Creative Education, 2019, 10, 2850-2858
https://www.scirp.org/journal/ce
ISSN Online: 2151-4771
ISSN Print: 2151-4755

The UKM Students Perception towards Cyber Security

Mohd Jasmy Abd Rahman, Mohd Isa Hamzah, Mohd Hanafi Mohd Yasin, Mohd Mokhtar Tahar, Zolkepeli Haron, Nur Kamariah Ensimau

Faculty of Education, The National University of Malaysia (UKM), Bangi, Malaysia
Email: mjas@ukm.edu.my

How to cite this paper: Rahman, M. J. A., Hamzah, M. I., Yasin, M. H. M., Tahar, M. M., Haron, Z., & Ensimau, N. K. (2019). The UKM Students Perception towards Cyber Security. *Creative Education, 10,* 2850-2858.
https://doi.org/10.4236/ce.2019.1012211

Received: October 21, 2019
Accepted: November 26, 2019
Published: November 29, 2019

Abstract

The world moved to digital era tremendously. Therefore the societies need to aware on the issue related to the cyber security. The purpose of this study was to identify the student perception, knowledge and awareness regarding cyber security. The research found that the student perception, knowledge and awareness were average. Thus, some program, such as awareness seminar, courses should be driven to take in order to highlight the society concern about cyber security.

Keywords

Cyber Security, Awareness, Concern

1. Introduction

In the new era of globalization, the world nowadays is full of technologies and internet that lead our humanity to a modern society and evolves from time to time. Almost every job and task nowadays require the usage of technologies especially internet, whether it is filing system, e-mail, important data recording or even a meeting. Other than that, the people's social life also depending on the internet as it is considered as daily tools that they must have (Ishak & Ghani, 2015; Ilham, 2016). As we can see, users these days are getting "obsessed" with uploading their personal information such as their routine and identity like the place they went and pictures on their Facebook, Instagram, etc. (Sandi, 2007). Therefore, individuals need to acknowledge the importance of cyber security to ensure their identity and work is well protected.

Moreover, with an insufficient knowledge in the cyber security gave a way to the unauthorized person to hack into our network which can lead to identity theft cases such as "catfish" (Rahman, 2012; Pitchan & Omar, 2019). That is not

the only thing can happen with a weak protection, the hacker might as well send a virus to crush down the firewall and eliminate our important works. These cases can be a minor problem but it can also be a major one when the hacker is able to use our identity or works to get the ransom and threatening our family (Rahman, 2012).

Having a secure and solid cyber security will protect our system on every device that we have. This notorious action does not only target an individual but also big companies, society, and even the nation. The main prey in this situation is usually the youngster. This is because most youngsters do not have a sufficient knowledge about any of this security system and how exposing they to the world in the social media can bring harm if the proper measurement is not taken.

Cyber security may seem unimportant to us at some time, but having a protected system and free from virus definitely may save us from being encrypted and losing all of our private work. Hacker might seem dangerous but internet scammers are also the newest parasite in these modern days. Scamming/users in order to receive their information like credit card or bank account numbers are easily can be done using a trick such as sending a gift cards, advertisement offer and even in online shopping. Anti-spyware and anti-malware can protect the users from receiving any of the virus which may potentially affecting the device used when visiting unusual sites that popped out as well.

2. Problem Statement

Nowadays, the numbers of cyber-criminal which better known as the Blackhat are increasing not just globally but also domestic. This increment is not just about the numbers of the crime and the numbers of the Blackhat but it is also their skills in the Information Technology (IT). Abidin et al. (2018), said there are various cyber medium used by criminals to attack their victims such as social media platform like Facebook. For example, Mark Zuckerberg the founder of the famous social network Facebook originally just an ordinary IT student who find that hacking is nothing but the word ease himself. Unfortunately, most of the time those with such skills tend to violate their own ability by using it for the wrong purposes and more worst for those who have less IT skills with their chances of becoming a cyber-crime victim.

Cyber-crime activity is becoming a great risk to three main parties which are the individual, community and the government of country if no action taken to overcome this problem. This crime has affected individual especially the youngster due to 90% of them actively uploading a various personal and family information. Unfortunately, their information becomes the leverage to the Blackhat to hack into their privacy such as banking information, house location or address and others that can threaten our safety. As a precocious step, adults should monitor educate youngster especially children under-age in sharing information. Arifin et al. (2019) said users at this age need parental guidance and

support because they are still naïve or immature to understand the risks of Internet (Bonk, 2015; Jansen et al., 2016).

This kind of crime may cause other serious risk which may lead to catastrophe as nowadays modern technology is not only about the gadget but also everything business investment area. Investment nowadays is widely operated under cyber platform to make every works such as filings, stocks information and others more convenient but in the other side vulnerable at risk of being penetrated by Blackhat.

To keep the safety of the country, a solid and high cyber security system is very important to constraint the hacking progress each day. (Salamzada et al., 2015; Hasen, 2019) stated the importance of cyber space for country development, many countries have invested large amount of money for cyber space application show how this matter need to be taken seriously by all country. As discussed above, if the country cybersecurity falls to the hand of these cybercriminals, the country safety is at risk as they could access sensitive information including national top secret and confidential information such as government's administration and the military information (Kallet, 2004). Such information could be sold to other countries and used as their leverage for ransom and self-interest.

3. Purpose of This Study

The purpose of this research also to define the respondents' point of view in applying their knowledge regarding cyber security in their daily routine and suggestion on how to overcome the crisis faced by the user when they encounter problems like virus attack, hacker, scammers, etc. Their answers will be identified by us critically and detailed. These 3 aspects which are from their understanding, opinion and their way of overcoming the situation are studied in order to get the complete report

4. Objectives of the Research

In the research, it contains few main objectives that we provide in the survey for 30 respondents in order to study and analyze their answer that is given. Through the survey, we are able to collect a complete research to convey a conclusion on the given topic. The objectives that are provided are:

1) The knowledge of the respondent regarding the cyber security and their understanding concerning the issue in details.

2) Their perception or view of cyber security that involves in hacking, scamming and even virus that can affect their devices and information.

3) The respondents deal with the suggestion in overcoming problems related to cyber security

5. Methodology

According to Bryman Alan, methodology refers to a discussion of the underlying

reasoning why particular methods were used. This discussion includes describing the theoretical concepts that inform the choice of methods to be applied, placing the choice of methods within the more general nature of academic work, and reviewing its relevance to examining the research problem. The discussion also includes a thorough review of the literature about methods other scholars have used to study the topic. Basically, this section discussing how the data or the information was collected or generated and how was it analyzed. A study of the methodology is focusing on two (2) kind of ways in order to collect the data which known as the Qualitative Research and the Quantitative Research.

6. Findings

6.1. Respondents Knowledge on Cyber Security

The first statement is "I understand that the definition of cybersecurity is the use of technology, processes, and activities that are specially designed to protect computer's programs and data chain from attacks and illegal access. Most of the respondents strongly agree (46%) to this statement. The second statement is "I do not take cybersecurity lightly" and there are 39% respondents which are the highest agree with this statement. The third statement is "I know the consequences if cybersecurity were not monitored intensively" and the highest scale which the respondents chose is agreed (46%). The fourth statement is "I know about the "WannaCry" attack that happened in our country early this year" and the respondents agree that they do know about this attack (42%). The fifth statement is "I know the ways to reduce the risks of "WannaCry" attack from happening again" and most of the respondents (27%) chose neutral. The sixth statement is "I apply cybersecurity in all the devices that I use" and the scale which has the highest pick is agreed (46%). The seventh statement is "I never knew or never been expose to anti-virus software" and there are 33% respondents which is the highest number strongly disagree with the statement (Figure 1).

6.2. Respondents Consent on Enhance Cyber Security

The first statement is "The usage of the password is important to prevent illegal access to sensitive information from happening" and the highest scale (69%) that the respondents chose is strongly agreed. The second statement is "It is encouraging to use safe network chain to access any information" and most of the respondents (46%) strongly agree with this statement. The third statement is "User can shop online without doing any background check on the company that involves", this is a negative statement which brings the respondents (51%) which is the highest to strongly disagree with it. The fourth statement is "The anti-virus scanning only needed to be done when the virus has affected the system", this statement is also a negative statement and the scale that has the highest number (55%) is strongly disagree. The fifth statement is "Having online contact can expose personal information which can bring risks" most of the respondents (58%) chose neutral. The sixth statement is "Accessing the cyber without authorizing

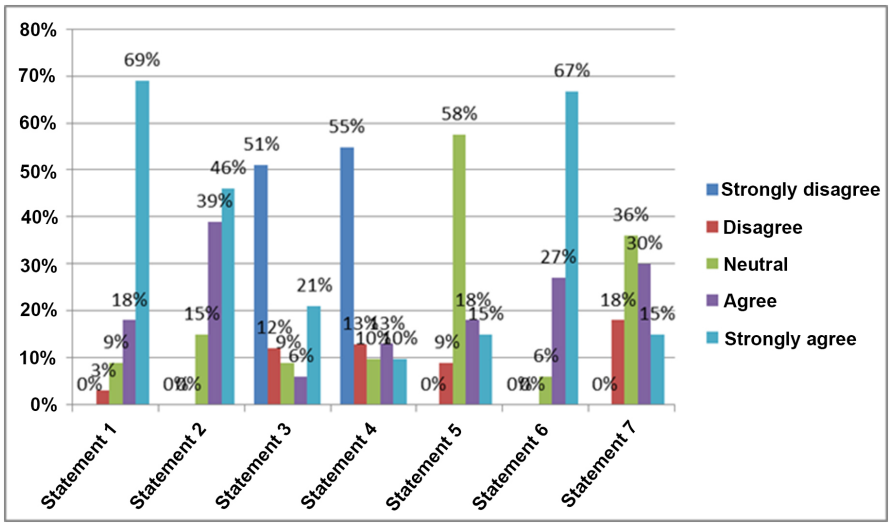

Figure 1. Knowledge on cyber security.

permission does not only brings danger to your filing but also expose you to the stealing of identity" and 67% respondents which are the highest strongly agree to this statement. The seventh statement is "Fan-made websites can contribute to cyber security problems" and there are 36% respondents (the highest) chose neutral (Figure 2).

6.3. Respondents Concern on Risk if Not Aware of Cyber Security

The first statement is "The possibility of being a target of scammers is one of the main reasons of why we have to protect our personal information" and most of the respondents (57%) strongly agree to this statement. The second statement is "Weakly-structured password is one the reasons why cybercrime happened" and 49% respondents which are the highest also agree with this statement. The third statement is "The lack of concern about cybersecurity contribute to cybercrime" and the highest scale is strongly agreed which has 49% respondents. The fourth statement is "A virus can attack the system and files up to a critical stage without us knowing" and most of the respondents (47%) agree with this statement. The fifth statement is "The false advertisement of well-known brands is one of the ways to attract users to expose their personal information" and the highest number of respondents (42%) only agree to this statement (Figure 3).

6.4. Respondents Awareness on Cyber Security

The first question is "Installing anti-virus software could help in preventing virus attack" and the highest number of respondents strongly agree to this statement. The second statement is "Users are not encouraged to surf any suspicious websites or advertisement" and the third statement "Attending seminar/classes for cyber security can help to increase awareness regarding cybersecurity" has the highest number of respondents (49%) strongly agreeing to this. While the fourth statement "Users are not encouraged to surf suspicious websites or

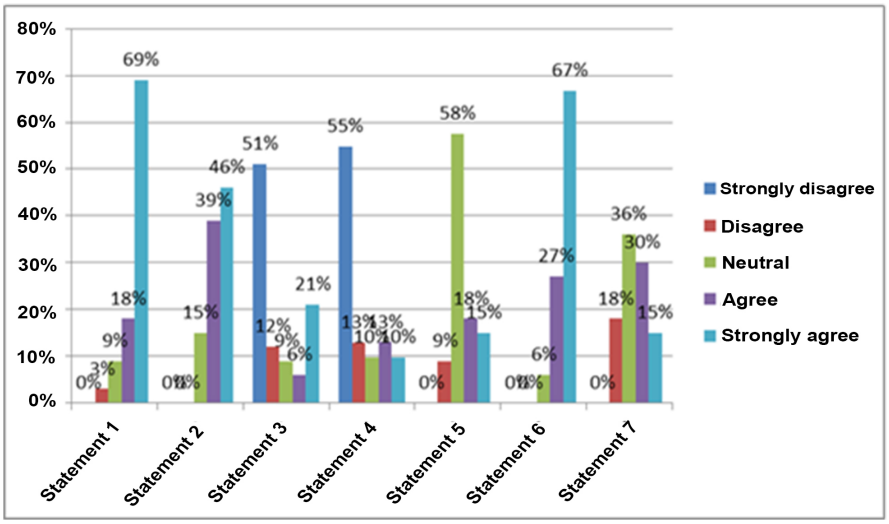

Figure 2. Way to enhance cyber security.

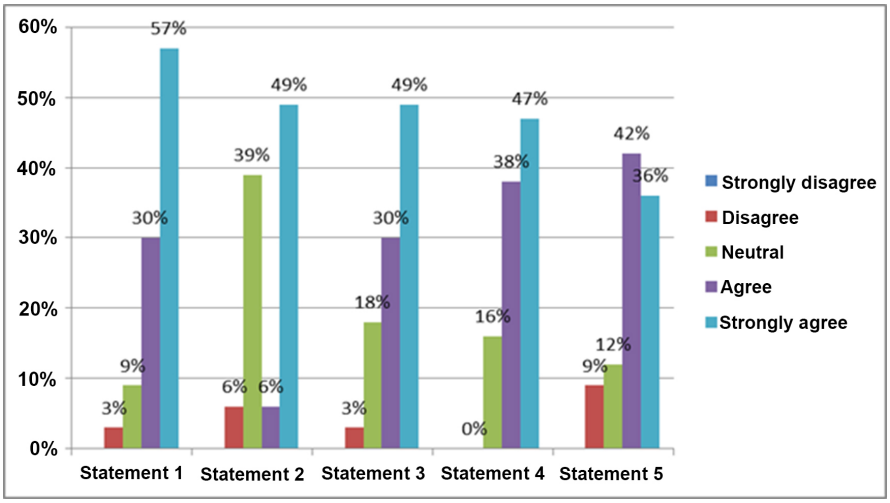

Figure 3. Risk if not aware on cyber security.

advertisements" and the fifth statement "I will do anything to ensure my cyber is secure" only agree with these statement (Figure 4).

7. Discussion

Based on our research, issues related to cyber security is more concern to individual as well as government, businesses, law and other parties. There are a few solutions that can be used to minimize the chances of cybercrime to occur.

Firstly, it is advisable for the individual users or other parties to install anti-virus software on their devices. A few examples of anti-virus programs that can prevent viruses from invading your devices are McAfee, Norton, AVG, and Kaspersky. The purpose of anti-virus software is to identify and remove computers viruses and obscure programs. Therefore, anti-virus software enables the scanning of viruses from time to time because frequent virus scanning is

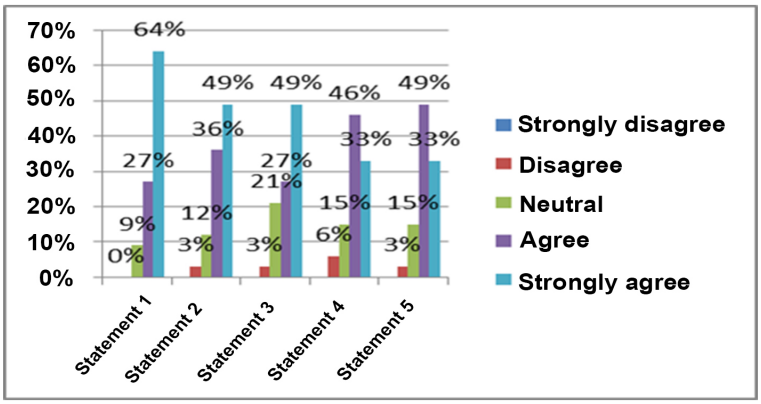

Figure 4. Awareness on cyber security.

essential to prevent the viruses from invading the devices as installing anti-virus software does not keep the devices fully safe from being attack by viruses. Also, individual users and other parties must be reminded to update the anti-virus software because the computer is highly likely to be threatened by new viruses to harm the devices.

Secondly, installation of the firewall for devices and home networking is encourageable for the benefit of the individual users especially big businesses. The internet firewall is designated for the purpose of protecting the computer from data accessing and viruses that are not wanted. Nowadays, all the devices come with the firewall program which the firewall is responsible for checking and installation that occurs in the devices. Besides that, the firewall is important to every device as it helps to protect the users from being victims of hackers without them being aware. Individual users and parties can be the decision maker on how much they want the content to be filtered and which websites are safe to browse.

Thirdly, individual users should not open suspicious emails from the unknown sender. This solution is applied to all the individual users who have email accounts. Every user must always be reminded that email is a platform which is commonly used for an intentional crime such as spreading the viruses such as Trojan, worm, spyware, malware and more. Therefore, users must make it as practice to scan the email attachments for any viruses before opening it. Also, it is advisable for users to delete the suspicious emails although it is from someone the users know because the sender might not aware of the email contained viruses. Opening email attachment with the file name ending with .exe and .vbs is not advisable because such attachment is commonly used to transmit viruses.

Fourthly, another effective solution to minimizing the cybercrimes from happening is by taking the issues related to password seriously. In order to protect an account, the user must use a unique and difficult password degree. For example, a password must contain 8 alphanumeric characters with the use of either lower or upper case such as maryisabel THP99. Users are advised to never exposed password to strangers as the action opens the opportunity for the hackers

to harm users devices, steal information or to do ransom attack. Besides that, keeping information regarding the password on the computer or laptop is also not advisable as anyone can access those devices and try to access the users' accounts for bad purposes.

Lastly, users should always make sure that the websites that are visited begin with https://. HTTPS stands for Hyper Text Transfer Protocol Secure (HTTPS). It is an improvised version of HTTP. The purpose of HTTPS is to encrypt the communication between users' browser and the website. Besides that, users are also encourage able to do online transaction only with trusted suppliers for the safety of personal identifiable information such as account number, name, address and others from being used for the bad intention for identity thefts.

There are other solutions that are able to help minimize cybercrime from happening. Even so, we think that the five (5) points suggested are among the solutions that are important and considered as early steps of preventing the users from being victims of cybercrime.

8. Conclusion

In conclusion, societies from the digital era should have the basic knowledge and awareness of the issues related to cyber security as the problems related to cyber security arises rapidly throughout the years. Societies have to be well aware that many problems could occur in this technology-based century. Besides that, issues related to cyber security seem to give drawbacks toward the individual, society, nation, and country. Therefore, we should be well reminded that this issue is not something to be taken lightly as it gives impacts in many aspects. Everyone should be well informed of what is cyber security and the crimes that occurred when the security level is too low. They should also take notes on how to prevent themselves from becoming cyber-crime victims. All in all, cyber-crimes are complex problems to be curbed especially when it involves malicious activities which are why everyone should play their roles in securing their cyberspace from being invaded and also from becoming victims to cyber-crimes.

Acknowledgements

This research was partially supported by grant received from the Faculty of Education, Universiti Kebangsaan Malaysia code PP-FPEND-2019.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Abidin, N. Z. et al. (2018). Knowledge and Protective Practice towards Love Scam among Female Facebook Users in Malaysia. *Jurnal Komunikasi: Malaysian Journal of Communication, 34,* 113-133. https://doi.org/10.17576/JKMJC-2018-3404-07

Arifin, N. et al. (2019). Parental Awareness on Cyber Threats Using Social Media. *Jurnal Komunikasi: Malaysian Journal of Communication, 35,* 485-498. https://doi.org/10.17576/JKMJC-2019-3502-29

Bonk, C. J. et al. (2015). *MOOCs and Open Education around the World*. New York: Routhledge Taylor & Francis Group.

Hasan, A. S. (2019). Media Democratization and Security Challenges in the Digital Age. *Jurnal Komunikasi: Malaysian Journal of Communication, 35,* 237-251. https://doi.org/10.17576/JKMJC-2019-3501-16

Ilham, M., Madiha, N., & Salleh, M. A. O. (2016). Privasi Dan Keselamatan Maklumat Dalam Kalangan Pengguna Instagram Ketika Membeli Produk Secara Dalam Talian. *Journal of Social Sciences and Humanities, 11,* 32-44.

Ishak, M. S., & Ghani, J. A. (2015). Pengurusan Privasi Facebook Penjawat Awam: Pengaruh Intensiti Penggunaan, Kemahiran Swaawas Dan Orientasi Privasi Organisasi. *Jurnal Komunikasi: Malaysian Journal of Communication, 31,* 61-82. https://doi.org/10.17576/JKMJC-2015-3102-05

Jansen, D., Rosewell, J., & Kear, K. (2016). Quality Frameworks for MOOCs. In *Open Education: From OERs to MOOCs* (pp. 261-281). Lecture Notes in Educational Technology (LNET), Berlin: Springer. https://doi.org/10.1007/978-3-662-52925-6_14

Kallet, R. H. (2004). How to Write the Methods Section of a Research Paper. *Respiratory Care, 49,* 1229-1232.

Pitchan, M. A., & Omar, S. Z. (2019). Cyber Security Policy: Review on Netizen Awareness and Laws. *Jurnal Komunikasi: Malaysian Journal of Communication, 35,* 103-119. https://doi.org/10.17576/JKMJC-2019-3501-08

Rahman, A. (2012). *Keselamatan Cyber*. https://www.slideshare.net/azierahman/keselamatan-cyber

Salamzada, K., Shukur, Z., & Abu Bakar, M. (2015). A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia, 4,* 1-10. https://doi.org/10.17576/apjitm-2015-0401-01

Saudi Mohd, M. (2007). User Awareness in Handling Computer Viruses Incident for Windows Platform. *Jurnal Teknologi Maklumat & Multimedia, 4,* 53-72.