Journal of Social Sciences

Original Research Paper

Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia

[1]Md Shamimul Hasan, [2]Rashidah Abdul Rahman,
[3]Sharifah Farah Hilwani Binti Tengku Abdillah and [1]Normah Omar

[1]Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Malaysia
[2]Faculty of Economics and Administration, King Abdul Aziz University, Jeddah, Saudi Arabia
[3]Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam, Malaysia

Article history
Received: 20-05-2015
Revised: 23-09-2015
Accepted: 22-10-2015

Corresponding Author:
Md Shamimul Hasan
Accounting Research Institute,
Universiti Teknologi MARA, Shah Alam, Malaysia
Email: dr.mdshamimulhasan@rocketmail.com

Abstract: Cybercrime is a criminal (unethical and unlawful) activities using internet facilities such as virus infections, identity theft and hacking. There is high risk of becoming a victim especially for young internet user. The purpose of this study is to protect them by providing empirical evidence to the policy makers in combating cybercrime. The study examines the relationship between perception and gender, age and knowledge as well as the relationship between awareness and gender, age and knowledge towards cybercrime. A field survey is conducted among 342 students in the faculty of accountancy of Universiti Teknologi MARA (UiTM) with a structured questionnaire that covers demographic information and seven most known cybercrimes. Percentile analysis, correlation matrix, multivariate regressions are done to test the hypotheses. In addition, Post Hoc test is conducted to locate where the significant differences lies. The study finds: (1) Female students are more aware and have affirmative insights than male, (2) students in the age group of 18-23 years have lower perception and awareness than those aged 24 years and above and (3) those with higher academic qualifications are more aware at cybercrime and perceived the issue of risk differently. The study provides empirical evidence to the top management of the higher level institutions on the needs to improve their policies and procedures to protect young generation reducing the high risk of becoming a victim.

Keywords: Cybercrime, Internet Crime, Cyber Security, UiTM, Higher Academic Institutions, Internet Users, Malaysia

Introduction

The rapid changes in computer connectivity and innovation in digital technology provide numerous benefits to human life but it is not out of side affect such as cybercrime. Cybercrime is a new wave of crimes using internet facilities, which needs to be addressed urgently and earnestly by policy planners to protect the young generation as there is a high risk of becoming a victim of this crime (Asokhia, 2010; Mensch and Wilkie, 2011). Center for Strategic and International Studies (CSIS) reported that every year there is a financial loss of 445 billion dollar in world economy due to cybercrime (The Daily Amar Desh, 2014). Cyber Security Malaysia reported that the total number of cybercrimes was 1038 in 2007 and it increased to 2123 in 2008 (The Star, 200). Cybercrime statistics along with an increasing number of research studies indicate that young people do not always behave ethically in online activities and hence, there is a chance of every internet user becoming a victim (McQuade, 2009). Chen *et al*. (2008) state that human factors are involved in security awareness process. Human beings are usually the first line of defence to secure information assets, no matter how advanced and rigid the security technology solutions may be. All the security breaches such as virus infections, identity theft and hacking are the direct cause of carelessness and lack of knowledge and action on the part of users (Chen *et al*., 2008). A high level awareness about information security and cybercrime issues amongst users at home, in government and educational institutions, especially

young people, would decrease the occurrence of cybercrime (Sembok, 2003). The effectiveness of combating cybercrime among users' especially young users will work if they are familiar and adroit while using online. Therefore, human factors such as gender, age, knowledge and skills (experience) may assist in augmenting the levels of awareness among young people. Students' perceptions of risk and awareness on security of the internet and information should be profoundly addressed (Wang *et al*., 2008). Past studies have examined students' attitude towards computer skills and ethics among educators (Shariff and Deni, 2005; Aris *et al*., 2004; Sembok, 2003). The majority of earlier studies are focused on approaches of law and enforcement agency tools in combating cybercrime. However, only few studies are conducted to examine students' awareness and their perception of risk against cybercrime. Thus, this study is carried out with an aim of examining the actual level of awareness and the perception of students at the faculty of accounting, UiTM, Shah Alam, Malaysia about cybercrime rise. The purpose of this study is to investigate the awareness of the respondents about cybercrime and how they perceived the risk of such crime. The specific objectives are to examine (1) the level of awareness towards 'Cybercrime' in terms of gender, age and knowledge; (2) the level of perception towards 'Cybercrime' in terms of gender, age and knowledge and (3) the relationship between level of perception and level of awareness on cybercrime.

The following sections present review of literature and hypotheses development, conceptual model, method, test of hypotheses and findings and conclusion.

Review of Literature and Hypotheses Development

Colfer (2007; Li, 2006) state that there are dissimilar perceptions and awareness between men and women. According to Titi (2003) women are more aware of cyber regulations and have superior ethical values compared to men. Women are less likely to become victims as compared to men. Lifestyle Theory states that sex is an often-mentioned demographic characteristic that is associated with difference in lifestyle (Reyns, 2010; Ngo and Paternoster, 2011; Wolak *et al*., 2006; Choi, 2008).

Neiss *et al*. (2009) state that perception and awareness of young people are dissimilar between age groups. It is because young people and older people have different perspectives. Young people give more negative emotional perception than older adults. Lifestyle Theory suggests that individual of different ages participate in different kinds of lifestyle. These lifestyle differences, therefore, expose individuals of different ages to varying levels of risk of victimisation (Reyns, 2010; Ngo *et al*., 2011; Wolak *et al*., 2006; Choi, 2008). It has been persistently reported that younger people are more likely to be victimised than older people. The Australian Youth Affairs Coalition (AYAC, 2010) submitted a report on cyber safety to the office of Privacy Commissioner in which they state that the students in the age group of 18-24 are in high risk environments when expose to online activities.

Knowledge is very important for young people to prevent cybercrime (Curtis and Colwell, 2000; Wang *et al*., 2008). Chawki (2005) states that educating young people would help decrease the risk of students in cyberspace. Asokhia (2010) finds that the level of education contributes significant differences to the students' perceptions of cybercrime. Knowledge helps people to be more aware on cybercrime (Levin *et al*., 2008). The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies & regulations and sufficient protection of personal information (Choi, 2008; Levin *et al*., 2008; Chawki, 2005; Bougaardt and Kyobe, 2011). Choi (2008) emphasises on the effectiveness of university programs in promoting knowledge and values about cybercrime as these programs could improve future behaviour of students' towards cybercrime in terms of safety and security. This would establish norms and adjust prospects for illegal or delinquent behaviours. Based on the review of above literatures it is anticipated that gender, age and knowledge have significant influences on cybercrime. The following six hypotheses are developed based on the above assumption and in line with the objectives of this study. Hasan *et al*. (2015) present a table providing the definition and measurement of the variables and the range of their values. Likewise, the definition and measurement of the variables and the range of their values for this study are presented in Table 7 (Appendix-1).

H_1 = There is an association between perception of cybercrime and gender
H_2 = There is an association between awareness of cybercrime and gender
H_3 = There is an association between perception of cybercrime and age group
H_4 = There is an association between awareness of cybercrime and age group
H_5 = There is an association between perception of cybercrime and knowledge level
H_6 = There is an association between awareness of cybercrime and knowledge level

■■■

Conceptual Framework

A diagram is designed to form a graphical view of the diagnostic pattern of the problem under study. The diagram shows that six hypotheses are tested such as hypothesis 1 test the relationship between gender and perception on cybercrime, hypothesis 2 tests the influence of gender on awareness, hypothesis 3 tests the impact of age on perception, hypothesis 4 tests the link between age and awareness on cybercrime, hypothesis 5 tests the association between knowledge and perception and hypothesis 6 tests the bonding between knowledge and awareness on cybercrime. Finally, we examine the correlations between the level of awareness and the level of perception. The conceptual framework of this study can be viewed in Fig. 1.

Research Approach

Primary data is used to examine the influence of age, gender and knowledge on both awareness and perception in this study. A field survey is conducted in the faculty of accountancy of Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia. For this, a structured questionnaire is developed and distributed randomly among 342 students who are pursuing diploma, under-graduate and post-graduate programmes. They completed the questionnaires and returned it back to us in time. In the questionnaire we covered demographic information and seven most known crimes such as (1) unauthorised access to computer material, (2) unauthorised access to internet to commit further offences, (3) unauthorised modification of the contents of any computers, (4) wrong communication, (5) people involved in abetments and attempts would be punished, (6) cyber terrorism and (7) cyber nuisance.

Frequency and percentile analysis are done to examine the level (very low, low, moderates, high and very high) of perceptions about above-mentioned most known crimes. Multicollinearity analysis is done to examine the multicolllinearity among age, gender, knowledge of threats and knowledge of offences. Multivariate analyses are done to examine the level of perception and level of awareness of age, gender and knowledge. A further analysis is done digging of age level, education level and knowledge level in order to have a concrete outcome of the study. We use Post Hoc Games-Howell (multiple comparison test) technique to examine the relationship between perception and age, level of education and knowledge of offences. In case of awareness, we use Post Hoc Least Significant Difference (LSD) test technique to realize the relationship between awareness and age, level of education and knowledge of offences. Finally, we check the correlation between level of perception and level of awareness of cybercrime.

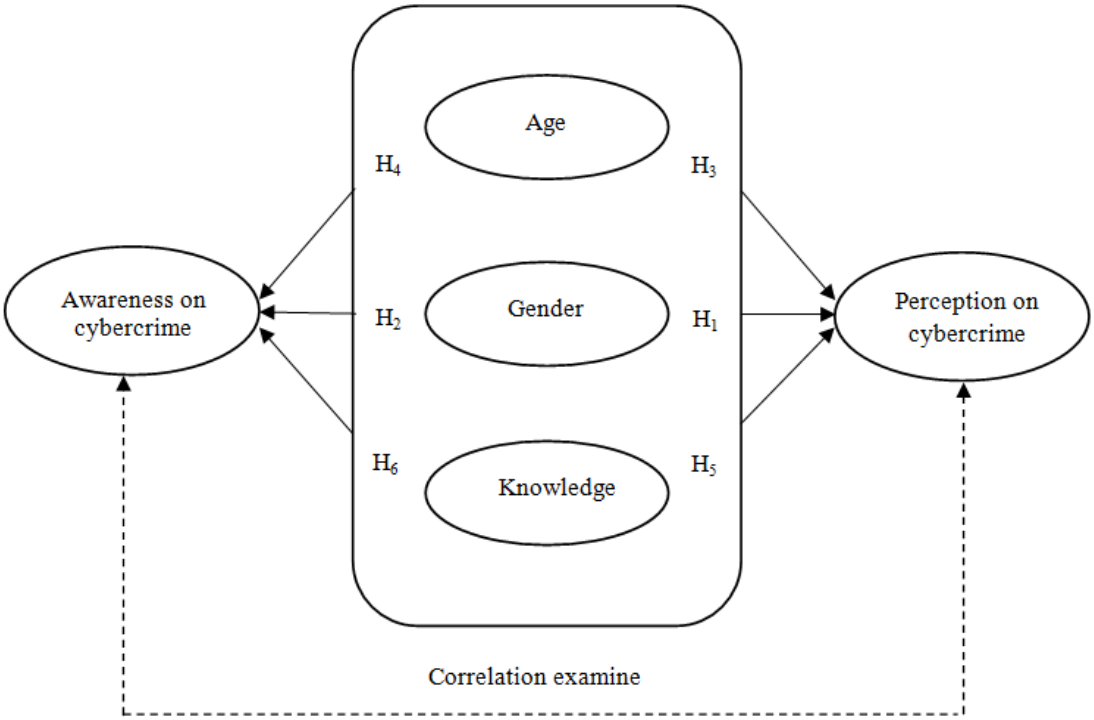

Fig. 1. Conceptual framework

■■■

Results and Discussion

If we look at the percentile analysis of demographic data we find that 63.2% of the respondents are female and 36.8% are male. 25.4% (majority) of the respondent are in the age group of 22-23; 42.73% (majority) of the respondents are undergraduates; 31.6% (majority) of the respondents have 3-5 years' experiences; 31.3% (majority) of the respondents' use internet for 2-4 h; 46.8% (majority) of the respondents have internet access through broadband; 41.8% (majority) have knowledge of the most dreadful known virus threats; 32.2% (majority) of the respondents have knowledge of worst known threats hackers and only 26% (majority) have knowledge of fraud.

If we look at the percentile analysis on respondents' knowledge about seven common crimes, Table 1 shows that respondents have different levels of knowledge of unauthorised access to computer material that is, 37.4% moderate, 28.4% high, 17.8% low, 8.5% very high and 7.9% very low knowledge respectively. Thus it could be deduced that the majority of the respondents have moderate knowledge. In case of unauthorised access with intent to commit further offenses, the result shows that the majority of the respondents have moderate knowledge at 36.8%. While 39.5% of the respondents have moderate knowledge of unauthorised modification of the contents of any computers, 36.5% have moderate knowledge of wrong communication, 39.5% have moderate knowledge of people involved in abetments and attempts and 29.5 have low knowledge of cyber terrorism. In case of cyber nuisance, 32.7% respondents have high level of knowledge of cyber nuisance. It can be concluded that the majority of the respondents have moderate knowledge of five most known offences, low knowledge of cyber terrorism and high level knowledge of cyber nuisance.

We use Pearson's pair wise product moment correlation coefficient (r) to examine the multicollinearity between variables such as age, gender, knowledge of threats and knowledge of offences. A correlation matrix table is produced for all the variables using SPSS and the results are presented in Table 2.

If we look at Table 2, we see that the highest level of correlation existed between knowledge of offences and knowledge of threats (0.167). Some authors (Judge *et al*., 1985; Bryman and Cramer, 1997) suggest that simple correlation between variables should not be considered harmful until and unless it exceed 0.80 or 0.90. Thus we find no multicollinearity between variables. As such, there is no problem with these variables in the interpretation of the results of multivariate analysis.

Next, we use multivariate analysis technique (Z-test and F-test) to have overall outcome of accepting or rejecting the hypotheses. We use z-test for gender and f-test for age and knowledge. We analyse the results from both aspects such as level of perception and level of awareness for gender, age and knowledge. The results of multivariate analysis for gender are shown below.

Table 1. Perceptions of respondents

Cases	f & %	Very low	Low	Moderate	High	Very high	Total
Unathorised access to computer material	f	27.0	61.0	128.0	97.0	29.0	342
	%	7.9	17.8	37.4	28.4	8.5	100
Unathorise access to intent to commit further offences	f	34.0	85.0	126.0	79.0	18.0	342
	%	9.9	24.9	36.8	23.1	5.3	100
Unathorised modification of the contents of any computers	f	38.0	79.0	135.0	66.0	24.0	342
	%	11.1	23.1	39.5	19.3	7.0	100
Wrong communication	f	36.0	94.0	125.0	64.0	23.0	342
	%	10.5	27.5	36.5	18.7	6.8	100
People involved in abetments and attempts would be punished	f	27.0	101.0	135.0	48.0	31.0	342
	%	7.9	29.5	39.5	14.0	9.1	100
Cyber terrorism	f	34.0	101.0	95.0	87.0	25.0	342
	%	9.9	29.5	27.8	25.4	7.4	100
Cyber nuisance	f	24.0	67.0	87.0	112.0	52.0	342
	%	7.0	19.6	25.4	32.7	15.3	100

Table 2. Correlation matrix

	Age	Gender	Knowledge of threats	Knowledge of offences
Age	1.000	-0.134	0.010	0.054
Gender	-0.134	1.000		
Knowledge of Threats	0.010	-0.188	1.000	0.167
Knowledge of Offences	0.054	-0.128	0.167	1.000

If we look at Table 3, we find p-values of both level of perception and level of awareness show that there are significant differences between male and female regarding the level of perception as well as the level of awareness of cybercrime at 5% level of significance. It indicates that the male and female of accounting students in UiTM have different level of perception and awareness of cybercrime. These findings support hypothesis 1 and hypothesis 2. Therefore, H_1 and H_2 are accepted. The results of multivariate analysis for age are shown below.

Table 4 reveals that the p-values of both level i.e., level of perception and level of awareness are significant differences among students in different age groups relating to their perception and awareness of cybercrime at 1% level of significance. It indicates that there are significant difference between young people's perception and their age as well as between awareness of cybercrime and their age. Therefore, H_3 and H_4 are accepted. The results of multivariate analysis for knowledge are shown below.

If we look at Table 5, the p-values show that the level of education and knowledge of offences contributed significantly to the differences of the students' perception of cybercrime. Similarly, the level of education and knowledge of offences contributed significantly to the differences of the students' awareness of cybercrime. Having good knowledge can help people be more aware of cybercrime (Levin *et al*., 2008). People who have knowledge will have different perception and awareness on cybercrime and would affect their reaction Perl, 2009; Bougaardt and Kyobe, 2011; Choi, 2008; Chawki, 2005; Levin *et al*., 2008). There is significant dissimilarity between young people's perception and awareness of cybercrime and their knowledge. Therefore, H_5 and H_6 are accepted.

At this stage of analysis, we only know that all of our hypotheses are accepted. Therefore, we could say that there are significant relationships between perception and age, gender and knowledge. Similarly, there are significant relationship between awareness and age, gender and knowledge. But this is not enough for us to identify the influence of different age groups, knowledge of offences and level of education on perception as well as awareness. So, we need to carry out further analysis to portray a conclusive scenario of this study. Games-Howell post hoc multiple comparison test is carried out to examine the relationship between perception and different age groups, knowledge of offences and level of education. Least Significant Difference (LSD) post hoc multiple comparison test is carried out to examine the relationship between awareness and different age groups, knowledge of offences and level of education.

Figure 2 it portrays the summarised result of Games-Howell post hoc multiple comparison test between age groups and perception of cybercrime. There are significant differences between age groups towards perception of cybercrime. Figure 2 reveals that the perception of different age groups are statistically varied between students in the age group of 18-19 years (M = 3.73) and those of 22-23 years (M = 4.05) and 24-25 years (M = 4.07). Students in the age group of 22-23 years and 24-25 years reported significantly higher perception on cybercrime compared to students of 18-19 years. There are no significant differences between other groups.

Table 3. Level of awareness and perception-gender

Level	Gender	N	Mean	SD	Mean difference	z-value	p-value	Remarks
Level of perception	Male	126	3.87	0.436	-0.118	-2.362	0.019	Significant
	Female	216	3.98	0.452				
	Male	126	3.22	0.723	-0.187	-2.583	0.010	Significant
Level of awarness	Female	216	3.40	0.597				

Table 4. Level of awareness and perception-age

Level	Variables	F	p-value	Remarks
Level of perception	Age	6.880	0.000	Significant
Level of awarness	Age	4.508	0.001	Significant

Table 5. Level of awareness and perception-knowledge

Level	Variables	F	p-value	Remarks
Level of perceptions	Knowledge of Offences	14.153	0.000	Significant
	Level of Education	9.140	0.000	Significant
Level of awarness	Knowledge of Offences	24.113	0.000	Significant
	Level of Education	6.426	0.002	Significant

■■■

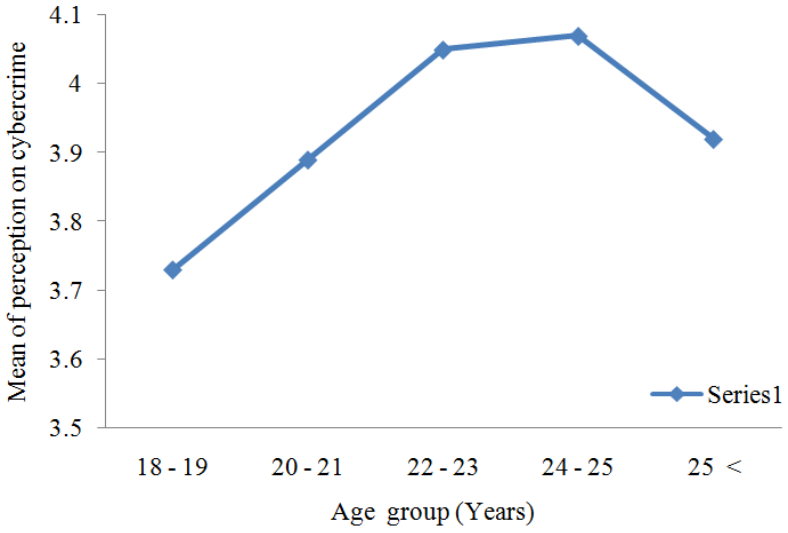

Fig. 2. Relationship between perception and age

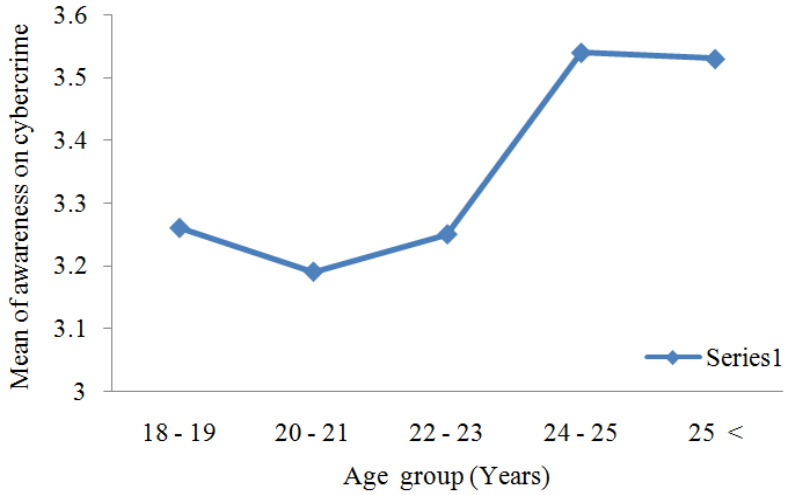

Fig. 3. Relationship between awareness and age

Figure 3 portrays the summarised result of Least Significant Difference (LSD) post hoc multiple comparison test between age and awareness of cybercrime. There are significant differences between different age groups regarding awareness of cybercrime. Figure 3 reveals that the awareness of different age groups are statistically varied between students of 18-19 years (M = 3.26) and those of 24-25 years (M = 3.54) and more than 25 years (M = 3.53). Other age groups of 20-21 years (M = 3.19) and 22-23 years (M = 3.25) also reveals significant differences with those of 24-25 years and more than 25 years. The result reports that students in the age group 24-25 years and more than 25 years have significant higher awareness of cybercrime compared to those of 18-23 years. There are no significant differences between other groups.

The summarised result of Games-Howell Post Hoc multiple comparison test between knowledge of offences and perception of cybercrime are shown in the following Fig. 4. The results demonstrate significant difference between perception of cybercrime and knowledge of offences. The perception of different knowledge groups are statistically varied between students' with very low knowledge of offences (M = 4.11) and those who have moderate knowledge (M = 3.81) and very high knowledge (M = 4.74). Students' with moderate and very high knowledge of offences have significant differences in perception of cybercrime. The results indicate that students who have high knowledge about offences would have high/positive perceptions of cybercrime.

■■■

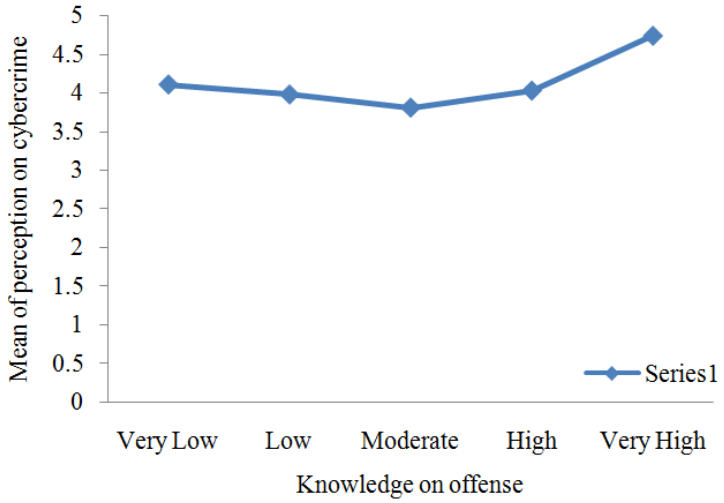

Fig. 4. Relationship between perception and knowledge of offences

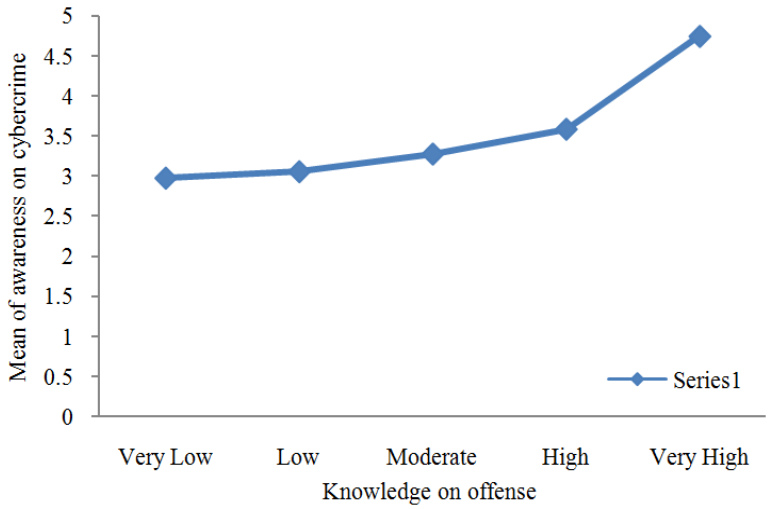

Fig. 5. Relationship between awareness and offences

The summarised results of Least Significant Difference (LSD) post hoc multiple comparison test between knowledge of offences and awareness of cybercrime are shown in Fig. 5. It is observed that all levels of knowledge about offences i.e., very low (M = 4.11), low (M = 3.98), moderate (M = 3.81), high (M = 4.03) and very high (M = 4.74) have significant differences between groups. Students who have very high knowledge about offences have greater awareness of cybercrime than other groups.

The summarised results of Games-Howell post hoc multiple comparison test between levels of education and perception of cybercrime are shown in the following Fig. 6. The perception of different levels of education were statistically dissimilar between diploma students (M = 3.77) and those in undergraduate (M = 4.01) and postgraduate levels (M = 3.99). The results state that undergraduate and postgraduate students have higher significant perception compared to other level of education Thus students with higher level of education have higher perception of cybercrime than those with lower level of education. However, there are no significant differences in other groups.

The summarised results of LSD post hoc multiple comparison test between levels of education and awareness of cybercrime are shown in the following Fig. 7. It is observed that diploma students (M = 3.77) have significant difference with postgraduate students (M = 3.99) and undergraduate students (M = 4.01). Thus postgraduate students have high significant difference in awareness of cybercrime compared to others group. The results suggest that students with higher level of education have better awareness of cybercrime than those at lower levels. However, there are no significant difference in other groups.

■■■

At this stage of analyses we know the specific relationship between perception and age, gender, knowledge and level of education. We also know the relationship between awareness and age, gender, knowledge and level of education. But at this moment we do not know the relationship between awareness and perception of cybercrime. We believe that there is a positive relationship between awareness and perception of cybercrime. Therefore, we examine the Pearson correlation between them. If we look at the following Table 6, it shows that there is a positive correlation between respondents' perception level and awareness level of cybercrime at 1% level of significance. This suggests, the higher the level of awareness, the higher the level of perception.

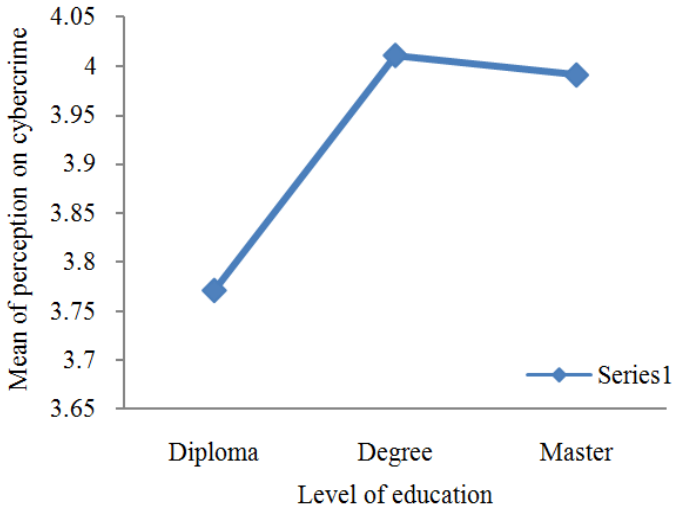

Fig. 6. Relationship between perception and level of education

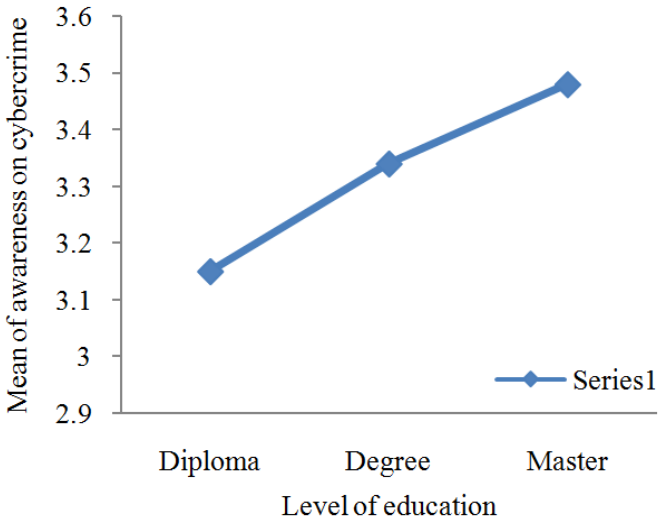

Fig. 7. Relationship between awareness and level of education

Table 6. Correlation between level of perception and level of awareness of cybercrime

		Perception on cybercrime	Awareness on cybercrime
Perception on cybercrime	Pearson correlation	1	0.281**
	Sig. (2-tailed)		0.000
	N	342	342
Awareness on cybercrime	Pearson correlation	0.281**	1
	Sig. (2-tailed)	0.000	
	N	342	342

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

■■■

Conclusion

This study concludes that gender, age and knowledge have significant influences on the level of perception and awareness of cybercrime. We test three hypotheses on the relationships between perception and age, gender and knowledge. We also test other three hypotheses on the relationship between awareness and age, gender and knowledge. All six hypotheses are supported by this study. We find female students are more aware than male students about cybercrime. For age group, we find students in the age group of 23-25 years have significantly higher perception of cybercrime than those of 18-19 years and the age group of 24-25 and more than 25 years have significantly higher awareness of cybercrime compared to those of 18-23 years. This suggests students with greater awareness and perceptions of cybercrime are more cautious about the same. For knowledge of offences and level of education, we find students with knowledge of cyber offences and high level of education have high perceptions and awareness of cybercrime. More revealing fact is that perception and awareness are positively correlated at 1% level of significance. The findings indicate that the level of awareness and the level of perception of the respondents regarding cybercrime are equal. The study suggests students having higher knowledge of cybercrime also have better awareness of the cybercrime. Curtis and Colwell (2000; Atkinson *et al*., 2009) mentioned that unambiguous knowledge of cybercrime would help young people in preventing and avoiding this delinquency. By education, students can develop positive attitudes towards cyberspace (Wang *et al*., 2008). Thus the result of this study is to some extent similar to the findings of previous studies.

This study recommends necessary policy measures to be taken by the higher learning institutions including UiTM to prevent alarming cybercrime as well as cyber war. Educating young people with some knowledge on cybercrime would help increase their level of awareness and also perceptions on cybercrime. Further investigation and experimentation into cybercrime is strongly recommended. Conceivably the growth of cybercrime in Malaysia, as all over the world is on the rise and to curb its scope and complexity is the pertinent need today. Hence factors that strongly influence level of perceptions and awareness on cybercrime among students in Malaysia higher institutions could be more relevant and feasible to be explored for the benefit of all.

Acknowledgement

The researchers gratefully acknowledge the financial support and generosity of Accounting Research Institute (ARI) and the Ministry of Education, Government of Malaysia without which the present study could not have been completed.

Author's Contributions

The contribution of all authors is treated equally and there is no conflict of interest among them.

Ethics

This is an original research work. Ethical issues are not involved here.

References

Aris, A., R. Zainuddin, R. Kamarudin and Z.M. Daud, 2004. The Impact of students' background and attitudes on their computer skills: A case study on three selected secondary schools in Segamat, Johor. Proceeding of the Seminar Hasil Penyelidikan Peringkat Kebangsaan, (PPK' 04), pp: 249-261.

Asokhia, M., 2010. Enhancing national development and growth through combating cybercrime internetfraud: A comparative approach. J. Soc. Sci., 23: 13-19.

Atkinson, S., S. Furnell and A. Phippen, 2009. Securing the next generation: enhancing e-safety awareness among young people. Comput. Fraud Security, 7: 13-19. DOI: 10.1016/S1361-3723(09)70088-0

Bougaardt, G. and M. Kyobe, 2011. Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. Electr. J. Inform. Syst. Evaluat., 14: 167-178.

Bryman, A.E. and D. Cramer, 1997. Quantitative Data analysis with SPSS for Windows: A Guide for Social Scientists. 1st Edn., Routledge, New York and London, ISBN-10: 0415147190, pp: 336.

Chawki, M., 2005. A critical look at the regulation of cybercrime. ICFAI J. Cyberlaw, 3: 1-55.

Chen, C.C., B.D. Medlin and R.S. Shaw, 2008. A cross-cultural investigation of situational information security awareness programs. Inform. Manage. Comput. Security, 16: 360-376. DOI: 10.1108/09685220810908787

Choi, K., 2008. Structural equation modeling assesment of key causal factors in computer crime victimization. Ph.D Dissertation, Indiana University of Pennsylvania, USA.

Colfer, E., 2007. Online privacy and people's awarness: A study of Irish students. MSc Thesis, School of Science, Worldford Institute of Technology, Ireland.

Curtis, P.A. and L. Colwell, 2000. Cybercrime: The next challenge: An overview of the challenges faced by law enforcement while investigating computer crimes in the year 2000 and beyond. School of Law.

Hasan, M.S., N. Omar and Z.S. Hossain, 2015. Corporate attributes and market capitalization: Evidence from Bangladesh. AESTIMATIO IEB Int. J. Finance, 11: 92-105. DOI: 10.5605/IEB.11.4

▪▪▪

Judge, G., W.E. Griffiths, R.C. Hill, H. Lutkepohl and T.C. Lee, 1985. The Theory and Practice of Econometrics. 2nd Edn., John Wiley, New York, ISBN-10: 047189530X, pp: 1090.

Levin, A., M. Foster, B. West, M.J. Nicholson and T. Hermandez *et al*., 2008. The next digital divide: Online social network privacy. Privacy and Cybercrime Institute, Ryerson University, Canada.

Li, X., 2006. The criminal phenomenon on the internet: Hallmarks of criminals and victims revisited through typical cases prosecuted. Univcersity Ottawa Technol. J., 5: 125-140.

Mensch, S. and L. Wilkie, 2011. Information security activities of college students: An exploratory study. Acad. Inform. Manage. Sci. J., 14: 91-116.

Neiss, M., L. Leigland, N. Carlson and J. Janowsky, 2009. Age differences in perception and awareness of emotion. J. Neurobiol Aging, 30: 1305-1313. DOI: 10.1016/j.neurobiolaging.2007.11.007

Ngo, F.T. and R. Paternoster, 2011. Cybercrime victimization: An examination of individual and situational level factors. Int. J. Cyber Criminol., 5: 773-793.

Perl, R., 2009. Reflections on emerging cyber threats and international co-operative responses. Proceedings of the 12th Annual NYS Cyber Security Conference, (CSC' 09), Empire State Plaza, Albany, USA.

Reyns, B., 2010. Being pursued online: Extent and nature of cyberstalking victimization from a lifestyle/routine activities perspective. PhD Dissertation, University of Cincinnati, Ohio, USA.

Sembok, T.M., 2003. Ethics of information technology. Proceedings of the Regional Meeting on Ethics of Science and Technology, RUSHAP, UNESCO, Nov. 5-7, Bangkok.

Shariff, S. and S. Deni, 2005. An exploratory study of level of awareness and perception towards computer ethics among it educators of institutes of higher learning in Lembah Klang. Technical Report, Universiti Teknologi MARA, Malaysia.

The Daily Amar Desh, 19th June 2014, Bangladesh

The Star, 1st January 2009, Malaysia.

Titi, K.M., 2003. Code of ethics, professionalism and responsibilities. Al-Ahliyyah Amman University, Ardhah, Jordan.

Wang, H.S., C.H. Chou and S.N. Tsai, 2008. A preliminary study of the education of internet security implied in a movie based English class in Taiwan's private vocational continuation high school. CNTE2008, Chichu, Taiwan.

Wolak, J., K. Mitchell and D. Finkelhor, 2006. Online victimization of youth: Five years later. Report # 07-06-025, National Center for Missing and Exploited Children Bulletin, Alexandria, VA.

Appendix -1

Table 7. The definition, measurement and range of values of variables

Variables	Definition	Measurement	Range of Values
Gender (Sex)	Gender is defined as 'male and female category of respondents'.	This is a binary variable. This variable is measured as 0 for male and 1 for female	0,1
Age Group (Years)	Age is defined as 'how old the respondents are'. Young people and older people give a different perspective.	This is a continuous variable. The value of this variable is measured within a specific range which is as under: 18-19, 20-21, 22-23, 24-25 and above	18-25 and above
Knowledge Level	Knowledge of threats is defined as 'the knowledge of respondents on virus, hacker and fraud'.	This is a nominal variable. This variable is measured on the basis of following threats: 1.Virus, 2. Hacker, 3. Fraud and 4. Others	1, 2, 3 and 4
	Knowledge of Offenses is defined as 'the knowledge of respondents on seven selected offenses in this study'.	This is an ordinal variable. Seven statements relating to offense are surveyed among respondents through a structured questionnaire. In each statement, a five point rating scale is used to measure their knowledge of offense.	1-5
	Level of Education is defined as 'the academic degree of respondents'.	This is a nominal variable. This variable is measured by clustring the respondents on the basis of their academic degree which is as follows: 1. Diploma, 2. Degree and 3, Masters	1, 2 and 3
Perceptions on Cybercrime	Perceptions is defined as 'the way in which the respondents mind chose which stimulation to accept and reject based on their experiences and how they make sense of cybercrime'.	This is an ordinal variable. Ten statements are surveyed among respondents regarding their perceptions on cybercrime. In each statement, a five point rating scale is used to measure the percepion of the respondents about the statement.	1 - 5
Awareness on Cybercrime	Awareness is defined as 'the consciousness of the respondents about cybercrime. In this level of consciousness, sense data can be confirmed by the respondents without necessarily implying understanding.	This is an ordinal variable. Respodents opinion on the awareness of cybercrime are measured by surveying nine statements through a structured questionnaire. A five point rating scale is used to measure their opinion on awareness on cybercrime.	1 - 5

■■■