AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

A Study of Security Awareness in Using Wireless Networks

[1]A.K. Aini Zuriyati, [1]M. Muriati, [1]N. Akhyari, [2]A. Zurairah

[1]*Faculty of Computer Media & Technology Management, TATI University College, 24000 Terengganu, MALAYSIA*
[2]*Center of Preparatory & General Studies, TATI University College, 24000Terengganu, MALAYSIA*

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 24 January 2014
Accepted 29 January 2014
Available online 5 April2014

Keywords:
Security awareness, wireless network, knowledge, threat

ABSTRACT

The purpose of this paper is to identify and study the security awareness among users when using wireless network. In this study, we found that student's traffic dominated all internet traffic for web surfing, particularly in residences populated by newer students; students are increasingly choosing a wireless laptop as their primary computer. Although web protocols were the single largest component of traffic volume, network backup and file sharing contributed to unexpectedly large amount to the traffic. Due to this situation, the study was done to identify the awareness towards security among users that using wireless network. Most of the people using wireless network does not realise the threat that occurs in wireless network. They only know and want to learn how to use wireless broadband but not really concern on the security. The method being used to obtain the data is by distributed the questionnaires. The study used questionnaire distribute to over 300 students for obtaining the data. Some 200 respondents have returned their feedback. The respondents have been selected from various programs available at TATIUC which is from certificate to master levels. Meanwhile, the analysis of the data was done by using descriptive statistic analysis and cross tabulation measure. The descriptive statistic includes frequency and percentage, while cross tabulation measure is based on percentage of the value to measuring the data. Based on the result it shows that, the knowledge of security networks is very least among the users. This situation shows that their awareness towards security is not a major concern. They only concern on the wireless functioning rather than concern on the threat that they should alert over the wireless network itself. Due to this situation, the respondent should be educating with basic platform of security networks in order to alert their awareness towards wireless network. This could help them preventing their private data from being stolen or destroyed in the future.

To Cite This Article: A.K. Aini Zuriyati, M. Muriati, N. Akhyari, A. Zurairah., A Study of Security Awareness in Using Wireless Networks. ***Aust. J. Basic & Appl. Sci.,*** *8(4): 35-39, 2014*

INTRODUCTION

Wireless local-area networks (WLANs) are increasingly common, particularly on university and corporate campus. For example, a contemporary survey of 392 academic institutions found that nearly all plan to install a wireless network, about half already have a limited deployment, and a 7% have a "comprehensive" deployment (D. Kotz ,K. Essien, 2002) Wireless technology allows a computer to be connected to a wireless local area network (WLAN) by means of ''access points'' through radio waves without the need for cables or wires. This allows multiple users to share the same WIFI access point or 'hotspot' within a particular range. Wireless networking presents many advantages productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. 'WI-FI mooching', 'piggybacking', 'joyriding' or 'hitchhiking' are common hazards of an open WI-FI connection. These different names describe the same activity of obtaining wireless Internet access without the permission or knowledge of the subscriber. If too many people log on, this could significantly slow down subscribers' Internet access speeds. As pointed out earlier, a number of data points indicate the rapid growth of wireless LANs. In 2001, 8 million WLAN chipsets were sold, an increase of 23% over the previous year; in 2002, this number grew to 11.6 million chipsets giving an increase of 65% (Cahner In-Stat, 2002. Durand , Schwartz, 2000).

Corresponding Author: A.K. Aini Zuriyati, Department of Computer Science, Faculty of Computer, Media & Technology Management, TATI University College, 24000 Terengganu, MALAYSIA.
E-mail:aini@tatiuc.edu.my

Australian Journal of Basic and Applied Sciences, 8(4) Special 2014, Pages: 35-39

WLANs for the home and small businesses are expected to grow by 103% and for enterprise by 32% (M. Paolini, R. Pow, 2002). Given the rising of the popularity in using WIFI, this paper will discuss on the activity respondents that *like to surfs over the internet, type of threat over the internet* and *security awareness in using WIFI*. Security awareness is important especially for academic environment. It can reduce human error, theft, fraud, and also the wrong ways of used computer assets. Due to these reasons, many researchers compete to each others in providing meaningful information of security awareness. (Kruger, Kearney, 2006), report on development of a prototype model for measuring information security awareness. The model makes use of a simple data gathering process and weighting system. It then was combined with multi criteria problem solution techniques, provided a quantitative measurement of security awareness levels. This model offers several opportunities for enhancement and several aspects are currently considered to improve the model (Kruger, Kearney, 2006) A study by (Drevin, Kruger, Steyn, 2007) is focused on ICT security awareness and how to identify key areas. Seven employees were interviewed and the result was a list of values that apply to ICT security awareness. Several objectives then are identified by constructing a network using the value focused approach (Drevin, Kruger, Steyn, 2007). (Rezgui, Marks, 2008) explores factors that affect information security awareness. General aim is to explore the levels of information system security awareness of higher education in developing country. The study found the environments and their setup play a major role in influencing information system security awareness (Rezgui, Marks, 2008).

2. Wireless network connection - collegenet@tatiuc:

TATI University College is a college university situated at Kemaman, Terengganu, Malaysia. Same with others university, TATIUC also provided internet access. The campus has 34 Mbps 802.11b coverage for nearly every building, including all administrative, academic, and residential buildings, student's hostel and also ITC. The internet can be access within the administration building. The details of wireless connection can refer in table 1. The analysis shows that, there are nearly one thousand users has been trace from the general campus within 20 buildings for 4 weeks academic term used wireless networks in TATIUC.

Table 1: AP SSID at TATIUC.

AP SSID	Accessibility
collegenet@TATIUC	All users within TATIUC area
guest@TATIUC	All user within TATIUC area
admin@TATIUC	TATIUC Admin staff only
staff@TATIUC	TATIUC's staff only
library@TATIUC	All users within library area

Every building is provided with wireless connection that attached to access point. Meanwhile, for certain building such as admin, lecturer's rooms and computer lab are attached with wired connection. There are 30 access points that located at several places such as hostels; there were 2 access points for each of the hostels building. Meanwhile, the categories of users at TATIUC can be divided into three parts which are students 70%, staffs and outsiders or guest 30%.

This paper will focus on the students since they are the highest ranking of network users at TATIUC which is 70%. In addition, they are the only categories of users who can be considered 24 hours were available at TATIUC. Meanwhile, TATIUC's staffs only use network connection during office hours which mean only at the day time that is eight hours only. To fulfill the objective of the analysis in analyzing the security awareness in using WIFI network at TATIUC, the analysis is focusing to the numbers of students based on ganders towards their preferable activities being done when they access the internet, type of threat over the internet that they realize and to identify their awareness towards security network.

Wireless is easier in accessing network rather than wired. At TATIUC, most of the network users access wireless to connect over the network. The SSID access point that have chosen for monitoring users network activity known as collegenet@TATIUC shown at fig. 1.In deciding the access point for analyse the internet usage, collegenet@TATIUC shows that the access point are mostly connected by students at TATIUC. Moreover, 90% of the users at TATIUC using wireless network to access internet and the rest are using wired such as at lecturer rooms, computer lab and administration office. The wireless connections are provided to all users to access the internet at TATIUC, meanwhile wired connection are limited to certain group of users.

Fig. 1: TATIUC wireless connections.

There are four access point SSID at TATIUC that are shown in fig. 1, but the access point collegent@TATIUC are the main access point that students choose to connect. collegenet@TATIUC access point SSID is the access point that provided to all the students at TATIUC to connect over the network without any login details. Besides, the access point also being provided with more bandwidth allocation compare to other access point. The bandwidth allocations for network at TATIUC are shown in fig. 2. Fig. 2 shows the network topology from core layer, distribution layer and access layer. There is also the bandwidth allocation provided to the network users. The wireless connections covering all the area at TATIUC, and the wired connection only provided to administration and few of faculties building. The circle shows the area of collegenet@TATIUC.

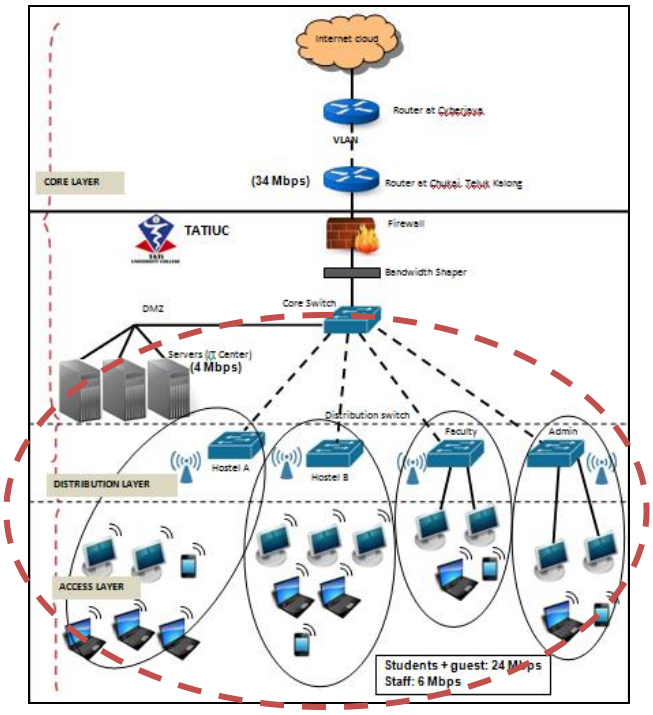

Fig. 2: TATIUC's network topology.

3. Methodology:

This study used questionnaire method to obtain data from the students that study at TATI University College from various programs that offered here. This study distributed questionnaire to collect data and also focusing on the respondents who have least knowledge on security networks even though they know how to surf the internet. In other words, students that often surf the internet did not aware or zero knowledge on security network. There were four sections of questionnaire being classified that are demographic profile, internet usage,

computer application and security awareness. Selected participant required to fill their personal profile such as gander, age and level of education. Then followed by answering questions on internet usage, type of application they often used and questions on their awareness towards security when surfing over the internet. Some 300 questionnaires were distributed among the students of TATIUC from various levels of education. Out of which 200 were usable in giving a return feedback. Descriptive statistic and cross tabulation analysis are used to analyze the data.

Result:

The result of the study is concentrated on the numbers of students based on gander towards their preferable activities being done when they access the internet, type of threats over the internet and to identify their awareness towards security network. Based on the questionnaire the following results are presented:

Result of internet usage preferable activities refer to gander:

Based on the demographic profile which refers to gander, male respondents is easier to participate. It shows that 63.5% given a response. Meanwhile, for female respondent only 36.5% has given their response. This is shown in table 2 below. This shows that male students interested more in exploring the internet.

Table 2: Respondent based on gander.

Item	Category	Frequency	Percent	Cumulative Percent
Gender	Male	127	63.5	63.5
	Female	73	36.5	36.5
Total		200	100.0	100

Furthermore, based on the activities, the question required the respondent to select *yes* or *no* to the activities listed below. The analysis of data is using cross tabulation to find the percentage between gander and the activity access over the internet. The percentage shows are based on respondent that selected *yes.* Three highest percentages are discussed based on gander. Referring to table 3, shows that male respondents like to play computer games where this is the highest percentage 69.1% compared to other activities. Followed by using various types of application, where the percentage is 67.6% which means that they like to explore different type of application available. They also like to send and receive email activities where the percentage is 66.3%. Meanwhile, female respondents prefer more on browsing the internet for entertainment. They like to watch movies over the internet. The percentage shows that 36.7% prefer entertainment over the internet. Followed by doing research and academic purpose, which is 36.6% and download music or video 35.3%. Table 3 below shows the activities that the respondents do when browsing the internet.

Table 3: Percentage of activities based on gander.

Activities	Percentage that agree with the activities	
	Male	Female
1. Use the world wide web for entertainment	63.3%	36.7%
2. Send or received email	66.3%	33.8%
3. Social Networking	65.8%	34.2%
4. Play computer game	69.1%	30.9%
5. Download music or video	64.7%	35.3%
6. Use other computer applications	67.6%	32.4%
7. Research or academic purpose	63.4%	36.6%

Result of threat over the internet:

Network threat can occur any time without realizing by users. In this study there are some types of threat being asked to the respondents in order to ensure they understand or they have knowledge towards the threat being discussed. The result is shown at table 4.

Table 4: Types of threat over the network

Category	Frequency		Percent	
	Yes	No	Yes	No
1. Know about chain email	88	111	44%	55.8%
2. Received spam email	114	81	57%	40.5%
3. Identify spy ware	137	60	68.5%	30.5%
4. Have experience hack by Hackers.	82	114	41%	57%

Based on table 4, shows the types of threat that might occur over wireless network. The analysis of data shows the result that based on the selection choice (1 to 5) which is the highest percentage was selected that if the respondent received chain email 22.5% that select to ignore the chain email. Meanwhile, if the respondent receives spam email 29.5% choose to delete the email. Followed by steps taken to overcome spy ware, it shows that 44% select to install spy ware application. Having experience hack by hackers, 25% of the respondent select to add security to their computer. This shows that the respondent knew only some types of threat over the wireless network but they still have least knowledge about network security. Referring to the percentage, they only recognize viruses and email that might attach with virus towards their email.

Result of security awareness:

Based on analysis of data, it shows that 82.8% respondents select that they like to surf internet using public WIFI. Unlikely, for rating the security and privacy of using public WIFI shows that 26.5% choose it is safe, 20% not safe, 25% I don't know, 14.5% I don't care and 3% others. It shows that the difference of their awareness toward public wireless network is only 5%. Besides, they do not realize how importance for them to alert with the security when using public WIFI.

There were many people's define safety as protection from adverse effects. Based on the skills of (1-5) which are *very concerned to least concerned* selection, the highest selection is 42% that is act neutral to safety of the computer. Meanwhile for rating the knowledge about security, by using the same skills (1-5) it shows that the highest percentage is also to act natural which is 40%. Table 5 illustrates the percentage of respondents concern of their computer safety and their knowledge towards security awareness.

Table 5: Summary of security awareness.

Questions	Very	Sometimes	Neutral	Somewhat	Least
Overall, concern on computer security.	17.3%	35.2%	42.9%	2.6%	2.0%
Overall, knowledge towards security of using WIFI	17.9%	33.3%	41.5%	5.1%	2.1%

Conclusions:

The overall conclusion shows that, the respondents know about the precaution towards the threat that they will face when using wireless network. Since the threat that happened was not aware by the respondents themselves because their knowledge towards security networks are very least. Besides, they taught that it is normal thing when discuss about security matter towards wireless network. This people should be educate by giving training or perform a specific module to deliver the knowledge on security awareness towards wireless network. Their attitude for not concerning about this situation will cause more damages towards the usage of wireless network in the future. Since using wireless network also has it own disadvantages that should put under consideration such as security, range, reliability and speed. If the respondent only acts natural to this situation it will cause more threat towards users and make the wireless network useful in the future. Because of that, the knowledge and awareness towards security is very important and needs to deliver.

ACKNOWLEDGEMENT

We would like to extend sincere appreciation to all the group members and students from all faculties at respective research area who involved in this study. The special thanks to Rector and Deputy Rector that encourage and allow us to do this research. Not forgotten also for funding this research. Thank you from all the group members.

REFERENCES

Cahner In-Stat/MDR, 2003. "Attractive cost of 802.11b drove Wi-Fi shipments in 2002", February 12, 2003. Available: http://www.instat.com/press.asp?ID=541&sku=IN 020181LN

Drevin, L., H.A. Kruger, T. Steyn, 2007. "Value-focused assessment of ICT security awareness in an academic enviroment". Computer & Security, 26: 36-43.

Durand, R. and J. Schwartz, 2000. "Single wireless standard needed". Communications News, 38(7): 4-5.

Kotz, D. and K. Essien, 2002. "Characterizing usage of a campus-wide wireless network". Technical Report TR2002-423, Dartmouth College, March 2002.

Kotz, D. and K. Essien. "Analysis of a Campuswide Wireless Network". Technical Report TR2002-423, Dartmouth College, March 2002.

Kruger, H.A. and W.D. Kearney, 2006. "A prototype for assessing information security awareness". Computers & Security, 25: 289-296.

Paolini, M. and R. Pow, 2002. "Public wireless LANaccess: US market forecasts 2002–2007 analyses". February 6, 2002. Available: http://www.analysys.com/ (News).

Rezgui, Y., A. Marks, 2008. "Information security awareness in higher education: An exploratory study". Computers & Security, 27: 241-253.