

MEASURING COMPUTER SECURITY AWARENESS ON INTERNET BANKING AND SHOPPING FOR INTERNET USERS

¹FATIMAH SIDI, ²MARZANAH A. JABAR, ³AIDA MUSTAPHA, ⁴NOR FAZLIDA SANI, ⁵ISKANDAR ISHAK, ⁶SITI ROZANA SUPIAN

¹Senior Lecturer, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

²Senior Lecturer, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

³Senior Lecturer, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

⁴Senior Lecturer, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

⁵Senior Lecturer, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

⁶Deputy Registrar, Registrar Office, Universiti Putra Malaysia

E-mail: ¹fatimahcd@fsktm.upm.edu.my, ²marzanah@fsktm.upm.edu.my, ³aida@fsktm.upm.edu.my, ⁴fazlida@fsktm.upm.edu.my, ⁵iskandar@fsktm.upm.edu.my, ⁶rozana@putra.upm.edu.my

ABSTRACT

Internet banking and shopping are two main e-commerce activities that are popular among Internet users. However, millions of dollars have lost due to the compromised bank account of users that have been hacked or intercept by irresponsible person through the Internet. The increase of threats towards online banking and shopping has made the study towards the awareness on internet banking and shopping to be important. In this study, a group of respondents with different academic background, age and gender responded to a survey that questions about their awareness of utilizing internet banking and shopping services. The results are then examined and analyzed by dividing them into group based on gender and education background. The results also analyzed based on the category of the questions related to basic and technical awareness towards the proper usage of internet banking and shopping. The results of the study showed majority of the users have good awareness especially on the basic Internet security steps taken while respondents with lower academic background lack technical awareness on Internet shopping and banking.

Keywords: *Awareness study, computer security, Internet banking, Internet shopping*

1. INTRODUCTION

Internet banking is a system that allows individuals to perform remote banking activities via the Internet [1]. The activities include daily and routine transactions such as balance inquiries, bill payment, stop-payment requests, and some even offer online loan and credit card or debit card application. Internet banking is widely used in e-commerce websites among business-to-business (B2B) or even business-to-customer (B2C) as it eases the transaction process. Because the 24-hour access to perform the transactions, Internet banking and shopping facility provide great convenience to the public. In addition, user does not require special software or access to a private network, but banking transactions are all conducted online via the Internet. Users of Internet banking are only required to have an active banking account,

customer's user ID, and the banking password to access the facilities provided.

The Malaysian Central Bank first endorsed locally owned commercial banks to offer Internet banking services back in June 2000. Since then, perception and receptiveness of Internet banking among Malaysian consumers has been widely researched [2,3,4] among which, security is found to be the main concern [5,6,7,8,9]. Internet banking in Malaysia is threatened by illegal online approach such as phishing [10], money laundering and virus attack [3], and hacking [11]. According to recent study on Internet banking in Malaysia, computer security threats regarding Internet usage have also spread to inflicting users and user terminal such as threats of user surveillance, theft of token, phishing, token attack tools, and malicious software installation), communication channel such as packet sniffing or session hijacking, as well as



brute-force attacks, website manipulation and bank security policy violation on Internet banking server [12].

Although safety measures such as firewalls or intrusion detection system are in place and enforced by the banks, end users still have to play an active role in safeguarding their Internet banking activities. CyberSecurity Malaysia, a non-profit organization under the purview of Ministry of Science, Technology and Innovation (MOSTI), published 13 security tips for safe Internet banking¹ upon which this study is based on. The first tip is to keep password/PIN code safe. Users are advised to memorize the password, to change them periodically and possibly to create different passwords for different online accounts. Passwords should also be unique and difficult to guess by using combination of alphabets and numbers.

Users are also taught to identify whether a website is secured by ensuring the URL is https:// instead of http:// at any login page. Another sign is the security icon in the form of locked padlock at the status bar, which shows the website has a valid digital certificate. Once the Internet transaction has been completed, log out from the website and clear the browser cache, cookies, and history to ensure no temporary information is left behind. At any time during conducting Internet transaction, whether online banking or shopping, users are also advised not to leave their computer unattended to avoid other person to use the computer and perform illegal transaction or tamper the personal details such as phone number or email address. If the computer security is doubtful, users should avoid using it to conduct Internet transactions.

The following tip concerns software updates and antivirus, as well as anti-spyware and personal firewall. Such security measures are available for download from the Internet and users should ensure their personal computer and browser are updated with the latest patches or fixes. CyberSecurity Malaysia advocates the use of Automated Update feature in individual Operating System, for example Windows Update for Windows users. With regards to online trust, users are reminded not to be influenced by appealing offers from unknown parties via promotional email or attachment download. When navigating the Internet, users

should make it into a practice to type the website address or choosing the link from the bookmark rather than copy and paste the address from emails. Users should not respond to emails asking for personal information, login information or changing password notification.

If the users decide to go to other website link via the Internet banking website, users are advised to read the privacy and policy information on the website before conducting any Internet transaction. Users are also reminded to always check their personal account balance or statement to ensure no unauthorized transaction has taken place, and check for date and time to match user's last login details. CyberSecurity Malaysia also calls for users to make reports should any of their bank account have been compromised.

Based on CyberSecurity's published document, this study attempts to measure the computer security awareness in Internet banking and shopping. As fraudulent and non-fraudulent issues increase day by day, user awareness on computer security is very important to protect users from unauthorized access and Internet security threats. The objective of this study is to investigate the demographic differences in computer security awareness in Malaysia. This is very important to determine the level of awareness that the respondents have in terms of online banking and shopping. The result of this study will also help any organizations to plan their future action in terms of promoting secure online transaction.

The remainder of this paper proceeds as follows. The next section describes the methodology of survey, which details out the form of questionnaire and source of data. The following section report the findings of the survey analyzed with respect to the objective of this study. Next section discusses the findings and implications before the paper concludes with some direction for future research.

2. METHODOLOGY

A total of 400 survey questionnaires were distributed to respondents last November 2011, and all of surveys are returned, yielding 100% response rate. There were 39 percent male respondents and 61 percent female respondents. In terms of academic background, 4.8% of the respondents were holders of SPM (Sijil Pelajaran Malaysia which is equivalent to United Kingdom's General Certificate of Secondary Education (GCSE) and

¹ Available at http://www.cybersecurity.my/data/content_files/11/33.pdf



below), 52.8% were pre-university and 42.5% were at least degree holders. Table 1 summarizes the demographic profile of the respondents according to gender, age, and level of highest education attained.

Female respondents dominates in the “Pre-University” and “Degree and above” category while the male respondents are slightly higher than women respondents in “SPM and below” education category.

Table 1: Demographic profile of respondents

	Male	Female	Percent
SPM and below	11	8	4.8
Pre-University	84	127	52.8
Degree and above	67	109	42.5
Percent	39.0	61.0	100.0

The questions in the survey were designed based a document on computer security guideline called “General Information Security Best Practices” published on online banking by CyberSecurity Malaysia. The computer security awareness survey questionnaire consisted of 12 questions related to Internet banking and shopping behaviors concerning passwords, secured websites, security measures, software updates and antivirus, knowledge of security policy, banking facilities, and various demographic.

The data was analyzed to investigate demographic differences in computer security awareness across gender (male and female) and education level of the respondents.

3. FINDINGS AND DISCUSSIONS

All surveys responses were recorded and used for statistical analysis. Descriptive cross tabulation method was used to conduct the data analysis using SPSS v20. The following analysis segregated findings based on gender and education level. The results are divided into two categories; Basic and Technical Awareness. Table 2 describes the questions used and the category for each question.

Table 2: Survey questions

ID	Questions	Security Awareness Category
1	Do you change password and pin codes regularly (at least 3 months)	Basic
2	Create unique password that is difficult	Basic

	to guess	
3	Look for https:// in URL and not http:// when you login	Technical
4	Look at the status bar for the security icon (locked padlock)	Technical
5	Clear the browser cache, cookies, and history once you complete you online transaction	Technical
6	Never leave your computer unattended when you are conducting your transaction	Basic
7	Install from trusted and supported sources. Regularly updated with current version	Technical
8	Updated with latest patches/files	Technical
9	Ensure all email attachments are scanned	Technical
10	Did not respond to emails asking for personal information, login information or change password notification	Basic
11	Read the privacy and policy information	Technical
12	Always check your account balances/statements to check for any unauthorized transaction	Basic

Basic Security Awareness: In this study, basic security awareness on Internet banking and shopping is determined through questions 1, 2, 6, 10 and 12. According to the results gained, 75.6% of male and 74.6% of female respondents change their password and pin codes regularly while 90.4% of males and 88.1% of females will create unique password during the registration of a website or an account. Therefore, the respondents’ awareness towards the password protection is very high, and there is not much difference between the level of awareness between male and female respondents.

The data from the questions “Do you change password and pin codes regularly (at least 3 months)” (63.2% SPM or below, 72.5% Pre-University and 79.4% Degree and above) and “Create unique password that is difficult to guess” (52.6% SPM or below, 86.3% Pre-University and 96.5% Degree and above) shows increasing on the percentage of awareness when the level of education is higher. This shows that the higher education level, the respondents are more sensitive and more responsible to their money. This is because most of the higher education respondents are more familiar with the Internet banking system; therefore they are more aware on the significance in protecting their password for the banking system.

Table 3: Internet banking and shopping security awareness based on gender

ID	Male		Female	
	Aware (%)	Unaware (%)	Aware (%)	Unaware (%)
1	75.6	24.4	74.6	25.4
2	90.4	9.6	88.1	11.9
3	70.5	29.5	57.8	42.2
4	68.6	31.4	58.6	41.4
5	80.8	19.2	71.7	28.3
6	82.7	17.3	84.8	15.2
7	80.1	19.9	84.4	15.6
8	80.1	19.9	74.2	25.8
9	85.3	14.7	81.1	18.9
10	87.2	12.8	89.3	10.7
11	76.3	23.7	78.3	21.7
12	72.4	27.6	80.7	19.3

gender recorded high awareness with 87.2% and 89.3% with women respondents recorded slightly higher than the men.

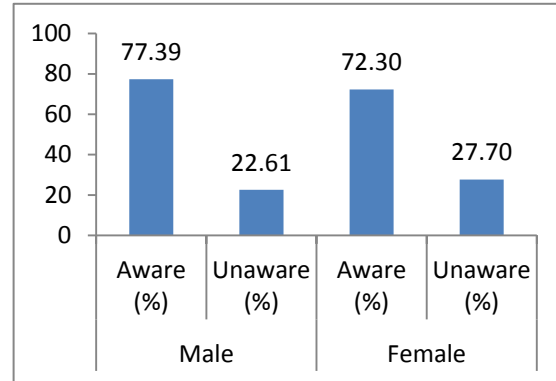


Figure 1: Average Data for Basic Awareness on basic security for Internet banking and shopping based on gender

Table 4: Internet banking and shopping security awareness based on education level

ID	SPM and below		Pre-University		Degree and above	
	Aware (%)	Un-aware (%)	Aware (%)	Un-aware (%)	Aware (%)	Un-aware (%)
1	63.2	36.8	72.5	27.5	79.4	20.6
2	52.6	47.4	86.3	13.7	96.5	3.5
3	47.4	52.6	59.2	40.8	68.8	31.2
4	52.6	47.4	55.9	44.1	71.8	28.2
5	57.9	42.1	72.0	28.0	81.2	18.8
6	52.6	47.4	79.6	20.4	92.9	7.1
7	42.1	57.9	78.7	21.3	92.4	7.6
8	47.4	52.6	72.5	27.5	84.7	15.3
9	47.4	52.6	80.1	19.9	90.0	10.0
10	68.4	31.6	85.3	14.7	94.7	5.3
11	26.3	73.7	72.5	27.5	89.4	10.6
12	36.8	63.2	73.5	26.5	87.1	12.9

On average, male respondents recorded 77.39% of basic security awareness for Internet banking and shopping which slightly exceed women respondents who only recorded 72.3%. This shows that male respondents have higher awareness in terms of basic awareness approach for internet banking and shopping. Although women respondents are lower than the men, the difference is very small with only 7.2% difference between them. Figure 1 summarizes the average for basic awareness on basic security for Internet banking and shopping.

In terms of technical awareness, on average, respondents with degree and above background recorded the highest. Pre-University respondents came second with 79.44% while respondents with SPM and below recorded 54.72%. This shows that, respondents with higher academic background have higher basic awareness on Internet banking and shopping. The differences with other groups of respondents can be considered large with 10% difference with Pre-University and 36% difference with respondents with SPM and below. Figure 2 summarizes the average for basic awareness on basic security for Internet banking and shopping.

Another basic security measures is asked on question number 6 about users leaving their computer unattended. Based on the results, it shows that respondents from both gender showed high awareness. In terms of education background, the respondents with the lowest academic background; SPM and below; recorded only 52.6% of awareness on similar question. Both the pre-university respondents and respondents with bachelor degree and above recorded 79.6% and 92.9% of awareness respectively. In terms of responding to e-mails asking personal details, respondents from both

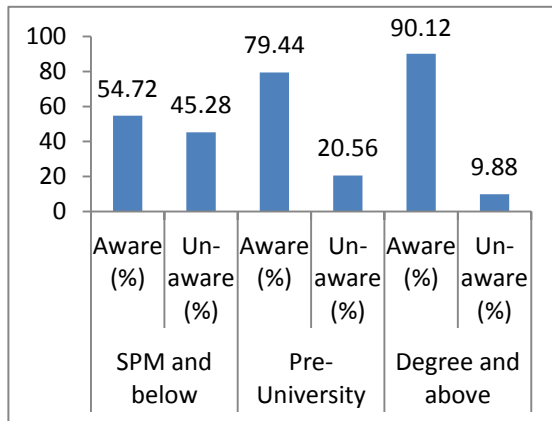


Figure 2: Average Data for Basic Awareness on basic security for Internet banking and shopping based on academic background

Technical Security Awareness: Technical Security Awareness is determined through survey questions number 3, 4, 5, 7, 8, 9 and 11. According to the statistic shown on Table 4, around 70% percent of male knows about secured transfer protocol https:// and the security icon; meanwhile there is only around 58% of female respondent realized about these security indicators. The high contrast in the percentage of male and female respondent may due to lack of interest of female towards information technology compared to male. The ability of female to make use of the technology is not as well as male [13].

However, judging from the result above, it shows that most of the respondents do know about the existence of the indicator that checks the trustworthiness of a web site. This friendly features provided by web server helps to alert the users when they are visiting insecure web site.

Table 4 also clearly show that majority of respondents with the 3 different educational level (57.9% SPM or below, 72.0% Pre-University and 81.2% Degree and above) are aware about the importance of clearing browser cache, cookies, and history once they complete the online transactions. This result also indicate that the higher educational level, the higher the awareness towards this issue as they are more often in using the computer to finish their daily work, and therefore, they have more experience and specify knowledge on cache used.

On the question “Read the privacy and policy information” (26.3% SPM or below, 72.5% Pre-University and 89.4% Degree and above), it has significantly shows that the respondents which

higher education level are more aware in terms of the privacy and policy information. This is because the higher educated respondents are exposed to more information and current issues, and they are more alert and sensitive towards their privacy. Therefore, they tend to be more careful during the online transactions.

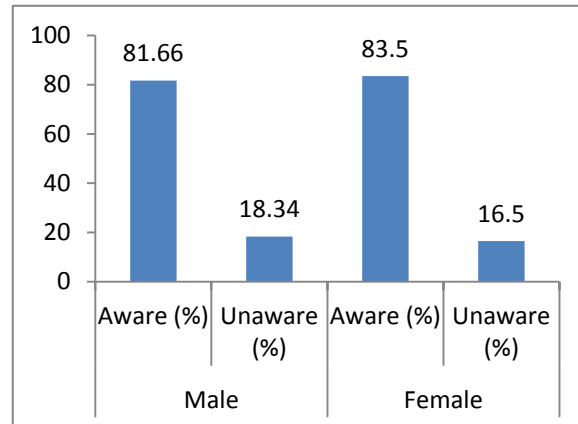


Figure 3: Average Data for Technical Awareness on basic security for Internet banking and shopping based on gender

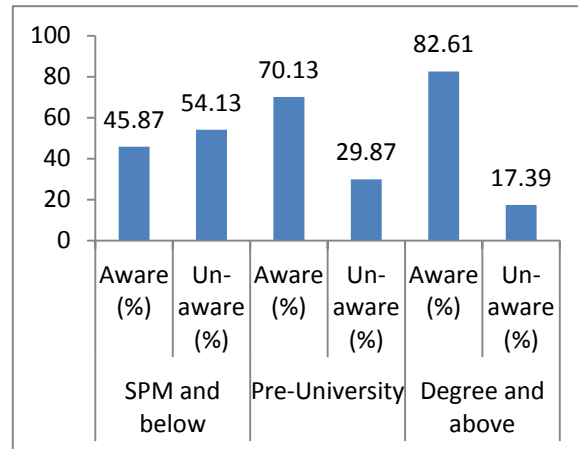


Figure 4: Average Data for Technical Awareness on basic security for Internet banking and shopping based on academic background

On average, genders from both gender recorded higher average technical awareness of Internet banking and shopping. Male respondents recorded 81.66% while female respondents recorded higher technical awareness with 83.5%. The respondents who are found to be not aware of technicalities of the similar purpose are found to be low with 18.34% and 16.5% respectively for both genders. Figure 3 summarizes the average data for Technical Awareness on basic security for Internet banking and shopping.



In terms of academic background, respondents with degree and above recorded highest average of technical awareness for Internet banking and shopping with 82.61% awareness while respondent with pre-University education came second with 70.13% of awareness. Respondents with SPM and below education recorded the lowest average technical awareness with 45.87%. They also recorded the highest average percentage of technical unawareness with 54.13%. Figure 4 describe in details the average data for Technical Awareness on basic security for Internet banking and shopping based on academic background.

4. CONCLUSION

The present study was aimed to measure the level of computer security awareness on online banking and shopping. It shows that most of the respondents have high awareness on computer security resulting from frequent use of the computer and Internet in work and studies. In terms of gender, female respondents have similar awareness level as compared to the male respondents. However, the awareness of computer security for the respondents with higher education level is more significant than those with lower education level.

This is shown through their focus which was more on the easier security measures such as password changing, creating unique password and checking the status bar. Both men and women especially with lower educational background were lacking in terms of technical measures such as updating latest patch, scanning e-mail attachments, and reading privacy and policy information.

The increase of cyber crime is inevitable, hence, greater promotional efforts to create greater awareness among respondents is very important to protect them from becoming victims to Internet security threats. Based on the findings, the target of the promotion and campaign should be given more to the users with lower educational background.

REFERENCES:

- [1] Michael Stanton, "The State of Online Banking", *Research and Analysis of e-Finance*, 2005, pp. 1-10.
- [2] Khalil M.N, Pearson J.M. (2007). The Influence of Trust on Internet Banking Acceptance. *Journal of Internet Banking and Commerce*, , vol. 12, no.2, 2007, pp. 1-10.
- [3] Mohamad Rizal Abdul Hamid, Hanudin Amin, Suddin Lada, Noren Ahmad. 2007. A Comparative Analysis of Internet Banking in Malaysia and Thailand. *Journal of Internet Business*, Vol. 4, 2007.
- [4] Yenyuen Y, Yeow PH. User Acceptance of Internet Banking Service in Malaysia. *Proceedings of the 4th International Conference on Web Information Systems and Technologies (WEBIST)*, Madeira (Portugal), May 4-7, 2009, pp. 295-306.
- [5] R Suganthi, K G Balachandher, Balachandran. Internet Banking Patronage: An Empirical Investigation of Malaysia. *Journal of Internet Banking and Commerce*, Vol. 6, No. 1, 2001.
- [6] T. Ramayah, Muhamad Jantan, Mohd Nasser Mohd Noor, Koay Pei Ling, and Razli Che Razak. Receptiveness of Internet Banking by Malaysian Consumers: The Case of Penang. *Asian Academy of Management Journal*, Vol. 8. No. 2, 2003, pp. 1-29.
- [7] Nelson Oly Ndubisi and Queenie Sinti.. Consumer Attitudes, System's Characteristics and Internet Banking Adoption in Malaysia. *Management Research News*, Vol. 29, No. 1, 2006, pp. 16-27.
- [8] WC Poon.. User's Adoption of E-Banking Services: The Malaysian Perspective. *Journal of Industrial Marketing*, Vol. 23, No. 1, 2008, pp. 56-69.
- [9] Ahasanul Haque, Arun Kumar Tarofder, Sabbir Rahman, and Md. Abdur Raquib. Electronic Transaction of Internet Banking and its Perception of Malaysian Online Customers. *African Journal of Business Management*, Vol. 3, No. 6, 2009, pp. 248-259.
- [10] Gerald Goh Guan Gan, Tan Nya Ling, Goh Choon Yih, and Uchenna Cyril Eze. Phishing: A Growing Challenge for Internet Banking Providers in Malaysia. In *Proceedings of the 10th International Business Information Management Association Conference*, 30 Jun – 1 July, 2008, Kuala Lumpur, Malaysia.
- [11] Raju Sudha, A.S. Thiagarajan and A. Seetharaman. The Security Concern on Internet Banking Adoption among Malaysian Banking Customers. *Pakistan Journal of Biological Sciences*, Vol. 10, 2007, pp. 102-106.



-
- [12] Rabiah Ahmad, Evaluation Model for Security Components: A Case Study of Malaysian Internet Banking. 2011. In Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011, 8-9 June, 2011 Bandung, Indonesia.
- [13] N. Primo, "Gender Issues in the Information Society", UNESCO Publications for the World Summit on the Information Society, pp. 18-22, 2003.