Users' Perspectives and Attitudes Towards Web Application Security

Leonard Ticualu

Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

Part of the Information Security Commons

Recommended Citation

This Thesis is posted at Research Online. https://ro.ecu.edu.au/theses_hons/1142
You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author’s moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
Users' Perspectives and Attitudes towards Web Application Security

By Leonard Ticualu

This thesis is presented in partial fulfilment of the requirements for the degree of Bachelor of Science (Computer Science) with Honours

Faculty of Computing Health and Science
Edith Cowan University

Supervisor: Dr Justin Brown

2007
USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.
Abstract

The Internet has become an integral part of the society in many parts of the world. However, as the Internet becoming more important and useful, the problems with Web security have also increased. More people today have experienced Web security threats such as viruses, spyware, keyloggers, and phishing; and a not insignificant number have encountered financial fraud because of the online activities they conducted. This research investigated the security concerns and level of awareness of users in regards to the use of web applications, by identifying users' concerns of web applications, examining the relationship of users' technical knowledge and users' attitudes, as well as investigating the types of web applications that dictate users' concerns towards security.

The findings from a survey of 124 respondents within this research indicated that nearly all respondents, across genders and education levels had high levels of awareness of Internet security issues. This research found that the length of users' involvement in actively using the Internet drives their level of understanding of Internet security. In terms of the way the users conducted online activities, this research found that younger respondents were less fearful than older respondents. Based on the findings of this research, it is hoped that users' education regarding web application security can be more effectively developed in this increasingly web-centric society.
COPYRIGHT AND ACCESS DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

Signed.

Date....
Table of Contents

1. INTRODUCTION ........................................................................................................ 1
   1.1. BACKGROUND TO THE STUDY ...................................................................... 1
   1.2. SIGNIFICANCE OF THE STUDY .................................................................... 2
   1.3. PURPOSE OF THE STUDY .............................................................................. 4
   1.4. RESEARCH QUESTIONS .................................................................................. 4
   1.5. CONCLUSION ................................................................................................. 7

2. LITERATURE REVIEW ............................................................................................. 8
   2.1. THE INTERNET ................................................................................................. 8
      2.1.1. Internet Benefits .................................................................................. 11
      2.1.2. Internet Growth .................................................................................. 12
   2.2. WEB APPLICATIONS ....................................................................................... 16
      2.2.1. Web Application Usage Statistics ......................................................... 20
   2.3. CYBER CRIME ................................................................................................ 21
      2.3.1. Denial of Service (DoS) ....................................................................... 22
      2.3.2. Viruses, Worms, and Trojans ............................................................... 22
      2.3.3. Spywares and Keyloggers .................................................................... 23
      2.3.4. Phishing and E-mails .......................................................................... 23
      2.3.5. Impact and Statistics .......................................................................... 24
   2.4. USERS AND WEB APPLICATIONS ................................................................. 26

3. RESEARCH METHODOLOGY AND DESIGN ....................................................... 33
   3.1. RESEARCH METHODS SELECTION PROCESS ............................................. 33
   3.2. RESEARCH METHODOLOGY ....................................................................... 34
   3.3. RESEARCH DESIGN ...................................................................................... 36

4. ANALYSIS ............................................................................................................... 39
   4.1. BACKGROUND ............................................................................................... 42
   4.2. OPINIONS ON SECURITY ............................................................................. 45
4.3. WEB APPLICATIONS USAGE ................................................................. 53
4.4. BEHAVIOURS TOWARDS SECURITY .................................................... 54
4.5. WEB APPLICATIONS INFORMATION .................................................. 56
4.6. SECURITY ISSUES .................................................................................. 59

5. DISCUSSION ............................................................................................... 67

5.1. FIRST SUPPORTING RESEARCH QUESTIONS: IS THERE A RELATIONSHIP BETWEEN TECHNICAL KNOWLEDGE OF WEB APPLICATION SECURITY AND USERS' ATTITUDES?... 67

5.1.1. Respondents' Background ................................................................. 67
5.1.2. Technical Knowledge and Levels of Caution .................................... 68
5.1.3. Web Application Usage ................................................................. 72
5.1.4. Source of Knowledge and Information of Web Application Security ................................................................. 76

5.2. SECOND SUPPORTING RESEARCH QUESTION: DOES THE TYPE OF WEB APPLICATIONS DICTATE THE LEVEL OF USERS' SECURITY CONCERNS? .................. 77

5.2.1. Respondents' Concern of Different Types of Web Applications .......... 77
5.2.2. Respondents' Experiences with Fraud ............................................. 80
5.2.3. Respondents' Awareness of the Web Security Environment ............. 81

6. CONCLUSION ............................................................................................ 82

6.1. KEY FINDINGS ......................................................................................... 82
6.2. RECOMMENDATIONS FOR FUTURE RESEARCH ................................. 83
6.3. CONCLUSION ......................................................................................... 84

7. REFERENCES ............................................................................................ 85

APPENDIX A – ONLINE QUESTIONNAIRE .................................................. 93
APPENDIX B – INFORMATION LETTER ..................................................... 97
Table of Tables

TABLE 2-1. WORLD INTERNET USAGE AND POPULATION STATISTICS ..........12
TABLE 2-2. INTERNET USERS AND POPULATION STATISTICS FOR OCEANIA.....13
TABLE 2-3. TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS 14
TABLE 2-4. TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET DSL BROADBAND SUBSCRIBERS.................................................................15
TABLE 2-5. ESTIMATED QUARTERLY RETAIL SALES IN UNITED STATES.......20
TABLE 4.1 – BACKGROUND: GENDER....................................................42
TABLE 4.2 – BACKGROUND: AGE ..........................................................42
TABLE 4.3 – BACKGROUND: EDUCATION ACHIEVEMENT .....................42
TABLE 4.4 - BACKGROUND: OCCUPATION .............................................43
TABLE 4.5 – BACKGROUND: YEARS OF USING WORLD WIDE WEB ..........44
TABLE 4.6 – BACKGROUND: HOURS OF ACCESSING INTERNET IN A WEEK ...44
TABLE 4.7 – OPINIONS ON SECURITY: RISKS AND THREATS AWARENESS WITH USING ONLINE APPLICATIONS ..................................................45
TABLE 4.8 – OPINIONS ON SECURITY: VIRUSES THREATS ......................46
TABLE 4.9 – OPINIONS ON SECURITY: SPYWARE THREATS .....................47
TABLE 4.10 – OPINIONS ON SECURITY: KEYLOGGER THREATS .................47
TABLE 4.11 – OPINIONS ON SECURITY: PHISHING THREATS ....................48
TABLE 4.12 – OPINIONS ON SECURITY: TROJAN/BACKDOOR THREATS ......48
TABLE 4.13 – OPINIONS ON SECURITY: MAN IN THE MIDDLE ATTACK .......49
TABLE 4.14 – OPINIONS ON SECURITY: CONCERN ON ONLINE BANKING OR SHOPPING MORE THAN ACCESSING E-MAIL ........................................49
TABLE 4.15 – OPINIONS ON SECURITY: COMFORT IN GIVING CREDIT CARD WHEN SHOPPING ONLINE .........................................................50
TABLE 4.16 – OPINIONS ON SECURITY: AWARENESS OF SECURITY VERIFICATION

TABLE 4.17 – OPINIONS ON SECURITY: COMFORT IN GIVING LOGIN ID AND PASSWORD WHEN ACCESSING E-MAIL

TABLE 4.18 – OPINIONS ON SECURITY: UP TO DATE NEWS ON ONLINE SECURITY

TABLE 4.19 – WEB APPLICATIONS USAGE: REGULAR ONLINE ACTIVITIES

TABLE 4.20 – BEHAVIOURS TOWARDS SECURITY: URL CONFIRMATION

TABLE 4.21 – BEHAVIOURS TOWARDS SECURITY: CONSISTENCY OF LOGIN ID AND PASSWORD

TABLE 4.22 – BEHAVIOURS TOWARDS SECURITY: RESPONDENTS’ ONLINE ACTIVITIES

TABLE 4.23 – BEHAVIOURS TOWARDS SECURITY: AWARENESS OF NON-ENCRYPTED FORUM

TABLE 4.24 – WEB APPLICATIONS INFORMATION: FREQUENTLY USED WEB BROWSERS

TABLE 4.25 – WEB APPLICATIONS INFORMATION: SECURITY GUARD SOFTWARES

TABLE 4.26 – WEB APPLICATIONS INFORMATION: SOURCE OF ONLINE SECURITY INFORMATION

TABLE 4.27 – WEB APPLICATIONS INFORMATION: TYPES OF INTERNET ACCESS

TABLE 4.28 – WEB APPLICATIONS INFORMATION: PLACE OF CONDUCTING ONLINE ACTIVITIES

TABLE 4.29 – SECURITY ISSUES: COMPARISON OF HOME AND OFFICE/UNIVERSITY SECURITY

TABLE 4.30 – SECURITY ISSUES: FRAUD EXPERIENCES

TABLE 4.31 – SECURITY ISSUES: FRAUD RESOLUTION

TABLE 4.32 – SECURITY ISSUES: LEVEL OF SECURITY CONCERN
TABLE 4.33 – SECURITY ISSUES: LEVEL OF SECURITY PROTECTION ...............62
TABLE 4.34 – SECURITY ISSUES: LEVEL OF SECURITY KNOWLEDGE .............63
TABLE 4.35 – SECURITY ISSUES: ONLINE BANKING RANKING ..................64
TABLE 4.36 – SECURITY ISSUES: ONLINE SHOPPING RANKING ..................64
TABLE 4.37 – SECURITY ISSUES: BROWSER-BASED E-MAIL RANKING ..........64
TABLE 4.38 – SECURITY ISSUES: INSTANT MESSAGING SERVICES RANKING ....64
TABLE 4.39 – SECURITY ISSUES: FORUMS / MESSAGE BOARDS RANKING ......65
TABLE 4.40 – SECURITY ISSUES: GOVERNMENT WEBSITES RANKING ..........65
TABLE 4.41 – SECURITY ISSUES: UNIVERSITY PORTAL / ENROLMENT MANAGEMENT RANKING .................................................................65
# Table of Figures

**FIGURE 2.1.** TCP/IP PROTOCOL STACK ....................................................................... 9  
**FIGURE 2.2.** INTERNET PROCESS DIAGRAM ................................................................. 9  
**FIGURE 2.3.** STATIC HTML PROCEDURES ................................................................. 17  
**FIGURE 2.4.** SCRIPTING LANGUAGE PROCEDURES .................................................... 17  
**FIGURE 2.5.** DATA FLOW BETWEEN THE WEB APPLICATION’S COMPONENTS .......... 18  
**FIGURE 2.6.** NUMBER OF ONLINE ADULTS WHO EXPERIENCED A PHISHING ATTACK ...(25  
**FIGURE 2.7.** CLOSED PADLOCK ICON EXAMPLE ...................................................... 29  
**FIGURE 2.8.** THE CONCERNS OF U.S. ONLINE ADULT CONSUMERS ABOUT CYBER CRIME ........................................................................................................ 32  
**FIGURE 4.1.** DATABASE VIEW OF ONLINE QUESTIONNAIRE ........................................ 40
1. Introduction

1.1. Background to the Study

The Internet has become an integral part of society for many people and businesses. Many people are using the Internet through a web browser, which is one of the primary mediums for the Internet to be accessed. A web application refers to an application that is accessed using a web browser over a network, such as the Internet. Some examples of web applications are e-mail, forums, discussion boards, online banking, online shopping, and online auctions. Many companies conduct their businesses using the Internet network. They are usually referred to as e-commerce companies, because they are doing business electronically over the Internet.

As Internet use has become more widespread, "Internet security has become a consistent and growing problem" (Gehling & Stankard, 2005). An emerging threat is growing in the area of web applications. A survey by Pollara of 1250 Canadians has observed that "45 per cent of B.C. residents and 41 per cent of those surveyed in Ontario do not feel safe from threats such as hackers and identity theft while shopping online. In fact, four in 10 Canadians feel unsafe when shopping online, and nearly one in four when banking online" (McLean, 2005). Another survey that was conducted by Forrester Research found that "50 per cent of American consumers surveyed mistrust financial firms' handling of their personal information, and 94 per cent says the risk of providing personal information online are outweighing the benefits" (Guzman, 2006).

Zhang (2005, pp. 46-47) conducted a survey regarding users' security awareness and Internet usage habits; the responding groups included 252 people, of whom 54 percent were males and 46 percent were females. The
findings showed that the respondents spent an average of 8.55 hours per week surfing the Internet. In regards to the online activities, 84 percent of the respondents purchased goods online, whilst 58 percent of them conducted e-banking, and 45 percent paid the bills online.

Sallet (2003) stated that the Internet is an open architecture, meaning that "a network of networks in which data can be transmitted between users". The open nature of the Internet is a reason why it is becoming more popular, particularly given the variety of computing devices that are now able to connect to it. Clark, Sollins, Wroclawski, and Faber (2003, p. 1) stated that the Internet is regulated by technical mechanism. However, technical mechanisms are not the only regulation, as the Internet may function like real society in some aspects. As the Internet is mainly technical in nature, it is important for Internet users to understand its use, including the threats of using the Internet.

1.2. Significance of the Study

Understanding how trust may be established and maintained is critical when providing web application services. Several researchers have investigated users' level of trust in doing online transaction such as online banking and online shopping. One of the researchers that conducted the research with a survey instrument, Zhang (2005) concluded that his 252 survey respondents "do not have sufficient knowledge about security, privacy, and spyware", as there were only 54 percent of the respondents who are deemed to have enough knowledge about these matters. Therefore, because there are many users with limited understanding about the threats and risks related to conducting any form of transaction over the Internet, this research investigates users' attitudes and perspectives towards security in web applications.
There are three components of this research. The first component is to identify users' concerns in using web applications. According to Gehling and Stankard (2005), many users feel uncomfortable about giving personal information over the Internet. There are many reasons that contribute to this insecurity, and that is what the research aimed to identify.

The second component is to discover the relationship between users' attitudes and their technical knowledge of web application security. Gehling and Stankard (2005) stated that "most users have only vague ideas about the threats and risk related to conducting business over the Internet. They also have a very limited understanding of the technical and legal options for minimizing their risk". Therefore this research sought to establish the relationship, if any, between users' attitudes and technical knowledge in regards to web application security.

The third component of the research is to examine the types of web application that may dictate the level of users' security concerns. This aim is to investigate whether users are more careful when conducting a particular online activity. For example, some users may be more careful when using online banking than when using e-mail. As an example, do people check if any form of security is in place, such as whether there is a https in the URL or security seals / icons on the web browser when logging to systems that need account details from the users. In Kimery and McCord's research, as quoted by Kim, Steinfield and Lai (2004) among respondents who reported seeing a sort of assurance or security seal on the website, "only 7.5% were interested or knowledgeable enough to click on the seal to reveal additional information about the seal and the merchant".
1.3. Purpose of the Study

The purpose of the study is first to obtain information from users about their attitudes and perspectives towards web application security by examining the users' concerns, technical knowledge, and behaviours towards different types of web applications. Secondly, this study analysed the perceptions of online application usage, with an aim to establish results that could be used as a basis for user education activities and policy development for web applications use.

Thirdly, the researcher aimed to make the results of the research available for continuous or extended research or analysis on a broader topic; or for education purposes. A journal article by Chen and Gillenson (2004, p. 14) uses the research that was conducted by Greene to support his writing about consumer acceptance. Chen and Gillenson stated the result from Greene's (1997) research in his article, that "42% of respondents leave Web sites when asked to give personal information due to privacy concerns". This is one example where the results of the research by Greene can be used by Chen and Gillenson to support their research. In a similar vein, it is the focus of this research to provide such a foundation for further research on this topic.

1.4. Research Questions

The research questions consist of one primary question with 2 supporting questions. The aim of the supporting questions is to support the primary question and address the overall aims of the study.
Primary research question:
What are the security concerns and level of awareness of users in regards to the use of web applications?

The scope of this primary research question is to investigate users’ concerns and awareness in regards to using web applications, such as online banking, online shopping, e-mail, discussion boards, and almost any other online systems which requires users to hand over their personal or financial details.

Supporting question one:
Is there a relationship between technical knowledge of web application security and user attitudes?

The purpose of the first supporting question is to understand the relationship between users' technical knowledge of web application security and users' attitudes. This question seeks to establish whether people of a higher technical skill level and knowledge of web application security are more or less cautious than people with more or less technical knowledge. This question also seeks to find how the users gained their technical skill and knowledge of web application security.

Dourish, Grinter, Flor, and Joseph (2004, p. 394) found in their survey that the younger respondents with a “relatively longer exposure to computer systems express a much greater confidence in their abilities with computer systems .... In particular, they are more likely to report encountering situations in which security services proved problematic”.

This question also looked at users' concerns regarding security in using web applications. For example, are users more concerned about identity theft or loss of privacy through the use of online systems? According to Forrester Research, "concern about online phishing threats has caused 14 per cent of customers to
stop using online banking or bill payments, and 20 per cent have not enrolled in online banking or bill payments at all” (Guzman, 2006). Chen and Gillenson (2004, p. 14) found that according to a survey by Benassi (1999), privacy is in the top list of consumer concerns in regards to using the Internet. Furthermore, a survey by Lee and Kim (c. 2004) found that "92% of survey respondents indicated that they do not trust companies to keep their information private, even when the companies promise to do so" (Kim, et al., 2004).

**Supporting question two:**

*Does the type of web application dictate the level of users' security concerns?*

The aim of the second supporting question is to investigate whether different types of web applications dictate the level of users' security concerns. This question examines whether users are more careful when using a particular type of web application, such as online banking than other types of web applications such as e-mail or forums. This question also investigates whether users pay attention to security signs or logos when engaged in online activities which involve them to reveal their personal information or account details on a particular website.

Xia (2005) in his article found that the web security mechanisms such as server certificates and Secure Sockets Layer (SSL), in theory should protect users from attacks. However, “most users do not check or understand servers' certificates or ignore warnings that a certificate cannot be verified. Consequently, existing Web mechanisms provide little real security to most users".
1.5. Conclusion

The Internet is an open communication network and it is technical in nature; therefore not many general users have enough knowledge when it comes to using the Internet with its security threats and risks. As the Internet grows and becomes an integral part of society, the threats and risks related to the use of web applications that are connected through the Internet will continue to grow accordingly.

As Internet security is becoming a consistent and growing problem, it is important to examine users' behaviour towards these Internet security issues. Therefore, the aim of this research was to examine users' perspectives and attitudes towards the security of web applications. The research aimed to examine the relationship between users' technical knowledge on web application security and users' attitudes as well as identify users' concerns in using web applications. The research also investigated the types of web applications that may dictate the level of users' security concerns.
2. Literature Review

2.1. The Internet

The Internet can be defined as a collection of computers that are all connected to each other. Hassler (2001) said that "the Internet is a large and convenient network for transferring data", whilst Hefley and Morris (1995, p. 1) stated that the Internet "has become the foundation for tomorrow's electronic community, providing access to government, media, scientists, and friends and relatives". They further stated that the access to the Internet is now becoming a necessity for many companies to conduct business.

Clark, et al (2003, p. 1) indicate that the Internet is a complex system that it is technical in nature and that there are a number of underlying processes which make the Internet available for use throughout the world. Shuler (2002) explained that the "Internet addresses are in the form of nnn.nnn.nnn.nnn, where nnn must be a number from 0 [to] 255". This address is known as an IP (Internet Protocol) address; it contains two pieces of information, which is the network portion (known as the IP network address) and the local portion, known as the local or host address.

Computer systems need operating systems such as Windows, Macintosh, or UNIX to serve as the platform to connect to the Internet. To connect to the Internet, TCP/IP (Transmission Control Protocol/Internet Protocol) is needed, because it serves as the protocol for communication between computers, which is used as a standard for transmitting data over networks. In other words, TCP/IP is used because it is routable, as it controls the delivery of data between the computers as well as guaranteeing that packets will be delivered in the same order in which they were sent. Figure 2.1 below describes the TCP/IP protocol stack.
<table>
<thead>
<tr>
<th>Protocol Layer</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Protocols Layer</td>
<td>Protocols specific to applications such as WWW, e-mail, FTP, etc</td>
</tr>
<tr>
<td>Transmission Control Protocol Layer</td>
<td>TCP directs packets to a specific application on a computer using a port number</td>
</tr>
<tr>
<td>Internet Protocol Layer</td>
<td>IP directs packets to a specific computer using an IP address</td>
</tr>
<tr>
<td>Hardware Layer</td>
<td>Converts binary packet data to network signals and back (e.g. Ethernet network card, modem for phone lines, etc)</td>
</tr>
</tbody>
</table>

Figure 2.1. TCP/IP protocol stack (Shuler, 2002).

Adamson (1999) explained that in order to get the IP address, the computer sends a request to DNS (Domain Name Server); then the computer sends the message. The message may be broken down into smaller chunks of data, known as packets. This is because data sent over the Internet are sent in manageable chunks. The packets will travel through the Application Layer and continue to the TCP layer. Each packet is assigned a port number, which is used to identify the specific program which belongs to the particular port. Then the packets continue to travel through the IP layer; in this layer the packet receives its destination address. Once the packets have a port number and an IP address, they are ready to be sent over the Internet. The process of how the Internet works can be seen in Figure 2.2 below.

Figure 2.2. Internet process diagram (Shuler, 2002).
Next, the hardware layer turns the packets into electronic signals and transmits them over the phone line. On the other end, the ISP (Internet Service Provider) - the company who provides the Internet connection - examines the destination address and determines where to send it. In other words, the computer acts as the doorway connecting the ISP with the Internet, and decides what packets belong inside the network. In the end, the packets should reach the computer and travel upwards from the Hardware layer through to the IP layer, TCP layer, and lastly the Application layer. When the data reaches the top of the stack, the packets are then re-assembled into their original form; and then the message is displayed by the application layer.

To know the way the Internet works technically is important, as this is related to the research topic regarding web application security. As explained previously, the Internet is an open communication networks, which means that there are always chances of security breach or infringement. Since the packets travel through the open network, there is a possibility that the packets may be intercepted as they pass through various layers or nodes. Chen and Gillenson (2004, p. 15) stated that "information sent over the Internet travels through many unsecured computer systems, and it is at risk of interception and misuse". As a lot of users are unaware of this, they may not tend to think of security beyond what they physically see in front of them, i.e. if there is no problem on the web browser when they are doing online activities, they may think that it must be secure once the data leaves the web browser.

Many consumers are still hesitant about transmitting private information, especially financial information, over this open electronic network. Evidence shows that many online merchants are vulnerable to security breaches, and such evidence seriously affects consumer perception of the security of online shopping. Consumer trust can only be inspired if the risks associated with online purchases are reduced to a level that is tolerable to consumers.
2.1.1. Internet Benefits

There are many benefits of using the Internet. Hefley and Morris (1995, p. 1) stated that through the Internet, users can access the latest weather maps or stock exchange quotes. Users can also send and receive electronic mail to colleagues all over the world, for example by using Yahoo mail, Hotmail, or Gmail; browse through the online shops (e.g. shopping.yahoo.com); by buying goods online, including music albums, songs, and books such as Amazon or Yahoo music; participate in online auctions such as eBay, eBid, and TotalBids; participate in online betting such as Blue Square, Ladbrokes, and Paddy Power.

Other benefits of using the Internet include access to the latest update on electronic magazines and books (e.g. ebooks.com); the ability to download and see travel guides; browse and book flights, hotels, and tours online (e.g. flightcentre.com.au); communicate with friends and relatives: online chatting with text, voice, and video conversation such as using MSN Messenger, Yahoo Messenger, mIRC, or ICQ; make a phone call such as using VoiP (Voice over Internet Protocol); pay bills online; gain access to information such as online newspapers, anytime and anywhere in the world (e.g. smh.com.au); express users' opinions, make discussion with other users using message board or forums (e.g. thefootballforum.net).

While all of these benefits are useful and heavily used by different groups of people around the world, however, many of them are open to the exploitation of poor security practice, particularly when private or financial details are involved. This is not only due to the lack of security guard hardware or software, but this is also due to their lack of security knowledge.
2.1.2. Internet Growth

There are several factors that lead to the growth of the Internet, including "increased bandwidth, relaxation of government restrictions, and less expensive connection options" (Hefley & Morris, 1995, p. 1). Hefley and Morris (1995, p. 1) further explain that one of the major factors that led the popularization of the Internet is the World Wide Web (WWW). According to Louisiana State University (2003), the WWW is a hypertext-based system, providing a uniform and user-friendly interface for accessing Internet information and resources. The WWW contains various media types such as text, images, and sounds. Therefore, WWW is the media layer, whilst Internet is the medium for data transmission.

Statistics from Internet World Stats (2007c) indicate that as of March 2007 out of a world population of 6,574,666,417, there are 1,114,274,426 people using the Internet on a consistent basis; which means that 16.9 percent of the world population are using the Internet. Internet World Stats (2007c) also found that the usage growth from 2000 until 2007 in the world total is 208.7 percent. More detailed results may be found in Table 2-1 below.

Table 2-1. World Internet Usage and Population Statistics (Internet World Stats, 2007c).
Table 2-2 below indicates Internet users and population statistics for Oceania, including Australia. It was found that Internet users in Australia are 14,729,191 out of 20,984,595 people. It means that 70.2 percent of the Australian population are using the Internet; and the usage growth from 2000 to 2007 is 123.2 percent.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>American Samoa</td>
<td>64,411</td>
<td>0.2 %</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.0 %</td>
</tr>
<tr>
<td>Antarctica</td>
<td>1,446</td>
<td>0.0 %</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.0 %</td>
</tr>
<tr>
<td>Australia</td>
<td>20,984,595</td>
<td>60.9 %</td>
<td>14,729,191</td>
<td>70.2 %</td>
<td>79.9 %</td>
<td>123.2 %</td>
</tr>
<tr>
<td>Australia, Ext. Ter.</td>
<td>3,760</td>
<td>0.0 %</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.0 %</td>
</tr>
</tbody>
</table>

Table 2-2. Internet Users and Population Statistics for Oceania (Internet World Stats, 2007a).

Internet World Stats (2007b) also indicates that the United States is the country with highest number of Internet users with 211,108,086 users out of the population of 301,967,681. The United States is then followed by China, Japan, and Germany; while Australia is in the 18th place. More detailed results can be found in Table 2-3 below.
Table 2-3. Top 20 Countries With Highest Number of Internet Users (Internet World Stats, 2007b).

Table 2-4 below is taken from Internet World Stats (2005), depicting the 20 countries with the highest number of Internet DSL (Digital Subscriber Line) broadband subscribers as of 2004. DSL is the technology for bringing high-bandwidth data connections to the computers. Campbell (2003) explained that with a DSL Internet connection, the IP address is static, meaning that the IP address does not change; and as this DSL connection tends to be online continuously, it may invite intruders to breach the security.

In the list below, it was found that United States is the country that has highest number of Internet DSL broadband subscribers, with 33,900,000 subscribers.
China came second with 25,800,000 subscribers, followed by Japan, Korea, and Germany. Australia is in 15th place with 910,000 subscribers.

Table 2-4. Top 20 Countries With The Highest Number of Internet DSL Broadband Subscribers (Internet World Stats, 2005).

Based on the statistics about Internet usage above, it can be seen that as there are over one billion people all over the world that using the Internet, it influences the global economy; because many companies conduct their businesses over the Internet. Hence, there are a lot of transactions that happen every day over the Internet; and therefore there are lots of people spending and making money on the web. However, with such big amounts of money being exchanged every day over the Internet, some people use this to attain profits for their own benefit;
especially with the fact that Internet is an open communication network, therefore there are strong possibilities that exploitation on the Internet may happen.

2.2. Web Applications

As described briefly in the introduction, web application refers to applications that are accessed over networks, such as the Internet. However, as many people refer the web applications specifically to the World Wide Web (WWW), therefore it may be interpreted as applications that run on a web browser using http as the protocol. Web applications are accessed by users through various means, including web browsers (e.g. Internet Explorer, Firefox, Netscape, Opera, and Safari). Web applications have become one of the most important communication channels between users on the Internet, as they have the ability to deliver integrated information and communication channels via a common HTML interface. Starr Sites (1999) explained that HTML or Hypertext Mark-up Language is the coding language used to create the World Wide Web.

Hassan and Holt (2002, p. 350) said that web applications “contain many components that are linked together to deliver the functionality of the application”. Web applications include any forms of online systems which require users to give their personal or financial details; some of the examples are online shops or sales (including airline tickets, hotel vouchers, travels and holidays, concert tickets, clothing and fashion, books / e-books, magazines / e-magazines, foods and drinks, inventory, office supplies, jewelleries, cosmetics, mobile phones, electrical goods, gadgets, flowers, gardening, computers, movie DVDs, music CDs, toys, video games), online auctions, online banking, online chat, e-mails, and forums.

Scripting language is different from HTML. A scripting language refers to a programming language which can be interpreted and performed according to the users’ contributions. This means that scripting language is dynamic, as it can
perform depending on the users' reaction, whereas HTML is static, where the system does not perform based on users' involvement. How the static HTML works can be seen in Figure 2.3 below.

![Static HTML procedures](image)

**Figure 2.3. Static HTML procedures (Ryerson University, 2004).**

With HTML, when users open a particular site on a browser, the web server will look at the file system to find the particular site and then display it to the user. Whereas with the scripting language, shown in Figure 2.4 below by Ryerson University (2004), after the users request to open a particular site on a browser through the Internet, the web server then receives the request and executes the script. The script may query a data source from the database, then the result of the query and script returns the output to the web server. After that, the web server sends the script output back to be displayed by the web browser.

![Scripting language procedures](image)

**Figure 2.4. Scripting language procedures (Ryerson University, 2004).**
There are generally two types of scripting in web application: client-side scripting and server-side scripting. Client-side scripting refers to the web page that runs on the users' side. Haringa (2003) explained that client-side scripts are "downloaded by the browser, interpreted by the browser, and executed by the browser"; examples of client-side scripting languages are JavaScript and VB Script.

On the other hand, server-side scripting refers to the web page that runs on the server side, therefore it needs web server. If there are lots of data used concurrently and many users access the website, it is important to have a reliable web server that has large memory and speed. Examples of server-side scripting language are PHP, ASP, JSP, and Perl. For many e-commerce companies, the websites are usually created dynamically, so that the companies can interact with the customers. Therefore, this characteristic requires e-commerce websites to have web servers, application servers, and database management system (DBMS) to generate and serve users' requested content dynamically. Figure 2.5 below shows the data flow between the components of a server-side web application.

![Data flow between the web application's components](image)

Figure 2.5. Data flow between the web application's components (Hassan & Holt, 2002, p. 350).

Hassan and Holt (2002, p. 351) also described the data flow as follows. When users click on links or fill in forms, the web browser transmits users' actions to the web server using the HTTP protocol. Then the web server determines whether
the request can be performed directly or if the application server is needed. Static HTML pages and multimedia objects such as audios, videos, and images are served directly by the web server. If the application server is needed, the application server transacts with the web objects, databases, and active pages and returns the result back to the web server as static HTML pages. After that, the web server dynamically generates the result to the web browser, which then the users can read.

Hao and Mendes (2006, p. 17) stated that “over a decade the World Wide Web has grown from a small collection of Web sites to modern complex Web applications, which run large-scale software applications ... and provide services for e-commerce, information distribution, entertainment, collaborative working, surveys, and numerous other activities”.

Nowadays, many companies use a variety of web applications to perform and/or improve their business. Companies need the web applications to be secure and able to handle large amount of traffic concurrently. Otherwise, if there are problems in any of these areas, it can affect the entire business negatively such as losing money, decrease in profits or even worse going bankrupt. Fraternali (1999, p. 227) summarised it in several points: security, availability, and scalability; interoperability (the ability of a system to cooperate with other systems) with legacy systems and data; and ease of maintenance.

While the number and the importance of web applications increase, at the same time the quantity and impact of security vulnerabilities in such applications grow as well. Security vulnerabilities may lead to the loss of sensitive information such as identity theft, as well as the cost of the resulting damages. There are many reason behind this, such as “financial constrains, limited programming skills, and lack of security awareness on part of the developers” (Jovanovic, Kruegel, & Kirda, 2006, p. 27).
2.2.1. Web Application Usage Statistics

The United States' Census Bureau of the Department of Commerce (2007b) announced that the estimation of "U.S. retail e-commerce sales for the fourth quarter of 2006 was $30.6 billion", which is an increase of 5 percent from the third quarter of 2006 which was $29 billion; while the estimation of U.S. retail e-commerce sales for the first quarter of 2007 was $31.5 billion, which is an increase of 3 percent from the fourth quarter of 2006. Further detail of the estimated quarterly U.S. retail sales from the second quarter of 2005 to the first quarter of 2007 are shown in Table 2-5 below.

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Retail Sales (millions of dollars)</th>
<th>E-commerce as a Percent of Total</th>
<th>Percent Change From Prior Quarter</th>
<th>Percent Change From Same Quarter A Year Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st quarter 2007</td>
<td>999,540</td>
<td>31,517</td>
<td>3.2</td>
<td>1.7</td>
</tr>
<tr>
<td>4th quarter 2006</td>
<td>983,132</td>
<td>30,592</td>
<td>3.1</td>
<td>0.0</td>
</tr>
<tr>
<td>3rd quarter 2006</td>
<td>983,229</td>
<td>29,040</td>
<td>3.0</td>
<td>0.8</td>
</tr>
<tr>
<td>2nd quarter 2006</td>
<td>975,243</td>
<td>27,949</td>
<td>2.9</td>
<td>0.7</td>
</tr>
<tr>
<td>1st quarter 2006</td>
<td>968,243</td>
<td>26,613</td>
<td>2.7</td>
<td>3.1</td>
</tr>
<tr>
<td>4th quarter 2005</td>
<td>939,189</td>
<td>24,756</td>
<td>2.6</td>
<td>0.5</td>
</tr>
<tr>
<td>3rd quarter 2005</td>
<td>934,041</td>
<td>24,059</td>
<td>2.6</td>
<td>1.9</td>
</tr>
<tr>
<td>2nd quarter 2005</td>
<td>917,744</td>
<td>22,750</td>
<td>2.5</td>
<td>2.1</td>
</tr>
</tbody>
</table>

Table 2-5. Estimated Quarterly Retail Sales in United States (US Census Bureau, 2007a).

According to a study conducted by ACNielsen (2005, October 19), "more than 627 million people have shopped online, including over 325 million [people] within the last month." That means that approximately one-tenth of the world population had at some point, shopped online. ACNielsen (2005, October 19) further announced the different items that the online shoppers bought:

- More than 135 million people purchased DVDs and/or video games;
- Nearly 135 million made plane reservations;
- More than 128 million purchased articles of clothing, accessories or shoes;
- More than 112 million paid for music downloads and/or CDs;
- More than 106 million purchased electronic devices, such as cameras;
- Nearly 98 million bought computer hardware; and
- More than 86 million made hotel and/or tour bookings.

ACNielsen (2005, October 19) also conducted a survey of Internet users around the world about their online shopping experiences. There were more than 21,100 Internet users from 38 markets from the Asia Pacific, Europe, North America, Latin America, and South Africa who responded to the survey. Europe and North America were found to have the highest number of online shoppers, with at least 95 percent of Internet users having purchased items online. In the Asia Pacific, online shoppers in Singapore, Taiwan, China, and Australia made an average of five to six purchases in the month prior to the survey. This survey also found that 59 percent of the respondents used credit card to make payments, whilst 23 percent of them used bank transfer. Hence, based on this survey it was found that credit card was the most popular payment method online.

In another survey that ACNielsen (2006, September 18) conducted in Australia only, it was found that the annual online spending in the 12 months to June 2006 reached a record high with a total of $11.35 billion, or around $1,900 annually per shopper. ACNielsen gathered the data from approximately 23,000 regular Internet users on their online purchasing attitudes. The result also found that the number of customers shopping online "had jumped by 13 percent in the past 12 months to 5.9 million and, of these shoppers, over half (51 percent) had made repeat purchases" (ACNielsen, 2006, September 18).

### 2.3. Cyber Crime

Many people who use web applications and the Internet are aware of the negative side of web applications and the Internet. This includes dissemination of malicious computer programs, such as computer viruses, worms, Trojans, or spyware; computer misconduct such as breaking into databases and hacking into
computer servers; unwanted or abusive e-mail, such as spam advertising; and fake e-mail or websites with the purpose of getting users' information such as phishing attacks.

Cyber crime refers to the use of computers and the Internet to commit crimes against individuals, including companies or customers. In short, cyber crime is an online criminal activity. Foreign Affairs and International Trade Canada (2004, August 16) stated that cyber crime “consists of specific crimes dealing with computers and networks and the facilitation of traditional crime through the use of computers (child pornography, hate crimes, telemarketing / Internet fraud)”. Some of the main threats of cyber crime are explained below.

2.3.1. Denial of Service (DoS)

Rigby (2005, p. 14) explained that denial of service (DoS) works by flooding the targeted server or site with many requests that the server cannot handle. This traffic is not viruses or worms; in fact it may look just like legitimate requests. However, the massive volume of these requests will crash the targeted servers or eat up the bandwidth; as a result of the crash, the targeted server and website will be unavailable for customers. The Asian School of Cyber Laws (2004) stated that denial of service attack have brought down websites like Amazon, Yahoo, CNN, and eBay in the past.

2.3.2. Viruses, Worms, and Trojans

The Asian School of Cyber Laws (2004) described viruses as programs that “attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network”. A worm is similar to a virus, however the difference is that the worm resides in memory, and, if not removed, may eat up all the available spaces on the computer's memory; whereas Trojan is another malicious software which have the capability of destroying and deleting users' files, and also stealing users' confidential data such as "passwords, credit card
information, log files, e-mail address, or instant messaging contact lists” (Jupitermedia, 2006).

2.3.3. Spywares and Keyloggers

Hu and Dinev (2005, p. 61) explained that spyware is a program or software that watches users’ web surfing habits and then sends that information to the attacker over the Internet. Spyware is typically installed without users’ knowledge and permission. Spyware can become the source of identity theft and fraud, as it is associated with keyloggers; Hu and Dinev (2005, p. 61) described keyloggers as the more malicious type of spyware that tracks each keystroke of the user and sends the information to the attacker. From the users’ keystroke, there are a lot of information that can be obtained, including users’ bank account numbers, credit card numbers, and passwords. Such information can be used by the attacker to commit financial crimes.

2.3.4. Phishing and E-mails

Another source of identity theft and fraud is phishing. Phishing has become a significant threat to Internet users and online businesses. Wu, Miller, & Garfinkel (2006, p. 71) found that phishing attacks typically use legitimate-looking but fake emails and websites to deceive users into disclosing personal or financial information to the attacker. Phishing e-mails can result in very negative outcomes for users, as it can deceive many users to think that the e-mails are original and sent by the original companies; while in truth these phishing e-mails are sent by the attackers with a purpose to deceive the users so that the attackers can get something out of the users, such as confidential information including user IDs, passwords, bank account numbers, and credit card numbers.

Wu, Miller, and Garfinkel (2006, p. 71) further explained that users can also be tricked into downloading and installing malicious program or software, which may be able to search the users’ computers or monitor their online activities to steal
confidential information. Therefore, Litan (2005, p. 5) stated that user's concerns about online attacks through e-mail have affected their trust in e-mail from individuals or companies that they do not know personally.

These types of criminal activities are the most relevant to this study as they typically occur as a result of the lack of security management by the user, whereas DoS is typically out of the users control in terms of the attack. Kristen Johnsen, the Microsoft's senior director of security, as stated by US Federal News (2006, p. 1) explained four simple steps that Microsoft recommends for computer users to protect themselves from the majority of online hazards: users are recommended to "using a firewall, running regular software updates, using anti-virus protection, and [using] anti-spyware software".

2.3.5. Impact and Statistics

A survey conducted by the Australian High Tech Crime Centre (AusCERT) to 181 various Australian organisations, including information technology, manufacturing, federal and state government, utilities, finance, and education sector organisations; as cited by the Australian Institute of Criminology (2005, p. 56); claimed that the total estimated cost of computer crimes experienced by the organisations surveyed was $16.9 million, which include the virus, worm, and trojan infection with a cost of $2.7 million.

Mello (2006, April 27) stated that according to a recent survey by security products vendor McAfee (2006), of the 14,464 respondents, 97 percent of them are just a click away from infecting their computers with adware and spyware. Therefore, Mello (2006, April 27) stated that it is fair to say that the vast majority of users clicking on a website can potentially expose them to spyware. This is really worrying as spyware has the capability of monitoring activities and gathering users' data, which may include getting users' personal details such as bank account number, PIN number, and password. This type of attack is one that
this research focuses on, as it has affected a lot of people negatively who have inadvertently disclosed their personal information as a result of their poor security practice.

According to a survey by Litan (2005, p. 2) of 5000 online U.S. adult consumers in the 12 months ending in May 2005, it was found that “an estimated 73 million U.S. adults who use the Internet said they definitely received or think they received an average of more than 50 phishing e-mails in the past year”. She stated that this means the number of phishing attacks to e-mail recipients grew 28 percent compared with the previous 12-month period. Figure 2.6 below depicts the number of online adults who experienced a phishing attack.

Litan (2005, p. 2) predicted that “online U.S. commerce growth will be lowered by 1 percent to 3 percent in the next three years, as service providers struggle to find the right solutions that do not inconvenience consumers and are cost-effective to implement”.

![Pie Chart]

Figure 2.6. Number of Online Adults Who Experienced a Phishing Attack (Litan, 2005, p. 3).
Litan (2005, p. 3) also found that there were nearly 11 million consumers who clicked on the links in phishing e-mails and provided the requested information, and about 1.8 million of them recall filling in the information requested. She also found that consumers endanger themselves just by clicking on a link that is embedded in a phishing attack e-mail even without providing any sensitive data; this is because the phishing website can easily insert malicious software on the users' computers. This malicious software can record the keystrokes that users are typing, including their confidential information such as user IDs, passwords, bank account numbers, or credit card numbers.

Furthermore, when the survey asked the consumers on what they thought they knew about the attacks, Litan (2005, p. 3) found that "many individuals are not even aware that phishing attacks are being launched against them, which may result in the theft of their account information and eventually their money".

2.4. Users and Web Applications

When users shop on the Internet, many of them do not think about what is happening in the background. Online shopping is generally quite easy, as the users click on the particular site, purchase the required goods or services by adding it to a cart, and then enter their own details including credit card numbers, and the goods can be delivered in a couple of days. This whole process appears very simple; however, the companies and customers must know that the information may not be as secure as they believe. According to Chen and Gillenson (2004, p. 14), a number of studies suggest that the reason why many people have not yet shopped online is due to "the lack of trust in online businesses". The safety and security of the customers' personal information lies within the hands of the companies, therefore they need to make sure that they develop a reliable and secure server so that the users feel safe and comfortable in doing the transaction online.
An article from Chan (2006, p. 62) stated that a new report has found that recent cyber crime have centred "less on external attacks such as worms and viruses and more on the misuse of user names and passwords [and] log-on security breaches". This is because these types of attacks are designed to steal personal identity such as bank account numbers from the users. The article further stated that most of the attacks where big damage is done were launched to the users who obtain a valid user ID and password.

This type of attack can occur when users fail to protect their confidential information and leave it exposed; or when someone such as an employee intentionally abuses his or her privileges. Keren Cummins, the public-sector vice president at Phoenix Technologies stated that "a very significant number of these crimes would have been prevented if device identity and user identity verification was present" (Chan, 2006, p. 62). Therefore, it is important for Internet users to have enough technical skill and knowledge about cyber crime and Internet security.

The US Federal News Service (2006, p. 1) described that according to the survey by AARP, it was found that 89 percent of Washington Internet users report that they have received spam and 45 percent of them have received phishing e-mails. This survey further stated that 49 percent of the respondents are unaware that banks do not send e-mails to their customers requesting that they click on a link to verify account information. This may result in the users being deceived into providing confidential information to the phishing websites without knowing that they are being deceived.

Furthermore, the survey discovered that 46 percent of the respondents have found spyware on their computers and 38 percent reported that they have discovered worms or viruses on their computers. However, the respondents get high mark for protecting themselves with tools such as antivirus (91 percent),
firewalls (80 percent), and anti-spyware (79 percent). However, the survey also showed that “they are dangerously unaware of the warning signs of some of the most common Internet scams and of how their personal information is tracked online” (US Federal News Service, 2006, p. 1).

Even though it is reassuring to see that most of the respondents at least have some tools to protect themselves from cyber crime, such as antivirus, firewalls, and anti-spyware, however, they still do not know enough to prevent other types of attacks. Over half of the respondents are unaware of the way their information is tracked online, leaving them open to Internet scams.

According to the above statistics, most Internet users surveyed do not have enough technical skill or knowledge of cyber crime issues or of computer and Internet security. This conclusion is supported by another result of the survey, that 73 percent of the Internet users surveyed were unaware that even when a website has a privacy policy, it does not prevent its creators from sharing customers' personal information with others.

Other survey findings also found that 50 percent of respondents were unaware that a company’s website can share customers’ personal information with an associate company without revealing customers’ names; while 72 percent of the respondents have downloaded programs and files from the Internet, and 24 percent of them said that the program or file caused their computers to malfunction. Furthermore, approximately 24 percent of the respondents have opened e-mail attachments from someone they did not know, and 33 percent of them said that it caused their computer to malfunction.

Dhamija, Tygar, and Hearst (2006, p. 582) stated that many cyber crimes happen to Internet users because of their lack of computer system knowledge and lack of knowledge of security and security indicators. They put forward the notion that some users do not understand the meaning or the syntax of domain names, and
cannot distinguish between legitimate and fraudulent URLs. For example, they may think that http://www.commonwealthbank.com.au is the same as http://www.comonwealthbank.com.au, where in fact the latter URL may bring them to a phishing website to get their confidential information such as user IDs and passwords. Another attack strategy is by forging the e-mail header, as many users do not have the skills to differentiate between legitimate headers and forged headers.

Regarding the lack of knowledge on security indicators, Dhamija, et al (2006, p. 583) found that "many users do not know that a closed padlock icon in the browser indicates that the page they are viewing was delivered securely by SSL". An example of a closed padlock icon can be seen in Figure 2.7 below.
Dhamija, et al (2006, p. 583) further explained that even if users understood the meaning of the icon, they still may be deceived by its placement within the body of a web page; as it is supposed to be outside the body of the web page if the security icon is authentic. This lack of understanding by the users may be exploited by the attackers; moreover, many users also do not know how to check and understand the information presented on the SSL certificates, as this content can be technical and jargonistic in nature.

Users may obtain knowledge on security from many sources; one possibility is by tutorial sessions. Shropshire (2006, p. 1) stated that according to Lorrie Cranor, the director of the Usable Privacy and Security Laboratory at Carnegie Mellon University, it is hard for average computer users to keep track of all the potential and existing cyber crimes. Therefore, Cranor and his team tried to give a tutorial to help some of the average computer users to gain more knowledge about cyber crime. As quoted by Businessline (2005, p. 1), Vaman Kamath, the managing director and CEO of ICICI Bank expressed his opinion that customers should be educated and must be aware of cyber crimes.

Other sources that the users can get security knowledge from are online and offline newspapers (e.g. The Australian, The West Australian, Sydney Morning Herald), online and offline books, friends, based on their own experiences, schools or universities, workplaces, tutorial sessions, news or current affairs on television, Internet (e.g. information portal such as Yahoo, BBC, NineMSN), and even movies that are cyber crime related (e.g. AntiTrust, The Core). In the Web, there are also plenty guides and tips about Internet security which people can access so that they have more knowledge about the security. For example, IT Security (2007) in their website itsecurity.com, provided a guide of what they called “20 minute guides to PC security”, which consist of many useful tips of making the computer more secure; for example, one of the tips is for the users to tailor their password often so that it cannot be easily guessed.
However, some of the sources may be alarmist and inaccurate to be sources of knowledge for the novice users, but at least it makes them aware of such security issues. For example, a book with a title of Hacker Proof: The Ultimate Guide to Network Security that is being sold by Amazon.com (1997) has been told by one of the reviewers that this book contains inaccurate information.

A study from The European Opinion Research Group (2005), as cited by Office of Fair Trading (2006), found that 10 percent of the Internet users surveyed said that “they never bought goods and services online because of security concerns, with a further 19 percent reporting that they are deterred from buying online to a large extent because of such concerns”.

The BBC (2005, May 24) stated that a survey carried out by a software firm Intervoice (2005) found that 17 percent of the respondents stopped banking online while 13 percent abandoned online shopping. One of the reasons of this result is because of the growing incidence of identity theft; as identity theft can result in the users’ confidential information such as user IDs, passwords, credit card number, or bank account number being exposed, so that attackers may use that information to gain access to their finances and steal money from them.

According to a survey that was conducted by Litan (2005, p. 4) to 5000 online U.S. adult consumers in the 12 months ending May 2005, it was found that “consumers are taking notice of increasing cyberattacks, numerous disclosures of unauthorized access to consumer data, and misplaced consumer data files”. In fact, the unauthorized access to credit report and other data pose the highest concern to the consumers, more than the concern regarding computer viruses, other online attacks, spyware, and phishing. Figure 2.8 below display the graph of the result.
Unauthorized Access to Credit Report, Other Data

Computer Viruses, Other Online Attacks

Spyware

Phishing

Figure 2.8. The Concerns of U.S. Online Adult Consumers about Cyber Crime (Litan, 2005, p. 4)

Litan (2005, p. 5) also stated that more than 42 percent of surveyed consumers said that their concerns about online attacks affect their online shopping behaviours. Nearly three-quarters of these 42 percent respondents are more cautious about where they purchase goods online; and nearly one third of the group bought fewer items than they otherwise would. Regarding online banking, more than 28 percent of the respondents said that online attacks have influenced their online banking activities; with more than three-quarters of this group noting that they login less often; nearly 14 percent of them stopped paying bills via online banking; and more than 4 percent discontinued online banking totally.

In conclusion, as the Internet has became more integrated in this society, with so many Internet users around the world, the threats of cyber crime also increase. Types of cyber crime that have been discussed in this chapter were denial of service, viruses, worms, trojans, spywares, keyloggers, and phishing. There are many benefits in using the Internet; however Internet users must also pay great attention to the security part of the Internet to prevent any harmful acts.
3. Research Methodology and Design

3.1. Research Methods Selection Process

There were different research methods that have been considered before applying one of them. The timeframe of this study ruled out longitudinal methodologies which may have been appropriate, such as studying people's web usage habits over a prolonged period of time. An ethnographic study was not used for this reason, with further consideration revealing that such study would have been unsuitable for this research, because in ethnography the researcher "looks at an entire group – more specifically a group that shares a common culture – in depth" (Leedy & Ormrod, 2005, p. 137). Leedy and Ormrod (2005, p. 137) further explained that in ethnography, the researcher studies the group in its natural setting for a lengthy period of time, often several months or even years. In getting users' opinion about web application security, this method is inappropriate because the researcher did not have the ability to observe people on everyday behaviours in their "social and cultural context" (Myers, 1997).

Action research was not adopted as the preferred method for this research, because the researcher in action research becomes "involved with changing society and takes on the role of activist" (Coombes, 2001, p. 39), whereas this research was more focussed on problem identification. Moore (2000, p. xii) explained that action research "involves integrating research into a process of social development to monitor what happens and to evaluate the outcomes"; therefore it also takes longer timeframe to conduct action research. This is inappropriate for this research, as the timeframe of this research was not sufficient to conduct a good action research. It is also inappropriate because in collecting users' feedback about web application security, the researcher does not need to get involved in the process and do not have to go in a "continuous cycle of planning, action, and review of the action" (Moore, 2000, p. xii).
Experimental research was considered unsuitable to be used as a method for this research, because the experimental method is "particularly associated with the physical sciences, where materials and non-human life-forms are more amenable to experimentation" (Blaxter, Hughes, & Tight, 1998, p. 68). Therefore, Coombes (2001, p. 44) stated that many people have serious doubts that this method can be successful when applied to humans. As this research is very much related to humans, experimental research was considered to be inappropriate.

Case study was considered to be one of the methods that could be used for this research. Case study method is used "when it is necessary to develop a detailed understanding of what is happening in complex circumstances" (Moore, 2000, p. xii), because often large-scale survey do not provide the required depth of understanding. Therefore it might become necessary to look in detail at what is happening in a smaller number of instances or cases. When considering the case study method for this research, it appeared that this method is very much suitable for further research, with a longer timeframe and focusing on "one, two, or three" (Blaxter, et al., 1998, p. 66) particular useful and/or interesting area of the previous research's outcome. However, for this research case study was considered to be inappropriate because the research did not focus on a highly specific subject, rather a series of related concepts associated with web users' behaviours.

3.2. Research Methodology

The research method employed was survey research. Schloss and Smith (1999, p. 65) explained that "the purpose of a survey is to collect information directly from a sample of individuals". This survey provided snapshot information about a large group of users who have a greater understanding and awareness of the issues being examined in this survey. For this research, the gathered information was recorded from a population sample of web application users so as to
generalise a set of results against the specified research questions. Schloss and Smith (1999, p. 65) further explained that a survey typically takes one of three forms, which are questionnaire, personal interview, or questions over the phone. Survey research was considered to be the best method to do this research; this is because the research is dependant largely on users' feedback regarding their opinions and behaviours towards web application security. The form of survey that was used in this research was an online questionnaire.

The reasons that this research used online survey as the research method was because it is inexpensive and quick (saves cost and time), could reach many people throughout the world, and easier to analyse as the collected data is written directly to digital form (stored in a database). Furthermore, as the information was given anonymously, "people are more likely to be truthful" (Coombes, 2001, p. 38). Mitchell and Jolley (1998, p. 285) explained that a survey is especially useful if the researcher wishes to know about "people's attitudes, values, beliefs, experiences, and intentions". They further explained that a survey can also be used for identifying relationships among variables. This is exactly what the researcher would do, because when the data was collected, the data was used to identify any relationships among the variables; and by knowing that these relationships exists, it lead the researcher to a hypothesis about the reason for that relationship. For example, if the researcher conducted a survey that demonstrated a relationship between users who have been using the Internet for more than 10 years and their level of awareness towards Internet security, the researcher might hypothesise that users' experience with the Internet leads to an increase in their awareness towards Internet security.

The survey was anonymous, meaning that no identifying information of the respondents was taken and published. The questionnaire was web-based; this means that the respondents could only answer the questions through the World Wide Web (WWW). The questionnaire had different type of questions. It provided opportunities for respondents to choose their answers from closed response
questions (multiple choice questions and Likert-scale matrix questions i.e. strongly disagree, disagree, neutral, agree, and strongly agree) and open response questions, so that they might provide additional comments if they wish. Some parts of the questionnaire used contingency questions (Trochim, 2006), meaning that if the respondents answer a particular question, the answer of the respondents may lead to another question, depending on the answer; e.g. if a respondent answer “no”, it lead them to question 10, otherwise if the respondent answer “yes”, it lead them to question 11.

The target population was varied, ranging from different education level, occupation, and expertise. However, a majority of the respondents were expected to come from within the School of Computer and Information Science, particularly from the student population. It was hoped that at least some of the respondents have done some form of online transactions before, such as buying goods online. It was also preferable to have some respondents who have more advanced knowledge of web application and the Internet, such as the university students studying degrees related to computer, for instance computer science, computer security, or electronic commerce.

3.3. Research Design

As the survey was conducted online, a number of technologies were used in order to facilitate this online survey. These include a web server (i.e. Apache); a scripting language (i.e. PHP); web browsers to test the functionality (i.e. Internet Explorer, Mozilla Firefox, Opera, Netscape Navigator, and Safari), and a software to create the scripting language (i.e. Macromedia Dreamweaver 8). Because of the anonymous nature of the survey, no user details were contained in the database, however the database was also password protected. The system and online questionnaire were tested by running the questionnaire on different operating systems (i.e. Microsoft Windows, Apple Macintosh, and Linux) and different web browsers (i.e. Internet Explorer, Mozilla Firefox, Opera, Netscape
Navigator, and Safari). The survey aim to get the highest number of respondents as possible; therefore this web-based questionnaire was placed on many websites. For the respondents in Edith Cowan University, the online questionnaire was available on the School of Computer and Information Science (SCIS) website and SCISSA discussion boards.

When the web-based system, software, and all the questions had been established, the system and the questionnaire were tested with the purpose to make sure that they ran correctly, to detect any logic or syntax errors and fix the errors before it was made available to the public, as well as to identify any security holes. Essentially, the purpose of this test was to avoid any security breaches and avoid any errors so that respondents may answer the questions without any interruptions.

An invitation to participate was placed online on the SCIS website. School lecturers were also notified about this survey with a request that they inform their students using MyECU Blackboard to participate in this survey. For respondents outside the Edith Cowan University environment, the link to the online questionnaire was provided in a number of forums. The data integrity of the online questionnaire was considered; therefore to prevent this, the system recorded the length of time each user took from opening the questionnaire until submitting it.

The questions in the questionnaire were set up in a way that it reflected the purpose of the research. Before conducting the actual survey, a sample survey was conducted with a small number of individuals. The purpose was to get their feedback and hence to improve the actual survey if it was found that there were something more needs to be done during the pre-survey, as well as “to evaluate the reliability and validity of the instrument[;] and to ensure that ... [the] data analysis techniques match ... [the] expected responses" (Kitchenham & Pfleeger, 2002, p. 21).
Before answering the questionnaire, the respondents were asked to read the beginning part of the questionnaire which consists of the explanation of the purpose of the survey, how the confidentiality of the data and respondents would be preserved, and contact details if the respondents had any questions regarding the survey.

The questionnaire would then continue with several parts of questions. The introductory part of the questions consisted of the questions regarding respondents' background, such as their gender, age, education achievement, and occupation. The first section in the questionnaire consisted of questions regarding respondents' opinions on security, whereas the second section contained questions about web applications usage of the respondents. The third section ascertained the respondent's behaviours towards security, while the fourth section sought to find information regarding respondents' web applications information. The final section in the questionnaire consisted of questions regarding security issues in web applications. The aim of all these questions was to gather data to help address each supporting research question. A copy of the questionnaire can be found in Appendix A.
4. Analysis

The questionnaire was administered in the third week of the semester for one week period. The questionnaire was published online through a website, and the respondents were recruited from a number of sources, such as ECU’s SCIS (SCISSA) message boards, SCIS’s (School of Computer and Information Science) current students’ homepage, general IT forums, fellow university students and members of academic staff. The questionnaire was conducted anonymously; therefore individual respondents could not be identified.

Initially there were 133 responses collected, however nine responses were discarded because all of the answers were empty. As a result, 124 responses were gathered from this online questionnaire. The online questionnaire was published using HTML front-end form with PHP as the scripting language and MySQL as the database server in order to allow the data to be stored in the server side. The data itself was stored using MySQL Front as the data repository software. The physical database server of data was placed securely in Dr Justin Brown’s office at Edith Cowan University Mount Lawley campus, therefore the data was 100 percent secure.

The database consisted of AnswerID as a unique number to identify each response. The database also consisted of beginning time and ending time to identify the time each respondent take to answer the questions. The purpose is to gauge the seriousness of the respondents in answering the questions; for example, if there was only one minute difference between the beginning and ending time, which could indicate that the respondents did not answer the questions in detail.
The screenshot of the database view of the analysed data can be seen in Figure 4.1 below.

The questionnaire contained open-ended questions, check-box list questions, multiple choice questions, and Likert-type questions, which allowed respondents to select Strongly Disagree (SA), Disagree (D), Neutral (N), Agree (A), or Strongly Agree (SA). For the Likert-type questions, each of the scale items was encoded with a numerical value, starting at +2 for the Strongly Agree (SA) response through to -2 for the Strongly Disagree (SD) response. A copy of this questionnaire can be found in Appendix A.

Positive responses to the Likert-type questions are defined in this report as the joint percentage of agree and strongly agree responses, whereas the negative responses are defined as the joint percentage of disagree and strongly disagree responses. For example, if a question received 15 disagree and 25 strongly disagree responses out of total 100 responses, the negative response would be 40%. Percentages have been rounded to the nearest whole number.
The questionnaire was divided into six parts:

1. **Background**
   This section asked the respondents about their background details. There are six questions in this part. The purpose of these questions is to know the background and Internet experience of the respondents, including their gender, occupation, age range, and years of using the Web.

2. **Opinions on security**
   The focus of this section was to obtain respondents' opinions on web application security, such as their awareness of the risks and threats in web application security, including their attitudes or behaviours towards viruses, spywares, keylogger, and phishing.

3. **Web application usage**
   This section consisted of the web application usages of the respondents. This part focused on getting respondents' answer of the amount of online activities they conducted, including online banking, online transactions, online chatting, message boards and government websites.

4. **Behaviours towards security**
   The focus of this section was to identify respondents' behaviours towards security, such as whether the respondents use same login ID and password for all their e-mails, or whether they let their web browsers remember username and password.

5. **Web applications information**
   This section asked the respondents to inform the researcher regarding their web applications. For example, the types of security guards that the respondents use, their sources of web application security information, and type of Internet access they have at home.

6. **Security issues**
   This last section of the questionnaire focuses on some web security issues. For example, do they think it is more secure to conduct online activity in office compared to home? This section also asked the respondents of their experience regarding fraud.
4.1. **Background**

1. **Gender**

<table>
<thead>
<tr>
<th></th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>104</td>
<td>20</td>
</tr>
</tbody>
</table>

*Table 4.1 – Background: Gender*

Most of the respondents were male (84%), compared to female (16%). Most of the respondents were coming from within the School of Computer and Information Science (SCIS) at Edith Cowan University. This is indicated from the data that 65% of the female respondents and 55% of the male respondents were students. As a result, this lead to a gender imbalance as the school has a large male population.

2. **Age**

<table>
<thead>
<tr>
<th></th>
<th>Under 21</th>
<th>21 - 30</th>
<th>31 - 40</th>
<th>41 - 50</th>
<th>Over 50</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>45</td>
<td>66</td>
<td>11</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Table 4.2 – Background: Age*

3. **Education achievement**

<table>
<thead>
<tr>
<th></th>
<th>High School</th>
<th>College</th>
<th>Undergraduate</th>
<th>Postgraduate</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>9</td>
<td>20</td>
<td>74</td>
<td>20</td>
<td>1</td>
</tr>
</tbody>
</table>

*Table 4.3 – Background: Education achievement*

The most common age range was 21 to 30 years old (53%), whereas a considerable number of respondents were under 21 years old (36%). Most of the respondents had undergraduate educations (60%), with college and postgraduate educations (16%) equally following after it; while there was 7% of
the respondents who had high school education only. This indicated that they were educated respondents, because 92% of the respondents had at least achieved college education. College education in this survey means an education that is equal to TAFE, such as Certificate IV, Diploma, and Advanced Diploma.

Furthermore, of the male respondents, almost half (46%) were between 21 and 30 years old with undergraduate or postgraduate education; while most of the respondents under 21 years old already had undergraduate education (76%). These data indicated that most of the respondents appeared to have come from within the school. In addition, more than half (51%) of the 21-30 years old respondents had undergraduate education, while 20% of them had a postgraduate education.

4. Occupation

<table>
<thead>
<tr>
<th></th>
<th>Student</th>
<th>IT Related</th>
<th>Other</th>
<th>Unspecified</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>70</td>
<td>24</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 4.4 - Background: Occupation

According to the responses, more than half of the respondents were student (56%), while 19% of the respondents were on IT related job, including programmer, IT support assistant, IT consultant, IT manager, data analyst, and server administrator. These IT-related job respondents may have good level of knowledge of computer systems as they were IT intensive jobs. Other occupations of the respondents (16%) were accountant, finance officer, marine painter, hotel receptionist, and labourer.
5. How long have you been actively using the World Wide Web?

<table>
<thead>
<tr>
<th></th>
<th>Under 1 year</th>
<th>1 - 3 years</th>
<th>4 - 6 years</th>
<th>7 - 9 years</th>
<th>Over 9 years</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>11</td>
<td>11</td>
<td>47</td>
<td>39</td>
<td>16</td>
</tr>
</tbody>
</table>

*Table 4.5 – Background: Years of using World Wide Web*

There were 38% respondents who reported that they have been actively using the World Wide Web (WWW) from four to six years, while 31% of them have been actively using the WWW from seven to nine years. In accordance to the data, of the 38% respondents who have been actively using the WWW from four to six years, more than half (57%) of them had undergraduate education and 17% of them had postgraduate education; while of the 31% respondents who have been actively using the WWW from seven to nine years, more than half (51%) of them had undergraduate education. These data showed that most of the respondents who have been actively using the WWW for more than four years were at least having undergraduate education, which means that they might be actively using the WWW as a part of their education (i.e. as a student).

6. How often do you access the Internet approximately a week?

<table>
<thead>
<tr>
<th></th>
<th>Under 5 hours</th>
<th>5 – 18 hours</th>
<th>19 – 32 hours</th>
<th>33 – 45 hours</th>
<th>Over 45 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>13</td>
<td>27</td>
<td>28</td>
<td>19</td>
<td>37</td>
</tr>
</tbody>
</table>

*Table 4.6 – Background: Hours of accessing Internet in a week*

Question 6 asked respondents about how often they access the Internet approximately in a week. From the data in Table 4.6, most of the respondents of this survey were frequent Internet users, with 30% of the respondents accessing the Internet approximately over 45 hours a week, while 23% of the respondents accessing the Internet approximately from 19 to 32 hours a week.
From the data above as well as the previous data, it has been found that the majority of the respondents who accessed the Internet approximately over 45 hours a week were between 21 and 30 years old (59%), while 62% of the respondents who accessed the Internet approximately from 19 to 32 hours a week were also between 21 and 30 years old.

From the data, it has also been discovered that 70% of the respondents who accessed the Internet between 19 and over 45 hours a week were the respondents who were between 21-or-under and 30 years old and had at least an undergraduate education. One of the possible reasons that they accessed the Internet over 19 hours per week was because they might use the Internet as a part of their education as a student, such as to do research on the assignment or report.

In addition, it has been found that a large number of the respondents who accessed the Internet from 19 to over 45 hours approximately a week were male (88%), whereas most of the female respondents (65%) accessed the Internet from 5 to 18 hours approximately per week. Therefore, male respondents spent a relatively larger amount of time accessing the Internet every week compared to the female respondents.

4.2. Opinions on Security

7. I have a very good awareness of the risks and threats associated with using online applications

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>0</td>
<td>5</td>
<td>15</td>
<td>74</td>
<td>30</td>
</tr>
</tbody>
</table>

Table 4.7 – Opinions on Security: Risks and threats awareness with using online applications
The aim of the first question was to get the respondents' awareness level of the risks and threats associated with using online applications. The result showed that more than half of the respondents (84%) had at least good awareness of the risks and threats associated with using online applications. The result also indicated that more than half of the respondents (53%) between 21 and 30 years old had good awareness of the risks and threats associated with using online applications. Furthermore, out of the female respondents, 90% of them gave positive responses; hence leaving only one female respondent who gave neutral response.

8. Please list your response for each of the following:

a. Virus

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of viruses threats</td>
<td>1</td>
<td>9</td>
<td>27</td>
<td>59</td>
<td>28</td>
</tr>
<tr>
<td>ii. I am very concerned about being hit by a virus when online</td>
<td>3</td>
<td>11</td>
<td>22</td>
<td>53</td>
<td>35</td>
</tr>
<tr>
<td>iii. I would not go online on a machine which is not protected against viruses</td>
<td>4</td>
<td>27</td>
<td>33</td>
<td>32</td>
<td>28</td>
</tr>
</tbody>
</table>

Table 4.8 – Opinions on Security: Viruses threats

While more than 70% of the respondents had good understanding and concerns about viruses and such threats, more than half (52%) were still willing to go online on an unprotected machine. Majority of the female respondents (75%) and male respondents (68%) gave positive responses for all three questions. Approximately 65% of the respondents who had good understanding and concerns about viruses' threats were between 21 and 30 years old.
b. Spyware

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of spyware threats</td>
<td>4</td>
<td>11</td>
<td>23</td>
<td>56</td>
<td>30</td>
</tr>
<tr>
<td>ii. I am very concerned about spyware threats</td>
<td>3</td>
<td>12</td>
<td>25</td>
<td>51</td>
<td>33</td>
</tr>
<tr>
<td>iii. I would not go online on a machine which is not protected against spyware</td>
<td>4</td>
<td>29</td>
<td>39</td>
<td>33</td>
<td>19</td>
</tr>
</tbody>
</table>

Table 4.9 – Opinions on Security: Spyware threats

Similar to the results from question 8a, nearly 70% of the respondents indicated that they had at least a good understanding of spyware threats and also concerned about such threats. However, the majority of the respondents (27% negative, 31% neutral) might go online on a machine that does not have spyware protection, while 42% of them would only go online on a machine that has spyware protection.

c. Keylogger

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of keylogger threats</td>
<td>14</td>
<td>19</td>
<td>20</td>
<td>43</td>
<td>28</td>
</tr>
<tr>
<td>ii. I am very concerned about keylogger threats</td>
<td>10</td>
<td>19</td>
<td>23</td>
<td>40</td>
<td>32</td>
</tr>
</tbody>
</table>

Table 4.10 – Opinions on Security: Keylogger threats

There were no questions on whether the respondents would or would not go online on a machine which is not protected against keylogger, phishing, backdoor, or man in the middle attack, because there were not many software that were targeted specifically to protect against keylogger, phishing, backdoor, or man in the middle attack.

At least 57% of the respondents believed that they had a good understanding as well as concern about keylogger threats; while approximately 25% of the
respondents did not believe having a good understanding and concern about such threats. Approximately 84% of the respondents who had a good understanding and very concerned about keylogger threats were between 21 and 30 years old, while 15% of them were under 21 years old.

d. Phishing

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of phishing threats</td>
<td>15</td>
<td>15</td>
<td>28</td>
<td>39</td>
<td>27</td>
</tr>
<tr>
<td>ii. I am very concerned about phishing threats</td>
<td>15</td>
<td>19</td>
<td>30</td>
<td>36</td>
<td>24</td>
</tr>
</tbody>
</table>

*Table 4.11 – Opinions on Security: Phishing threats*

Approximately half of the respondents reported that they had a good understanding and concern about phishing threats; and nearly 60% of the respondents who gave positive responses for both questions were student with age between 21 and 30 years old.

e. Trojan / backdoor

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of trojan/backdoor threats</td>
<td>4</td>
<td>12</td>
<td>25</td>
<td>55</td>
<td>28</td>
</tr>
<tr>
<td>ii. I am very concerned about trojan/backdoor threats</td>
<td>4</td>
<td>6</td>
<td>28</td>
<td>51</td>
<td>35</td>
</tr>
</tbody>
</table>

*Table 4.12 – Opinions on Security: Trojan/backdoor threats*

There were 68% of the respondents who reported that they had good understanding and great concern about trojan / backdoor threats. In addition, around 55% of the respondents who gave positive responses to these questions were between 21 and 30 years old, whereas 37% of them were under 21 years old. Most of the respondents who gave positive responses for the first question (i) also gave positive responses for the second question (ii).
f. Man in the middle attack

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. I have a very good understanding of man in the middle attack</td>
<td>20</td>
<td>35</td>
<td>32</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>ii. I am very concerned about man in the middle attack</td>
<td>12</td>
<td>22</td>
<td>56</td>
<td>25</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 4.13 – Opinions on Security: Man in the middle attack

It appeared that there were not many respondents who had a good understanding of man in the middle attack, with 70% (including 25% neutral) reported that they did not have good understanding of man in the middle attack, leaving only 27% of the respondents who were concerned about such attack. Apparently, 71% of the respondents who had undergraduate education did not have a good understanding of man in the middle attack, and only 26% of them were concerned about such attack. Therefore, it appeared that man in the middle attack is the least known threats out of these six threats.

9. I am more concerned about security threats when conducting online banking or online shopping than say accessing an e-mail account

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
</table>

Table 4.14 – Opinions on Security: Concern on online banking or shopping more than accessing e-mail

There were a large number of respondents (87%) who gave positive responses that conducting online backing or online shopping have more security threats than accessing e-mail account. All the female respondents gave positive responses to this question, compared to 71% of the male respondents.
10. I feel comfortable in giving my credit card number when shop online

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>34</td>
<td>39</td>
<td>23</td>
<td>22</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 4.15 – Opinions on Security: Comfort in giving credit card when shopping online

According to the data from the respondents, 59% of the respondents did not feel comfortable in giving their credit cards number when shop online, while 23% of the respondents felt comfortable in giving their credit card number when conducting online shopping. Accordingly, 86% of the respondents who gave positive responses in this question were regularly conducting transaction online, while almost half (47%) of the respondents who gave negative responses for this question were rarely conducting transaction online. This means that most of the respondents who regularly conducted online transaction felt comfortable in giving their credit card number when shop online.

11. I am aware of the https sign or other signs of security verification on my web browser when conducting online activities (e.g. online banking)

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>4</td>
<td>6</td>
<td>24</td>
<td>50</td>
<td>40</td>
</tr>
</tbody>
</table>

Table 4.16 – Opinions on Security: Awareness of security verification

A large number of respondents (73%) reported that they aware of the https sign or other signs of security verification on their web browser when conducting online activities, while less than 10% of the respondents were unaware of it. Of the respondents who aware of the security signs, 75% have increased their security knowledge by a great deal since they used the WWW, while 24% have increased it by a little bit. Nearly 75% of the respondents under 21 years old were
aware of the https sign or any other signs of security verification on their web browser when conducting online activities such as banking or shopping.

Furthermore, out of the 10 respondents who were unaware of the security sign: seven respondents were under 21 years old, two respondents were between 21 and 30 years of age, and one respondent were over 50 years old. This means that as most of the respondents between 21 and 30 years old had at least undergraduate education, they were more likely aware of the security sign when conducting online activities.

12. I feel comfortable in giving my login ID and password when opening the e-mail even without the security verification

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>10</td>
<td>21</td>
<td>44</td>
<td>44</td>
<td>5</td>
</tr>
</tbody>
</table>

*Table 4.17 – Opinions on Security: Comfort in giving login ID and password when accessing e-mail*

There were mixed responses on whether the respondents felt comfortable in giving their login ID and password when opening e-mail even without the security verification. The respondents gave equal responses of 35% for each neutral and agree responses regarding the comfort in giving respondents' login ID and password when opening the e-mail even without security verification; whereas 25% of the respondents gave negative responses for this statement. However, there might be a possibility that the respondents with neutral response did not actually understand the question asked. Of the respondents who did not feel comfortable in giving their login ID and password when opening the e-mail, 86% of them were also aware of the https sign or other signs of security verification on their web browser when conducting online activities.
Furthermore, almost half (48%) of the respondents who gave positive responses for this statement were between 21 and 30 years old. As most of the respondents between 21 and 30 years of age were student, this indicates that most of them did not really care whether there was any security verification took place or not when accessing their e-mail account.

13.1 keep up to date on current news and information that are related to online security

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>7</td>
<td>27</td>
<td>31</td>
<td>40</td>
<td>19</td>
</tr>
</tbody>
</table>

*Table 4.18 – Opinions on Security: Up to date news on online security*

There were 25% neutral responses from the respondents on whether or not they keep up to date on current news and information that are related to online security, which means they might or might not keep up to date on such news. However, nearly half of the respondents (48%) reported that they keep up to date on such news; while 27% did not keep up to date on such news. Of the respondents who keep the latest information related on online security, 78% of them were often conducting online banking and/or online transactions.
4.3. **Web Applications Usage**

14. I often conduct these following activities:

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. Online banking (include bill payment)</td>
<td>18</td>
<td>32</td>
<td>12</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>ii. Online transactions (include shopping)</td>
<td>17</td>
<td>31</td>
<td>22</td>
<td>37</td>
<td>17</td>
</tr>
<tr>
<td>iii. Browser-based e-mail</td>
<td>1</td>
<td>2</td>
<td>11</td>
<td>46</td>
<td>64</td>
</tr>
<tr>
<td>iv. Instant messaging services (chatting)</td>
<td>2</td>
<td>7</td>
<td>11</td>
<td>37</td>
<td>67</td>
</tr>
<tr>
<td>v. Forums / message boards</td>
<td>2</td>
<td>6</td>
<td>13</td>
<td>45</td>
<td>58</td>
</tr>
<tr>
<td>vi. Government websites</td>
<td>13</td>
<td>22</td>
<td>42</td>
<td>32</td>
<td>15</td>
</tr>
<tr>
<td>vii. University portal / enrolment management</td>
<td>25</td>
<td>8</td>
<td>30</td>
<td>36</td>
<td>25</td>
</tr>
</tbody>
</table>

*Table 4.19 – Web Applications Usage: Regular online activities*

When asking the respondents regarding the types of activities they usually conducted, 50% of the respondents conducted online banking, while only 44% of the respondents usually conducted online transaction. Majority of the respondents who conducted online banking (77%) were also conducting online transaction such as online shopping. More than half of the respondents (53%) who conducted online banking and/or online transaction were between 21 and 30 years old, whereas 30% of them were under 21 years old.

Most of the respondents (89%) usually used e-mail; while a fewer number of respondents (84%) used instant messaging services for online chatting. There were 83% of the respondents who appeared to be regularly using forums / message boards, whereas only 38% of the respondents who seemed to use government websites on regular basis. Of the respondents who used government websites on regular basis, 68% of them had business-related
occupation (did not include student). As 56% of the respondents were students, nearly 90% of these respondents appeared to use the university portal / enrolment management regularly.

4.4. **Behaviours towards Security**

15. When giving out personal information online, I check the URL that I have typed to make sure it is spelled correctly

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>2</td>
<td>19</td>
<td>24</td>
<td>60</td>
<td>19</td>
</tr>
</tbody>
</table>

*Table 4.20 – Behaviours towards Security: URL confirmation*

There were 64% of the respondents who checked the URL that they have typed to make sure it is spelled correctly before they gave out any personal information when conducting online activity. This question was asked in relation to phishing attack; hence, this question was specifically asked in order to know how the respondents act to prevent phishing attack.

From the respondents who gave positive responses to this question, 59% of them were between 21 and 30 years old, while 27% of them were under 21 years old.

16. I use the same login ID and password for all my e-mails and/or forums

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>33</td>
<td>55</td>
<td>11</td>
<td>17</td>
<td>8</td>
</tr>
</tbody>
</table>

*Table 4.21 – Behaviours towards Security: Consistency of login ID and password*
17. I let my web browser remember usernames and passwords

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>Never</th>
<th>Some Websites</th>
<th>All Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>53</td>
<td>63</td>
<td>8</td>
</tr>
</tbody>
</table>

*Table 4.22 – Behaviours towards Security: Respondents’ online activities*

18. I am aware that if my forum’s password is the same as my e-mail’s password, it can be used to open my e-mail if the forum’s database is not encrypted

<table>
<thead>
<tr>
<th># (n = 124)</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>102</td>
<td>23</td>
</tr>
</tbody>
</table>

*Table 4.23 – Behaviours towards Security: Awareness of non-encrypted forum*

The three questions above (question 16, 17, and 18) were asked to identify the behaviours of the respondents on how they acted on preventing any security threats. Majority of the respondents (71%) did not use the same login ID and password for all their e-mails and/or forums; and more than half of the respondents (51%) only used ‘remember username and password’ in their web browser for some websites only, while 43% of the respondents never used such feature. Most of the respondents (82%) were aware that if their forum’s password is the same as their e-mail’s password, it can be used to open their e-mail if the forum’s database was not encrypted.

From these results it was found that most of the respondents were cautious regarding the use of their usernames and passwords as it can be stolen by others without their authorization, therefore one way to minimize this threat is by using different login ID and passwords as well as do not use ‘remember username and password’ features that most of the web browsers have, especially for important websites such as bank or government websites.
4.5. Web Applications Information

19. Please check the web browsers you most frequently use

<table>
<thead>
<tr>
<th>#</th>
<th>Internet Explorer</th>
<th>Mozilla Firefox</th>
<th>Opera</th>
<th>Safari</th>
<th>Netscape Navigator</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>98</td>
<td>22</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

*Table 4.24 – Web Applications Information: Frequently used web browsers*

Majority of the respondents used Mozilla Firefox and Internet Explorer. Nearly 80% of the respondents used Mozilla Firefox as their web browser, while more than half (53%) used Internet Explorer. Nearly half of the respondents used both Internet Explorer and Mozilla Firefox web browser. Of the respondents who often conducted online banking and/or online shopping, 73% of them used Mozilla Firefox; while only 37% of them used Internet Explorer. There were 32% of the respondents who accessed the Internet over 45 hours a week that used Mozilla Firefox as their web browser, while there were 17% and 13% of Mozilla Firefox’s users who accessed the Internet between 19 and 32 hours and between 33 and 45 hours respectively.

20. Please check the following security guard software(s) that you currently use

<table>
<thead>
<tr>
<th>#</th>
<th>Antivirus</th>
<th>Firewall</th>
<th>Anti spyware</th>
<th>Phishing Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>115</td>
<td>101</td>
<td>85</td>
<td>34</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Popup Blocker</th>
<th>Spam Blocker</th>
<th>Advert Remover</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>94</td>
<td>57</td>
<td>40</td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

*Table 4.25 – Web Applications Information: Security guard softwares*
This question asked the respondents about the security guard softwares that they currently use. This question contains a partially open-ended question, i.e. an ‘other’ option, which allowed respondents to specify content that were not included on the list. Although nine respondents selected the ‘other’ option, five respondents did not provide any written content.

The most popular security guard software that the respondents used at that time was antivirus, with firewall, popup blocker, firewall, and anti spyware following respectively. Other security guard softwares that were not listed in the questions of which the respondents used were mail and web antivirus and JavaScript blocker.

According to the data, there were 8% of the respondents who did not use antivirus; however, 6% of them used firewall, popup blocker, and advert remover. There were 77% of the respondents who used both antivirus and firewall, while nearly 60% of the respondents used antivirus, firewall, and anti spyware all together. Of the respondents who used all these three softwares together, 38% of them were student and 27% of them were respondents on IT related-job. There were 84% of the respondents who had IT-related job who used antivirus, firewall, and anti spyware all together, while there were only 38% of the students’ respondents who used these three softwares.

From this result, it can be seen that almost all the respondents with IT-related job used antivirus, firewall, and anti spyware to protect themselves from any security threats; while most of the students did not really pay much attention on protecting themselves using all these three softwares. Most of the students (68%) used antivirus and popup blocker as the security guard softwares.
21. Please check the following sources of news or information to which you like to pay attention to

<table>
<thead>
<tr>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Television</td>
<td>88</td>
</tr>
<tr>
<td>Magazine</td>
<td>67</td>
</tr>
<tr>
<td>Newspaper</td>
<td>70</td>
</tr>
<tr>
<td>Internet Portal</td>
<td>100</td>
</tr>
<tr>
<td>Other</td>
<td>11</td>
</tr>
</tbody>
</table>

Table 4.26 - Web Applications Information: Source of online security information

The respondents seemed likely to pay attention to Internet portal as their main sources of news or information about Internet security, with television, newspaper and magazine following correspondingly. Other sources of information that were specified by the respondents were forum, game, movie, RSS feed, radio, and trusted mailing list.

Of the 81% of respondents who chose Internet portal as their sources of information, 31% were respondents who accessed the Internet over 45 hours a week, while 18% accessed the Internet between 33 and 45 hours, and 27% accessed the Internet between 19 and 32 hours.

There were 48% of the respondents who used television and newspaper together as their source of online security information, while 40% of the respondents used Internet portal and newspaper as their source of information about online security, and there were 58% of the respondents who used Internet portal, television, and newspaper all together as their source of online security information.

22. Please choose the type of internet access that you have at home

<table>
<thead>
<tr>
<th>Access</th>
<th># (n = 124)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-up</td>
<td>23</td>
</tr>
<tr>
<td>Broadband</td>
<td>80</td>
</tr>
<tr>
<td>Wireless</td>
<td>17</td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.27 - Web Applications Information: Types of Internet access
23. Please check the following places of where you typically conduct online activities

<table>
<thead>
<tr>
<th></th>
<th>Home</th>
<th>Office</th>
<th>College / University</th>
<th>Internet Cafe</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>109</td>
<td>42</td>
<td>74</td>
<td>30</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.28 – Web Applications Information: Place of conducting online activities

Most of the respondents (64%) used broadband to access their Internet at home, while 18% and 14% of the respondents used dial-up and wireless Internet respectively. Most of the respondents typically conducted online activities at home, while more than half conducted online activities at college / university and at their offices. One respondent conducted online activities at their friend's house, and another respondent conducted online activities in a public area with wireless connection. Majority of the students' respondents (64%) stated that they conducted online activities at home and college / university. Of the respondents who conducted online activities in Internet café, 30% of them were students, while the remaining respondents were from IT-related job respondents.

4.6. Security Issues

24. Do you think it is more secure to do online activity in office or university compare to your home?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>47</td>
<td>77</td>
</tr>
</tbody>
</table>

Table 4.29 – Security Issues: Comparison of home and office/university security

There were 62% of the respondents who did not think that it is more secure to do online activity in their offices or universities compare to their homes. Of the
respondents who gave negative responses, 88% of them conducted online activities at home. The data indicated that they conducted online activities at home because they did not think that it is more secure to do online activity in other places such as office or university compare to home.

Of the respondents who typically conducted online activities at home, more than half (55%) specified similar reasons that they did not think it is more secure to do online activity in other places such as office or university compare to home. However, 38% of the respondents thought that it is more secure to do online activities in office or university compare to do it at home. Interestingly, out of the respondents who gave positive responses, 87% of them conducted online activities at office and/or university.

25. Have you ever had your personal information used without authorization as a result of conducting online activities?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>9</td>
<td>115</td>
</tr>
</tbody>
</table>

Table 4.30 – Security Issues: Fraud experiences

It appeared that less than 10% of the respondents ever had their personal information used without authorization as a result of conducting online activities. Of the nine respondents who had their personal information used without authorization because of conducting online activities, three of them were students, two of them were unemployed, one of them did not specify his job, and three of them were in IT-related occupations (i.e. software engineer, data analyst, and lead engineer).
a. How did you discover this problem?

This question was open-ended rather than close-ended, with qualitative responses rather than numerical, a summary of which is included below:

- When the respondent checked his bank statement (respondent 86)
- When the respondent's artwork was being used on another website without his permission (respondent 99)
- When the respondent got a call from his bank saying that his personal details have been used and he has been told to get a new credit card (respondent 116)
- When the respondent's Yahoo e-mail password has been changed without his knowledge and permission (respondent 103)
- When there were some unauthorized activities listed in the respondent's account (respondent 45)

b. Did you manage to resolve the situation?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 9)</td>
<td>6</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 4.31 – Security Issues: Fraud resolution

The respondents who did not manage to resolve the situation prefer not to explain the reasons why. However, some of the respondents also manage to resolve the situation and give brief explanation. One respondent (respondent 116) reported that it was not difficult to solve the problem, since the credit card company was very helpful. For the respondent who had an artwork that was misused by someone else (respondent 99), he decided to pester the individual with requests to remove the artwork from his website, and finally threatened him with acts to go to his ISP and police.
26. Since I began using the World Wide Web, my level of security concern has:

<table>
<thead>
<tr>
<th></th>
<th>Increased great deal</th>
<th>Increased a little bit</th>
<th>Not changed</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>76</td>
<td>43</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 4.32 – Security Issues: Level of security concern

Since began using the World Wide Web, the level of security concern has increased great deal for 61% of the respondents, while it increased a little bit for 35% of the respondents. Of the respondents who have increased the security concern by great deal, 60% of them were from respondents who had undergraduate education, while 14% of them were from respondents who had postgraduate education.

Of the respondents who have been actively using the WWW up to three years, half of them have increased their security concern by a great deal; while of the respondents who have been active from four years or more, 60% of them have increased their security concern by a great deal.

27. Since I began using the World Wide Web, my level of security protection has:

<table>
<thead>
<tr>
<th></th>
<th>Increased great deal</th>
<th>Increased a little bit</th>
<th>Not changed</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>81</td>
<td>39</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.33 – Security Issues: Level of security protection

Majority of the respondents (65%) have increased their level of security protection by great deal, while only less than 5% who have not changed their level of security protection. Most of the respondents who had undergraduate education (69%) and more than half (55%) of the respondents who had
postgraduate education reported that their level of security protection have increased by great deal, while 28% of the respondents who had undergraduate education and 45% of the respondents who had postgraduate education showed that their level of security protection have increased by a little bit. Of the respondents who have been actively using the WWW up to three years, 68% of them have increased their security protection by a great deal; while out of the respondents who have been active from four years or more, 66% of them have increased their security protection by a great deal.

28. Since I began using the World Wide Web, my level of security knowledge has:

<table>
<thead>
<tr>
<th></th>
<th>Increased great deal</th>
<th>Increased a little bit</th>
<th>Not changed</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>84</td>
<td>37</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 4.34 – Security Issues: Level of security knowledge

Most of the respondents (67%) agreed that their security knowledge have increased by a great deal since they began using the World Wide Web, while 30% of them have increased their security knowledge by a little bit. Very similar number to question 27, majority of the respondents who had undergraduate education (69%) and 60% of the respondents who had postgraduate education reported that their level of security knowledge have increased by great deal. Of the respondents who have been actively using the WWW up to three years, 73% of them have increased their security knowledge by a great deal; while of the respondents who have been active in using the Internet for four years or more, 68% of them have increased their security knowledge by a great deal.

Therefore, from these three questions, the respondents who have increased their level of security concern, protection, and knowledge by a great deal was between 60% and 70% of the total respondents. Furthermore, out of the respondents who have been actively using the WWW up to three years, approximately within the
range of 55% to 75% of them have increased their security concern, protection, and knowledge by a great deal; while out of the respondents who have been active from four years or more, approximately 60% to 70% of them have increased their security knowledge by a great deal.

29. Please rank your security concerns of web applications in an approximate order (1 for the greatest security concern):

a. Online banking

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>91</td>
<td>9</td>
<td>3</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>11</td>
</tr>
</tbody>
</table>

Table 4.35 – Security Issues: Online banking ranking

b. Online shopping

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>38</td>
<td>49</td>
<td>12</td>
<td>11</td>
<td>1</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 4.36 – Security Issues: Online shopping ranking

c. Browser-based e-mail

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>18</td>
<td>13</td>
<td>37</td>
<td>17</td>
<td>16</td>
<td>15</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 4.37 – Security Issues: Browser-based e-mail ranking

d. Instant messaging services (chatting)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>12</td>
<td>8</td>
<td>15</td>
<td>22</td>
<td>22</td>
<td>16</td>
<td>29</td>
</tr>
</tbody>
</table>

Table 4.38 – Security Issues: Instant messaging services ranking
e. Forums / message boards

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>10</td>
<td>8</td>
<td>18</td>
<td>26</td>
<td>25</td>
<td>20</td>
<td>17</td>
</tr>
</tbody>
</table>

Table 4.39 – Security Issues: Forums / message boards ranking

f. Government websites

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>14</td>
<td>5</td>
<td>17</td>
<td>13</td>
<td>21</td>
<td>28</td>
<td>26</td>
</tr>
</tbody>
</table>

Table 4.40 – Security Issues: Government websites ranking

g. University portal / enrolment management

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># (n = 124)</td>
<td>15</td>
<td>9</td>
<td>18</td>
<td>20</td>
<td>21</td>
<td>16</td>
<td>25</td>
</tr>
</tbody>
</table>

Table 4.41 – Security Issues: University portal / enrolment management ranking

Based on the respondents’ result from Table 4.35 – Table 4.41 above, online banking was the greatest security concern (74%); followed by online shopping in as the second greatest security concern. E-mail came third, followed with forums / message boards (4th), university portal / enrolment management (5th), government websites (6th), and instant messaging services (7th) respectively.

There were 77% of the respondents who often conducted online banking that picked online banking as the online activity who has greatest security concerns; whereas almost half (46%) of the respondents who often conducted online shopping ranked online shopping in the first and second place.
Of the 30% respondents who ranked browser-based e-mail in the third greatest security concern, 81% of them used browser-based e-mail often. There were 41% respondents who often used forums, picked the fourth rank for forums; while 45% of respondents who often used government websites, ranked the government websites in the 6th or 7th place. Of the respondents who ranked instant messaging services as the least security concern, 86% of them used such services online.

At the end of the questionnaire, the respondents were given the opportunity to make any comments about any of the questions or related topics. Most of the respondents (68%) did not give any comments.

All of the data above was obtained from the survey that has been made by the researcher. These data are confidential and only used for research purposes. These data have been gathered from various resources, including ECU’s SCIS website, IT forums, and fellow peers and academic staff members. Overall, the target for the amount of respondents to do this questionnaire was achieved, and their responses were satisfactory in that all of the respondents answered all the questions. It also appeared that it took at least eight minutes for each respondent to submit this questionnaire, which indicated that they took the questionnaire seriously.

This survey showed how the respondents answer the questions. As most of them were students and others who used Internet a lot, the result of this data can be very useful to analyse and examine their attitudes towards web application security. This questionnaire provided clear picture of how they used the Internet to do online activities, and what are their concerns towards Internet security as well as their attitudes. The responses to this questionnaire showed many interesting results and information as well as played big part in finding the outcomes of the research. Therefore, in the discussion part, these responses are examined thoroughly in order to get the outcomes of this research.
5. Discussion

This chapter examines and discusses the data that have been obtained from the survey instrument. The responses of the respondents were gathered and analysed with a purpose to identify the attitudes of the respondents toward web application security. Some interesting results were found and are discussed in this section. This section also examines how these data can be used in order to address the supporting research questions, and ultimately to answer the primary research questions. The data and analysis presented in this section is divided into two sections, based on the supporting research questions.

5.1. First supporting research questions: is there a relationship between technical knowledge of web application security and users’ attitudes?

This section focuses on the survey responses regarding the relationship between respondents’ technical knowledge of web application security and respondents’ attitudes. As stated in the introduction, the first supported research question seeks to establish whether people of a higher technical skill level and knowledge of web application security are more or less cautious than people with less technical knowledge; as well as seeks to find how the users gained their technical skill and knowledge of web application security.

5.1.1. Respondents’ Background

Majority of the respondents who participated in this survey have undergraduate education (60%), with respondents who had postgraduate (16%) and college education (16%) following after it; while there was 7% of the respondents who
had high school education only. Most of the respondents were male and almost half of them were between 21 and 30 years old with undergraduate or postgraduate educations; while most of the female respondents had undergraduate educations. Furthermore, 76% of the respondents under 21 years old had undergraduate education. From the acquired data, it was found that a majority of the respondents has had completed or were in the process of completing a tertiary level of education.

As displayed in Table 4.5, there were 82% of the respondents who had been actively using the World Wide Web for at least four years; while in Table 4.6, 68% of the respondents accessed the Internet for at least approximately 19 hours a week. This indicated that not only most of respondents were regular Internet users, but it also indicated that they were likely to have developed some level of understanding of issues in web security over this time.

Furthermore, 19% of the respondents had IT-related occupation such as programmer, IT support assistant, IT consultant, IT manager, data analyst, and server administrator; while 56% of the respondents were student, including students from the School of Computer and Information Science at Edith Cowan University. Hence, from these results, it can be assumed that nearly all of the respondents were knowledgeable enough to participate in this questionnaire, as they were not only had high level of education, but they were also regular Internet users and having sound knowledge of computer and/or Internet.

5.1.2. Technical Knowledge and Levels of Caution

As a part of this research, any links between the levels of technical knowledge of web applications security and levels of user caution in using such applications was examined. The result showed that most of the respondents (84%) have at least good awareness of the risks and threats associated with using online
applications. There were 85% of male respondents and 90% of female respondents who were aware of such risks and threats. Of the respondents with high school education, only one respondent gave neutral responses, while the rest of them reported that they have a good awareness of the risks and threats associated with using online applications. Therefore, this result showed that nearly all respondents, across genders and education levels indicated that they had high level of awareness of Internet security issues.

However, when comparing to other surveys regarding users' awareness of web application security, it was found that some of the surveys discovered that many of the respondents did not have good awareness of web application security. For example, a survey that was conducted by Litan (2005, p.3) found that "many individuals are not ... aware that phishing attacks are being launched against them, which may result in the theft of their account information and eventually their money". In another survey that was conducted by Dhamija, et al (2006, p. 583), it was found that "many users do not know that a closed padlock icon in the browser indicates that the page they are viewing was delivered securely by SSL".

By looking at some of the findings of the surveys above, it appeared that their findings contradicted of the findings that this research has found. However, there are many considerations takes place that have to be checked which might affect the result of the survey. For example, see whether other surveys were anonymous or not. According to Coombes (2001, p. 38), with anonymous survey "people are more likely to be truthful", as there is no personal information given. Also look at the target audience, for example, most of the respondents in this research have been actively using the Internet for at least four years; and this also have indicated that majority of them used the Internet as their main source of information for web application security.

Furthermore in this survey, majority of the respondents indicated that they were concerned and have good understanding for most of the security threats that
were listed on the questions, such as viruses, keylogger, phishing, trojan, and spywares. More than half of the respondents also stated that they would not go online on a machine which is not protected against viruses and spywares. The majority of the respondents who had good understanding of security threats such as viruses, spywares, and keylogger were also concerned of such threats. Likewise, majority of the respondents who did not have good understanding of such threats were not concerned of such threats.

There were nearly three quarter of the respondents with lower level of education (i.e. high school and college) who indicated that they were concerned and have good understanding for most of the security threats that were listed on the questions (including viruses, spywares, keylogger, and trojan); while approximately 70% of respondents with high level of education (i.e. undergraduate and postgraduate) indicated such responses. Furthermore, nearly 80% of respondents under 21 years old and approximately three quarter of respondents between 21 and 40 years old were aware of the security verification signs on their web browser when conducting online activities. Therefore, this result indicated that older respondents or respondents with higher education did not tend to understand Internet security better than the younger respondents or respondents with lower education.

Furthermore, when the survey asked the respondents about their growth in their security concern, knowledge, and protection since began using the World Wide Web, it was found that approximately 60% to 70% respondents have increased their level of security concern, protection, and knowledge by a great deal. However, it was not only the respondents with undergraduate or postgraduate education who have made such increase, but also the respondents with high school or college education. This indicated that their level of security concern, knowledge, and protection have increased regardless of their education background. Instead, it was more to do with how long they have been actively using the Internet. The result indicated that out of the respondents who have
been actively using the WWW up to three years, approximately within the range of 55% to 75% of them have increased their security concern, protection, and knowledge by a great deal; while out of the respondents who have been active from four years or more, approximately 60% to 70% of them have increased their security knowledge by a great deal.

This findings from the two paragraphs above is in line with what Dourish, et al (2004, p. 394) found, which was the "age and experience are correlated with attitudes towards security, [as] younger respondents with a relatively longer exposure to computer systems express a much greater confidence in their abilities with computer systems". In particular, they were also more likely to report when encountering situations in which security services proved to be problematic. Therefore, the result showed that the longer the respondents spend time on the Internet, the more likely the increase of their level of online security concern, protection, and knowledge.

The majority of the respondents who conducted online banking (77%) were also conducting online transaction such as online shopping. More than half of the respondents (53%) who conducted online banking and/or online transaction were between 21 and 30 years old, whereas 30% were under 21 years old. This means that most of the respondents (83%) who conducted online banking and transaction were from 21 years old-or-under to 30 years old. From the survey that was conducted by James and Graycar (2000, p. 28), it was found that "older people have higher levels of fears [of crime] than other age groups". Furthermore, a survey by NCAVAC (1998, p. 8) stated that "age is an important indicator of perceived risk and worry about crime", with older people have higher level of worry that younger people. The Seniors Task Force (2006, p. 14) was also in the same notion, stating that "older adults are particularly fearful of crime".

A majority of the respondents (64%) checked the URL that they have typed to make sure it is spelled correctly before they gave out any personal information
when conducting online activities. This question was asked in order to know how the respondents act to prevent phishing attack. From these results, it was a high possibility that majority of the respondents were aware of phishing attack; because they checked their URL again before conducting any online activities.

Nearly three quarter of the respondents did not use the same login ID and password for all their e-mails and/or forums; and more than half of the respondents used 'remember username and password' feature in their web browsers for some websites only, while 43% of the respondents never used such feature. Most of the respondents (82%) were aware that if their forum's password is the same as their e-mail's password, it can be used to open their e-mail if the forum's database was not encrypted. From these results it was found that most of the respondents were cautious regarding the use of their usernames and passwords as it can be used by others for committing cyber crimes or other illegal and unethical acts. Therefore, one way to minimize this threat is by using different usernames and passwords and prevents using the 'remember username and password' feature that most of the web browsers have, especially for important websites such as bank or government websites. While it was not obvious from the data how the respondents were aware of the issues with using the same usernames and passwords across multiple systems, it may have been picked up during exposure to the numerous security tips and hints that are now so common on the web. For example, IT Security (2007) provided 20 minute guide to PC security, consisting of many useful tips of making the computer more secure; for example: “use a firewall, install the latest operating system’s service pack, handle e-mail attachments carefully, and set up email filters”.

5.1.3. Web Application Usage

Majority of the respondents used Mozilla Firefox and Internet Explorer. Nearly 80% of the respondents used Mozilla Firefox as their web browser, while more
than half (53%) used Internet Explorer. Of the respondents who often conducted online banking and/or online shopping, 73% of them used Mozilla Firefox; while only 37% of them used Internet Explorer. According to ComputerWorld (2006), Mozilla Firefox is the most secured web browser, ahead of Internet Explorer, Opera, and Safari. This might be one of the reasons why most of the respondents who often conducted online banking and/or online shopping used Mozilla Firefox more than Internet Explorer or any other browsers, although this question was not specifically posed to the respondents. One of the respondents who used Mozilla Firefox as the web browser stated that “security should be of the highest concern for any web applications handling financial transactions” (Respondent 51).

The most popular security guard software that the respondents used was antivirus, with firewall, popup blocker, and anti spyware following respectively. Other security guard softwares that were not listed in the questions of which the respondents used were mail and web antivirus and JavaScript blocker. Viruses, spywares, and Trojan were the security threats that the respondents most concerned about. According to the data, there were 8% of the respondents who did not use antivirus; however, 75% of those 8% used firewall, popup blocker, and advert remover. There were 77% of the respondents who used both antivirus and firewall, while nearly 60% of the respondents used antivirus, firewall, and anti spyware. There were 84% of the respondents who had IT-related job who used antivirus, firewall, and anti spyware all together, while there were only 38% of the students' respondents who used these three softwares.

These results showed that most of the respondents with IT-related job used antivirus, firewall, and anti spyware to protect themselves from any security threats; while most of the students' respondents (68%) used antivirus and popup blocker as the security guard softwares. One of the respondents gave advice that in conducting online activity, users must ensure that security guard softwares
such as antivirus, firewall, anti spyware, and popup blocker are installed properly, in order to avoid any unwanted behaviour to their systems (Respondent 28).

Antivirus was used by nearly all respondents because they were the basic, core, and most common security guard software, along with anti spyware, popup blocker and firewall. Many respondents did not use phishing filter, this was perhaps because they did not know about it or they had it but they did not realize. For example, Internet Explorer 7 has incorporated phishing filter in it; however there were possibilities that the many of them respondents did not know about this phishing filter; and at the time of data collection, Internet Explorer 7 was still in beta testing, therefore it was not included in the original survey questions.

Kristen Johnsen, the Microsoft’s senior director of security, as stated by US Federal News (2006, p. 1) explained how computer users can protect themselves from the majority of online hazards: "Microsoft recommend four simple steps people can take to keep themselves safe from the majority of online threats. This includes using a firewall, running regular software updates, using anti-virus protection and anti-spyware software". This statement is in line with the result of the survey, as most of the IT-related respondents protect themselves using antivirus, firewall, and anti spyware. In accordance to the survey, another survey that was conducted by AARP, as reported by US Federal News (2006), found that the respondents get high marks for protecting themselves with tools such as antivirus (91%), firewall (80%), and anti spyware (79%).

Most of the respondents (64%) used broadband to access their Internet at home, while 18% and 14% of the respondents used dial-up and wireless Internet respectively. Most of the respondents typically conducted online activities at home, while more than half conducted online activities at college / university and at their offices. Majority of the students’ respondents (64%) stated that they conducted online activities at home and college / university. Of the 24% of
respondents who conducted online activities in Internet café, 30% of them were students, while the remaining respondents were from IT-related job respondents.

There were 62% of the respondents who did not think that it is more secure to do online activity in their offices or universities compare to their homes. Of these 62% respondents, 88% of them conducted online activities at home. Therefore, the data indicated that they conducted online activities at home because they did not think that it is more secure to do online activity in other places such as office or university compare to home.

There were various reasons why the respondents believed that conducting online activities in the office or university is not more secure than conducting online activities at home. Most of the respondents gave similar responses which were that they felt more comfortable to conduct online activities at home because they had complete control of it; whereas in office or university, they did not have complete control. They stated that at home at least they knew the security guard softwares that they installed and used; furthermore, it is okay if they forgot to log off his e-mail for example, because there were no other users who used their computers. One of the respondents (respondent 43) summed it up with a statement that “computers in office or university may give a false sense of security, because I do not know exactly what kind of security measured they have put in place[,] while at home, I know what I have secured and to what extent”.

Of the respondents who believed it is more secure to do online activities in office or university comparing to do it at home, 87% of them conducted online activities at office and/or university. Majority of the respondents stated that the office or university provided more security restrictions such as using proxy server and firewall, which resulted in better security; while one respondent (respondent 81) stated that he believed his web applications at home did not have enough security protection.
5.1.4. Source of Knowledge and Information of Web Application Security

Internet portals were the main source of online security information to which the respondents liked to pay attention to, with television, newspaper and magazine following correspondingly. Other sources of information that were specified by the respondents were Internet forum, game, movie, RSS feed, radio, and trusted mailing list. Of the 81% of respondents who chose Internet portal as their sources of information, 31% respondents accessed the Internet over 45 hours a week, while 45% accessed the Internet between 19 and 45 hours. This indicated that most of the respondents who used Internet portal as their main sources were the ones who were online over or equal to 19 hours per week; whereas majority of respondents who were online under 19 hours a week use television and newspaper as their source of information. Procter (2001, p. 8) stated that users preferred to use Internet as source of information, rather than newspaper, TV, or radio. Procter (2001) further explained that “what is interesting is the Internet has branded itself the free information media”, unlike newspaper and pay-TV. One of the reasons why many people preferred Internet as the source of information was because people can get the latest and up to date news from around the world, and they also can look at specific subjects or things that they want to see or learn.

Nearly half of the respondents kept themselves up to date on current news related to online security; and of these respondents, 78% were conducting online banking and/or online shopping. This signified that most of the respondents who conducted online banking and/or online shopping were also keeping themselves up to date on current information related to online security. One of the possible reasons for keeping up to date on current news regarding online security was for the respondents to see whether there are new threats takes place so that they
are aware of it and hopefully have some information on how to prevent such threats. Another reason might be for the respondents to keep themselves up to date on latest security software guards such as antivirus or anti-spyware. When it comes to money, people make sure that they have sufficient knowledge to keep their money safe. For example, Microsoft (2000) stated that people endangered themselves if they conducted online activities without having knowledge on Internet security. As "knowledge is power for internet privacy and security" (Microsoft, 2000), people are willing to sacrifice their time to increase their knowledge about security in order to keep their money secure, such as by protecting confidential information.

5.2. **Second supporting research question: does the type of web applications dictate the level of users' security concerns?**

This section focuses on analysing the responses of the respondents regarding on whether the type of web applications dictate the level of respondents' security concerns. The second supported research question examined whether users are more careful when using a particular type of web application (e.g. online banking) than other type of web application (e.g. e-mail / forum); as well as investigates whether users pay attention to security signs or logos when engaged in online activities which involve them to reveal their personal information or account details on a particular website.

5.2.1. **Respondents' Concern of Different Types of Web Applications**

The respondents appeared to be much more concerned about security threats when conducting online activities such as online banking and online shopping than accessing e-mail account, with 87% giving positive responses. From the
respondents' feedback, it was found that here were three main reasons of why the respondents did not concern about the security of accessing e-mail account as much as conducting online banking. The first reason was because the respondents did not store any confidential data such as credit card number, usernames, or passwords in their e-mail. The second reason was because even though they did not know about the security threats when using e-mail, but they did not store any confidential information in their e-mail. The third reason was because the respondent simply knew that their e-mail may be vulnerable and therefore they did not store any confidential data.

In giving their credit card number when shopping online, nearly 60% of the respondents felt comfortable to do so, while 23% did not feel comfortable. Accordingly, 86% of the respondents who felt comfortable in giving their credit card number were regularly conducting transaction online, while almost half (47%) of the respondents who did not feel comfortable were rarely conducting transaction online. This indicated that most of the respondents who regularly conducted online transaction felt comfortable in giving their credit card number when shop online. One of the respondents (respondent 39) who felt comfortable in giving his credit card number stated that he felt confident with the level of security protection of his computer, and therefore he felt save to conduct online shopping.

Interestingly, only a quarter (25%) of the respondents who had been hit by fraud were also the respondents who felt comfortable in giving their credit card number. One of the respondents who were hit by fraud gave his advice "Don't dare to give your personal information in the web, no matter how good is your personal web security" (Respondent 59). This result might indicate that most of the respondents who had been hit by fraud did not feel comfortable any more in shopping online. Thus, this might signify that the level of concern the respondents have was dependant on how often they conducted the online activities which lead to such threats. From a survey that was conducted by
Forrester Research, as stated by Thomas (2005), 83% of Internet users that they surveyed “have stopped banking online because of security fears”. GlobalFS (2006) stated that in a research conducted by ESTA (2005) to European citizens; it was found that “11% of them had been hit by card fraud, translating to around 22 million people”. As a result of this, 33% of these respondents who were hit by fraud have stopped conducting online activities.

Based on the respondents' ranking, online banking was ranked as having the greatest security concern (74%). The respondents ranked online shopping in the second place with 40%; whereas e-mail came third, followed with forums / message boards (fifth), university portal / enrolment management (sixth), government websites (seventh), and instant messaging services (eight) respectively.

There were 77% of the respondents who often conducted online banking that picked online banking as the online activity that has greatest security concerns; while there were more than half of the respondents who often conducted online shopping that ranked online shopping in the first and second rank. This is interesting that even though they thought online banking or online shopping has the greatest or second greatest security concerns, but majority of them were still conducting it. In accordance, BBC (2005) stated that in a survey commissioned by Intervoice (2005), it was found that only 17% of the respondents stopped banking online and 13 percent stopped shopping online. Of the respondents who stopped online banking and online shopping, BBC (2005) stated that the reason was because they were worried by online ID theft, as identity theft can result in the users' confidential information such as user IDs, passwords, credit card number, or bank account number being exposed; so that attackers may use that information to gain access to their finances and steal money from them. Therefore, majority of the respondents still conducted online shopping even though they knew the risks, except those that had been hit by such fraud.
Of the 30% respondents who ranked browser-based e-mail in the third greatest security concern, 81% of them used browser-based e-mail often. Approximately 40% of the respondents who often used forums picked the fourth rank for forums; while 45% of respondents who often used government websites ranked the government websites in the sixth or seventh place. This signified that nearly half of them, even though they used government website, did not really concern them about the security threats. Of the respondents who ranked instant messaging services as the least security concern, 86% of them used such services online.

5.2.2. Respondents’ Experiences with Fraud

Less than 10% of the respondents ever had their personal information used without authorization as a result of conducting online activities. Of the nine respondents who had their personal information used without authorization because of conducting online activities, three of them were student, two of them were unemployed, one of them did not specify his job, and three of them were in IT-relayed occupation (i.e. software engineer, data analyst, and lead engineer). They discovered this problem by various reasons: [1] when the respondent checked his bank statement (respondent 86); [2] when the respondent's artwork was being used on another website without his permission (respondent 99); [3] when the respondent got a call from his bank saying that his personal details have been used and he has been told to get a new credit card (respondent 116); [4] when the respondent’s Yahoo e-mail password has been changed without his knowledge and permission (respondent 103); [5] when there were some unauthorized activities listed in the respondent’s account (respondent 45).

The respondents who did not manage to resolve the situation prefer not to explain the reasons. However, some of the respondents who managed to resolve the situation gave brief explanation: [1] for the respondent who had his credit card being used (respondent 116), he reported that it was not difficult to solve the problem, since the credit card company was very helpful; [2] for the respondent
who had an artwork that was used without permission (respondent 99), he decided to pester the individual with requests to remove the artwork from his website, and finally threatened him with acts to go to the ISP (Internet Service Provider) and police.

5.2.3. Respondents’ Awareness of the Web Security Environment

There were 73% of the respondents who were aware of the https sign or any other signs of security verification on their web browser when conducting online activities such as banking or shopping, while only less than 10% who did not aware of it. Of the respondents who aware of the security signs, 75% have increased their security knowledge by a great deal since they used the WWW, while 24% have increased it by a little bit. Thus, this percentage indicated the reason of how nearly three quarter of the respondents were actually aware of security signs on their web browser when conducting online activities, which was because of the big increase in their security knowledge.

There were mixed responses on whether the respondents felt comfortable in giving their login ID and password when opening an e-mail even without the security verification. The respondents gave equal responses of 35% for each neutral and agree responses, whereas 25% of the respondents gave negative responses for this statement. One of the possible reasons of why there were mixed responses for this question is because of the words 'even without the security verification'. If the respondents did not see that words, most of them might gave positive responses (i.e. felt comfortable in giving their login ID and password); as most of the respondents (84%) used e-mail regularly. However, by the words 'even without security verification', this informed the users that if their e-mail were not secure, there is a possibility of the data inside their e-mail being stolen, which may lead to cyber crime (e.g. credit card fraud, bank account fraud, defamation).
6. Conclusion

6.1. Key Findings

Most of the respondents within this research were regular Internet users and also have indicated that they were likely to have developed some level of understanding of issues in web security over this time. A majority of the respondents were concerned and claimed to have had a good understanding of most of the security threats, including virus, spyware, keylogger, and phishing; and they were cautious regarding the use of their usernames and passwords. Majority of the respondents were aware of security signs on their web browser when conducting online activities and also checked their URL again before conducting any online activities. As stated, the results of this research indicated that nearly all respondents, across genders and education levels indicated that they had high levels of awareness of Internet security issues.

This research also found that younger respondents were less fearful than older respondents in terms of the way they conducted online activities. The result of the research further indicated that the length of the respondents’ involvement in actively using the Internet reflects their level of understanding of web application security, including their security concern, knowledge, and protection.

Internet portals were the main source of online security information for respondents who were online quite often (typically in excess of 19 hours per week); while television and newspapers were the main sources of online security information for respondents who were not online as often (typically less than 19 hours per week).

Most of the respondents who regularly conducted online transaction felt comfortable in giving their credit card number when shop online, while a majority
of the respondents still conducted online shopping even though they knew the risks, except those that had been hit by fraud. As well as levels of experience using the Internet, this research found that the level of concern the respondents have was dependant on whether they had been a victim of web based security threats. This could be ascribed to the human condition of 'it will never happen to me', until it actually does.

The result of the research also signified that most of the respondents who conducted online activities who have greater risks such as online banking and/or online shopping were also keeping themselves up to date on current information related to online security. When it comes to money, people make sure that they have sufficient knowledge to keep their money safe, even if that means they need extra effort.

6.2. Recommendations for Future Research

This research has found that nearly all respondents, across gender and education levels indicated that they had high level of awareness of web application security issues. However, other research also found that there are many users who do not have good awareness of web application security. Due to the anonymous nature of the survey, a case study research in this area is recommended, which concentrates on a group of individuals with a purpose to analyse the relationship between their demographic details and their knowledge on web application security. For example, the researcher may monitor these people who use the web application, in order to observe their behaviours.

This research also found that majority of the respondents still conducted online shopping even though they know the risks. Furthermore, the younger respondents appeared to be less fearful than older respondents in terms of the way they conducted online activities. Hence, further research can be done in
analysing and comparing the demographic details of the risk takers, such as their age, gender, or culture, with their online activities habit.

The result of the survey also discovered that three quarter of the respondents did not have good understanding of man in the middle attack, and half of the respondents did not have good understanding about phishing threats. It is recommended to do further research in this subject of why many people are not up to speed on these particular threats. It is also recommended for institutions to teach Internet users of these areas so they are more familiar with these threats.

6.3. **Conclusion**

Since the introduction of the Internet and then the WWW, the technology has grown rapidly and become an integral part of life for many people and businesses throughout the world. As web applications and the WWW become more useful and important, the security threats and risk increase as well. These security threats and risks are becoming a barrier to many businesses and users when it comes to online transactions or any other activities that involves personal details or login accounts.

This research aimed to identify and analyse users’ perspectives and attitudes towards web application security. In essence, this research provided an introductory roadmap to some of the current security issues facing web based applications and how the web users perceive and deal with such issues. By building on the findings of this research, it is hoped that user education in regards to web applications security can be more effectively developed and targeted at the ever growing numbers of web users in modern society.
7. References


James, M. & Graycar, A. (2000). Preventing Crime Against Older Australians
es.com/prevelderlycrime.pdf

detection of web application vulnerabilities, Proceedings of the 2006
workshop on Programming languages and analysis for security (Vol. 13).
Ottawa, Ontario, Canada: ACM Press.

http://www.webopedia.com/TERM/D/Data_Sending_Trojan.html

seals in consumer trust, Proceedings of the 6th international conference

turning lemons into lemonade. SIGSOFT Software Engineering Notes,
26(6), 16-18.

questionnaire evaluation. SIGSOFT Software Engineering Notes, 27(3),
20-23.

New Jersey: Pearson Education, Inc.


from http://www.lsu.edu/university_relations/webpolicy/definitions.htm


Appendix A – Online Questionnaire

Introduction

Users’ Perspectives and Attitudes towards Web Application Security

This questionnaire is part of an honours research project regarding users’ perspectives and attitudes towards security in web applications. This questionnaire should only take a few minutes of your time, and is completely confidential and anonymous. Your participation in this research is very much appreciated. If you have any questions regarding the questionnaire or research, please contact me, Leonard Ticualu, by e-mail at (lticualu@student.ecu.edu.au), or contact my research supervisor Dr Justin Brown at (j.brown@ecu.edu.au)

Respondents’ Background

Gender: Male Age: Under 21

Education achievement: Undergraduate Occupation: 

How long have you been actively using the World Wide Web? Under 1 year

How often do you access the Internet approximately a week? Less than 5 hours

Section 1 – Opinions on Security

SECTION 1. Opinions on Security

<table>
<thead>
<tr>
<th></th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>I have a very good awareness of the risks and threats associated with using online applications</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>2.</td>
<td>Please list your response for each of the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Viruses</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. I have a very good understanding of virus threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>ii. I am very concerned about being hit by a virus when online</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>iii. I would not go online on a machine which is not protected against viruses</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>b) Spyware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. I have a very good understanding of spyware threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>ii. I am very concerned about spyware threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>iii. I would not go online on a machine which is not protected against spyware</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>c) Keylogger</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. I have a very good understanding of keylogger threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>ii. I am very concerned about keylogger threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>d) Phishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. I do not understand phishing threats</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>
6. I am very concerned about phishing threats  
   c  c  c  c  c  c  
7. I have a very good understanding of Trojan/backdoor threats  
   c  c  c  c  c  c  
8. I am very concerned about Trojan/backdoor threats  
   c  c  c  c  c  c  
9. Man in the middle attack  
   c  c  c  c  c  c  
10. I have a very good understanding of man in the middle attack  
    c  c  c  c  c  c  
11. I am very concerned about man in the middle attack  
    c  c  c  c  c  c  
12. I am more concerned about security threats when conducting online banking or online shopping than say accessing an email account  
    c  c  c  c  c  c  
13. I feel comfortable in giving my credit card number when shopping online  
    c  c  c  c  c  c  
14. I am aware of the https sign or other signs of security verification (such as the padlock symbol) on my web browser when conducting online activities (e.g. online banking)  
    c  c  c  c  c  c  
15. I feel comfortable logging into my email system even if the https address or padlock symbol is not shown  
    c  c  c  c  c  c  
16. I keep up to date on current news and information that are related to online security  
    c  c  c  c  c  c  

Section 2 – Web Applications Usage

<table>
<thead>
<tr>
<th>SECTION 2. Web Applications Usage</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. I often conduct the following activities:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Online banking (include bill payment)</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>b. Online transactions (include shopping)</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>c. Browser-based e-mail</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>d. Instant messaging services (chatting)</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>e. Forums / message boards</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>f. Government websites</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>g. University portal / enrolment management</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
</tbody>
</table>

Section 3 – Behaviours towards Security

<table>
<thead>
<tr>
<th>SECTION 3. Behaviours towards Security</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. When giving out personal information online, I check the URL that I have typed to make sure it is spelled correctly</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>10. I use the same login ID and password for all my emails, forums, online shopping and wherever possible</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>11. I let my web browser remember usernames and passwords</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>12. I am aware that if my forum’s password is the same as my email’s password, it can be used to open my email if the forum’s database is not encrypted</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
</tbody>
</table>

94
Section 4 – Web Applications Information

13. Please check the web browsers you most frequently use

- Internet Explorer
- Mozilla Firefox
- Opera
- Safari
- Netscape

14. Please check the following security guard software(s) that you currently use

- Antivirus
- Firewall
- Anti-spyware
- Phishing filter
- Popup blocker
- Spam blocker
- Advert remover
- Other (please specify)

15. Please check the following sources of news or information to which you pay attention

- Television
- Magazine
- Newspaper
- Internet portal (e.g., Yahoo / NineMSN)
- Other (please specify)

16. Please choose the type of internet access that you have at home

- Dial-up modem
- Broadband
- Wireless
- Other (please specify)

17. Please check the following places of where you typically go online

- Home
- Office
- College / University
- Internet cafe
- Other (please specify)
Section 5 – Security Issues

SECTION 5. Security Issues

10. Do you think it is more secure to do online activity in office or university compared to your home?
   - Yes (why? please explain)
   - No (why? please explain)

19. Have you ever had your personal information used without authorization as a result of conducting online activities?
   - Yes (go to question 20)
   - No (go to question 21)

20. a) How did you discover this problem?
   - Yes (was it difficult? please explain)
   - No (why? please explain)

21. Since I began using the World Wide Web, my level of security concern has:
   - Increased greatly
   - Increased a little bit
   - Not changed

22. Since I began using the World Wide Web, my level of security protection has:
   - Increased greatly
   - Increased a little bit
   - Not changed

23. Since I began using the World Wide Web, my level of security knowledge has:
   - Increased greatly
   - Increased a little bit
   - Not changed

24. Please rank your security concerns for web applications in order from 1 (most concerned) through to 7 (least concerned):
   a. Online banking
   b. Online shopping
   c. Browser based e-mail
   d. Instant messaging services (chatting)
   e. Forums
   f. Government websites
   g. University portal / enrolment

25. Please feel free to make any further comments about any of these questions or related topics

Submit
Appendix B – Information Letter

This research aims to investigate users’ perspectives and attitudes towards security in the use of web applications. You are being asked to participate in this research by kindly completing the attached Web Application Security Survey so as to provide data about the way in which web users interact with and use web applications, from a security perspective.

The online survey is completely voluntary and anonymous, and your agreement to participate is signalled by your completion of the survey instrument. The collected data will not be used for any purposes other than for the conduct of this research. Result of the research will be published in a thesis, and possibly in an academic conference or journal.

Any questions regarding the project may be directed to Leonard Ticualu on 94709328 or e-mail lticualu@student.ecu.edu.au or his supervisor Dr Justin Brown on 93706174 or e-mail j.brown@ecu.edu.au. However, if you have any concerns about the project and would like to talk to an impartial person, you may contact Michael Collins, School of Computer and Information Science, Edith Cowan University on 93706828 or e-mail m.collins@ecu.edu.au.

Thank you very much for your time and consideration regarding my research.

=================================

I/we Leonard Ticualu have read the above information and any questions I/we have asked have been answered to my satisfaction.

I/we agree to participate in this activity by completing the attached survey instrument, realising I/we may withdraw at any time without prejudice. I/we agree
that the research data gathered for this study may be published provided I/we are not identifiable.

Participant(s) or authorised representative

Leonard Ticualu

Investigator

Date:

02\textsuperscript{nd} November 2006