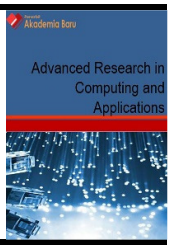
Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage: www.akademiabaru.com/arca.html
ISSN: 2462-1927



Analysis of Information Security Awareness within Users' Preference, Practice and Knowledge

Open Access

T. T. Ting[1,*], Z. H. Eu[1], S. B. Lim[1], K. S. Chong[1]

[1] Department of Information and Communication Technology, Faculty of Computing and Information Technology, Tunku Abdul Rahman University College, 53300 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 5 December 2017
Received in revised form 19 July 2019
Accepted 22 July 2018
Available online 1 August 2018

Keywords:
Information security awareness, countermeasure, preference, knowledge, practice

ABSTRACT

As the technology keeps on improving, the Internet is becoming essential in daily living. Online shopping, social media, e-banking are among the common activities carried out in the Internet which involved private information storage and sharing. Therefore, information security issues arise as one of the main concerns among the Internet users. Experts believed that the main cause of security issue is the reckless behaviour of user such as ignorance, lack of awareness, and resistance. This research is carried out to explore the Internet users' security awareness in Malaysia in terms of users' preference, practice and knowledge. It was found that there is a difference between user's preference, practice and knowledge regarding information security countermeasures. It is crucial to explore the user's security awareness in order to provide better solutions to assist users in securing their private information and thus reducing the Internet threats.

1. Introduction

The Internet has brought numerous of conveniences in solving problems, increases productivity, and eases communication with lower cost. However, the private information stored and shared in the Internet might cause information theft that may lead to adverse consequences. For example, black hat hacker hi-jacks the public Wi-Fi connected computers to retrieve personal information such as bank accounts credentials. On the other hand, existing security strategies are deemed not sufficient in securing privacy, authentication and integrity of online transactions. Hence, there is a need to evaluate and provide remedies that counteract these discrepancies [6].

In terms of security awareness among users, Katz found that while many employees of the university understand and utilize appropriate physical measures to secure their information, they need to become more aware of and skilled in using technical security methods [5]. On the other hand, user behavior appeared as one of the keys that leads to the cyber-attack. Recent worms, viruses, and

* *Corresponding author.*
E-mail address: T. T. Ting (tingtt@tarc.edu.my)

denial of service attacks show that the Information Technology (IT) workforce is not prepared to handle such attacks due to low security awareness and lack of security training provided [10]. According to a survey - "Hacker Homelands" of third quarter in 2003 by Internet Security Systems Inc., approximately 84.95% of cyber-attacks originate from North America [3]. These attacks alerts the educators in starting the security education as early as possible among citizens.

The awareness of user toward information security and possible consequences are the fundamental of using the Internet safely. Although security awareness is one of the most effective security methods for the information security assurance, statistics indicate that the problem of Information Security Awareness is not resolved in all US organizations because many IT users do not undergo the basic security training due to insufficient budgets or the strategies for training [11]. Information security awareness, knowledge and experience play vital roles in this domain.

Information security risk management encompasses two aspects: 1. security software and features, such as pop-up blocking function, anti-spyware, and anti-virus software, and 2. security conscious or behavior related to computer and Internet usage [1,15]. Experts believed that the technology aspects of information security cannot solely guarantee a secure environment and that human information security behavior should be taken into consideration [12]. A recent study was carried out in Italy and found that security awareness among digital natives (students) are related to their knowledge, regions, financial and culture background [15].

Meanwhile, there are many Internet users surf online for leisure activity such as watch YouTube video and surf Social Network. The reputation of these Social Network site has been tarnished by number of incidents in news media such as massive worldwide spam campaign in Quechup, sexual predators, stalkers, and child molesters. The top privacy problem is that Social Network site do not inform users of the dangers of divulging their personal information. Although privacy and safety issues have been much discussed in the media, according to OfComm, these issues still did not emerge as 'top of mind' for most users of Social Network site [13]. They are seemingly unwilling to consider the privacy issues in Social Network sites. Most of the Social Network Site only allow users to set their data either public (available for everyone) or private (available only for Friends) for their profile but not every part of it.

Facebook is one of the few Social Network site that provide very detailed privacy settings. However, the current Facebook privacy interface is too complex to the users. Moreover, the service providers of Social Network site have unlimited access to users' data. With this enormous amount of information, there are many commercial opportunities for businesses on social networking sites. Marketers who target specific kind of consumers can use stated, personal information gathered from SNS for purposes other than intended by the users. eMarketer.com reported that $900 million dollars were spent in the United States on Social Network advertising in 2007 and that the amount will nearly tripled to $2.5 billion by 2011 [2].

Many of Malaysian company nowadays provide online services to attract a larger pool of customer and improve the efficiency of the services. In order to increase security awareness among these companies, culture change within community is necessary with approaches as proposed by Gardner and Valerie4. Recently, hackers have developed fake websites for users to download free anti-virus software from their websites. Many users downloaded the anti-virus software from these fake websites and lost their private information [1]. This would confuse the Internet users between true and fake websites of a genuine company.

There is a long list of information security countermeasures. The easiest way is to install an anti-virus program to scan personal computer (PC) from time to time, and update the software. The present generation of anti-virus software detects and removes the infected harmful files by scanning the code characteristics of the virus-infected files that may enable intrusions [13]. All staff should

ensure that PCs are logged off or 'locked' when left unattended for any period of time (for example, in Windows, using Ctrl+Alt+Del keys). Staffs should also be restricted from saving files to the local disk. Staffs should be instructed to only save files to their allocated network drive [14]. While surfing online, one shall not download file from untrusted site. Users shall not share account password to anyone even they are the most trusted person.

With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave businesses a balance between security and simple outbound access to the Internet, which was mostly used, for e-mail and web surfing [7]. The company can also send their employee to attend some courses that are related to security awareness and ways to avoid security threads. Punishment can be introduced in a company to employees who ignore or refuse to practice information security strategies [8, 9].

This research explores the information security awareness level among Malaysian. The gap between users' preference, actual practices, and knowledge is revealed through an online questionnaire. It is crucial to reveal this truth in order to conceal the needs of increasing security awareness to combat the increasing security threats.

2. Research Methodology

An online questionnaire is conducted throughout Malaysia and distribute through Facebook. Before the questionnaire is distributed, it is tested by Cronbach's Alpha test for reliability of the questionnaire. The objectives of this research are as follows.

1. To explore security awareness level among Malaysian.
2. To study the difference between users' preference, practice and knowledge regarding information security.
3. To explore user's perception on security awareness education.

3. Results and Discussion

3.1 Sample Data Description

Table 1 shows that there is a total of 578 respondents collected in this survey. 53.81% are male and 46.19% female. Most of the respondents are with college education level.

Table 1
Description of Sample Data

		Number of Respondents	Percentage of Respondents
Gender	Male	311	53.81%
	Female	267	46.19%
Education Level	Primary School	6	1.03%
	Secondary School	64	11.07%
	College	252	43.60%
	University	241	41.70%
	Others	15	2.60%

Table 2 shows that the questionnaire's Cronbach's Alpha is 0.708, which indicates a very high level of internal consistency of the questionnaire. The following subsections will discuss the result based on the objectives.

Table 2
Cronbach's Alpha Test

Cronbach's Alpha	Cronbach's Alpha Based on Standardized items	Number of items
0.708	0.801	41

3.2 Malaysian's Security Countermeasure Preference

Figure 1 shows in term of countermeasures preference, the top five countermeasures are: 1. Using password (72.32%), 2. Never share sensitive information such as password (54.67%), 3. Backup file (52.25%), 4. Install antivirus (46.89%), 5. Activate PC firewall (39.79%). The average percentage for each countermeasure is 44.73%. Therefore, Malaysian has moderate security awareness (around 50%). The statement "What is the counter measure you prefer" is used to test the respondents' preference on the countermeasures they used. The preferred countermeasures might/might not be really practiced in their life. Therefore, the next subsection will discover the user's practice in life.

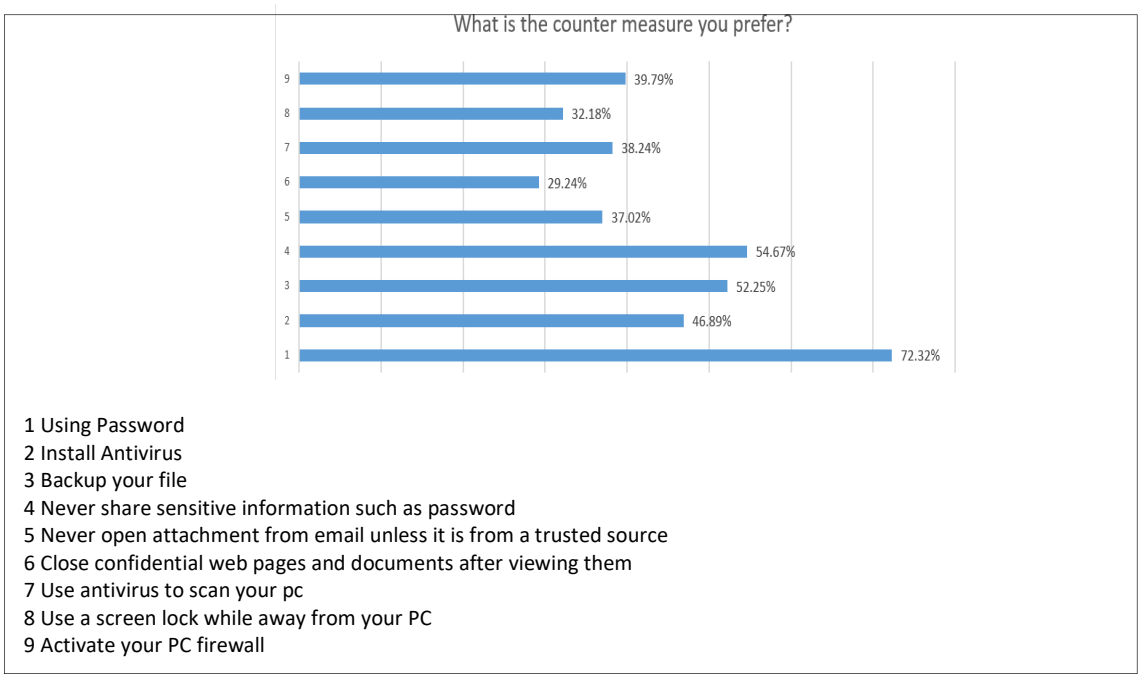


Fig. 1. Security methods preferred by users

3.3 Malaysian's Security Countermeasure Practice

Table 3 reveals that the top five most common information security practices among Malaysian are: 1. Scan PC (77%), 2. Never reveal password (69%), 3. Install antivirus (68%), 4. Backup files (65%), and 5. Update antivirus (48%). This data is slightly different from users' preferred countermeasures in Section B which reveal that the most preferred countermeasure is using password.

Table 3
Summary of Information Security Practices

Security Practice	Percentage of User
2-Never reveal password	69%
3-Never try to open and download attachment from email/from untrusted source	25%
4-Activate firewall	35%
5-Install additional firewall	26%
6-Configure firewall by themselves	24%
7-Perform full backup	
-Once every 3 months	30%
-Monthly	19%
-Weekly	12%
-Daily	4%
8-Activate Screensaver with password	45%
9-Install antivirus	68%
10-Update antivirus	48%
11-Scan PC	
-Monthly	46%
-Weekly	22%
-Daily	9%
12-Full scanning	38%
13-Never leaving PC unattended	18%

3.4 Malaysian's Security Countermeasure Knowledge

This section further explore users' knowledge in protecting one's information security. Figure 2 shows in term of countermeasures knowledge among Malaysian. 79.24% of Malaysian think that using password is the most effective way to protect their information, followed by never share sensitive information such as password (63.15%), backup their file (56.57%), install antivirus (54.67%), activate their PC firewall (47.06%), use antivirus to scan PC (44.98%), never open attachment from email unless it is from a trusted source (47.23%), use a screen lock while away from PC (46.71%), close confidential web pages and documents after viewing them (42.21%). The average percentage of countermeasure knowledge is 53.54%. Hence, the knowledge level is moderate. The following section compares between user's preference, practice and knowledge on information security.

3.5 Comparison between User's Security Countermeasure Preference, Practice and Knowledge

Table 4 reveals that there is a slight difference between user practices and user's preference and knowledge regarding information security. This result uncover that users might know about using password and never share password to others but this might not be the priority in their practice. Users rank backup file as second important strategy to protect their information yet in practice this strategy ranked forth. This is an interesting phenomena showing that educating users might not be practical but high effective and convenience tools might be useful in protecting users' information. This is proven by the most popular countermeasure among Malaysian is Scan PC as this can be done automatically by using build in software in all PC or laptop. There is a slight different between user's preference and practice. However, there is no difference between user's preference and knowledge. The following section further explore users' perceptions regarding security awareness education.

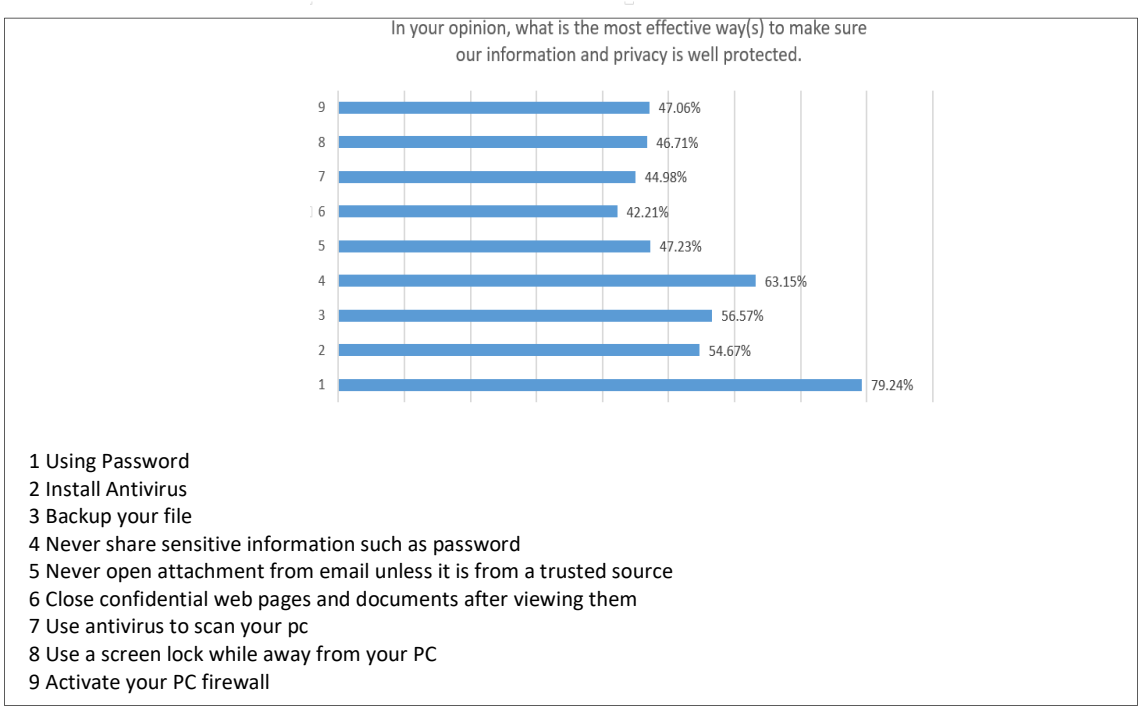


Fig. 2. Security methods adoption by users

Table 4
Summary of User's Information Security Countermeasure Preference, Practice, and Knowledge according to Ranking

Countermeasure	User Preference	User Practice	Knowledge
Never reveal password	1	2	1
Never try to open and download attachment from email/from untrusted source			
Activate firewall	4		4
Install additional firewall			
Configure firewall by themselves			
Backup files	2	4	2
Activate Screensaver with password			
Install antivirus	3	3	3
Update antivirus		5	
Scan PC	5	1	5
Full scanning			
Never leaving PC unattended			

3.6 User's Perception on Security Awareness Education

Figure 3 shows that 71% of respondent think that Information Security Awareness should be introduced to school, 21% think that maybe it should be, and 8% of respondent think that Information Security Awareness should not be introduced to school.

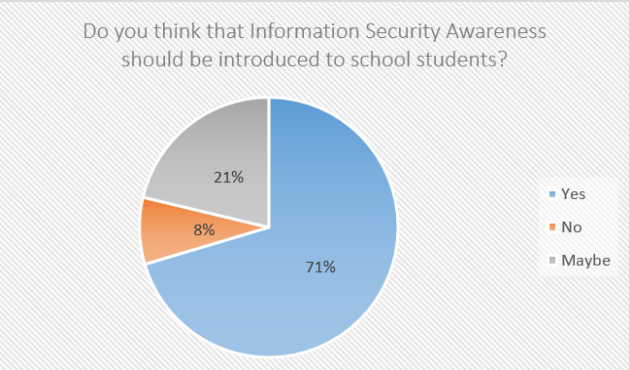


Fig. 3. User's perception on security awareness education

The following figure explains the difference between user's practice and knowledge in Backup File. Figure 4 shows that 39% of respondent face "time is consuming" challenge when back up files, 25% of respondent face "data require more storage space" challenge, 23% of respondent face "back up for large amount of data" challenge, 8% of respondent face "back up data security" challenge and 5% of respondent face "high utilization" challenge when back up files. This explains the possible reason why Backup File is perceived second best countermeasure (Table 4, ranking = 2) but is not practiced commonly among users (Table 4, ranking = 4). In conclusion, the efficiency of a tool might hinder a user from practicing certain security countermeasure.

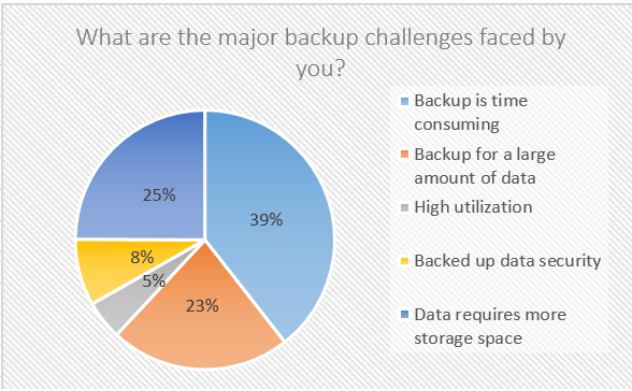


Fig. 4. Backup challenges faced by users

4. Conclusion

In conclusion, the security awareness among Malaysian is moderate. The most popular information security countermeasure practiced is scan PC. This is different from user's preferred countermeasure and knowledge which reveal that password and never reveal password as the most efficient countermeasure. This phenomena shows that although education on security awareness is important, convenient and easy to use tool is comparatively important in encouraging users to practice what they have learnt. Further research can be carried out to explore the challenges in practicing the information security countermeasure in order to assist both the educators and manufacturers to improve on their services/products.

References

[1] Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. "Information security conscious care behaviour formation in organizations." *Computers & Security* 53 (2015): 65-78.

[2] Chen, Xi, and Katina Michael. "Privacy issues and solutions in social network sites." *IEEE Technology and Society Magazine* 31, no. 4 (2012): 43-53.

[3] Hentea, Mariana. "A Perspective on Achieving Information Security Awareness." *Issues in Informing Science & Information Technology* 2 (2005).

[4] Gardner, Bill, and Valerie Thomas. *Building an information security awareness program: Defending against social engineering and technical threats*. Elsevier, 2014.

[5] Katz, Frank H. "The effect of a university information security survey on instruction methods in information security." In *Proceedings of the 2nd annual conference on Information security curriculum development*, pp. 43-48. ACM, 2005.

[6] Zimucha, Tafadzwa, Ngonidzashe Zananwe, Kerina Chimwayi, Elijah Chakwizira, and Petronella Mapungwana. "An evaluation of the effectiveness of e-banking security in Zimbabwe: a case study of Zimbabwean Commercial Banks." (2012).

[7] Q. Li, "Design and Implementation Of Network Firewall System Based On Godson CPU," Journal of Computer Applications vol. 28, no. 6, 2008, pp. 1372-1375.

[8] Grosse, Eric. "Computer security using virus probing." U.S. Patent 6,205,551, issued March 20, 2001.

[9] D'Arcy, John, Anat Hovav, and Dennis Galletta. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach." *Information Systems Research* 20, no. 1 (2009): 79-98.

[10] McConnell, Mike. "Information assurance in the twenty-first century." *Computer* 35, no. 4 (2002): supl16-supl19.

[11] Furnell, Steven M., Alastair G. Warren, and Paul S. Dowland. "Improving security awareness through computer-based training." In *Security education and critical infrastructures*, pp. 287-301. Springer, Boston, MA, 2003.

[12] Furnell, Steven, and Nathan Clarke. "Power to the people? The evolving recognition of human aspects of security." *computers & security* 31, no. 8 (2012): 983-988.

[13] Ofcom. Digital Progress Report. Digital TV, Q4 (London: Ofcom), 2007.

[14] Schwartz, Marc. "Protecting Patient Data Confidentiality in the Healthcare Environment." *EDPACS: The EDP Audit, Control, and Security Newsletter* 21, no. 3 (1993): 12-18.

[15] Gkioulos, Vasileios, Gaute Wangen, Sokratis K. Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou. "Security awareness of the digital natives." *Information* 8, no. 2 (2017): 42.