IBIMA Publishing
Journal of Information Assurance & Cyber security
http://www.ibimapublishing.com/journals/JIACS/jiacs.html
Vol. 2017 (2017), Article ID 800299, 13 pages
DOI: 10.5171/2017.800299

Research Article

Cyber Security Behaviour among Higher Education Students in Malaysia

Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samsudin

Tunku Abdul Rahman University College, Tanjong Bungah. Pulau Pinang. Malaysia

Centre for Instructional Technology & Multimedia, Universiti Sains Malaysia, Pulau Pinang, Malaysia

Correspondence should be addressed to: Michael Abelar; miabelar@ctemc.org

Received date: 25 November 2016; Accepted date: 29 November 2016;

Published date: 3 February 2017

Academic Editor: Choo-Kim Tan

Abstract

This study explores the current state of cyber security behaviour among higher education students in Malaysia. The respondents' cyber security behaviour was assessed in the following aspects: password usage, phishing, social engineering, online scam and malware. A questionnaire comprised of the aforementioned five cyber security issues was distributed to students in a well-established university college located in the Northern region of Peninsular Malaysia. The returned questionnaires were analyzed to identify the cyber security behaviour among Malaysian students. The study shows that cyber security behaviour among respondents was generally unsatisfactory in all five cyber security issues that had been studied in this research.

Keywords: cyber security, behaviour, higher education students

Introduction

The Internet is one of the most sophisticated technology ever created. The Internet and its related technologies are constantly evolving. The number of Internet users and the dependence on Internet is increasing steadily around the globe. Malaysians are also not excluded from the rapid advancement in technology as their lives are increasingly relying on the Internet to accomplish their daily chores (Daka Advisory, 2014). The number of Internet users in Malaysia is expanding exponentially. Muniandy and Muniandy (2012) reported that after the year 2000, the Internet penetration rate in Malaysia continued to grow rapidly. Internet users in Malaysia grew from 0.1% in 1995 to 37.9% in 2005. Malaysian Communications and Multimedia Commission (2015) had also noted that the Internet penetration rate among Malaysians in the first quarter of 2014 was at 66.6% or approximately 20.1 million Internet users.

Cite this Article as: Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samsudin (2017), "Cyber Security Behaviour among Higher Education Students in Malaysia", Journal of Information Assurance &

Although the country had benefited from the advancement in Internet technology, increasing cyber security incidents are a cause for concern. According to Ramendran (2013), in the first seven months of 2013, RM1.07 billion was recorded in losses from thousands of various scams, corporate fraud and other commercial crimes. Also, Malaysia was positioned in the sixth place of being at high risk for online fraud and malware attacks. Most of these cyber security incidents targeted young Internet users. Garnaeva, Chebyshev, Makrushin, Unucheck and Ivanov (2014) reported that Malaysia was ranked in the 9th position for top 10 countries with the most number of attacked users through malware. Also, Malaysia was placed at the tenth spot for top 10 countries with high risk of infections with malware. Ramendran (2014) reported that a malware known as Zeus is being used in phishing attacks targeting smartphone and tablet users who performed online banking activities. It was reported that eight victims have lost approximately RM 60,000.

Gan, Ling, Yih and Eze (2008) claimed phishing attacks and identity theft as an obstacle for the growth of online banking in Malaysia as the number of attacks launched on financial institutions had continuously increased since the year 2000. Hamudin and Ariffin (2014) reported that Sophos Security Threat Report 2013 exposed Malaysia as the sixth most vulnerable country targeted for cybercrimes, purportedly losing RM1 billion to cybercrimes. Citing the reports by Malaysia Computer Emergency Response Team (MyCERT), the authors also reported that the cybercrime rate in Malaysia had increased from 9,986 cases in 2012 to 10,636 cases in 2013.

The rapid rise of Internet users in Malaysia correlates with increased cyber security incidents in Malaysia. This fact is supported by Wechuli, Muketha, and Mateko (2014) when they claimed that the growing number of reported cyber security incidents indicates that cybercrimes are worsening. The researchers strongly believed that the actual percentage of cybercrimes in Malaysia would be much higher than what has been reported as not all victims would come forward and report such incidents to the relevant authorities. For example, Kshetri (2010) noted that less than 10% of cybercrimes are ever reported to the relevant authorities.

Background of the study

Although cyber security is an important issue affecting Internet users not only in Malaysia but also across the globe, this study intends to only explore the cyber security behaviour among Malaysian higher education students. This is due to the following reasons: (i) Malaysians aged 16 to 24 years old are the most avid Internet users; and (ii) Higher education students, who are usually aged between 18-25 years old belong to this age category. According to Statista (2015), a survey on the daily Internet usage in Malaysia in the year 2014 showed that 73% of people in the 16-24 years old category are Internet users. A study by Malaysian Communications and Multimedia Commission (2015) also supported the fact that young adults in Malaysia are heavy Internet users. The same study also reported that among school-going respondents, over 62.5% of them were in universities or colleges, 34.90% in secondary school, while 2.40% of them were in primary schools and 0.20% in others. This corroborates the fact that higher education students are heavy Internet users compared to students at the primary or secondary level. Marketing Magazine (2011) also reported that the number of Malaysian young adults accessing the Internet and the total amount of time spent on the Internet is increasing rapidly (Marketing Magazine, 2011). It can be concluded that increasing Internet usage among this category exposes them to cyber security threats. This situation warrants a study to explore the cyber security behaviour among Malaysian higher education students, classified as belonging to the vulnerable group.

Muniandy (2010) reported that students are active users of the Internet to gain information. Vrana (2012) claimed that the current generation of students are heavy

Internet users. Students at the higher education level are also more vulnerable to cyber security threats as the majority of their daily communication and education related activities are performed on the Internet (Mensch & Wilkie, 2011). Devi and Roy (2012) acknowledged that students are more dependent on the Internet for their academic requirements. Furthermore, Mohd Ayub, Wan Hamid and Nawawi (2014) claimed that in Malaysia, the majority of Internet users are aged between 15-34 years and further added that this includes students who are pursuing higher education in Malaysia. However, Rezgui and Marks (2008) and Sheng, Holbrook, Kumaraguru, Cranorm and Downs (2010) reported that young adults, in the age group of 18-24 years old are more susceptible to cyber security threats. Thus, in the researchers' opinion, the current study is vital to understand higher education students' cyber security behaviour for the following three reasons: (i) they are the future workforce of Malaysia; (ii) they form the largest group of Internet users in Malaysia; and (iii) study findings would establish the next course of action that can be taken by the relevant parties.

Research Objective

This study intends to identify the cyber security behaviour of higher education students in Malaysia in the following aspects,

i) Malware
ii) Password usage
iii) Phishing
iv) Social engineering, and
v) Online scam

Research Question

This study seeks to answer the following research question:-

1.) What is the current state of cyber security behaviour in the aspects of malware, password usage, phishing, social engineering and online scam among higher education students in Malaysia?

Research Methodology

A questionnaire was used to gather the data pertaining to cyber security behaviour among students in a well-established private university college located in the Northern region of Peninsular Malaysia. Cyber Security Behaviour Instrument (CSBI) was designed by the researchers based on the literature review of existing studies on cyber security. CSBI instrument is divided into 2 sections. Section A assesses demographic information (2 items); Section B assesses cyber security behaviour (50 items). Section A consists of 2 items, which are gender and online activities. Online activities comprise of 6 items (refer to Figure 1). Under Section B, cyber security behaviour is divided into 5 subscales, namely, phishing, password usage, social engineering, online scamming and malware. Each of these subscales consists of 10 items. All the items in Section B subscales are designed with categorical Likert scale using five categories. The five categories are Strongly Agree, Agree, Don't know, Disagree and Strongly Disagree. Strongly Agree or Agree is measured as respondents' agreement with the particular statement while Strongly Disagree or Disagree is reflected as respondents' disagreement with a particular statement.

Two experts in the field of cyber security validated the instrument: an expert from human aspects of cyber security from United Kingdom and an expert in the field of human computer interaction from Malaysia. The researchers emailed the survey instrument to the respective experts for content validity. Post-validation, the experts emailed the commented instrument and additional suggestions to the researchers. The expert from Malaysia accepted all the subscales assessing the cyber security behaviour section of CSBI instrument without modifications. However, the expert provided feedback on improving the demographic section as well as adding an item to identify the respondents' online behaviour. The expert provided examples of online activities that could be included in the instrument. Hence, the instrument was improved with the suggested online

activities. The expert from the United Kingdom provided many constructive suggestions to improve the cyber security behaviour section. The expert provided many suggestions especially on the choices of words to describe the items. Among others, the expert recommended that certain terms such as phishing be defined as well as suggestions to rephrase the items in the instrument with appropriate wordings. Based on the feedback given by these two experts, the researchers viewed the instruments and made some necessary modifications on the CSBI instrument. Technical terms such as phishing were defined and some of the items were rephrased as suggested by the expert.

Prior to this actual study, CSBI instrument was pilot tested with a group of 30 students from the same research site. The researchers ensure that the participants for the pilot test do not participate in the actual study. The data collected from the pilot test were measured for reliability using Cronbach's alpha reliability coefficient (*see Table 1*). Sekaran (2000) reported that reliability coefficient that is less than .60 as poor, those in the range of .70 as acceptable and greater than 0.80 as good.

Table 1: CSBI Reliability Measurement

Cyber security subscales	Reliability (Cronbach alpha)
Malware	0.841
Password usage	0.702
Phishing	0.703
Social engineering	0.859
Online Scam	0.707

Prior to the data collection, the researchers obtained written consent from the relevant private university college to conduct the study among its students. A sample of 128 students participated voluntarily in this study. The researchers used self-administered paper-and-pencil survey to collect the data from the respondents to increase the response rate. The whole study was completed in a week. The questionnaires were printed, distributed and collected from the respondents within this period. The majority of the respondents completed and returned the questionnaire on the same day. Statistical Package for the Social Sciences (SPSS) version 22 was used for data analysis. The findings of the study are presented using descriptive statistics.

Findings of the study

In the following section demographic findings of the study are presented.

Demographic profile

Participants in this study comprised of 28 male and 100 female students. Figure 1 illustrates online activities often engaged by these 128 respondents.

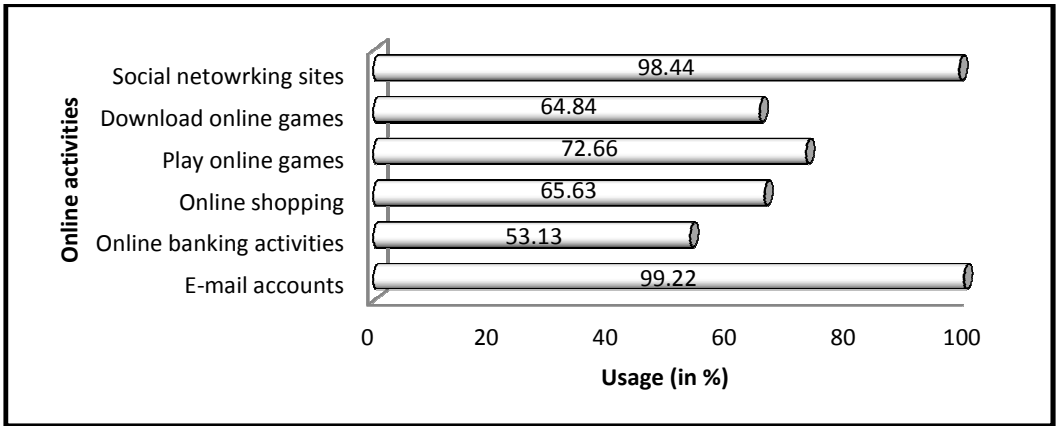

Figure 1: Online activities participated by the respondents

Based on the profiling on Figure 1, it can be seen that students at the higher education level are indeed heavy Internet users. Almost everyone participated in this study had at least used email as a communication medium (99.22%) and they are also heavy social networking site users (98.44%). Nearly half (53.13%) of the respondents used online banking. More than half of the respondents who participated in this survey shop online (65.63%) and download online games (64.84%). About 72.66% of the respondents play online games. Previous studies had ascertained that students of higher education used the Internet to look for information (Muniandy, 2010), daily communication (Mensch and Wilkie, 2010) and to accomplish their academic requirements (Devi & Roy, 2012). Malaysian students are also active users of social networking sites. Muniandy and Muniandy (2013) claimed that generally, the majority of Internet users of all ages in Malaysia are avid social networking users. This study also proved that Malaysian students are indeed avid users of social networking sites. In the researchers' opinion, students at the higher education level widely used the Internet for a diverse range of reasons.

Cyber security behavior findings

Table 2: Participants' cyber security behavior on malware

No	Items	Agree (%)	Don't know (%)	Disagree (%)
M1	Willing to open email attachments from strangers	16.41	11.72	71.88
M2	Interesting subject line causes the of opening an email attachment	38.28	17.97	43.75
M3	Very sure of the status of anti-virus software in personal computer	45.31	30.47	24.22
M4	Interested to open attachments with multiple extensions	17.97	26.56	55.47
M5	Sense something is wrong if computer runs extremely slow	82.03	4.69	13.28
M6	Download freeware on the Internet	56.25	8.59	35.16
M7	Scan removable drives prior to using it on my personal computer	46.88	6.25	46.88

M8	Installed anti-virus software, firewall and anti-spyware	73.44	12.5	14.06
M9	Willing to download materials from unsecure sites	28.13	17.19	54.69
M10	Apply security patches as soon as possible	28.91	46.09	25.00

The preceding Table 2 shows the findings for students' cyber security behaviour in relation to malware protections. Among the 10 items listed in the malware subscale, 6 of them indicate weak or dangerous cyber security practices among the respondents. The 6 items are M2, M3, M6, M7, M9 and M10. Malware protection mechanism among the respondents is insufficient as all the items that have unsatisfactory results were important in protecting users from malware threats. We could safely attest that cyber security knowledge regarding malware among users is also an important issue that must be given due consideration. This can be seen based on the respondents' response for items M3, M4 and M10. More than a quarter of the respondents answered "Don't know" for M3 and M4 while nearly half of the surveyed respondents said "Don't know" for M10. M3 is related to the status of anti-virus software in their personal computer and M4 is for opening an attachment with multiple extensions. M10 is related to applying security patches for software. Respondents had also ignored some of the best practices in protection against malware threats. For instance, more than half of the respondents surveyed admitted that they downloaded freeware available on the Internet. About 46.88% of the respondents claimed that they do not scan removable drives prior to using them in their personal computer. Although 73.44% claimed that they have installed antivirus software, firewall and anti-spyware but ignoring the best practices in malware protection by not scanning removable drives or by downloading freeware would still expose them to malware threats. Low awareness on applying security patches released by software vendors, not being aware of anti-virus software status or opening attachments with multiple extensions certainly would escalate malware threats.

Table 3: Participants' cyber security behavior on password usage

No.	Items	Agree (%)	Don't know (%)	Disagree (%)
P1	Password doesn't follow keyboard pattern	74.22	5.47	20.31
P2	Sharing password with other people	11.72	2.34	85.94
P3	Different passwords for different applications	34.38	6.25	59.38
P4	Password consists of lowercase, uppercase, numbers, special characters	43.75	8.59	47.66
P5	Passwords longer than 8 characters	75	6.25	18.75
P6	Passwords based on personal information	78.91	4.69	16.41
P7	Never change password	45.31	14.06	40.63
P8	Usage of "Remember my password" option	29.69	6.25	64.06
P9	Used to write down the password	39.06	4.69	56.25
P10	Never use "hint" to recover forgotten password	35.94	13.28	50.78

Table 3 shows the findings for password behaviour among the respondents. For the best practices of password usage, items P3, P4, P6, P7 and P10 do not produce satisfactory results. About three quarters of the surveyed respondents claimed that

they do not share their passwords or use passwords that are longer than eight characters and passwords that do not follow keyboard pattern. Yet only 34.38% of the surveyed respondents claimed that they use different passwords for different applications. A whopping 78.91% of the surveyed respondents claimed that their password is based on their personal information. About 45.31% of the respondents have never changed their passwords at all, while 14.06% of the respondents are not aware of the importance of changing password. Furthermore, 47.66% of the respondents' passwords do not consist of lowercase, uppercase, numbers and special characters while 8.59% claimed that they are not aware of this. Although the respondents apply some best practices in protecting their passwords, yet their behaviour and low awareness level in other aspects of password usage would still expose them to security threats

Table 4: Participants' cyber security behavior on phishing issues

No.	Items	Agree (%)	Don't know (%)	Disagree (%)
Ph1	Upgrading phishing knowledge by reading phishing materials	22.66	27.34	50.00
Ph2	Not a target phishing attacks due to student status	35.16	16.41	48.44
Ph3	Willing to provide confidential information to any types of emails	9.38	12.50	78.13
Ph4	Willing to click hyperlinks in email messages	25.78	22.66	51.56
Ph5	Trusting any email messages announcing contests / prizes	4.69	22.66	78.13
Ph6	URL must be "https" if I'm transmitting confidential information	35.16	28.13	36.72
Ph7	Padlock symbol a must to transmit sensitive information	34.38	39.84	25.78
Ph8	I prefer to type URL in new browser rather than clicking it on hyperlinks	17.97	22.66	59.38
Ph9	Receiving suspicious email will prompt me to contact the relevant party for verification	22.66	24.22	53.13
Ph10	Check URL spelling prior to any types of transactions	26.56	26.56	46.88

As for phishing issues, seven items indicated unsatisfactory results. Those items are Ph1, Ph2, Ph4, Ph6, Ph7, Ph8, and Ph10. As for phishing threats, 50.00% of the surveyed respondents claimed that they do not read to upgrade their phishing knowledge while 27.34% reported that they are not aware of the importance of reading to upgrade phishing knowledge. Even though this well-known university college is often subjected to phishing attacks, more than a quarter of the respondents surveyed believed that they are not the target for phishing attacks because of their status as students. About 51.56% of the respondents claimed that they do not click on the hyperlinks provided in the email, yet only 17.97% of the surveyed respondents reported that they prefer to type the URL in a new browser window. Furthermore, only 26.56% of the respondents would check URL spelling prior to performing any types of transactions. Ignoring the best practices in protection against phishing attacks made the respondents vulnerable to cyber security threats. Generally, it can be assumed that phishing awareness is also considerably low as more than a quarter of the respondents does not know the

importance of "https" or the existence of the padlock symbol while transmitting confidential information. Respondents are also not aware of many items in the subscale of phishing, such as, Ph1, Ph4, Ph5, Ph6, Ph7, Ph8, Ph9 and Ph10 as more than 20% of the respondents answered "Don't know" for these items.

Table 5: Participants' cyber security behavior on social engineering issues

No.	Items	Agree (%)	Don't know (%)	Disagree (%)
S1	Not interested in reading social engineering issues	53.91	21.10	25.00
S2	Willing to reveal username and password to anyone claiming to be system administrator	6.25	10.16	83.59
S3	Not a target of social engineering attacks due to student status	25.00	14.84	60.16
S4	Unwilling to respond to calls, SMS, or email messages to friendly / non-threatening strangers	79.69	7.03	13.28
S5	Willingness to follow instructions given by people who speak with authority	7.81	10.16	82.03
S6	Willingness to provide password to a help desk	16.41	12.50	71.10
S7	Check the authorization or identity of someone before talking on any issues	33.59	28.13	38.28
S8	Not feeling intimidated with questions by someone	36.72	40.63	22.66
S9	Wouldn't communicate with a stranger although his/her looks warrant sympathy	54.69	25.78	19.53
S10	Wouldn't reveal any confidential information under any circumstances	84.38	11.72	3.90

For social engineering issues, S1, S7 and S8 yield more negative responses than positive feedback from respondents. About 53.91% of the respondents claimed that they are not interested in reading social engineering issues (S1). Only a quarter of the surveyed respondents reported that they read materials related to social engineering issues. Therefore, a low level of awareness among respondents in social engineering issues are apparent as only 25.00% of the respondents claimed that they do read materials related to social engineering concerns. This alone would prevent them from learning about the latest social engineering issues reported in the newspapers or online news portals. A low awareness level would again expose them to the rapidly evolving social engineering threats. As for S7, which stands for checking the authorization or identity of someone before communicating, only 33.59% agreed with this item, while 38.28% selected to disagree. As for S8, not feeling intimidated with questions from someone, 40.63% of the respondents claimed they "Don't know", while 22.66% reported they were indeed intimidated with questions from someone.

Table 6: Participants' cyber security behavior on online scam issues

No.	Items	Agree (%)	Don't know (%)	Disagree (%)
O1	Established trusted online relationship with strangers	12.50	13.28	74.22
O2	Ignored emails from well-known organizations announcement on something unusual or too good	74.22	16.41	9.38
O3	Respond to SMS announcing contests involving huge sums of money	3.90	7.03	89.06
O4	Never trust strangers identity information given on the Internet	75.00	9.38	15.63
O5	Never consider any amount of money for services offered by an online site	64.06	14.84	21.09
O6	Willing to deposit money requested by online friends	4.69	10.16	85.16
O7	Aware of and able to identify the latest online scams	25.00	41.41	33.59
O8	Trust strangers' pictures posted on the Internet	14.84	32.03	53.13
O9	Never receive parcels and gifts from Internet friend	69.53	17.97	12.50
O10	Wouldn't hesitate to face-to-face with Internet friends	32.81	16.41	50.78

As for online scam, three items produced negative responses. For the item O7, awareness and the ability to identify the latest online scams, only a quarter of the respondents agreed with the statement and 41.41% of the respondents claimed that they "Don't know" how to identify the latest online scams while 33.59% of the respondents selected to disagree with the statement. Although 53.13% of the respondents reported they do not trust the strangers' pictures posted on the Internet, yet the researchers were baffled when 32.03% of the respondents said they "Don't know". For O10, 32.81% expressed willingness to meet online friends while 16.41% claimed "Don't know".

Discussions

We assess five types of cyber security threats, malware, password, phishing, social engineering and online scam. From the findings, the respondents' behaviour in all aspects are considerably vulnerable and their behaviour would certainly expose them to cyber security threats. The research findings conformed with previous studies conducted on numerous cyber security behaviour.

In a study conducted by Aytes and Connelly (2004) on undergraduate students' password usage, e-mail usage and data backup process, respondents who claimed to be knowledgeable users were still found to practice unsafe security behaviour. Teer, Kruck and Kruck (2007) conducted a study on undergraduate students' computer usage on antivirus software, firewalls, practices in opening email attachments, password usage and security patches. Their results also conform to the findings of other researchers as they concluded that respondents in their study had also practiced numerous unsafe security behaviours. A study by Bain, Hayden and Sneesby (2012) on password usage among college students reported that the respondents lack awareness in protecting their passwords and practiced some risky behaviour such as the failure to keep passwords secret, not changing passwords frequently and using the same password for multiple applications. Jones and Heinrichs (2012) claimed that past

research on students' computer security behaviour showed that students were lacking in computer security best practices. A study conducted by them also implied that undergraduate students' security behaviours were unsatisfactory while using their smartphones. As such, the findings from this study are not surprising and conform to the results of previous studies. The study is also significant in identifying the similarity of issues related to cyber security among developing and developed nations. It also establishes that cyber security incidents are rising everywhere partially due to the users' behaviour.

According to ESET Asia Cyber Savviness Report 2015, 93% of online users in Asia took notice over online security issues, yet only 40% of them were able to provide accurate answers for basic cyber security questions. Moreover, 38% of users across this region practiced risky online behaviour despite knowing the dangers of such behaviour. For instance, the ESET's study ranked Malaysia as the most 'cyber-savvy' nation yet Malaysians cyber security behaviour was not on par with Indonesia or India, which were ranked with lowest levels of cyber security awareness. Despite being ranked as countries with the lowest levels of cyber security awareness, respondents from these countries practiced better security behaviour compared to Malaysia that was ranked as the most 'cyber-savvy' country.

Recommendations

The preceding sections show that cyber security behaviour of these respondents would potentially make them vulnerable towards cyber security threats. Some of the threats possibly could be eliminated or at least reduced if only they are aware of these issues. Providing knowledge to upgrade their understanding about such issues is one of the few steps that could be taken by the relevant parties to protect such groups from the evolving cyber security threats. Thus, cyber security awareness education is important to protect the Internet users from potential cybercrimes as well as evolving cyber threats.

Although some security experts doubted the importance of the cyber security education or training (Schneier, 2013), yet many researchers believed that education or training is essential in protecting cyber users from cyber security threats (Moore, 2011; Muniandy & Muniandy, 2012, 2013). Education is important to address the cyber security threats as all protection factors play an essential role in curbing the evolving threats. Security experts believe that the weakest link in an information system is human factor. Addressing the human factor is necessary to solve many security issues especially those related to aspects that involve human interaction with Information systems (Howard & Prince, 2011; Mitnik & Simon, 2005; Whitman & Mattord, 2009).

Furthermore, these researchers strongly recommend that cyber security education be implemented as part of school as well as higher education curriculum in Malaysia, as currently cyber security is not taught formally. The majority of higher education students are not given the opportunity to learn and understand the evolving cyber security threats although previous studies had proven that higher education students are heavy Internet users. Rezgui and Marks (2008) and Sheng et al. (2010) reported that young adults, in the 18-24 year old age group are more susceptible to cyber security threats. Moreover, Rezgui and Marks (2008) claimed that only a small percentage of tertiary education institutions conduct security awareness training for its students and staff. Finally, Norum and Weagley (2007) claimed that because of students' tendency to use the Internet heavily, higher education students are at greater risk than the regular population, for example, in facing online identity theft. As such, it is important for them to get educated on these issues. Therefore, we recommend that cyber security education be incorporated into the syllabus of Malaysian students so that they are well equipped with the knowledge to protect them from cyber security threats. This could prepare them to face the real world upon their graduation and when they enter the work force in the future. Jones and Heinrichs (2012) also agreed

with the researchers on the importance for students to be educated in security issues prior to joining the workforce. Teer, Kruck and Kruck (2007) claimed that students should not bring their unsafe computer security behaviour to work. Sheng, Holbrook, Kumaraguru, Cranor and Downs (2010) admitted that while education is not going to cure all the security issues, nonetheless it is still an effective protection mechanism.

As per the preceding discussions, the researchers strongly recommend that a formal cyber security education is introduced to address the growing cyber security issues. Malaysia a rising cyber savvy nation but cyber security behaviour and awareness research is still lacking. Though Malaysia had spent billions on information technology infrastructure, yet the failure to invest in human education could be disastrous for the future generation.

Conclusion

In conclusion, this study, which focuses on Malaysian higher education students' cyber security behaviour, shows that the respondents are generally lacking in the best practices that will protect them from security threats. All five aspects in this study, namely, phishing, online scam, social engineering, malware and password usage show that students behaviour is unsatisfactory. These results conformed to other studies conducted in evaluating the students' cyber security behaviour.

The researchers strongly believed that all cyber space users must be educated on the importance of the best practices on the Internet. Moreover, the students at higher education level are heavy Internet users and they would be forming the future workforce. Such factors necessitate students to be educated on cyber security incidents. Although rising cyber security incidents may not be eliminated with education and training, Internet users must still be educated to increase their awareness of these incidents so that they would be able to take precautionary steps when necessary. Users must be empowered with the knowledge to protect themselves. Self-defence is the best shield while surfing the Internet.

References

1. Aytes, K and Connolly, T. (2004), 'Computer security and risky computing practices: A rational choice perspective,' *Journal of Organizational and end user computing,* 16(3), 22-40.

2. Bain, ZL., Hayden, M. and Sneesby, S. (2010), "An empirical study of user authentication: The perceptions versus practice of strong passwords," *Issues in information systems,* XI (1), 256-265.

3. Daka Advisory. (2014), "Digital development in Malaysia – An analysis of cyber threats and Responses," [Online], [Retrieved December 30, 2014], http://dakaadvisory.com/wp-content/uploads/DAKA-Malaysia-cyber-security-2014-web-version.pdf

4. Devi, BC and Roy, RN. (2012), "Internet use among university students: A case study of Assam University Silchar," *Pratidhwani – A Journal of Humanities and Social Science,* I (II), 183- 202.

5. ESET (Enjoy Safer Technology). (2015), "ESET Report: Huge gap in cyber security knowledge leaves Asia vulnerable," [Online], [Retrieved January 20, 2015], http://www.eset.com/au/about/press/articles/article/eset-report-huge-gap-in-cyber-security-knowledge-leaves-asia-vulnerable/

6. Forcht, KA., Pierson, JK., and Bauman, BM. (1988), "Developing awareness of computer Ethics," In Proceedings of the ACM SIGCPR conference on Management of Information Systems Personnel. Maryland USA, pp. 142-143.

7. Gan, GG., Ling, TN., Yih, GC., and Eze, UC. (2008), "Phishing: A growing challenge for Internet banking providers in Malaysia," *Communications of the IBIMA* (5), 133- 142.

8. Garnaeva, M., Chebyshev, V., Makrushin, D., Unucheck, R., and Ivanov, A. (2014), "Kaspersky Security Bulleting 2014. Overall Statistics for 2014," [Online], [Retrieved March 15, 2015], http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

9. Hamudin, N., and Ariffin, A. (2014), "Cyber crime target – Malaysians among most vulnerable to phishing worldwide," *theSun*, 24 September, p.6.

10. Howard, D. and Prince, K. (2011), Security 2020. Reduce Security Risks This Decade, Wiley Publishing, Inc., Indianapolis.

11. Internet World Stats. (2012), "Malaysia Internet Usage Stats and Marketing Report," [Online], [Retrieved December 23, 2012], http://www.internetworldstats.com/asia/my.htm

12. Internet World Stats. (2014), "Internet Penetration in Asia December 31, 2013," [Online], [Retrieved November 15, 2014], http://www.internetworldstats.com/stats3.htm#asia

13. Jones, HB., & Heinrichs, RL. (2012), "Do business students practice smartphone security?" *Journal of Computer Information Systems,* 22-30.

14. Kshetri, N. (2010), The global cybercrime industry: Economic, Institutional and Strategic Perspectives, Springer-Verlag, Berlin.

15. Malaysian Communications and Multimedia Commission. (2015), "*Internet Users Survey 2014,"* [Online], [Retrieved September 2, 2015], http://www.skmm.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2014.pdf

16. Marketing Magazine. (April 14, 2011), "Nielsen: Malaysian Internet Usage Hits 41%," [Online], [Retrieved February 28, 2012], http://marketing-interactive.com/news/25780

17. Mensch, S. and Wilkie, L. (2011), "Information security activities of college students: An exploratory study," *Academy of Information and Management Sciences Journal,* 14(2), 91-116.

18. Mitnik, DK., and Simon, LW. (2005), The Art of Intrusion – The real stories behind the exploits of hackers, intruders & deceivers, Wiley Publishing, Inc., Indianapolis.

19. Mohd Ayub, A., Wan Hamid, W., and Nawawi, M. (2014), "Use of Internet for academic purposes among students in Malaysian institutions of higher education," *The Turkish Online Journal of Educational Technology,* 13(1), 232-241.

20. Moore, R. (2011), Cybercrime Investigating high-technology computer crime, MA: Anderson Publishing, Burlington.

21. Muniandy, B. (2010), "Academic use of Internet among undergraduate students: A preliminary case study in a Malaysian university," *International Journal of Cyber Society and Education,* 3(2), 171-178.

22. Muniandy, L. and Muniandy, B. (2012), "State of Cyber Security and the Factors Governing its Protection in Malaysia," *International Journal of Applied Science and Technology,* (2)4, 106-112.

23. Muniandy, L. and Muniandy, B. (2013), "The impact of social media in social and political aspects in Malaysia: An Overview," *International Journal of Humanities and Social Science,* 3 (11), 71- 76.

24. Munir, A. and Yasin, SM. (2010), Information and Communication Technology Law : State, Internet and Information – Legal and Regulatory Challenges, Sweet & Maxwell Asia, Petaling Jaya, Selangor.

25. Norum, SP. and Wealey, O.R. (2007), "College students, Internet use, and protection from online identity theft," *J.*

Educational Technology Systems, 35(1), 45-59.
26. Ramendran, C. (2013), "RM1.07 bil lost in commercial crimes," theSundaily, viewed 1 October 2013, from http://www.thesundaily.my/news/811693
27. Ramendran, C. (2014), "Beware 'Zeus' – Police warn of danger of e-banking via smartphones and tablets," theSun, 25 September, p.1.

28. Rezgui, Y., and Marks, A. (2008), "Information security awareness in higher education: An exploratory study," *Computers & Security,* 27, 241-253.

29. Schneier, B. (2013), "Schneier on security - Security awareness training," [Online], [Retrieved September 1,2015], https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html

30. Sekaran, U. (2000), Research Methods for Business (3rd ed.), John Wiley & Sons, Inc, New York.

31. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, LF., and Downs, J. (2010), "Who falls for
32. phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA.

33. Siponen, MT. (2001), "Five Dimensions of Information Security Awareness," *Computers and Society,* (31) 2, 24-29.

34. Statista. (2015), "Daily Internet usage rate in Malaysia in 2014, by age group," [Online], [Retrieved September 1, 2015], http://www.statista.com/statistics/348017/daily-internet-usage-age-group-malaysia/

35. Talib, S., Clarke, NL., and Furnell, SM. (2010), "An analysis of Information Security Awareness within Home and Work Environments," In 2010 International Conference on Availability, Reliability and Security, Krakow, Poland: IEEE, 15-18 February, 2010, pp.196-203.
36. Teer, PF., Kruck, ES., and Kruck, PG. (2007), "Empirical study of students' computer security practices/perceptions," *The Journal of Computer Information Systems,* 47 (3), 105-110.

37. Vrana, R. (2012), "Internet a safer place: students' perceptions about Internet security threats," In Central European Conference on Information and Intelligent Systems, Croatia, 19-21 September 2012.

38. Wechuli, NA., Muketha, MG., and Matoke, N. (2014). "Survey of Cyber Security Frameworks," *International Journal of Technology in Computer Science & Engineering*, 1(2), 33-39.

39. Whitman, EM., and Mattord, JH. (2009), Principles of Information Security (3rd ed.), Thomson Course Technology, Canada.

40. Yar, M. (2013). Cybercrime and society (2nd ed.), SAGE Publications Inc., London.