Investigating Tertiary Students' Perceptions on Internet Security

V. Sithira D/O Vadivel
James Cook University
Singapore
Sithira.Vadivel@jcu.edu.au

Yok-Yen Nguwi
James Cook University
Singapore
Yokyen.Nguwi@jcu.edu.au

***Abstract*—Internet security threats have grown from just simple viruses to various forms of computer hacking, scams, impersonation, cyber bullying, and spyware. The Internet has great influence on most people. It has profound influence and one can spend endless hours on internet activities. In particular, youth engage in more online activities than any other age group. Excessive internet usage is an emerging threat that has negative impacts on these youth; hence it is vital to investigate youths' online behavior. This work studies tertiary students' risk awareness, and provides some findings that allow us to understand their knowledge on risks and their behavior towards online activities. It reveals several important online issues amongst tertiary students; Firstly, the lack of online security awareness; second, a lack of awareness and information about the dangers of rootkits, internet cookies and spyware; thirdly, female students are more unflinching than male students when commenting on social networking sites; fourthly, students are cautious only when obvious security warnings are present; and finally, their usage of internet hotspots is common without fully understanding its associated danger. These findings enable us to recommend types of internet security habits and safety practices that students should adopt in future when they are exposed to online activities. A more holistic approach was considered which aims to minimize any future risks and dangers with online activities involving students.**

***Index Terms*—internet; threat; rootkits; internet cookies; spyware**

I. Introduction

The Internet has been a beneficial tool, providing access to immeasurable amount of information. It is magnificent to understand how the wide area network connects and shares vast amounts of information swiftly in split seconds. The rapid growth of the Internet gives rise to the associated risk of improper usage. These risks can be ruthless and may have devastating effects.

Internet security relates to the wide dissemination of many forms of "malware" (short for "malicious software") that can infect a computer. Internet safety is important and youths' understanding in this area should be strengthened before they embark into the workforce.

Internet threats affect every individual who uses the Internet. Issues such as cyber bullying on social networking sites, the spread of spyware and malware, and numerous other related issues are growing day by day. These activities can create disruptive impacts on how a computer operates, as well as stealing personal information, or even allowing a computer to be remotely controlled and be used for illegal activities. This is one of the biggest concerns in the information security field.

Organizations face great challenges in educating their employees on internet security. Internet security breaches and other risks not only create functionality and productivity losses for the victims, but they may also give rise to third-party liability cases involving clients and consumers. Cyber risks continue to grow in number and complexity, according to a recent survey conducted by the Computing Technology Industry Association (CompTIA) in Illinois. More than 56% of the 500 organizations responding to the CompTIA Study on IT Security and the Workforce reported suffering from internet attacks; such as Internet hacking that uses the Internet browser and user system rights and permissions to interrupt computer and servers functions, in the year of 2004 [1].

According to Vinton G. Cerf, the vice president and chief Internet evangelist at Google, "the Internet to be a place to innovate and share information, however it should be balanced by protection from potential harm to the visited users" [2]. Internet risks are always a problem in many communities and it is difficult to solve if no proper guidance is given. These problems will become increasingly challenging for organizations to face, and the recovery process can be demanding. This is a problem that well deserves research attention to explore youth behavior on Internet activities.

Youth aged between 13 and 23 are very vulnerable to threats and attacks. They have fully embraced the use of information technologies to make new friends and maintain contact with existing ones. They send e-mails, create their own blogs and web sites, post personal messages on blogs, send messages using SMS (short message service) and images via cell phones, message each other through instant messaging services, partake in chat rooms, and use discussion boards.

This work attempts to find out issues related to this growing trend. Internet users in the age range of 13 to 23 often make it easier for would-be identity thieves to phish for information, as adolescents often do not even realize that they are handing over personal information that can be used for identity theft. Many of these scam activities operate online. They make use of pop-up windows or emails that ask for verification of account information, credit card information, or any other kind of personal data. Other ways to trick people include false employment opportunities that require the user to give personal information such as credit card details.

Internet activities place young adults at a greater level of risk if no proper vigilance is observed. Individuals belonging to this age group (age 13-23) may not have in-depth knowledge or skills on Internet security. This age group often does not understand the required level of protection when accessing certain sites, downloading materials, and during communication over social networking sites.

The next section presents the framework design and data analysis, and discusses how the study was shaped. This paper ends with a discussion and conclusion, which describes important findings from this work.

II. FRAMEWORK AND ANALYSIS

The framework of this study was shaped in such a manner to provide sufficiently detailed understanding of the risks and problems faced by the younger generation. Concurrently, it aimed to identify the necessary skills needed for this group to engage in the Internet safely. The survey invited 50 student participants from the James Cook University Singapore, School of Business and Psychology to participate. The survey contained 14 questions, including a combination of open-ended and closed-ended questions. The open-ended questions aimed to invite input from participants to allow us to have a deeper understanding in this area. The corresponding results are presented in the subsequent sections.

A. Student Online Activities

The first question we addressed is the type of online activities participants performed whilst on the web environment. Participants were given the options of emailing, social networking, chatting, online shopping, e-banking, downloading/uploading, or all of the above. Amongst the 50 participants being surveyed, 43 of them (86%) indicated that they performed all of the activities specified, providing a clear and indicative result of the types of internet activities common amongst the student community.

Downloading material from the Internet is a common practice amongst many people, but can be a serious security issue, especially from unknown and illegitimate sites. Based on Microsoft's Security Intelligence report, in three-quarters of the time, people who attempt to obtain free software online end up with malware-infected material on their computers [3].

TABLE I. FREQUENCY AND CUMULATIVE PERCENTAGE OF STUDENTS' ONLINE ACTIVITIES

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Social Networking	4	8.0	8.0	8.0
	Downloading/uploading	3	6.0	6.0	14.0
	All of the above	43	86.0	86.0	100.0
	Total	50	100.0	100.0	

TABLE II. FREQUENCY AND CUMULATIVE PERCENTAGE OF STUDENTS' ONLINE ACTIVITIES

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Everyday	19	38.0	38.0	38.0
	Every Week	23	46.0	46.0	84.0
	Every Month	2	4.0	4.0	88.0
	I do it, but very rare	6	12.0	12.0	100.0
	Total	50	100.0	100.0	

TABLE III. STUDENTS' EMOTIONS ON ONLINE BANKING

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very uneasy	4	8.0	8.0	8.0
	Skeptical	8	16.0	16.0	24.0
	Somewhat hesitant	13	26.0	26.0	50.0
	Mostly comfortable	20	40.0	40.0	90.0
	Very confident	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

The survey indicates that 38% of respondents downloaded every day, and 46% downloaded every week. This percentage suggests that students prefer to obtain material from the Internet as it is a convenient way of getting material they want, instantly and without much hassle. The cumulative percentage shows that at least 84% of the respondents downloaded materials every week. The type of material and/or information frequently downloaded by this group was not known in this study.

B. Student Reactions to Online Activities

Online activities seem to be common amongst many people, especially students (TABLE I and II). Respondents were asked on how they felt doing some of the following activities: online banking, online shopping, giving personal information and email address online, and writing offensive views online.

TABLE IV. STUDENTS' EMOTION ON E-COMMERCE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very uneasy	3	6.0	6.0	6.0
	Skeptical	14	28.0	28.0	34.0
	Somewhat hesitant	12	24.0	24.0	58.0
	Mostly comfortable	18	36.0	36.0	94.0
	Very confident	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

TABLE V. CROSS TAB SHOWING THE EMOTIONS BETWEEN GENDER GROUPS AND E-COMMERCE ACTIVITIES.

		E-commerce					Total
		Very uneasy	Skeptical	Somewhat hesitant	Mostly comfortable	Very confident	
Gender	Female	1	4	4	6	1	16
	Male	0	6	5	6	1	18
Total		1	10	9	12	2	34

For online banking, TABLE III shows that 25 out of 50 respondents (50%), were very uneasy, skeptical, or hesitant when involved with online banking. The other 50% of the respondents were comfortable or confident in this activity. This can be considered a good balance and suggests that students are aware of the risks involved in this sort of activity if they were not careful.

Respondents were also asked how they felt about the safety of online shopping (TABLE IV). Some felt uneasy (6%), sceptical (28%) or hesitant (24%) when online purchases are done, compared to those who feel comfortable (36%) or confident (6%).

The same information (E-commerce) was used to examine the differences perceived between genders (refer to TABLE V and Fig. 1). A sample of 34 students (16 female and 18 male) were randomly picked and it shows an equal number for male and female responded with mostly comfortable (6 respondents from each group) and very confident (1 respondent from each group) when involved in purchasing online. The statistics provide a good understanding on students' feelings and how males and females perceive online purchases and online credit card payments. This data demonstrates that there is no notable difference between male and female perceptions towards E-commerce activities.

Students also responded to a question about providing personal information online (TABLE VI) during activities such as online chatting, and the response showed a cumulative figure of 68% were either uneasy, skeptical or hesitant compared to 32% were comfortable or confident. The high

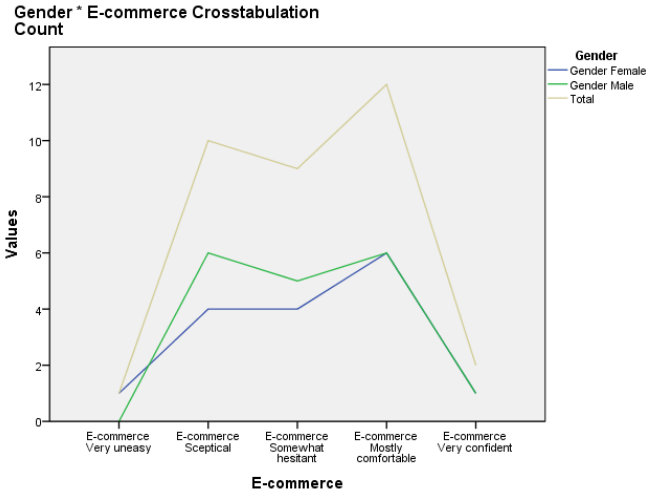

Fig. 1 Cross tab plotted as line chart to show the trend on gender emotions on e-commerce activities

percentage of 68% suggests that students are cautious and vigilant when providing personal details online. Analysis was carried out between gender groups; showing that female students were more comfortable than their male counterpart in providing personal information and email addresses online (refer to TABLE VII and TABLE VIII).

This data supports previous analysis by Odell, Korgen, Schumacher and Delucchi, who concluded that female students' more frequently use the Internet for email and school research, compared to male students who often play games,

TABLE VI. STUDENTS' EMOTION WHEN PROVIDING PERSONAL DETAILS DURING ONLINE CHAT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very uneasy	12	24.0	24.0	24.0
	Skeptical	7	14.0	14.0	38.0
	Somewhat hesitant	15	30.0	30.0	68.0
	Mostly comfortable	14	28.0	28.0	96.0
	Very confident	2	4.0	4.0	100.0
	Total	50	100.0	100.0	

TABLE VII. CROSS TABULATION SHOWING THE EMOTIONS BETWEEN GENDER GROUPS WHEN PROVIDING PERSONAL INFORMATION DURING ONLINE CHAT

		Giving personal info in chat					Total
		Very uneasy	Skeptical	Somewhat hesitant	Mostly comfortable	Very confident	
Gender	Female	3	0	6	7	0	16
	Male	4	5	5	3	1	18
Total		7	5	11	10	1	34

TABLE VIII. CROSS TABULATION SHOWING THE EMOTIONS BETWEEN GENDER GROUPS WHEN PROVIDING EMAIL ADDRESS

		Giving out email addresses					Total
		Very uneasy	Skeptical	Somewhat hesitant	Mostly comfortable	Very confident	
Gender	Female	2	0	4	10	0	16
	Male	0	5	4	6	3	18
Total		2	5	8	16	3	34

TABLE IX. CROSS TABULATION SHOWING THE EMOTIONS BETWEEN GENDER GROUPS WHEN DOWNLOADING PROGRAMS AND MUSIC FILES FROM INTERNET

		Downloading programs and music files					Total
		Very uneasy	Skeptical	Somewhat hesitant	Mostly comfortable	Very confident	
Gender	Female	0	0	4	11	1	16
	Male	1	5	2	7	3	18
Total		1	5	6	18	4	34

TABLE X. STUDENTS' EMOTIONS WHEN WRITING OFFENSIVE VIEWS ONLINE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very uneasy	12	24.0	24.0	24.0
	Skeptical	6	12.0	12.0	36.0
	Somewhat hesitant	10	20.0	20.0	56.0
	Mostly comfortable	15	30.0	30.0	86.0
	Very confident	7	14.0	14.0	100.0
	Total	50	100.0	100.0	

and listen to, or copy, music [4]. However, the data also proves otherwise when responses for question on downloading music files were asked (refer to TABLE IX), where female students (12 out of 16) were more comfortable and confident compared to male students (10 out of 18).

C. Student Social Networking Interactions

Respondents were also asked their opinions on writing offensive views on social networking sites. TABLE X displays these results. About 56% were uneasy, skeptical or hesitant when writing offensive views, compared to 44% who were comfortable or confident. This result also indicates another difference when comparing the views between gender groups. In a sample of 16 females and 18 males, as shown in TABLE XI, 8 females reported being comfortable and confident when writing offensive views compared to only 4 males, suggesting that female students to be more daring and audacious when it comes to writing offensive views on social networking sites.

TABLE XI. CROSS TABULATION SHOWING THE EMOTIONS BETWEEN GENDER GROUPS WHEN WRITING OFFENSIVE VIEWS

		Writing offensive views on social networking sites					Total
		Very uneasy	Skeptical	Somewhat hesitant	Mostly comfortable	Very confident	
Gender	Female	4	1	3	6	2	16
	Male	6	3	5	3	1	18
Total		10	4	8	9	3	34

TABLE XII. STUDENTS SECURITY OBSERVATION OF HTTPS DURING E-SHOPPING

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not sure	15	30.0	30.0	30.0
	No, I don't	15	30.0	30.0	60.0
	Yes, I do observe the HTTPS on the URL	20	40.0	40.0	100.0
	Total	50	100.0	100.0	

TABLE XIII. CROSS TABULATION SHOWING THE HTTPS OBSERVATION BETWEEN GENDER GROUPS

		Observe HTTPS during e-shopping			Total
		Not sure	No, I don't	Yes, I do observe the HTTPS on the URL	
Gender	Female	8	5	3	16
	Male	5	5	8	18
Total		13	10	11	34

D. Student Internet Security Perceptions

A question on students' ability to observe internet security whilst performing online activities was also asked. The response to this question is shown in TABLE XII; 60% (cumulative percentage) were not sure or did not observe HTTPS during e-shopping compared to 40% who observed the security on the URL. When these outcomes were analyzed using gender grouping (refer to TABLE XIII), 13 females were not sure or did not observe, compared to just 3 females who did observe HTTPS on the URL. For male respondents (out of 18), 8 observed the security feature compared to another 10 who were not sure or did not observe, demonstrating that males were relatively more observant of the HTTPS security feature. This data provides a clear warning sign that students lack awareness about such security feature during online-shopping.

A weak positive correlation is observed when comparing student's behavior in downloading programs and music files, and knowledge about the danger of rootkits (refer to TABLE

TABLE XIV. CORRELATIONS BETWEEN PROGRAM DOWNLOADING AND THE DANGER OF ROOTKITS

		Downloading programs, music files	Knowing the danger of rootkits
Downloading programs, music files	Pearson Correlation	1	0.067
	Sig. (2-tailed)		0.646
	N	50	50
Knowing the danger of rootkits	Pearson Correlation	0.067	1
	Sig. (2-tailed)	0.646	
	N	50	50

TABLE XV. CORRELATIONS BETWEEN DOWNLOADING OF PROGRAMS AND THE DANGER OF SPYWARE

		Downloading programs, music files	Knowing the danger of spyware
Downloading programs, music files	Pearson Correlation	1	0.034
	Sig. (2-tailed)		0.815
	N	50	50
Knowing the danger of spyware	Pearson Correlation	0.034	1
	Sig. (2-tailed)	0.815	
	N	50	50

TABLE XVI. CORRELATIONS BETWEEN OBSERVING SECURITY (HTTPS) AND THE DANGER OF SPYWARE

		Observing HTTPS during e-shopping	Knowing the danger of spyware
Observing HTTPS during e-shopping	Pearson Correlation	1	0.590**
	Sig. (2-tailed)		0.000
	N	50	50
Knowing the danger of spyware	Pearson Correlation	0.590**	1
	Sig. (2-tailed)	0.000	
	N	50	50

XIV) and spyware (refer to TABLE XV). There are weak positive relationships between these 2 variables; the value r for Pearson correlation from TABLE XIV shows 0.067 and, and from TABLE XV shows 0.034. This explains that it does not (strongly) indicate that students are aware of the danger of downloading programs and files and the associated consequences of having rootkits and spyware installed on their computers.

An additional analysis was undertaken on the correlation of HTTPS observation and knowing the danger of spyware and rootkits (refer to TABLE XVI and TABLE XVII). It shows a moderate positive correlation of the two variables in both analyses compared to the previous analysis. In this analysis, Pearson correlation from TABLE XVI shows the r value of 0.590, and for TABLE XVII an r value of 0.470, which is moderately close to 1. Therefore, theorize that students become aware of the consequences of their actions on internet activities when some security features are obvious, but not when they are unable to notice any apparent security features.

In the following data analysis, we asked students about the type of online activities they performed at internet hotspots (outside JCU). The data shows that out of 40 students, 19 reported accessing social networking sites and another 21 students reported using chat services, downloading files, emails, accessing Blackboard (university portal), and watching movies.

TABLE XVII. CORRELATIONS BETWEEN OBSERVING SECURITY (HTTPS) AND THE DANGER OF ROOTKITS

		Observing HTTPS during e-shopping	Knowing the danger of rootkits
Observing HTTPS during e-shopping	Pearson Correlation	1	0.470**
	Sig. (2-tailed)		0.000
	N	50	50
Knowing the danger of rootkits	Pearson Correlation	0.470**	1
	Sig. (2-tailed)	0.000	
	N	50	50

TABLE XVIII. WIRELESS ACCESS OUTSIDE JCU AGAINST KNOWING THE DANGER OF SPYWARE (MULTIPLE COMPARISONS)

(I) Knowing the danger of spyware	(J) Knowing the danger of spyware	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
I've not heard of spyware	Not sure, but heard of the danger of spyware	.14379	.27450	.860	-.5205	.8081
	Very sure and I've taken precautionary measures against spyware	.30556	.26027	.474	-.3243	.9354
Not sure, but heard of the danger of spyware	I've not heard of spyware	-.14379	.27450	.860	-.8081	.5205
	Very sure and I've taken precautionary measures against spyware	.16176	.21109	.725	-.3491	.6726
Very sure and I've taken precautionary measures against spyware	I've not heard of spyware	-.30556	.26027	.474	-.9354	.3243
	Not sure, but heard of the danger of spyware	-.16176	.21109	.725	-.6726	.3491

TABLE XIX. WIRELESS ACCESS OUTSIDE JCU AGAINST KNOWING THE DANGER OF ROOTKITS (MULTIPLE COMPARISONS)

(I) Knowing the danger of rootkits	(J) Knowing the danger of rootkits	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
I've not heard of rootkits	Not sure, but heard of the danger of rootkits	.11968	.20570	.830	-.3781	.6175
	Very sure and I've taken precautionary measures against rootkits	.16379	.35918	.892	-.7055	1.0330
Not sure, but heard of the danger of rootkits	I've not heard of rootkits	-.11968	.20570	.830	-.6175	.3781
	Very sure and I've taken precautionary measures against rootkits	.04412	.37423	.992	-.8616	.9498
Very sure and I've taken precautionary measures against rootkits	I've not heard of rootkits	-.16379	.35918	.892	-1.0330	.7055
	Not sure, but heard of the danger of rootkits	-.04412	.37423	.992	-.9498	.8616

Students' responses on wireless access outside JCU (ie. hotspots) were analyzed against their awareness about the danger of spyware, internet cookies and rootkits using one-way ANOVA analysis (refer to TABLE XVIII, TABLE XIX & TABLE XX). The multiple comparisons table does not show any statistically significant differences between groups as a whole for all 3 analyses (as the p value is above 0.05).

However, when comparing the number of students who are aware of the danger of spyware (refer to TABLE XXI), 9 out of 50 students have not heard of spyware whereas 24 out of 50 students were very sure and had taken precautionary measures against spyware. When associating these figures with the number of students who are aware of the danger of rootkits (refer to TABLE XXII), 29 out of 50 students have not heard of rootkits, whereas 4 out of 50 students are very sure and have taken precautionary measures against rootkits. This statistic shows a stark contrast in the figures for both findings. Interestingly, we conclude that many students are aware of the danger of spyware, but not rootkits.

E. Student Perceptions on Risk

In the open-ended qualitative analysis section, sample of 40 respondents' answers were analysed. From the sample, 24 (60%) respondents identified giving out personal information including credit card details and personal information as the most risky activity online. Loss of money and personal information, as well as misuse of this information, were the reasons acknowledged by this group of students. Another 16 (40%) respondents identified downloading as the most risky activity as the possibilities of their computers being infected with malware is high.

Students are more apprehensive about misuse of information and money compared to a possibility of malware infected systems. This view could be related to the fact that malware infected systems could be easily cleaned, compared to loss of information and money.

III. DISCUSSION AND CONCLUSIONS

The data analysis above identifies a few evident issues on the habits of students. Students lack awareness of the risks and dangers on certain internet activities which involves rootkits, spyware and internet cookies. Downloading material from Internet sites seems to be common amongst this group of students; however, considerations of the associated dangers were not apparent amongst them in these findings. Cookies are one complex component of the Internet that has both positive and negative attributes depending on the purpose of its usage [5]. On the other hand, when malware exploits rootkits, it makes itself invisible to security systems such as anti-virus tools and system diagnostic tools [6]. The danger of spyware lies in that it allows others to spy on your systems. Spyware characteristics include stealing files, logging keystrokes and mouse movements, capturing screen images, and other dangerous behaviours [7].

TABLE XX. WIRELESS ACCESS OUTSIDE JCU AGAINST KNOWING THE DANGER OF INTERNET COOKIES (MULTIPLE COMPARISONS)

(I) Knowing the danger of internet cookies	(J) Knowing the danger of internet cookies	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
I've not heard of cookies	Not sure, but heard of the danger of cookies	-.05556	.25971	.975	-.6841	.5730
	Very sure and I've taken precautionary measures against cookies	.28655	.26560	.532	-.3562	.9293
Not sure, but heard of the danger of cookies	I've not heard of cookies	.05556	.25971	.975	-.5730	.6841
	Very sure and I've taken precautionary measures against cookies	.34211	.20557	.230	-.1554	.8396
Very sure and I've taken precautionary measures against cookies	I've not heard of cookies	-.28655	.26560	.532	-.9293	.3562
	Not sure, but heard of the danger of cookies	-.34211	.20557	.230	-.8396	.1554

TABLE XXI. WIRELESS ACCESS OUTSIDE JCU AGAINST KNOWING THE DANGER OF SPYWARE (DESCRIPTIVES)

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Mini-mum	Maxi-mum
					Lower Bound	Upper Bound		
I've not heard of spyware	9	2.5556	.52705	.17568	2.1504	2.9607	2.00	3.00
Not sure, but heard of the danger of spyware	17	2.4118	.50730	.12304	2.1509	2.6726	2.00	3.00
Very sure and I've taken precautionary measures against spyware	24	2.2500	.79400	.16207	1.9147	2.5853	1.00	3.00
Total	50	2.3600	.66271	.09372	2.1717	2.5483	1.00	3.00

TABLE XXII. WIRELESS ACCESS OUTSIDE JCU AGAINST KNOWING THE DANGER OF ROOTKITS (DESCRIPTIVE)

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Mini-mum	Maxi-mum
					Lower Bound	Upper Bound		
I've not heard of rootkits	29	2.4138	.56803	.10548	2.1977	2.6299	1.00	3.00
Not sure, but heard of the danger of rootkits	17	2.2941	.77174	.18718	1.8973	2.6909	1.00	3.00
Very sure and I've taken precautionary measures against rootkits	4	2.2500	.95743	.47871	.7265	3.7735	1.00	3.00
Total	50	2.3600	.66271	.09372	2.1717	2.5483	1.00	3.00

The students surveyed may have heard of rootkits, spyware and internet cookies; however when considered in the context of the common activities they engaged in, we observe a significant finding that they are not prepared, and ill-informed, of the threats and risks involving rootkits, spyware and internet cookies. The consequences and potential impact of the activities were oblivious to them.

Using hotspots for internet activities was common among this group. The finding shows that a good number of students use Facebook, download files, chat, and play games at these hotspots. Some students also access their university portal and emails from these locations. Students should be aware of the potential consequences when undertaking these activities at hotspot locations, as there is a relative lack of security measures. In the hotspot access, attackers may create a rogue access point that pretends to be a legitimate access point [9]. This act will not be easily noticeable to users, and they may lose confidential information to the attacker. We have also found that students are more familiar with malware such as spyware compared to rootkits. This finding can be related to the known fact of antispyware features as part of antivirus software, but not anti-rootkit features. Students were well informed of general security protection, but not specific areas, which could have detrimental effects.

From these findings, we can also conclude that female students are bolder and more vocal compared to male students. Bold views and comments on social networking sites may portray a negative image to the readers, and may lead to undesired outcomes. This finding is supported with an earlier fact in an article by Gareth Walsh and John Elliott on female involvement in serious crime, and the figure is growing compared to a drop in male involving in crime [9]. Similarly, Thelwall and Kousha suggested that females are more active in social network sites than males (62% male and 71% female) [10].

The study results also suggest that students are more mindful of security threats when there are obvious security warnings, such as HTTPS. When one is accessing a web site where the URL begins with HTTPS://, the communication with that website is encrypted with either TLS or SSL [11]. Therefore, when they download music and files from internet sites with warnings such as HTTPS, or any other security features such as a pop-up blocker, it can be natural for them to verify and check prior to using the materials. However, during the absence of such security warnings, students are generally are not worried and begin to proceed with fetching and using the materials, without any further security considerations or verification on their own.

There are many illegitimate sites without HTTPS protocol which can cause serious dangers to its visitors. Not all sites contain security features to prove their authenticity. Websites can illegally use company logos to lure users into phishing schemes or download malware that can lead to Trojan attacks [12]. The danger begins when ambiguity sets in, and it is conveniently ignored by the internet users.

This finding puts forward a strong point on internet security lapse amongst the student community and suggests that security is secondary to them, and is not given any attention. From another perspective, there exists another discussion that students do not have a good foundational understanding of internet security; they have understood and perceive internet threats/risks through the little information they gathered along the way and through word of mouth. One reason for low internet security knowledge is that most students have not undertaken through any formal internet security awareness and training, as how large organizations do it. Security awareness programs in organizations covers various topics of concern including privacy concerns, credit card compliance, file access control and physical access control [13]. As the Internet is becoming a common tool used by many people, the risk exposure is increasing exponentially.

The findings also show that students are more concerned about privacy-related issues that could lead to loss of information if privacy is not well controlled. Previous research by Jiang and Zhou explored how malware infects android phones and leverages root level exploits that fully compromised Android security, which subsequent poses the highest level of threats to users' privacy and security. Malware infected phones can also be a bonnet which then communicates to a remote server [14].

The list of perils of malware is immeasurable. Based on another article, some German states of Bavaria, Lower Saxony, Bradenburg and North Rhine-Westphalia used Trojan (nicknamed R2D2) to spy on their citizen's computers. The Trojan is used to capture all activities from computers including keystrokes, capturing voice data, and even activating the computer's webcam and microphone, thus turning the infected system into all-purpose spying computer [15]. There are accounts such as iTunes or Microsoft accounts which store credit card information for accessibility in our computers. Therefore a malware infected computer system could also lead to loss of privacy and confidential information if not identified and appropriately resolved.

REFERENCES

[1] L. Strazewski. (2005, Sept). *Internet security - a growing risk for businesses*, [Online]. Available: http://www.roughnotes.com/rnmagazine/2005/september05/09p186.htm

[2] V. G. Cerf, "The Internet at risk," *IEEE Internet Computing*, vol. 17, no. 2, pp. 3-5, 2013.

[3] T. Greene. (2012, Oct). *Microsoft: users trying to get something for nothing wind up with malware*, [Online]. Available: http://www.networkworld.com/article/2160543/windows/microsoft--users-trying-to-get-something-for-nothing-wind-up-with-malware.html

[4] P. M. Odell, K. O. Korgen, P. Schumacher, and M. Delucchi, "Internet use among female and male college students," *CyberPsychology and Behavior*, vol. 3, no. 5, pp. 855-862, 2000.

[5] L. Weinstein and P. G. Neumann, "Inside risks: Internet risks," *Communications of the ACM*, vol. 43, no. 5, pp. 144, 2000.

[6] M. Russinovich, "Unearthing RootKits," *Windows IT Pro*, vol. 11, pp. 55-60, 2005.

[7] J. Aycock, *Spyware and Adware*. Dordrecht: Springer, 2008.

[8] B. Potter, "Wireless hotspots: petri dish of wireless security," *Communications of the ACM*, vol. 49, no. 6, pp. 50-56, 2006.

[9] G. Walsh and J. Elliott. (2004, Jan 18). *Serious female crime increases*, Sunday Times, [Online]. Available: http://www.thesundaytimes.co.uk/sto/news/uk_news/article248116.ece

[10] M. Thelwall and K. Kousha, "Academia.edu: social network or academic network?," *J. Assoc. Information Science and Technology*, vol. 65, no. 4, pp. 721-731, 2014.

[11] B. Leiba, "Aspects of Internet security," *IEEE Internet Computing*, vol. 16, no. 4, pp. 72-75, 2012.

[12] J. Wagley. (2008). *Internet threat management*, Security Management, [Online]. Available: http://www.securitymanagement.com/article/internet-threat-management

[13] T. J. Speed, *Asset Protection through Security Awareness*. Hoboken: Taylor and Francis, 2012.

[14] X. Jiang and Y. Zhou, "A survey of Android malware," in *Android Malware*. Dordrecht: Springer, 2013, pp. 3-20.

[15] B. Barrett. (2011). *German states used malware to spy on their citizens*, [Online]. Available: http://gizmodo.com/5848799/german-states-used-malware-to-spy-on-their-citizens

