Proceedings of The National Conference
On Undergraduate Research (NCUR) 2014
University of Kentucky, Lexington, KY
April 3-5, 2014

Assessing the Level of Knowledge About Cybercrimes Among Young Adults Within the United Arab Emirates

Sarah Bamatraf
Computer Science
Zayed University
Abu Dhabi, UAE

Faculty Advisor: Dr. Fatme Al Anouti

Abstract

Background: Our lives have tremendously changed because of technological innovations. Over the last few decades, there has been a remarkable increase in the use and reliance on internet and digital technology for research, education, healthcare, business and even fun. Despite the valuable convenience and benefits technology has added to our life styles, there is a serious risk associated with the reliance on such digital technology. Sometimes confidential and private information becomes accessible for hackers who launch unexpected attacks and as a result many individuals might fall victims for cybercrime attacks. The incidence of such cybercrime attacks has increased drastically over the last few years in the United Arab Emirates (UAE) which enjoys an advanced telecommunication network coverage. According to police reports, most cybercrime victims are young adults because they heavily use the internet for their day to day activities. Aim: The purpose of the study is to assess the level of knowledge about cybercrimes among a representative sample of young adult Emiratis. Design: This study uses a cross-sectional study design. Methodology: The participants were 130 students (113 females and 17 males) from two different universities namely Zayed University and Abu Dhabi university both in the capital city of the UAE. All participants completed an online questionnaire that was adapted from the Cybercrime Knowledge Questionnaire; developed by Katz, 2005. The online version of the questionnaire was sent to all students through campus announcement and twitter. It was utilized to calculate the cybercrime awareness index (CAI) which reflected the level of knowledge about cybercrimes by university students**.** Results**:** The mean value for CAI indicated a medium level of knowledge about cybercrimes by students. Only 32% of the participants had a high or adequate level of knowledge while the rest had low to medium levels of knowledge. There was a statistically significant difference in the level of knowledge in terms of student major but not gender. Students specializing in Computer Information Technology (accounting for 21.5% of the participants) had the highest levels of knowledge as compared to all other students from other majors. This was in concordance with another finding in the study which revealed a strong correlation between the level of knowledge and the use of the internet/digital technology. Participants with heavy use of internet technology had a high level of knowledge about cybercrimes. Conclusions: In conclusion, the findings of this study demonstrated that the level of knowledge about cybercrimes among university students is not adequate. These young adults should be more educated about the risks of technology use in terms of cybercrime attacks. Future research could focus on developing strategies to raise awareness and alert students to the risks of being victims of cybercrimes.

Keywords: Cybercrime, Cyber awareness, Cyber victims.

1. Introduction

Cybercrimes are crimes that involve the use of computers and internet network. The computer that is used can be the source of a crime or a target . Halder and Jaishankar (2011) defines Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Some of these crimes may have a slight impact on individuals, nonetheless, the majority of such crimes have a greater impact and could even threaten a nation’s security. Furthermore, cracking, hacking, copyright infringement, child pornography are all types of cybercrimes with different level of impact.

Some examples of cybercrimes include fraud that is caused by the manipulation of computer records, spamming, deliberate act of circumvention of computer security systems, the theft of intellectual property which includes software piracy, and Industrial espionage. Also, identity theft and creating or spreading computer viruses or worms are all types of computer crimes.

The intention of attackers often varies with some being driven by the thought of inflicting intimidation, some being motivated by the concept of being able to “control”, while other attacks are constantly committed by perpetrators who believe that their attacks are unlikely to be identified and hence cannot be punished for. Bullying, cyber stalking, hacking, defamation, pornographic images, and electronic blackmailing are all modern crimes that are committed by perpetrators who could be difficult sometimes to trace. (Halder and Jaishankar, 2011).

The United Arab Emirates(UAE); with all the advancement and technology it’s experiencing; has managed to change the status of its nationals and residents. It has become easier for all Emiratis to find what they are searching for with just a click. Unfortunately, some of them have fallen a victim of cybercrimes without even realizing it. The level of Cybercrimes and Cybercriminal attacks have increased significantly recently and this has necessitated the urgent need to raise awareness among the public.

According to Dass (2013), “Muscat: Cyber criminals are now using fake logos of the Royal Oman Police (ROP) and the International Criminal Police Organization (Interpol) to make money in the Sultanate”, this incident happened in Oman, and what these criminals have done is basically messing with the data, and asking for money in return for fixing it. A lot of cybercrime incidents are occurring in the Middle East region mainly because people lack the knowledge of how to handle such incidents. One cybercrime incident that took place in the UAE in RAK Bank, has resulted in the loss of millions of dollars. This huge financial loss alerted the UAE to the important need to combat cybercrimes

According to emirates247 website (2013) “35% of attacks targeted UAE’s banking sector, including ATM and Internet banking applications”. This indicates that most of the cybercrimes in the UAE are financial and require new procedures and rules to be reinforced in order to protect people’s personal belongings and stop cyber criminals from taking what others rightfully own before they sabotage other lives. Furthermore, 76% of UAE residents are victims of cybercrime, 2 out of 3 victims reported the cybercrime to police and 53% of users don’t have up to date security software. Furthermore, according to police reports; most cybercrime victims are young adults because they heavily use the internet for their day to day activities. (Emirates247 website, 2013)

Qatar is another country in the same region which could not avoid cybercrimes. According to Aguilar(2013), one of the reasons behind cybercrime attacks was that the average income of people in this country rank among the highest in the region. Thus, having a high income attracts criminals and makes it easy for cyber criminals to choose a victim.. In addition, the fact that cybercrimes are spreading worldwide shows that it is a serious matter, and should be taken seriously until finding some solution. These cybercrimes have triggered a feeling of insecurity among some people regarding saving money in banks and using credit card.

According to Ajbaili (2013) in a report recently published by Trend Micro Saudi Arabia and the United Arab Emirates rank as the most vulnerable of the Gulf countries to cybercrime attacks, Furthermore, what the criminals do is basically steal money from other companies by hacking into their system, and stealing important files and passwords which may end up in bankrupting these companies. This shows the importance of strict measures for dealing with cybercriminals and putting an end to cybercrimes.

2. Objectives

1. The aim of this study is to assess the level of knowledge about cybercrimes among a representative sample of young adult Emiratis.

Moreover, the goal of this study is to shed light on cybercrime and cybercriminal attacks so as to alert people to the importance of taking proper measures to ensure security and safety.

3. Methodology

3.1 Design

This study used a cross-sectional correlational design.

3.2 Measures

The participants that were targeted for this study were 130 students (113 females and 17 males) from two different universities namely Zayed University and Abu Dhabi university both in the capital city of the UAE. These two institutes were chosen in particular for the reason that they are highly recognized institutes in the UAE and their students are heavy users of technology.

All participants completed an online questionnaire that was adapted from the Cybercrime Knowledge Questionnaire; developed by Katz, 2005. The online version of the questionnaire was sent to all students through campus announcement. It was utilized to calculate the cybercrime awareness index (CAI) which reflected the level of knowledge about cybercrimes by university students.

4. Results

The results demonstrated that there is a correlation between usability and major, and also another correlation between students major and their level of knowledge regarding cybercrimes. Moreover, it showed that students in both universities are not aware enough about cybercrimes. Students majoring in IT had a significantly high level of knowledge about cybercrime (high CAI) as compared to students from other majors who had a lower knowledge (low CAI).

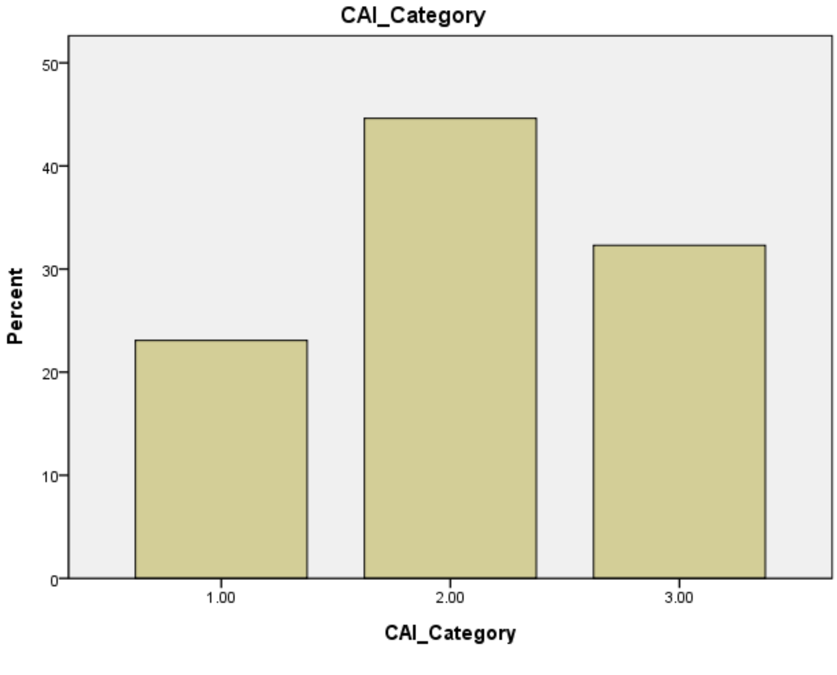

Figure1. Distribution of Participants according to Level of Knowledge about Cybercrime. The mean value for the Cybercrime awareness index (CAI) indicated a medium level of knowledge about cybercrimes by students. Students fall victim to cybercrime attacks due to their heavy use of the internet for their day to day activities.

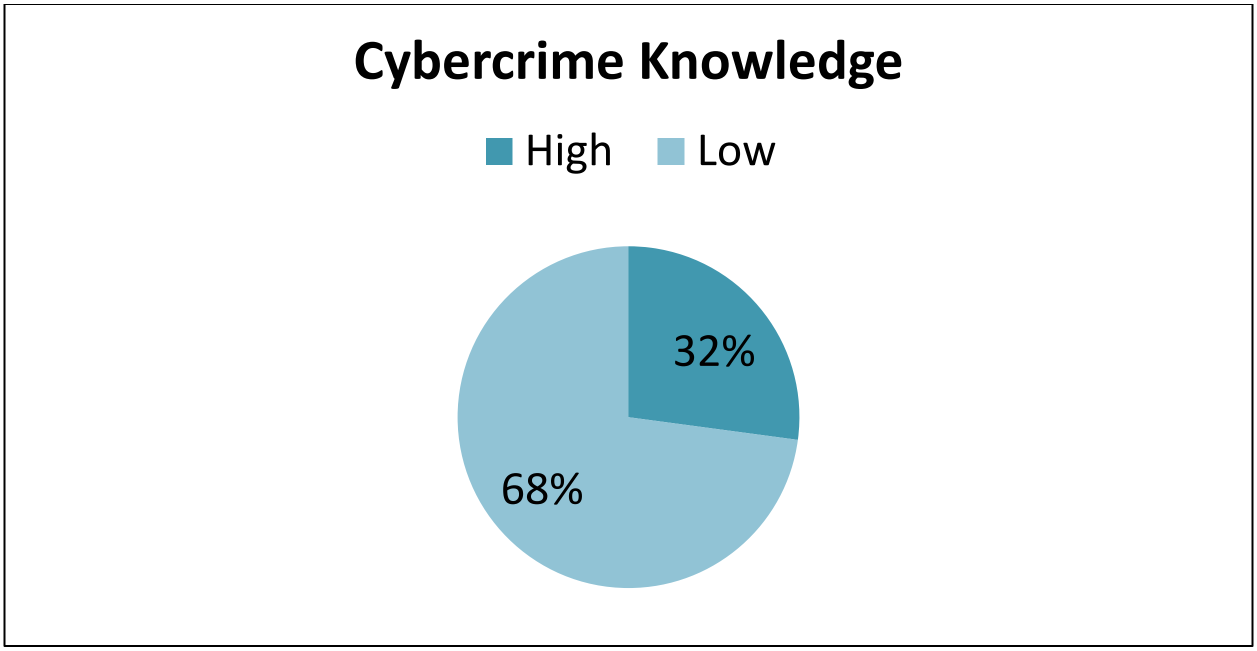

Figure2. Percentage of the overall level of Knowledge about Cybercrime. Only 32% of the overall participants had a high or adequate level of knowledge about cybercrime while the rest of the participants had low to medium levels of knowledge.

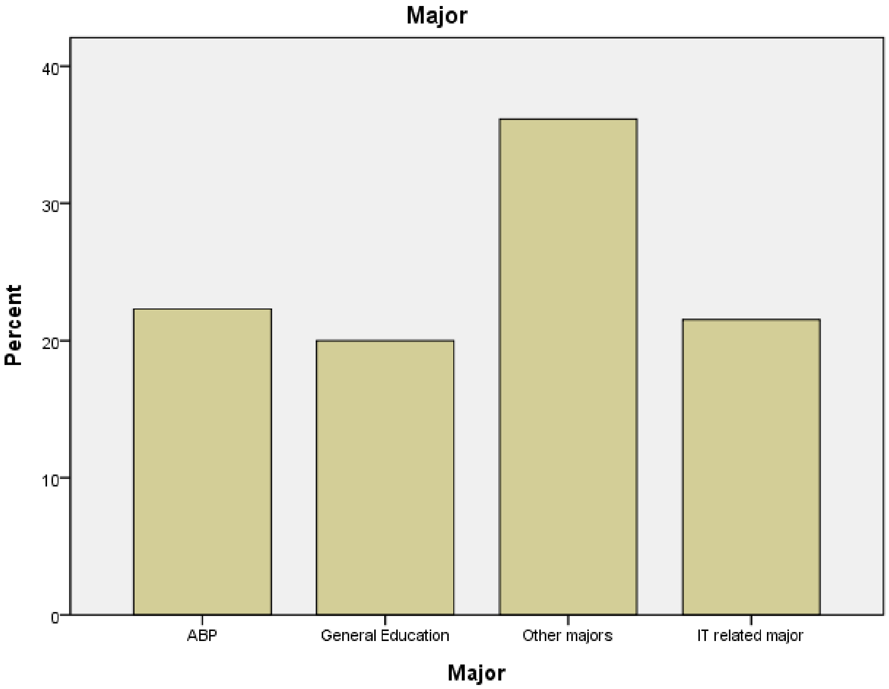

Figure 3. Distribution of Participants according to Major. According to the results there was a statistically significant difference in the level of knowledge in terms of student major but not gender. Students specializing in Computer Information Technology (accounting for 21.5% of the participants) had the highest levels of knowledge as compared to all other students from other majors.

Table (1): Correlation Analysis for Cybercrime awareness index (CAI) and other variables

		CAI	Gender	Major	Usability	University
CAI	Pearson Correlation	1	.020	.313**	.169	.197*
	Sig. (2-tailed)		.825	.000	.055	.025
	N	130	130	130	130	130
Gender	Pearson Correlation	.020	1	-.036	-.005	-.068
	Sig. (2-tailed)	.825		.683	.956	.440
	N	130	130	130	130	130
Major	Pearson Correlation	.313**	-.036	1	.248**	.068
	Sig. (2-tailed)	.000	.683		.004	.441
	N	130	130	130	130	130
Usability	Pearson Correlation	.169	-.005	.248**	1	.270**
	Sig. (2-tailed)	.055	.956	.004		.002
	N	130	130	130	130	130
University	Pearson Correlation	.197*	-.068	.068	.270**	1
	Sig. (2-tailed)	.025	.440	.441	.002	
	N	130	130	130	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Usability was positively correlated students major (r=.248), this relationship was significant (p < .05).Also, major was also positively correlated with CAI (r =.313) and this relationship was significant (p < .05).

5. Conclusion

In conclusion, the findings of this study showed that the level of knowledge about cybercrimes among university students is not adequate. These young adults should be more educated and more aware about the risks of technology use in terms of cybercrime attacks.

6. Future Work

Further research is needed to raise awareness about cybercrime in the United Arab Emirates. For instance; focusing on a larger samples and targeting more universities. Also, Future research could focus on developing strategies to raise awareness and alert students to the risks of being victims of cybercrimes.

New laws should be implemented regarding combating cybercrimes. The need for protection is highly recommended in the UAE, the current president of the UAE His Highness Shaikh Khalifa Bin Zayed Al Nahyan has issued new federal laws on combating cybercrimes, new laws regarding indecent acts, copyright issues, terrorist acts and state security. (Emirates247 website, 2013)

7. Acknowledgements

I would like to express my appreciation to my research advisor Dr. Fatme Al Anouti who supported me unremittingly by providing me with proper guidance and allowing me to pave my path in researching. Furthermore, I would like to thank the research office at Zayed University for providing its students with the Undergraduate Research Scholarship Program.

8. References

1. Aguilar, J. (2012). *Gulf Times*. Retrieved 6, 20, 2013, from Qatar 'an interesting target' for cyber criminals : http://www.gulf-times.com/qatar/178/details/356891/qatar--%E2%80%98an-interesting-target%E2%80%99-for-cyber-criminals-,-says-security-expert

2. Ajbaili, M. (2010). *Al Arabiya News*. Retrieved 7, 12, 2013, from Saudi & UAE at high risk to cyber-crime: report: Mustapha Ajbaili

3. Banking is the most targeted sector for cybercrime in UAE. (2013, January 13). Retrieved 8, 24, 2013, from emirates24/7: http://www.emirates247.com/news/emirates/banking-is-the-most-targeted-sector-for-cybercrime-in-uae-2013-01-14-1.490928

4. Das, R. (2013, June 03). *Cyber criminals using ROP logo to dupe people*. Retrieved August 22, 2013, from Times of Oman: http://www.timesofoman.com/News/Article-16881.aspx

6. Jaishankar & Halder. (2011). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.* Chicago: IGI Global.

7. Katz, I. (2005, February 5) Suit against bank of America to highlight cybercriminal
issues. *Knight Ridder Tribune Business News*, 1.