniandy et al. (2016) Arachchilage and Love (2014)	Interval 5-point Likert scale. 1 - Strongly Disagree 2 - Disagree 3 - Neutral 4 - Agree 5 - Strongly Agree
Third Independent Variable, Security Concern	Muniandy et al. (2016) Verkijika (2019)	Interval 5-point Likert scale. 1 - Strongly Disagree 2 - Disagree 3 - Neutral 4 - Agree 5 - Strongly Agree

Data Collection

The questionnaire was designed in Google Form. The links to the questionnaire were distributed to the 500 Generation Y individuals in the sample via WhatsApp, Facebook, Twitter, and Instagram.

The respondents were required to state their age in the questionnaire to ensure the validity of the response. The respondents must be between 26 to 42 years old in 2020 for their responses to be valid. All the respondents who answered the questionnaires informed the researchers after they had answered them. The number of responses received within the collection period of two months was 391, resulting in a response rate of 78.2%. This rate exceeded the average rate of 52.7% for data collected from individuals mentioned by Baruch and Holtom (2008). The number of responses also

exceeded the maximum sample size of 384 for this study, as suggested by Krejcie and Morgan's (1970) table of sample sizes shown in Table 1. Hence, it was decided to use all 391 responses for further analysis. Furthermore, all the responses were valid since they had no missing values. Thus, after all the data were collected, they were analyzed using the SPSS software.

RESULTS AND DISCUSSION

Demographic Analysis

Demographic analysis was used to identify the frequency and percentage of age, gender, marital status, education, and occupation of the respondents. The results of the demographic analysis are shown in Table 3.

Table 3: Results of Demographic Analysis

Variables		Frequency	Percent
Age	26 to 29 years old	210	53.7
	30 to 33 years old	70	17.9
	34 to 37 years old	38	9.7
	38 to 42 years old	73	18.7
	Total	391	100.0
Gender	Female	287	73.4
	Male	104	26.6
	Total	391	100.0
Marital Status	Single	236	60.4
	Married	153	39.1
	Divorced	2	0.5
	Total	391	100.0
Education	SPM	19	4.9
	STPM	2	0.5
	Diploma	66	16.9
	Bachelor's Degree	255	65.2
	Master	42	10.7
	PhD	4	1.0

Variables		Frequency	Percent
	International Certificate	3	0.8
	Total	391	100.0
Occupation	Private	267	68.3
	Government	79	20.2
	Self-Employed	45	11.5
	Total	391	100.0

Table 3 shows that the respondents were the Generation Y group since they were between 26 and 42 years old in 2020, indicating that they were born between 1978 and 1994. The age group was divided into four: 26 to 29 years old (53.7% of the respondents), 30 to 33 years old (17.9%), 34 to 37 years old (9.7%), and 38 to 42 years old (18.7%) Furthermore, 287 of the Generation Y respondents (73.4%) were females, while another 104 (26.6%) were males. There were 236 respondents (60.4%) who were single, 153 respondents (39.1%) were married, and 2 respondents (0.5%) were divorced.

Other than that, 255 respondents (65.2%) possessed a bachelor's degree. There were 66 respondents (16.9%) with a Diploma, 42 respondents (10.7%) had a Master's degree, 19 (4.9%) possess the Sijil Pelajaran Malaysia (SPM), 4 (1.0%) with a PhD, 3 (0.8%) had an International Certificate, and 2 (0.5%) possessed the Sijil Tinggi Pelajaran Malaysia (STPM). Concerning occupation, 267 respondents (68.3%) worked in the private sector, followed by 79 respondents (20.2%) working in the government sector, and 45 (11.5%) were self-employed.

Descriptive Analysis

Table 4 presents the results of the descriptive statistics for the variables of this study.

Table 4: Descriptive Statistics of the Dependent and Independent Variables

Variables		N	Mean	Standard Deviation (SD)
Dependent Variable Phishing Awareness	I know phishing is a cyber fraud, where the fraudster steals the users' sensitive data, such as username, passwords, and bank and credit card details.	391	4.59	0.739
	I know phishing usually threatens people through SMS, phone calls, online websites, and e-mails.	391	4.65	0.676
	I have read materials about phishing on bank websites, the internet, or social media.	391	4.29	0.868
	I would immediately report to the banks when there is a suspicious transaction.	391	4.51	0.856
	I know I can report to the Malaysian Communications and Multimedia Commission (MCMC) whenever I encounter any phishing e-mails or sites.	391	3.68	1.320
	I know phishing would lead to money losses, damage society, and ruin economic growth.	391	4.71	0.517
Overall			4.405	0.8293
First Independent Variable Influence of Social Engineering	I would panic and follow the instruction given by the people who speak as an authority, such as police officers or MACC, through phone calls, SMS, or e-mails.	391	2.21	1.270
	I would trust any offer or advertisements when many people have used, applied, and proven their success.	391	2.47	1.316
	I would reply to the messages announcing something urgent, such as getting a warrant from the authority or a family emergency.	391	1.93	1.223
	I would reply to the e-mails or messages announcing something exciting, such as winning vast sums of money.	391	1.42	0.867
	I would deposit money to strangers when requested.	391	1.20	0.604
Overall			1.846	1.056
Second Independent Variable Anti-Phishing Knowledge	I think the URL must be "https" when transmitting confidential information	391	3.59	1.126

Variables		N	Mean	Standard Deviation (SD)
	The padlock symbol is a must to transmit sensitive information.	391	3.96	0.981
	I prefer to type the URL in a new browser rather than clicking it on hyperlinks.	391	3.70	1.166
	I would check the URL spelling before doing any type of transaction or entering confidential information.	391	3.91	1.116
	I would check the sentence structure, grammar, and spelling of the e-mails or websites before doing any transactions or entering confidential information.	391	4.00	1.094
	I would check the logo's design and contact information on the e-mails or websites before doing any type of transaction or entering confidential information.	391	3.97	1.087
	I would be extra cautious when an external e-mail is sent in my office e-mail, as most e-mail scams begin with messages from an external e-mail system.	391	4.33	0.904
Overall			3.923	1.0677
Third Independent Variable Security Concern	I would scan all removable drives before using them on my computer.	391	3.88	1.032
	I install anti-virus software on my devices.	391	4.12	1.004
	I always update the anti-virus software on my devices.	391	4.00	1.062
	I would not easily download any freeware on the internet.	391	4.09	1.073
	I would ensure that my passwords consist of lowercase, uppercase, numbers, and special characters.	391	4.42	0.846
	I would ensure that my passwords have eight or more characters.	391	4.45	0.811
	I would use different passwords for different applications.	391	3.48	1.320
	I always change my passwords when required.	391	4.09	1.111
Overall			4.067	1.0324

As shown in Table 4, the dependent variable items sought to identify the level of awareness of phishing among the respondents. The results show that most respondents know that phishing is a cyber fraud where fraudsters steal users' sensitive data, such as username, passwords, and bank and credit card details (Mean: 4.59, SD: 0.739). Most of them know that phishing usually threatens people through SMS, phone calls, online websites, and e-mails (Mean: 4.65, SD: 0.676). These two items reflect the basic knowledge of phishing. Furthermore, most respondents have read materials about phishing on bank websites, the internet, or social media (Mean: 4.29, SD: 0.868).

Based on the Malaysian Communication and Multimedia Commission's (MCMC) website, most of the phishing attacks in Malaysia target internet banking users, where the fraudsters deceive the victims into revealing their sensitive information. This study showed that the respondents would immediately report to the banks when there is a suspicious transaction (Mean: 4.51, SD: 0.856). In addition, most of the respondents knew that phishing would lead to loss of money, damage society, and ruin economic growth. This item had the highest mean (Mean: 4.71, SD: 0.517). The respondents also knew that they could report to the MCMC whenever they encounter phishing e-mails or sites. However, this item had the lowest mean (Mean: 3.68, SD: 1.320). The overall mean was 4.405 with a SD of 0.8293, indicating a high level of awareness of phishing among Generation Y in Kuala Lumpur.

The items for the first independent variable sought to identify level of knowledge about fraudster social engineering techniques or influences among the Generation Y. The five items in Table 4 focused on the social engineering used by fraudsters to threaten victims by applying the five principles of social engineering. The first principle was authority, the second was social proof, and the third was similarity, liking, and deception. The fourth principle was distraction, and the fifth was commitment, integrity, and reciprocation (Ferreiraa & Telesa, 2019). The respondents were not supposed to be influenced by social engineering techniques used by fraudsters. The overall mean should be near 0 to indicate a lower influence of social engineering techniques.

One of the social engineering principles used by fraudsters is pretending to be an authority. The results showed that fewer respondents

would feel panic and follow the instructions given by the people who speak as an authority (Mean: 2.21, SD: 1.270). Furthermore, fewer respondents trusted any offer or advertisements where many people have applied and proven their success (Mean: 2.47, SD: 1.316). This item is an example of social proof used fraudsters. The fraudsters would also create fake e-mails and websites to catch victims' attention. Additionally, fraudsters would use distraction by creating a sense of excitement, urgency, and panic. However, as shown in the results in Table 4, fewer respondents would reply to messages announcing some urgencies, such as warrants from the authorities and family emergency (Mean: 1.93, SD: 1.223). Fewer would also respond to e-mails or messages promoting something exciting, such as winning vast sums of money (Mean: 1.42, SD: 0.867).

Apart from the above techniques, fraudsters would also take advantage of people's generosity, commitment, and integrity to deceive the victims into lending them money. Some fraudsters imitate charity organizations and ask people to donate money to them. Some other fraudsters would pretend that they need cash due to emergencies and ask people to lend them money. However, this study showed that fewer respondents would deposit money to strangers when requested (Mean: 1.20, SD: 0.604). The overall mean was 1.846, with SD: 1.056, showing an adequate level of social engineering awareness. In other words, the fraudsters' social engineering techniques do not influence most of the Generation Y respondents.

The items for the second independent variable sought to identify the level of anti-phishing knowledge among Generation Y in Kuala Lumpur. The seven items as shown in Table 4 focused on handling e-mails and websites before doing any type of transactions or entering confidential information to avoid phishing threats. The results showed that some respondents knew that a URL must have "https" when transmitting confidential information. This item had the lowest mean (Mean: 3.59, SD: 1.126). "Https" is crucial because it has a secured connection while transmitting confidential information on the websites (Muniandy et al., 2016). Furthermore, most respondents also knew that the padlock symbol is a 'must have' to transmit sensitive information (Mean: 3.96, SD: 0.981).

The results also show that the respondents prefer to type the URL in a new browser rather than clicking it on the hyperlink (Mean: 3.70,

SD: 1.166). They would also check the URL spelling before doing any type of transaction or entering confidential information (Mean: 3.91, SD: 1.116). Furthermore, before carrying out any type of transaction or entering confidential information, the respondents also would check the sentence structure, grammar, and spelling of the e-mails or websites (Mean: 4.00, SD: 1.094) and the design of the logo and contact information on the e-mails or websites (Mean: 3.97, SD: 1.087). Besides, the respondents would be extra cautious when an external e-mail is sent in their office e-mails (highest Mean: 4.33, SD: 0.904) because they know that most e-mail scams begin with messages from an external e-mail system. The overall mean was 3.923 with an SD: 1.0677, indicating an excellent level of anti-phishing knowledge among Generation Y in Kuala Lumpur.

The items for the third independent variable sought to identify the level of security concerns among Generation Y in Kuala Lumpur. The seven items as shown in Table 4 focussed on the security concerns of anti-virus and passwords to secure and protect data. The results showed that the respondents would scan all removable drives before using them to protect their computers against viruses (Mean: 3.88, SD: 1.032). Most of the respondents had also installed anti-virus software on their devices (Mean: 4,12, SD: 1.004), and they constantly updated the anti-virus software (Mean: 4.00, SD: 1.062). Furthermore, most respondents would not easily download any freeware from the internet (Mean: 4.09, SD: 1.073) because they know that some freeware might contain viruses that can harm their computers and devices.

Furthermore, most respondents would ensure that their passwords are secured by having the proper credentials, namely a mix of lowercase, uppercase, numbers, and special characters (Mean: 4.42, SD: 0.846). Most respondents would also ensure their passwords have eight or more characters (Mean: 4.45, SD: 0.811). Other than that, the respondents would also use a different password for different applications (Mean: 3.48, SD: 1.320), and most of them always change their passwords when required (Mean: 4.09, SD: 1.111). Using different passwords for different applications and changing the passwords when needed would help prevent fraudsters from detecting the passwords and accessing the users' accounts. The overall mean was 4.067 with a SD of 1.0324, showing a high-security concern among Generation Y in Kuala Lumpur.

Reliability and Normality Analysis

A Cronbach's alpha reliability test measures the internal consistency of the variables. Table 5 shows the values of Cronbach's alpha for every variable. Hair, Bush, and Ortinau (2003) stated that an alpha coefficient of less than 0.6 shows poor reliability strength. They also stated that alpha coefficients ranging from 0.6 to 0.7 show moderate reliability, 0.7 to 0.8 showed good reliability, 0.8 to 0.9 indicate very good reliability, and 0.9 and above show excellent reliability. These alpha coefficient ranges are supported by Churchill (1979), Hair, Ringle, and Sarstedt (2011), and Ursachi, Horodnic, and Zait (2015).

Based on the results as shown in Table 5, the Cronbach's alpha of the dependent variable, awareness of phishing among Generation Y in Kuala Lumpur, with six items was 0.661. This value showed that the items had moderate reliability. The Cronbach's alpha of the first independent variable, knowledge of social engineering, with five items was 0.608. This alpha value indicated that the social engineering items also had moderate reliability. Meanwhile, the Cronbach's alpha of the second independent variable, anti-phishing knowledge, with seven items was 0.780, indicating good reliability. Finally, the Cronbach's alpha of the third independent variable, security concern, with eight items was 0.824, indicating very good reliability. The overall Cronbach's alpha of the four variables with 26 items was 0.768. Hence, the measuring items of all the variables, on average, had good reliability.

Table 5: Results of the Reliability Analysis and Normality Test

Variable's Name	N of Items	Cronbach's Alpha	N	Skewness		Kurtosis	
				Statistics	Std. Error	Statistics	Std. Error
Phishing Awareness	6	0.661	391	-1.049	0.123	1.007	0.246
Social Engineering	5	0.608	391	0.720	0.123	0.619	0.246
Anti-Phishing Knowledge	7	0.780	391	-0.537	0.123	-0.021	0.246
Security Concern	8	0.824	391	-0.569	0.123	0.056	0.246
Total/Overall	26	0.768					

Apart from the reliability test, a normality test was also conducted to determine whether or not the data were normally distributed. The analysis

was performed using skewness and kurtosis values on phishing awareness, knowledge of social engineering, anti-phishing knowledge, and security concerns. According to George and Mallery (2010), skewness and kurtosis values ranging from -2 to +2 are acceptable to be considered as a normal distribution.

Table 5 above shows that skewness and kurtosis values for awareness of phishing ranged from -1.049 to 1.007. The values of skewness and kurtosis for knowledge in social engineering ranged from 0.720 to 0.619. The values for anti-phishing knowledge ranged from -0.537 to -0.021. For security concerns, the values ranged from -0.569 to 0.056. Since the skewness and kurtosis values for all the variables were within the range of -2 to +2, it was concluded that the mean scores of phishing awareness, knowledge in social engineering, anti-phishing knowledge, and security concern were normally distributed.

Pearson Correlation Coefficient Analysis

In the Pearson correlation coefficient analysis, the Pearson value (r) shows the strength of the relationship. The positive sign (+) before the r-value shows a positive relationship, and the negative sign (-) before the r-value shows a negative or inverse relationship. Ratner (2009) stated that r-values ranging from 0.70 to 1.00 (-0.7 to -1.00) indicate a strong positive (negative) relationship. The r-values that range between 0.30 to 0.70 (-0.30 to -0.70) indicate a moderate positive (negative) relationship, and r-values ranging from 0.00 to 0.30 (0.00 to -0.30) indicate a weak positive (negative) relationship. For the significance test, an alpha value or p-value of less than 0.05 indicates that the result is significant, while p-value of more than 0.05 shows that the result is not significant.

Table 6: Pearson Correlation Coefficient Results

		Phishing Awareness	Social Engineering	Anti-Phishing Knowledge	Security Concern
Phishing Awareness	Pearson Correlation	1	-0.379**	0.501**	0.431**
	Sig. (2-tailed)		0.000	0.000	0.000
	N	391	391	391	391

**Correlation is significant at the 0.01 level (2-tailed)

In this study, the Pearson correlation coefficient test was conducted to determine the relationship between the independent variables (social engineering influence, anti-phishing knowledge, and security concern) and the dependent variable (awareness of phishing among Generation Y in Kuala Lumpur). The results as presented in Table 6 above showed that social engineering had r = -0.379 (p-value = 0.000, <0.05), indicating that there was a significant inverse or moderate negative relationship between social engineering and awareness of phishing. In other words, as social engineering influence decreases, awareness of phishing increases. It means that when people do not tend to be influenced by social engineering used by fraudsters, they have a high level of awareness of phishing.

As for anti-phishing knowledge, the results in Table 6 show r = 0.501 (p-value = 0.000, <0.05). Thus, there was a significant moderate positive relationship between anti-phishing knowledge and awareness of phishing. In other words, as anti-phishing knowledge increases, phishing awareness also increases. Regarding the relationship between security concerns and awareness of phishing among Generation Y in Kuala Lumpur, Table 6 shows r = 0.431 (p-value = 0.000, <0.05). Therefore, there was a significant moderate positive relationship between the two variables. In other words, as security concern increases, awareness of phishing also increases.

Multiple Regression Analysis

The multiple coefficients of determination (R^2) measure the strength of the linear relationship between the dependent variable and its independent variables. The results as shown in Table 7 showed that there is a relationship between awareness of phishing and its three independent variables (R^2 = 0.329). R^2 = 0.329 means that only 32.9% of the variation in phishing awareness among Generation Y in Kuala Lumpur could be explained by variations in the three independent variables (influence of social engineering, anti-phishing knowledge, and security concern). The remaining 67.1% is explained by other factors affecting awareness of phishing.

Table 7: Multiple Regression Results

Model		β	t	Sig.	R^2	F
1	(Constant)	18.677	16.288	0.000	0.329	63.291
	Influence of Social Engineering	-0.190	-4.549	0.000		
	Anti-Phishing Knowledge	0.214	6.743	0.000		
	Security Concern	0.112	4.002	0.000		

a. Dependent Variable: Phishing Awareness
b. Predictors: (Constant), Security Concern, Social Engineering, Anti-Phishing Knowledge

The F-test is the first test in a multiple regression analysis, reflecting the regression model, i.e., whether the model explains a statistically significant proportion of the variance (Goos & Meintrup, 2016). Generally, the F-test is used for the model's overall significance, and it shows that there is a linear relationship between the independent variables and the dependent variable. The F-test statistics are significant when the p-value is less than 0.05. When the F-statistics are significant, the null hypothesis can be rejected. As shown in Table 7 above the p-value of the F-test was 0.000, which is less than 0.05, and F = 63.291. Thus, the model was adequate and statistically significant.

Also, as shown in Table 7, the coefficient β value of the influence of social engineering was -0.190. The β value for anti-phishing knowledge was 0.214, and the β value for security concerns was 0.112. As anti-phishing knowledge had the highest β value (0.214), it can be considered that anti-phishing knowledge was the most significant factor affecting phishing awareness among Generation Y in Kuala Lumpur compared to influence of social engineering and security concerns.

As shown in Table 7 the p-values for social engineering influence, anti-phishing knowledge, and social engineering were 0.000, < 0.05. The results indicated a significant relationship between all three independent variables and the dependent variable. In other words, the influence of social engineering, anti-phishing knowledge, and security concern were factors affecting awareness of phishing among Generation Y in Kuala Lumpur at the 5% significance level (p-value = 0.05). Thus, the null hypotheses for all three independent variables were rejected. Therefore, the multiple regression equation was:

Phishing Awareness = 18.677 - 0.190 (Influence of Social Engineering) + 0.214 (Anti- Phishing Knowledge) + 0.112 (Security Concern) + e

Discussion

The results indicated that most Generation Y respondents had a strong level of awareness of phishing; the mean value was more than 4 (Mean: 4.405, SD: 0.8293). However, only some respondents knew that they could report to the MCMC whenever they encounter any phishing e-mails or sites (Mean: 3.68, SD: 1.320). The MCMC would usually remove a phishing site immediately to protect Malaysian internet users from attacks. Thus, internet users should know the right channels to report phishing attempts to avoid phishing threats. The relationship between social engineering influence, anti-phishing knowledge, and security concerns, and awareness of phishing among Generation Y in Kuala Lumpur is discussed further in the following sections.

The first independent variable items about social engineering influence were designed to determine the awareness of Generation Y on the social engineering methods used by fraudsters. The results showed that fewer respondents are influenced by five social engineering methods identified by Ferreiraa and Telesa (2019). However, the overall results showed that the mean value was more than one but less than 3. If the mean value were less than 1, it would show that Generation Y was strongly not influenced by the social engineering methods. However, the mean for this study was not less than 1, probably because fraudsters always enhance their phishing methods and adapt to current situations. This reason is supported by Bhardwaj, Sapra, Kumar, Kumar, and Arthi (2020), who stated that phishing attacks have become highly creative and advanced during the Covid-19 global pandemic. In April 2020, it was reported that cybercriminals sent over 18 million phishing e-mails related to Covid-19, and a new phishing portal was launched every 20 seconds, which now included Covid-19 related phishing attacks (Bhardwaj et al., 2020).

In addition, people are not emotionally prepared and not thinking wisely when they are under phishing attacks. Muniandy et al. (2016) stated that most people panicked and did not check the authorization of someone

before talking on any issue. Kamruzzaman et al. (2016) stated that people were deceived by fake gifts offered by fraudsters on the internet. This study also showed that some of Generation Y tend to panic when fraudster spoke as an authority. They would also trust any advertisements and would deposit money to strangers when requested. It is crucial to stay calm and check the identity and originality of the persons, e-mails, SMSes, calls, and websites to evade the influence of social engineering. However, most of the Generation Y in this study tended to be not easily influenced by social engineering used by the fraudsters since social engineering influence was shown to have a negative relationship with the level of awareness of phishing. In other words, they had a high level of awareness of phishing. The results of this study supported H1 and were consistent with previous research (e.g., Muniandy et al., 2016; and Parsons et al., 2019).

Furthermore, the results indicated that most of the Generation Y respondents had good anti-phishing knowledge (overall Mean: 3.923, SD: 1.0677). The mean scores for the measurement items of anti-phishing knowledge showed that they knew that the URL must be "https" when transmitting confidential information, the padlock symbol is a must to transmit sensitive information, and they should type the URL in a new browser rather than clicking it on hyperlinks. The mean scores also showed that they knew they should check the URL spelling, the logo's design, and contact information on the e-mails or websites before doing any type of transaction or entering confidential information.

However, although Generation Y had good anti-phishing knowledge, the results also indicated that they were not fully aware of phishing on bank websites, the internet, or social media despite reading materials about them. Hence, Generation Y should always keep updating and gaining more anti-phishing knowledge, especially on current phishing trends used by fraudsters, to avoid phishing attacks. Updating oneself on anti-phishing knowledge is essential since this study has shown that anti-phishing knowledge had a positive relationship with the level of awareness of phishing. This finding indicated that H2 was supported. It is also in line with previous research (e.g., Bose & Leung, 2008; Arachchilage & Love, 2014; Baral & Arachchilage, 2019; Verkijika, 2019; and Jampen et al., 2020).

Regarding security concerns, the results of this study indicated that most of the Generation Y respondents had strong security concerns (overall Mean: 4.067, SD: 1.0324). However, the mean values were only moderate for scanning all removable drives before using it on their computers (Mean: 3.88, SD: 1.032) and using different passwords for different applications (Mean: 3.48, SD: 1.320). Kennedy et al. (2016) stated that users had extreme annoyance and fatigue in using different passwords for different applications. However, it is advisable that computer users scan all removable drives before using them to avoid virus attacks and use different passwords for different applications to prevent fraudsters from detecting the passwords and accessing their accounts (Kennedy et al., 2016). Overall, this study found that security concerns had a positive relationship with the level of awareness of phishing. Hence, H3 was supported. This finding is consistent with Huang et al. (2011), Topaloglu (2012), Chhikara et al. (2013), Kennedy et al. (2016), and Verkijika (2019).

Comparing this study with Muniandy et al.'s (2016) on higher education respondents, it would seem that the Generation Y respondents in Kuala Lumpur had a higher level of awareness of phishing than the respondents in higher education. For example, the results of this study showed that 89.5% of Generation Y respondents disagreed with replying to e-mails or messages announcing something exciting, such as winning vast sums of money. Whereas only 89% of the higher education respondents disagreed with responding to similar messages. Furthermore, 52.9% of the Generation Y respondents agreed that a URL must be "https" when transmitting confidential information, while only 35.16% of the higher education respondents agreed with the requirement. Moreover, 70.1% of the Generation Y respondents would check the URL spelling before doing any transaction or entering confidential information. In comparison, only 26.56% of higher education respondents would do the same.

Further comparison showed that 70.3% of the Generation Y respondents agreed that they always updated the anti-virus software on their devices. However, only 45.31% of higher education respondents would do so. 85.4% of the Generation Y respondents agreed to ensure having passwords with good credentials (i.e., comprising lowercase, uppercase, numbers, and special characters) compared to 43.75% of the higher education respondents. These results are not surprising. Even Jones and Heinrichs (2012) stated

that the security practices of undergraduate students were dissatisfying, and they took less safeguards when using digital devices.

One of the main reasons for the results between Generation Y and higher education respondents could be that 83.6% of the Generation Y respondents read materials about phishing on bank websites, the internet, or social media. In comparison, only 22.66% of the higher education respondents read materials on phishing (Muniandy et al., 2016). Reading about phishing would allow the reader to gain awareness and knowledge about current phishing trends and techniques to avoid phishing attacks, thereby avoiding loss of money and data.

Another reason why the higher education respondents had a lower level of awareness of phishing than the Generation Y respondents could be that the higher education respondents thought they would not become a target of phishing attacks due to their student status (Muniandy et al., 2016). However, Muniandy et al., 2016 also reported that 48.44% of the higher education respondents disagreed with this reason. Nonetheless, no one can avoid being attacked by phishing threats, and everyone should protect themselves from such threats.

CONCLUSION

This study focused on the level of awareness of phishing among the Generation Y (also known as Millennials) because they are generally influenced by technology, social media, digital media development, and the internet (Naumovska, 2017). Furthermore, the location chosen was Kuala Lumpur since it had high exposure to communication and technological advancement with many facilities having internet connection and usage of technological devices (Yau et al., 2016).

This study focused on the effect of three independent variables (social engineering influence, anti-phishing knowledge, and security concern) on the dependent variable (awareness of phishing among Generation Y in Kuala Lumpur). The results showed a negative relationship between the influence of social engineering influence and awareness of phishing among Generation Y in Kuala Lumpur. They also showed a positive relationship between

anti-phishing knowledge and awareness of phishing among Generation Y in Kuala Lumpur. There was also a positive relationship between security concerns and awareness of awareness of phishing among Generation Y in Kuala Lumpur.

Based on the findings of this study, people are advised to be alert of the influence of social engineering by always keeping updated on phishing methods and anti-phishing knowledge by reading more phishing materials. They should also secure their data by having good password credentials and installing anti-viruses. The findings of this study are also beneficial to Generation Y to have a better understanding and knowledge of phishing. Furthermore, companies and government agencies can benefit from this study to spread awareness among their employees and take relevant actions to combat phishing threats.

There are several limitations to this study. The first limitation is the scope of the study. This study was limited to Generation Y and did not cover other generations, such as Generation X and baby boomers. Furthermore, this study was also limited to the Kuala Lumpur area since the Malaysian government plans to transform it into a metropolitan area and a smart city. The other limitation is the independent variables used in this study. This study only examined three independent variables: influence of social engineering, anti-phishing knowledge, and security concern. Based on the multiple regression analysis, these factors only explained 32.9% of the variation in awareness of phishing among Generation Y in Kuala Lumpur. Therefore, there may be other factors affecting their awareness of phishing.

Future researchers could expand the study to include other generations, such as Generation X and baby boomers, to overcome the limitations. Furthermore, future researchers could apply other independents variables in addition to the influence of social engineering, anti-phishing knowledge, and security concerns. Other than that, researchers could also widen the study location to the whole country. It would be interesting to determine and compare the level of awareness of phishing in the different states in Malaysia.

ACKNOWLEDGMENT

The study was supported by the Fundamental Research Grant Scheme (FRGS, Reference code: FRGS/1/2019/SS01/UITM/02/34) provided by the Ministry of Higher Education (MOHE) of Malaysia and the authors thank the Ministry for its support. The authors also would like to thank the Universiti Teknologi MARA Selangor, Puncak Alam Campus for providing this opportunity.

REFERENCES

Anti-Phishing Working Group (APWG). (2018). Phishing activity trends report 2nd quarter 2018. Unifying the global response to cybercrime.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23-32.

Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualizing user's self-efficacy in phishing threat avoidance behaviour. In *2019 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 102-110). IEEE.

Baruch, Y., & Holtom, B.C. (2008). Survey response rate levels and trends in organizational research. *Human Relations, 61*(8), 1139-1160. https://doi.org/10.1177/0018726708094863

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security*, *2020*(9), 15-19.

Boateng, E. O. Y., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-307.

Bose, I., & Leung, A. C. M. (2008). Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decision Support Systems, 45*(4), 897–912.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247–256.

Chhikara, J., Dahiya, R., Garg, N., & Rani, M. (2013). Phishing & anti-phishing techniques: Case study. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 458-465.

Churchill, G. A. Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*(1), 64–73.

Department of Statistics Official Portal. Retrieved from https://www.mcmc.gov.my/en/make-a-complaint/complaint-circle

EY Global (2019). Is cybersecurity about more than protection? EY global information security survey 2018-19. Ernst and Young. Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Federal Territory of Kuala Lumpur. Department of Statistics Malaysia Official Portal. Retrieved from https://www.dosm.gov.my/v1/index.php?r= column/cone&menu_id=bjRlZXVGdnBueDJKY1BPWEFPRlhIdz09

Ferreiraa, A., & Telesa, S. (2019). Persuasion: How phishing e-mails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19-31.

Gavett, B. E. G., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS One*, *12*(2), e0171620.

George, D., & Mallery, P. (2010). *SPSS for windows step by step: A simple guide and reference, 17.0 update* (10th ed.). Boston: Allyn & Bacon.

Goos, P., & Meintrup, D. (2016). *Statistics with JMP: Hypothesis tests, ANOVA and regression.* John Wiley & Sons. Retrieved from https://ebookcentral.proquest.com/lib/staffordshire/detail.action?docID=4413728.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *International Conference on Computing, Communication and Automation (ICCCA2016)* (pp. 537-540). IEEE.

Hair, J. F., Bush R. P., & Ortinau, D. J. (2003). *Marketing research: Within a changing information environment.* New York: McGraw-Hill/Irwin.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Huang, C. Y., Ma, S. P., & Chen, K. T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications, 34*(4), 1292-1301.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, *10*(33).

Jones, H. B., & Heinrichs, R. L. (2012). Do business students practice smartphone security?. *Journal of Computer Information Systems*, *53*(2), 22-30.

Kamruzzaman , M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), 22-28.

Katkuri, S. (2018). Indian cyber law. *International Journal of Advanced Research and Development, 3*(1), 640-644.

Kennedy, A. M., & Parsons, P. (2012). Macro-social marketing and social engineering: A systems approach. *Journal of Social Marketing*, *2*(1), 37-51.

Kennedy, A. M., & Parsons, P. (2014). Social engineering and social marketing: Why is one 'good' and the other 'bad'? *Journal of Social Marketing, 4*(3), 198-209.

Kennedy, L. Z., Chiasson, S., & Oorschot, P. V. (2016). Revisiting password rules: Facilitating human management of passwords. In *2016 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-10). IEEE.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*, 607-610.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, I13-I22.

Lawson, P., Pearson, C. J., Crowson, P. A., & Mayhorn, C. B. (2020). E-mail phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, 86. DOI: 10.1016/j.apergo.2020.103084. Epub 2020 Mar 9. PMID: 32174448.

Make a complaint. Malaysian Communication and Multimedia Commission Official Portal. Retrieved from https://www.mcmc.gov.my/en/make-a-complaint/make-a-complaint

Muniandy, L., Muniandy, B., & Samsudin, Z. (2016). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security*. *2017*, 1-13.

Naumovska, L. (2017). Marketing communication strategies for Generation Y – Millennials. *Business Management and Strategy, 8*(1), 123 – 133.

Parsons, K., Butavicius, M., Delfabbroa, P., & Lilliea, M. (2019). Predicting susceptibility to social influence in phishing e-mails. *International Journal of Human-Computer Studies, 128*, 17-26.

Phishing Attack. Malaysian Communication and Multimedia Commission Official Portal. Retrieved from https://www.mcmc.gov.my/en/fa qs/ phishing-attack

Rahim, S. (2019, November 21). Hairdresser loses RM 14,900 in phone scam. *New Straits Times.* Retrieved from https://www.nst.com.my/ news/ nation/2019/11/540838/hairdresser-loses-rm14900-phone-scam

Rao, S. R., & Pais, A. R. (2019). Jail-Phish: An improved search engine-based phishing detection system. *Computers and Security*, *83*, 246-247.

Ratner, B. (2009). The correlation coefficient: Its values range between + 1 / − 1, or do they? *Journal of Targeting, Measurement and Analysis for Marketing, 17*, 139–142.

San, L. Y., Omar, A., & Thurasamy, R. (2015). Online purchase: A study of Generation Y in Malaysia. *International Journal of Business and Management, 10*(6), 1-7.

Suganya, V. (2016). A review on phishing attacks and various anti phishing techniques. *International Journal of Computer Applications*, *139*(1), 20-23.

Sun, J. C. Y., & Chen, A. Y. Z. (2016). Effects of integrating dynamic concept maps with interactive response system on elementary school students' motivation and learning outcome: The case of anti-phishing education. *Computers & Education*, *102*, 117–127.

Topaloglu, C. (2012). Consumer motivation and concern factors for online shopping in Turkey. *Asian Academy of Management Journal, 17*(2), 1-19.

Ursachi, G., Horodnic, I. A., & Zait, A. (2015). How reliable are measurement scales? External factors with indirect influence on reliability estimators. *Procedia Economics and Finance*, *20*, 679–686.

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296.

Why is HTTP not secure? | HTTP vs. HTTPS. Cloudflare. Retrieved from https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

Yau, K. L. A., Lau, S. L., Chua, H. N., Ling, M. H., Iranmanesh, V., & Kwa, S. C. C. (2016). Greater Kuala Lumpur as a smart city: A case study on technology opportunities. In *2016 8th International Conference on Knowledge and Smart Technology (KST)* (pp. 96-101). IEEE.

Zahari, A. I., Billu, R., & Said, J. (2017). E-commerce fraud: An investigation of familiarity, trust and awareness impact towards online fraud. *Journal of Research and Opinion, 6*(9), 2470-2480.