INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 10, Issue 16, (2020) E-ISSN: 2222-6990

Information Security Awareness among youth in Klang Valley: A Focus Group Discussion

[1,2] Siti Zobidah Omar, [2]Krishnapriyaa Kovalan, and [2]Jusang Bolong

[1]Institute for Social Science Studies, Putra Infoport, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia, [2] Faculty of Modern Languages and Communication, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia.

Email: zobidah@upm.edu.my, priyaa.kovalan@gmail.com, jusang@upm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v10-i16/8302 DOI:10.6007/IJARBSS/v10-i16/8302

Published Date: 30 November 2020

Abstract

Issues on the lack of understanding on the awareness of information security among the Internet user has become central debate now a day. User's ignorance and negligence towards awareness of information security, may lead to being the victim of cybercrime syndicates. This can be clearly seen through the increase of number in cybercrime statistics in Malaysia. Internet users has been scammed, cyberbullying and faced loss amount of money due to their unawareness of information security. The purpose of this study is to look at the youth understanding of information security awareness. Based on the focus group discussion with a total of 20 informants among youth, this research try to obtain the youth perspective and understanding on information security awareness. Using convenience sampling, youth were chosen as informants since they are mostly engaged with new media compared to other age groups. Discussions were audio-recorded, transcribed verbatim, and analyzed using thematic analysis. Results show that there were few themes emerge on the awareness of information security, such as secure password usage, information sharing, safe online shopping website, and safe online banking website. Generally, most of the youth have a basic knowledge on information security awareness, particularly on having a secure password usage and information sharing. This study on the other hand, creates awareness on the important of information security, thus educated them to become a safe Internet user. Future study emphasizing on the government's role in regulating the cybercrime issues and educating smart device users towards safe Internet usage is recommended.

Keywords: Awareness, Information Security, Internet, Focus Group Discussion, Youth

Introduction

Information security is the assurance of information and its critical elements (Whitman and Mattord, 2008). Information security is of great importance and interest to everybody in the

world of technology today, despite using any types of smart device. That is why information security is the most important in our everyday life. Lack of awareness in information security will be more likely to develop applications that are not secure or build networks that are insecure and easier for attackers to penetrate. Hence, information security awareness is mostly ideal in our everyday lives.

Young adults nowadays are arguably lack of safety precautions when using smart devices such as mobile phone, laptop, desktop, tablet and many more (Amirudin, 2014). Also, this is since people like to update their everyday activity on social media, social media has been the source of privacy intrusion. Besides, the government also has introduced a few concepts such as e-government, e-commerce which need an Internet connection. Frequent usage of the Internet certainly has positive impacts on the socio-economic life of young people, but it also has a variety of negative implications (Omar, Fadzil, & Bolong, 2019).

Although a lot of effort has been done to educate the public and Internet users, cybercrime rates keep increasing. This can be proven that awareness among youth Internet users in Malaysia is still very low. The low level of Internet awareness causes the users to discover cybercrime issues, such as a victim of online fraud, personal information disclosed, and others. As for how explained above, the effect of the low level of Internet awareness has an impact on cybercrime cases in Malaysia. Table 1 below shows the total statistic of the cybercrime incident from 2015 up to 2019. This statistic shows cybercrime categories, such as content-related, vulnerabilities report, intrusion attempt, cyber harassment, malicious codes, intrusion, fraud, spam, and spam e-mails. Table 1 shows the number of cybersecurity cases that has been increasing from 2015 till 2019 by MyCERT, CyberSecurity Malaysia.

Table 1
Statistics on Cybersecurity Incidents Year 2015-2019

Incident	**2015**	**2016**	**2017**	**2018**	**2019**
Content Related	33	50	46	111	298
Vulnerabilities Report	22	35	60	92	91
Intrusion Attempt	303	277	266	1805	1359
Cyber Harassment	442	529	560	356	260
Malicious Code	567	435	814	1700	738
Intrusion	1714	2476	2011	1160	104
Fraud	3257	3921	3821	5123	7774
Spam	3539	545	344	342	129
Total	**9877**	**8268**	**7922**	**10689**	**10753**

Source: MyCERT, CyberSecurity Malaysia 2020

From the above table, it can be concluded that cybercrime cases increased rapidly from 2015 to 2018. Rosly (2013) said that the knowledge level of safe Internet usage is still low among the public of Malaysia. The low awareness level makes youth to become a victim of cybercrime. High dependence on the Internet has made more cybercrime issues occur. When an individual is too dependent on the Internet, the cybersecurity element becomes a question of safe usage of the Internet (Brown, Howe, Ihbe, Prakash, & Borders, 2008; Huber, Mulazzani,

Kitzler, Goluch, & Weippl, 2011; Hull, Latulipe, & Lipford, 2011). Hence, as an Internet user, the responsibility of using the Internet safely is highly essential.

Methodology

The study used a qualitative approach using focus group discussion with an in-depth interview among youth. Focus group discussions are to gather information on a specific topic which examines participant's personal experiences, opinions, knowledge and attitudes through an interaction (Hayward, Simpson, & Wood, 2004). Researchers become a "moderator" and interview the informants, conducts a group discussion between informants and not between the researcher and the informants (Hohenthal, Owidi, Minoia, & Pellikka, 2015; Mahendran & Indrakant, 2014).

Using convenience sampling, youths aged from 21-40 were chosen as informants in this study. The reason youth were chosen because they are the heavy user of the Internet compared to other age groups. Hence, they would have a different opinion, experience and at the same time facing more information security issues when using the Internet. Twenty informants were participated in this focus group discussion and were divided into three groups. Two groups consisted of 7 informants and one group consisting of 6 informants. The duration of the focus group discussion is late within the one-and-a-half-hour to two hours precisely after receiving the agreement and consent from all informants. Informants were initially informed about the topic of the in-depth interview, 'Information Security Awareness among young Internet users'. The researcher was the interviewer of this discussion. Before the discussion began, the interviewer described the objectives if this study, ethics of the study, and information confidentiality to all the informants. The interview was then audio recorded using a voice recorder. Then, the recorded audio was later transcribed verbatim. Name of the informants was remained anonymous to protect its privacy and confidentiality. Data later were analysed using thematic analysis and constant comparison.

Results and Discussion

Based on the analysis, for the informants' profile, results show 75% were female, and 25% were male, with half of them (50%) are Malay, followed by Chinese and Indian ethnicity. Most of these youth are unemployed and still pursuing their education at higher institutions. Table 2 below summarized the demographic profile of the informants.

Table 2
Demographic profile of informants (N=20)

	Quantity	Percentage (%)
Gender		
Male	5	25
Female	15	75
Age		
21 - 30 years old	14	70
31 - 40 years old	6	30
Race		
Malay	10	50
Chinese	6	30
Indian	4	20
Highest Education Level		
Undergraduate	8	40
Postgraduate	12	60
Job Status		
Employed	2	10
Unemployed (student)	18	90
Marital Status		
Single	13	65
Married	7	35

Analysis of the focus group discussion among youth, several main themes were identified. Krippendorff (2004) asserted that identified themes should be internally homogeneous and externally heterogeneous. This means that there should be no similar data that falls in more than one group. As such, based on the analysis, awareness of information security from the youth perspective has been group into four main themes; password usage, information sharing, safe online shopping websites and safe online banking websites.

Password Usage

One of the important things that come across the mind of the youth when it comes into information security awareness is the use of password online. To them, password usage is highly crucial as negligence in using the password will have an effect on the information that can be retrieved and shared by others without the consent of the owner. A strong password is necessary as it can help to make sure that the information is at a safe place. As informant H1, a working female emphasized that:

> "I make sure that my password is secure with all types of keyboard characters. I will make sure that the application states that my password is very strong. This creates a secure and protected information online." (H1, female, Ph.D. student, married, 33 years).

For her, as a working married woman, the security of the information is highly necessary as it is dealing with office management, her performance at work and trust by others. Working for several years in a well know company in the city, requires her to be more careful in using the internet for information transactions. A strong and secure password is very important in maintaining the information at a safe place as what has been suggested by Pitchan & Omar (2019) argued that strong and secure password is the mean reputation for a company where it will create trust by the customer and thus creating a good image and reputation for the company.

Information security issues are highly at risk nowadays due to the heavy usage of the Internet and vast Internet users. Internet users have to be aware of the safety precautions when protecting their information online, such as secure password usage (Brandao, 2018). Forgery attack, offline and online password guessing, anonymous authentication, impersonation attack and identity theft are the most common information security threats. Password-based authentication can usually vary from the characters on the keyboard and keypad such as small letters, capital letters, numbers, special characters such as “, /, ?!, @ and many more. There are different types of authentication factor such as password or PIN, biometric, face recognition, retina or iris identification and many more. During this focus group discussion, informants stated that they use password using all types of keyboard characters, using biometric authentication, store password in a secure location, and do not allow websites to remember passwords.

This view is in line with informant H17, a female single student. For her, she is concerned when it comes to revealing the password to others, where the security of her password is her utmost important to be protected. She further accentuated that:

> “When we come across a new website, and the website requires us to save the password, never allow websites to do so. Always keep passwords safe by not recovering in your smart devices.” (H17, female, Bachelor student, single, 23 years)

Being a student at a renown research university, her involvement in searching for information to complete her academic task and assignments is essential. This entails her to access to another web-site which requires her to save the password, to get more information. However, for informant H17, protecting her password in very crucial. To a certain extend another youth would create two emails to safeguard the information that they would share, meaning that they have to use two different passwords. As informant H5 emphasized:

> I usually have two email addresses, one for my personal and study purposes, and the other email is for other uses. I divide my email for certain things because I feel that way it is safe. I do not open my second email so that I will not wonder who emailed me or whatsoever.” (H5, female, Masters Student, single, 26 years)

For her, having two emails and using two different passwords enable her to manage the information that she would like to share and protect.

Information Sharing

Another main issue that has been discussed intensively among the youth is information sharing. Information sharing happens when the other party requested the user to reveal certain information for them to be accepted or join certain web-site. Informants in this study stated that they will not share certain personal details, separates the usage of personal email and other purposes email, and social media information sharing is unnecessary. As informant H2, a PhD student stated that:

> "Sometimes it depends on the information they ask. If the site asks me for my identification card number, I will give because I feel that will not bring any harm to me." (H2, male, PhD student, single, 28 years).

For informant H2 perspective, giving his identification card number did not bring harm to him. This is because, after looking thoroughly at the authenticity of the web-site and he trusted the website, allowing him to reveal his identification card number. On the other hand, informant H16 further voices out that people nowaday always post their activities and information to the public. She stated that:

> "People nowadays post every information of their personal life on social media platforms such as their family, newly bought car, identity card details, and many more. Once I saw a well-known person uploaded her daughter's results slip with an identity card number, address, and other details. Public nowadays should be aware that everyone can become a victim of cybercrime regardless of their social status. I will not and have not posted or shared any personal details of myself or family on my social media platform. Social media platform should be handled with care, and our data is very precious." (H16, female, PhD student, single, 29 years).

Revealing personal information to the public may lead to the increase numbers of attacks on information security. These attacks increased due to the vast personal information being publicised online, such as family members, home address, phone number, and many more. Further, these are the information that regularly being saved and revealed by youth in their social media accounts. Feinberg (2011) stated that social media such as the Facebook is capable of using personal data of any users and share the data with advertising partners. This is why sometimes a social media user encounters watching advertisement related to their online posts or their daily needs. Facebook users not only have to worry about their Facebook friends maliciously exploiting their personal information, but Facebook itself has the capacity to use the data of its users in unseen ways, and likely unwanted, by the user.

Safe Online Shopping Websites

Online shopping is one of the new norms among youth, and it is quite popular among the young generations. The online shopping culture has bought changes to the youth lifestyle. However, security in the e-commerce transaction is extremely worrying. Online buyers need to be aware of the security breaches involves and also to protect their sensitive information shared online. A major information security issue in electronic commerce is a customer's privacy data intrusion (Cagaoan et al., 2014). The greatest public concern when purchasing

online is losing personal information (Masoud, 2013). This issue arises when the online shopping websites reveal and transmit customer's personal information to the public (Zhang et al., 2012). A privacy-conscious buyer will hesitate to provide correct and complete personal information to the online seller. In this regards, some informants did not prefer online shopping. As informants H14 stated that:

> "When performing an online transaction, make sure to recognize whether it is an authorized website or not. An authorized URL of a website always begins with https." (H14, female, Ph.D. student, married, 29 years).

In this study, informant H14 stated that they only purchase online if the website is authorized with https:// in URL and credible website. Informant H18 further emphasised that:

> "When performing an online banking transaction on the top right of the website, you can see a 'lock' sign. That means that website is safe to use. I mostly use Firefox compared to Google Chrome" (H18, female, Bachelor student, single, 22 years).

Niranjanamurthy & Chahar (2013) identified that buyers and sellers are not very much involved in e-commerce because of the challenges faced by security issues. That makes an online seller improve their understanding of online security issues. As informant H8 preferred to use his laptop rather than using smartphone when it comes to online transactions for safety and security reasons.

> "I always make an online transaction using a laptop because it is much safer than using smartphones." (H8, male, working, married, 32 years).

This opinion is also agreed by informant H15, by saying that:

> "It is not safe for us to use public Wi-Fi to perform online banking transactions. That is because some hackers may retrieve our online banking data from the public Wi-Fi" (H15, male, Bachelor student, single, 23 years & H13, male, working, married, 29 years).

However, when it come to purchasing electronic gadget, informant H6 is more concern on the quality of the gadget she purchases. She further says that:

> "I avoid purchasing electronic gadget online because I am afraid that my item will be not as quality as expected, and I might not like the colour or texture." (H6, female, PhD student, married, 28 years).

Safe Online Banking Websites

Another issue that has been highlighted by the youth is the online banking website. E-banking is a system that enables users to perform financial transactions on an online banking website. Almost all banks nowadays offer online banking system. The National Bank of Malaysia (2020) stated that 26 banks offer online banking system to their users in Malaysia. Any customer's

information can be compromised by expert hackers by adjusting the customer's online information. These hacking experts would spread the malicious virus to corrupt customer's personal data. Customers may experience a low quality of information system performance on an online banking platform (Jassal & Sehgal, 2013). Informants H8, H15 and H18 stated that:

> "I always make an online transaction using a laptop because it is much safer than using smartphones." (H8, male, working, married, 32 years).
>
> "It is not safe for us to use public Wi-Fi to perform online banking transactions. That is because some hackers may retrieve our online banking data from the public Wi-Fi" (H15, male, Bachelor student, single, 23 years).
>
> "When performing an online banking transaction on the top right of the website, you can see a 'lock' sign. That means that website is safe to use. I mostly use Firefox compared to Google Chrome" (H18, female, Bachelor student, single, 22 years).

The youth experience in e-banking makes them more cautious. They could hardly use public Wi-Fi, using their own gadget for online transactions. Pakojwar & Uke (2014) identified several factors to determine a safe online banking website experience. Firstly, have up-to-date security updates. Then, every online banking customers need to have anti-virus software and anti-spyware program. Storing password securely and use a password protected smart device is also a factor of secure online banking usage. Informants said that they only perform any online transaction when using a laptop rather than smartphones, the URL of a website is authorized, do not use public Wi-Fi, and websites with padlock sign at the right top of the online banking website.

Based on the youth understanding and perspective of the information security awareness, Table 3 below, summarizes the main themes and the sub-themes of the discussion above.

Table 3
Summary of main theme and sub themes of information security awareness

Theme	Sub themes
Password usage	• Use varieties of keyboard characters such as alphabets, numbers and special characters • Do not agree to save password in any website or application • Different authentication method can be used such as fingerprint authentication • Do not save any application's password in smart devices
Information sharing	• Demographic profile details • Do not give personal email/ Have a separate email address for other purpose

Safe online shopping websites	• Use authorized website which has *http://* at their website page • Do not perform online shopping because of security concerns • Purchase through credible website
Safe online banking websites	• Perform transaction only using laptop/ desktop • Use authorized website which has *http://* at their website page • Do not use public Wi-Fi to perform any transaction • Look for a 'padlock' image at the top right of the page

Conclusion

To understand the information security awareness among youth is crucial as youth are the heavy user of the Internet. Based on the focus group discussion with the youth, it is clearly shown that the youth have a basic knowledge and aware of the information security. Information security awareness to them is related to password usage, information sharing, a safe online shopping website and safe online banking websites. Their different perception of information security awareness has bought them to recommend several protective measures in reducing risks while using online activities. To conclude the summary of the main and the sub-themes discussion above are presented in Figure 1 below.

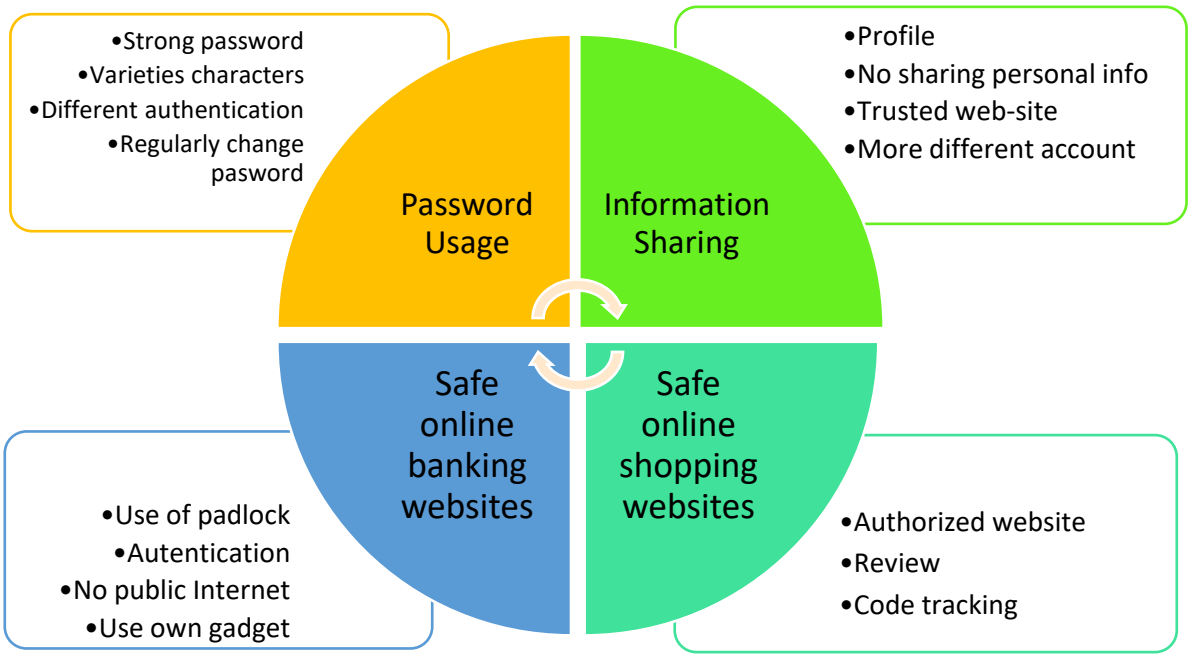

Figure 1: Information security awareness among youth

Password usage, information sharing, safe online websites and safe online banking websites is the most themes being discussed by the youth when it come to information security awareness. As the role of the the Malaysian government has played, they are also has been very much helpful in handling cases of information security despite vast cases are happening daily. Hence, more policies and laws has be emphasized and enforced in handling these cases,

especially in providing a safe Internet usage platform for the upcoming generation. Furthermore, using the youth perpective and experience from this focus group discussion, the researcher suggests that more attention should be given towards government's role in regulating the information security issues and educating smart device users towards safe Internet usage is recommended. More campaigns and social activity regarding basic information security awareness and safety practices when using the Internet could be held in schools and also in public places. In conclusion, it is hope that this study would provide some useful insights and suggestions to the government for further consideration.

Acknowledgements

The authors would like to thank the Ministry of Higher Education Malaysia for sponsoring this project under Fundamental Research Grants Scheme, Project Code 05-01-18-2036FR and FRGS/1/2018/SS09/UPM/ 02/1/5540161.

References

Amirudin. (2014). *Tingkatkan kesedaran keselamatan di Internet untuk cegah jenayah siber.* http://www.theborneopost.com/2014/12/02/tingkatkan-kesedaran-keselamatan-di-internet-untuk-cegah-jenayah-siber/#ixzz3gVKwJYm1 *(In Malay).*

Brandao, P. R. (2018). The Importance of Authentication and Encryption in Cloud Computing Framework Security. *International Journal on Data Science and Technology, 4*(1), 1-5.

Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008). Proceedings of the 2008 ACM conference on computer supported cooperative work. *Social networks and context-aware spam*. New York, NY: ACM.

Cagaoan, K. A. A., Buenaobra, M. J. A. V., Martin, A. T. M., Paurillo, J. C., & Jonathan, C. (2014). Privacy awareness in E-commerce. *International Journal of Education and Research, 2*(1), 1-6.

Feinberg, S. E. (2011). O privacy, where art thou? *Chance, 24*(2), 7-9.

Hayward, C., Simpson, L., & Wood, L. (2004). Still left out in the cold: Problematising participatory research and development. *Sociologia Ruralis, 44*, 95–108.

Hohenthal, J., Owidi, E., Minoia, P., & Pellikka, P. (2015). Local assessment of changes in water-related ecosystem services and their management: DPASER conceptual model and its application in Taita Hills, Kenya. *International Journal of Biodiversity Science, Ecosystem Services & Management, 11*, 225–238.

Huber, M., Mulazzani, M., Kitzler, G., Goluch, S., & Weippl, E. (2011). Friend-in-the-Middle attacks: Exploiting social networking sites for spam. *IEEE Internet Computing, 15(3),* 28-34.

Hull, G., Latulipe, C., & Lipford, H. R. (2012). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology, 13*(4), 289-302.

Jassal, R. K., & Sehgal, R. K. (2013). Comparative Study of Online Banking Security System of various Banks in India. *International Journal of Engineering, Business and Enterprise Applications (IJEBEA) 6*(1), 90-96.

Mahendran, A., & Indrakant, S. (2014). Public Distribution System in Tamil Nadu, India: Rice Supply Scheme of Prosperous, Problems and Policy. International Journal of Academic Research in Public Policy and Governace, 1(1), 17–29.

Krippendorff, K. (2004). *Content analysis: an introduction to its methodology*. Thousand Oaks, California: Sage Publications

Masoud, E. Y. (2013). The effect of perceived risk on online shopping in Jordan. *European Journal of Business and Management, 5*(6), 76-85.

National Bank of Malaysia. (2020). Financial Stability. Retrieved from, https://www.bnm.gov.my/index.php?ch=li&cat=banking&type=CB&lang=en

Niranjanamurthy, M., & Chahar, D. (2013). The study of E-Commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 2(7)*.

Omar, S. Z., Fadzil, M. F. B., & Bolong, J. (2019). The Relationship between Internet Usage and Subjective Wellbeing among Youths in Malaysia. *International Journal of Academic Research in Business and Social Sciences, 9*(7), 461–469.

Pakojwar, S., & Uke, N. J. (2014). Security in Online Banking Services – A Comparative Study. *International Journal of Innovative Research in Science, Engineering and Technology, 3*(10), 16850-16857.

Patton, M. Q. (2002). *Qualitative, research & evaluation methods*. Thousand Oaks, California: Sage publications.

Pitchan, M.A & Omar, S.Z. (2019). Dasar keselamatan siber Malaysia: Tinjauan terhadap kesedaran netizen dan undang-undang. *Jurnal Komunikasi: Malaysian Journal of Communication, 35*(1), 103-119

Rosly, Y. (2013). Tahap kesedaran keselamatan masih rendah. Retrieved 22 April 2020 from, http://ww1.utusan.com.my/utusan/Timur/20130926/wt_07?Tahap-kesedaran-keselamatan-masih-rendah (In Malay).

Whitman, M., E. & Mattord, H. J. (2008). *Management of information security*. Boston: Course Technology.

Zhang, L., Tan, W., Xu, Y., & Tan, G. (2012). Dimensions of consumers' perceived risk and their influences on online consumers' purchasing behaviour. *Communications in Information Science and Management Engineering, 2*(7), 8-1.