Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2020. Vol. 14(1): 174–184. DOI: 10.5281/zenodo.3748685
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Factors Associating with Social Media related Crime Victimization: Evidence from the Undergraduates at a Public University in Sri Lanka

Suresh Nalaka[1] **& Hemantha Diunugala**[2]
University of Sri Jayewardenepura, Sri Lanka

Abstract

In this paper the point of view of factors associating with social media related crimes victimization of youth are investigated with regards to University of Sri Jayewardenepura, Sri Lanka; university community due to its large numeral of youth population. In this study, stratified sampling technique has been applied on 420 (Four hundred and twenty) undergraduate sample populations through dictating faculties. A web based and paper-based questionnaire has been used to collect data. In order to reach the aim statistics techniques, such as descriptive analysis, binomial test, index construction, chi-square test and logistic regression are worked out. Consequently, relationship with family, income level, digital literacy, awareness, security management, privacy concentration, number of Facebook friends, hours spending on online, purpose of online surfing variables are found to significantly impact on social media related crime victimization of youth and 0.738, 1.814, 0.554, 0.591, 0.402, 0.511, 1.001, 1.147, and 0.029 odd ratios identified the influence characteristics.

Keywords: Social Media, Crime, Victimization, Youth.

Introduction

The 21st century is signified by the information era. Due to the progress of information technology, Internet accessibility has been increasing. Currently, over 3 billion people use the Internet; an increase of 923.9 percent from 2000 to 2016 (InternetWorldStats.com, 2017). Internet has been popular so as to fulfill the day today activities in individually and mutually. Today, it has being more popular in the fields of communication, education, entertainment, economic and commercial activities. Internet has created a global village where no physical or social boundaries deprive people from living in it.

Currently, social media have been rapidly adopted by many across the globe, mostly teenagers taking the lead. Further, Gartner (2012) describes social media as set of

[1] Lecturer (Probationary), Department of Social Statistics, University of Sri Jayewardenepura, Sri Lanka. Email: gpsnalaka@sjp.ac.lk

[2] PhD Candidate, School of Management and Economics, Beijing Institute of Technology, 5 Zhongguancun St, Haidian District, China, 100811. Emails: 3820182090@bit.edu.cn / hemantha@sjp.ac.lk

technologies and channels targeted at forming and enabling a potentially massive community of participants to productively collaborate. It is estimated that as of the fourth quarter of 2016, Facebook had 1.86 billion monthly active users. On the other hand, there are also concerns that social media increases the likelihood of new risks to the self, centering on loss of security, privacy, harassment, harmful contacts and much more. Computer criminals often search suitable targets in certain social media where online users are populated. Previous studies show that, with addiction of social media, people become more and more individualized and alienated as they tend to have lots of on-line and virtual friends. Further, identity theft and hacking into social media profiles could also challenge an individual's privacy.

According to the APCERT Annual Report (2015, pp. 188-189), incidents reported to SLCERT have increased to 2, 967 in the year 2015. In 2014, 2,368 incidents were reported. This represents a 25% increase in reported incidents compared to the year 2014. As the distribution of various types of incidents reported to SLCERT during 2015, over 90% of the incidents were related to social media. It was observed that the number of reported cases related to social media have also increased considerably in the last year. According to the HCIU, they are receiving 10-12 cybercrime complaints, which amount to over 400 cases per month and 70% of its related to the youth. It is obvious that youth are more victims of cybercrimes in Sri Lanka. As stated by Weeramantry (1998):

> the power of science and technology has grown largely out of social control, out of control of legal systems, out of control of human rights. This is one of major problems confronting all legal systems, domestic and international, at the present time. Currently, Sri Lanka faces a challenge in preventing cybercrimes. The growth of network-based crimes has raised difficult issue in respect of appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks (Jayasekara & Rupasinghe, 2015, p. 760).

Since the youth in every society is of great importance and concern to that society because they are looked upon as the leaders of tomorrow. They involve with internet related activities more closely than others. They use internet in order for maintaining relationships, entertaining, and searching new things under the circumstances. Especially, at present, the social media had taken a part of their day today's life. Usually, they are spending more time with these social media. Even though, the youth have concentrated it as a fascinating place, risky situations are happening beyond it. Therefore, this place had being force for several causes such as collapsed the relationships, meetings, harassments, corruptions etc.

In all over the world, scholars highly concern about the nature of cybercrime. In the field of criminology, also the traditional theories were applied to identify the elements of this new phenomenon. Basically, theories of routine activity and life exposure were applied in previous studies. In addition to the theoretical perspective it has being performed scholars in terms of using statistical techniques such as Logistic Regression, Structural Educational Modeling etc. In past studies, scholars discussed some determinants of cybercrime victimization such as online lifestyle, various socio-economic attributes and various individual and situation factors but not much focus uniquely on social media related crimes, especially in Sri Lankan context.

The youth in various socio-economic levels have victimized and they have various behaviors. It is important to study whether the individual characteristics and behaviors of them have effect on these crimes. To defend against a threat, one must understand its critical elements. Therefore, the main objective of this study is to identify the factors affecting the cybercrime victimization of youth. In order to achieve the main objective, the specific objectives can be defined as, to measure the level of victimization of the youth, to measure the technological skills and awareness about online security of the youth, to identify the socio-economic background of the and online lifestyles of youth, to identify the association between victimization and potential risk factors.

Literature Review

Social media is a label for digital technologies that allow people to connect, interact, produce and share content (Lewis, 2010, p. 2). Social media related crimes cover a wide range of crimes that are committed using networked computers. Some of these crimes lead to financial gains, such as Internet fraud or scams offering bogus goods or services for money, and identity theft like theft of debit/credit card. Other types of Cybercrimes do not lead to profits such as Cyberstalking, cyber harassment, viruses, and child pornography (Alshalan, 2006, p. 23). In addition, the younger generations are believed to be more likely to view a computer as a necessity of life than older generations are (Carter, 1995, p. 21).

Routine activity theory, as proposed by Cohen and Felson (1979, pp. 588-608), suggests that crime is likely to occur when three factors converge. These factors are: motivated offenders, suitable targets, and the absence of capable guardians against violation. Cohen and Felson (1979) argue that these three factors are to be present in order for crime to occur, and the absence of one of these factors is “sufficient to prevent the successful completion of a direct-contact predatory crime” Routine activity theory assumes that motivated offenders are a given. The second tenet of the theory is “suitable target” that refers to a person or an item that may influence the criminal propensity to commit crime. It is referred to the offender’s perception of the value of target to likely offender, the inertia of the target to likely offender, the visibility of the target to likely offender, and the access to easily exit from the offense location. The third tenet of routine activities theory is an “absence of capable guardianship”. According to the theory, guardianship can be defined in three categories: formal social control, informal social control, and target-hardening. The theory pays more attention to the convergence in time and space of the other two factors that is suitable targets and the absence of capable guardians, and argues that such convergence could lead to a large increase in crime rates without any change in the “situational condition” that motivates offenders. As Mustaine and Tewksbury (1998, p. 90) claim, “the strength of routine activity theory is based on the idea that crime does not randomly occur in a society, but rather it follows regular patterns regarding situation and behavior, and it examines how these interact with individual characteristics and behaviors.”

In 1978, Hindelang et al. (1978, p. 241) developed the lifestyle exposure model which focuses on the victims’ daily social interactions. Lifestyle exposure theory holds that criminal victimization results from the daily living patterns of the victims. They defined lifestyle as “routine daily activities” including “vocational activities (work, school, keeping house, etc.) and leisure activities” Also, they posited that the lifestyles of individuals are determined by “differences in role expectations, structural constraints, and individual and sub cultural adaptations.” Several studies have applied routine activity theory to account for online victimization and these studies have all employed samples of students and overall, they provide support for the utility of routine activity theory in understanding the risks of victimization in cyber space.

A research by Kennedy and Forde (1999) found that personal variables associated with the lifestyle, such as age, sex, marital status, and race significantly influence the level of criminal victimization risk. Alshalan (2006) performed a logistic regression analysis based on data collected via telephone interviews with a sample of U.S. adults living in households with Internet access. He found that males and whites are more likely to be victims of cybercrime. Notably, his studies show that young females are more often victims of sexual solicitation and harassment than males. Studies of Higgins et al. (2008) though focused on identity theft rather than cyber-theft, found that the proportion of males was negatively associated with identity theft victimization. However, studies of Ngo and Paternoster (2011) reveal that age and race were significantly related to cybercrime victimization, while, sex and marital status had no effects on the likelihood of becoming a victim in cyberspace. Using a sample of college students, they applied the lifestyle/routine activities framework to assess the effects of individual factors on seven types of cybercrime victimization.

Oksanen and Keipi (2013) performed a multinomial regression analysis to predict cybercrime victimization and their findings revealed that education and economic status show statistically significant differences. Further they assessed based on descriptive analysis that people with higher education and those who are not living in owner-occupied housing are more often victims of cybercrime. In addition to age, participation in online communities and previous violent experiences are most clearly connected to experiencing cybercrime.

Yucedal (2010, p. 152) expected that individuals who have better knowledge about cyber threats, the Internet and computer related terms, are less likely to be victims of spyware and adware in his studies. However, his results show that there are significant positive relationships between the computer literacy latent variable and spyware and adware victimization variables, which indicate that respondents who have better knowledge are more likely to be victims of spyware and adware infection. On the other hand, the computer literacy latent variable has a significant negative effect on the computer problems, which indicates that individuals who have better knowledge are less likely to experience computer problems.

Routine activity theory suggests that exposure to certain places at certain times increases victimization risk. The victimization literature has shown that risk of victimization increases when people spend more time in risky places. Cohen et al (1979, p. 507) define exposure as "the physical visibility and accessibility of persons or objects to potential offenders at any given time or place". Ngo and Paternoster (2011, p. 780) revealed that there is a significant impact of exposure to motivated offenders and target suitability on cybercrime victimization. Yucedal's (2010, pp. 139-140) findings show that when individuals use computers at more different places for personal purposes, they are more likely to become victims of computer viruses and online harassment. Moreover, individuals who own more computers are more likely to be victims of online harassment. Frequency of Internet use is used to predict individuals' online lifestyle by Yucedal (2010). He found that frequency of the Internet use has significant positive effects on both basic and leisure online activities.

Choi's (2008, pp. 315-333) study represents a more comprehensive application of both routine activity and lifestyle exposure theories to cybercrime by including measurements for suitable target and guardianship. He found that students who use digital guardianships (antivirus, antispyware and firewall programs) are less likely to be victims of cybercrime. Further, Choi shows that online users who have higher risky online behaviors are more likely to be victimized. And, online users who inadequately manage the installed computer security programs will more likely be victimized. Thus, the concept of Hindelang et al. (1978, p. 245) is proved that the occurrence of criminal victimization relies on "high risk times, places, and people". Gross and Acquisti (2007) analyzed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information included on the site by students, such as the potential ability to reconstruct users' social security numbers using information often found in profiles, such as hometown and date of birth.

Methodology

Data

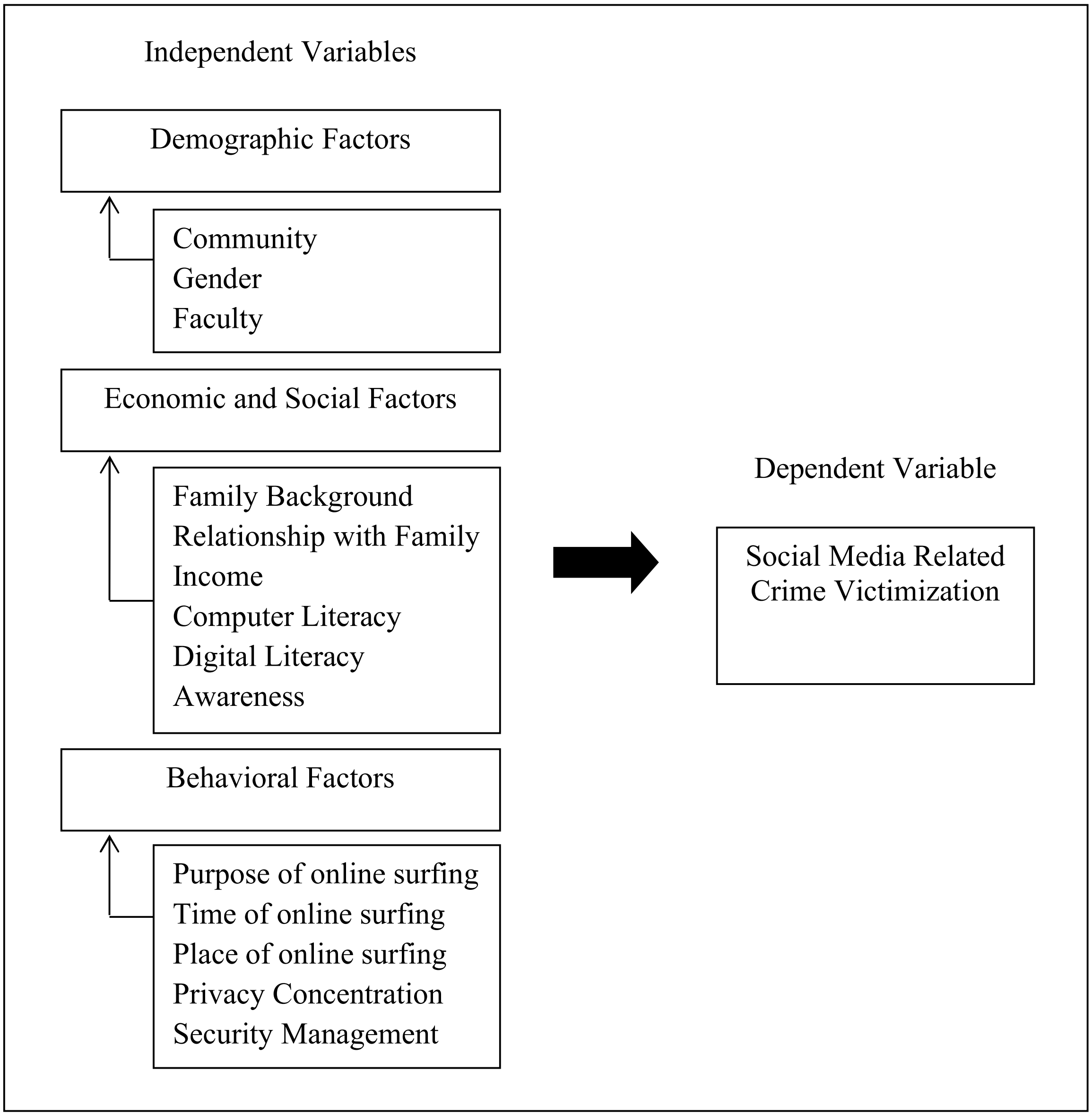
The undergraduates who are considerably representing the youth and are from different socio-economic backgrounds at the University of Sri Jayewardenepura where the larger community of undergraduates who are studying in all the academic streams were considered as the target population of the study. The researcher(s) derived the sample size of 420 which is covered 7.5% of the population. The study used stratified sampling. Sub-samples generated a proportionate sample size that reflected each faculty. This sampling method ensured that every undergraduate based on their faculty had an equal chance of becoming randomly selected for this study. Both primary data and secondary data were used for the purpose of study. The researcher(s) performed a web-based survey and a paper-based survey for collecting data. It permitted the researcher(s) to select an unbiased sample within the university. "Google Form" was used as the method of web-based survey after conducting a pilot survey.

Measures

Social media related crime victimization is used as the dependent variable. A set of questions were designed to assess whether respondents have been victims of five types of crimes: Fake Accounts, Hacking, Doxing, Cyberstalking and Internet Frauds during past year at social media platforms. Undergraduates were asked to recall 14 incidents which are considered as social media related cybercrimes for the one-year period prior to participation in the survey. This would allow the researcher to estimate the level of victimization during this period. The suggested cybercrime victimization factors derived from the survey questionnaires. First one is computer literacy. The researcher used criteria that suggested by Wilkinson, Roberts and While (2010) and similarly used by the Department of Census for their survey of Computer Literacy. The researcher(S) used seven items: MP3, PDF, Cookies, Spam, Bookmark, Download and Advanced Search to measure the digital literacy. These seven items were derived through the studies of multiple dimensions of digital literacy index by Hargittai (2005).

The questionnaire contained five survey items to rate the respondents' online security awareness. Respondents were asked to indicate for 8 statements and 6 statements on a range of between strongly agree and strongly disagree to measure the security management and privacy concentration. Furthermore, the researcher(s) considered variables to represent demographic, economic, social and behavioral factors. The linkage of independent variables with the dependent variable is illustrated by the conceptual framework of the study.

Figure 1. Conceptual Framework of the Study



Source: Constructed by the researcher(s)

Methods

Five responses out of 420 had to be eliminated due to incompleteness of the questionnaire. Missing values were found for some variables and the ratio of missing value is less than 5%. Due to the non-normality of the dependent variable, it is reconstructed as a binary variable by scaling "0 = non-victim" and "1=victim". Basically, data analysis was performed under three phases. The researcher(s) used appropriate data presenting tools such as histograms, bar charts, pie charts and so on to make a descriptive analysis. As the measurements of reliability and validity, Cronbach's alpha, Kaiser-Meyer-Olkin measure of sampling adequacy tests and the Bartlett's test were used. Chi-square tests were used to determine whether each factor was significantly independent with cybercrime victimization before the factors were entered to the logistic model. The Likelihood Chi-square statistic was used at the times that expected values were below 5. Since the dependent variable was in dichotomic scale, a binary logistic regression was suggested for identifying significant factors which are affected on cybercrime victimization of youth. Odd ratios were used to interpret the impact of each factor on victimization. Including "Hosmer and Lemeshow Test" diagnostic tools were used to assess the adequacy of the fitted model.

Results

The gender composition of the undergraduates in this study as females contribute 58% and males contribute 42%. In the sample, most of the undergraduates (265) are from hostels. Out of 415, 102 undergraduates are from boarding places. 42 undergraduates come to the university from their home. Altogether six undergraduates stay at relative's place or any other place. Undergraduates mostly visit their home once a month and It can be taken as a ratio of 194 out of 415. Most of the undergraduates (283) who are from hostels and boarding places contact with their parents via mobile at least once a day. This study revealed that 92% of the undergraduates have their own computer.

Smart phones are the popular devices that 292 undergraduates use to access internet, while, 112 undergraduates use computer to access internet. Most of the undergraduates (200) access internet at the university premises or at their hostels. Out of 415, 80 and 67 undergraduates access internet at their home and at their boarding places, respectively. Undergraduates mostly (71%) access internet at night and an undergraduate spends 4 hours as an average for surfing internet per day. Undergraduates use online for the purpose of entertainment, education and communication. Among them, entertainment is highly motivated and undergraduates to access online as the ratio of 133 out of 415. Secondly, education is motivated them to surf internet as indicating the main purpose of 126 of undergraduates. Also, 118 undergraduates spend time in online like social media platforms for the main purpose of communication. An undergraduate has average number of 500 friends in his or her Facebook account. More than half of the undergraduates communicate with their partners via social media.

The study revealed that a youth has more than half of chance to being a cybercrime victim since 54% of undergraduates experienced at least one of incidents which are identified as a social media related crime. When considering the cybercrimes that were mostly experienced by the undergraduates, cyberstalking is in lead and it is indicated as the value of 153. Secondly, 84 of the undergraduates experienced internet frauds. 80 doxing incidents were reported, while 56 of hacking incidents were reported. Incident related to fake accounts were experienced by 40 undergraduates. Since the reliability and validity of the Likert statements are met, the researcher(s) constructed five indices for computer literacy, digital literacy, online security awareness, security management and privacy concentration. Except computer literacy and digital literacy, the researcher(s) used Multiple Corresponding Analysis to observe the coordinates which have been weighted accordingly responses. The level of computer literacy among youth is 83.83%, which is a good sign. The composite indices suggested that the level of digital literacy among youth is 61.23% and it is not much higher as computer literacy; there is lack of online security awareness among youth, since the average level is indicated 51.23%; the level of security management among youth is 68.811%; and the level of privacy concentration among youth is 69.62%.

When considering the results of chi-square tests, 12 variables out of 22 are not independent with the cybercrime victimization of youth. They are digital literacy, online security awareness, security management, privacy concentration, brand of the mobile phone, price range of the mobile, number of FB friends, time of online surfing, hours spent on online, purpose of online surfing, education level of mother and relationship with family. In other hand, variables of computer literacy, accessory of online surfing, place of online surfing, communication with partner via social media, number of siblings, parents were died or not, education level of father, occupation of father, occupation of mother and the faculty are independent from the cybercrime victimization.

Table 1. Logistic Regression of Social Media Related Crime Victimization

Variable	Coefficient	Wald	Sig.	Odd ratio
Education Level of Mother	-.026	.045	.832	.975
Relationship with Family	-.303	4.420	.036	.738
Brand of the Mobile Phone	-.025	.050	.824	.975
Price Range of the Mobile Phone	.595	16.798	.000	1.814
Digital Literacy	-.590	4.961	.026	.554
Online Security Awareness	-.526	4.338	.037	.591
Security Management	-.911	9.465	.002	.402
Privacy Concentration	-.672	5.145	.023	.511
No. of FB Friends	.001	10.231	.001	1.001
Hours spent on Online	.137	13.544	.000	1.147
Time of Online Surfing	.275	1.387	.239	1.317
Purpose of Online Surfing	-3.550	22.607	.000	.029

Source: Constructed by the researcher(s)

The odd ratio represents the odds that an outcome will occur given a particular exposure, compared to the odds of the outcome occurring in the absence of that exposure. When controlling for every other variable in the model, for every one level increase in the frequency of engaging mobile phone with family the odds of becoming a victim of cybercrime decreases by 135.5%. Also, when controlling for all other variables in the model, the odds of undergraduate that has mobile phone with higher prices becoming victims of cybercrimes is 81.4% higher than the odds of undergraduate who has mobile phone with lower prices. Further, odds of undergraduate who are in high level of digital literacy becoming victims of cybercrime is 180.5% of lower than the odds of who are in low level of digital literacy. Same as digital literacy, odds of undergraduate who are in high level of online security awareness becoming victims of cybercrime is 169.2% of lower than the odds of who are in low level of online security awareness.

The odds of undergraduate who are in high level of security management becoming victims of cybercrime is 248.75% of lower than the odds of who are in low level of security management. Also, odds of undergraduate who are in high level of privacy concentration becoming victims of cybercrime is 195.69, lower than the odds of who are in low level of privacy concentration. For every one unit increase in the number of FB friends the odds of becoming a victim of cybercrime increases by 0.1% holding all other variables constant in the model. It is revealed that odds of becoming a cybercrime are increased by 14.7% when the one unit of hours spent on online is increased. According to table 1, the purpose of education significantly reduces the risk of cybercrime victimization since the odds of undergraduate who are indented in educational purpose becoming victims of cybercrime is 3448.27% lower than the odds of undergraduate who are not indented in educational purpose. It is found that there is no association between gender and cybercrime victimization differently from some scholars revealed that demographic factors such as gender significantly effect on cybercrime victimization.

Discussion

Findings from cybercrime victimization model shows youth who relatively maintain less relationship with the family are more exposed to cybercrime victimization. In the traditional victimization literature this point has been discussed much. However, under the scope of cybercrime victimization, there is not much concentration on impact of degree of relationship with family. The researcher(s) used price range of the mobile phone as an indicator of respondents' income level. According to the logistic regression model, the income level was significantly affected on cybercrime victimization. Further the likelihood of youth with higher income level becoming victims of cybercrimes higher than a youth with lower income level. When considering previous studies, Miethe and Meier (1990) found that people who carry larger amounts of money in public places and people who have a higher income level are more likely to be victims of a crime. Further, as lifestyle exposure theory explains, "rates of victimization are closely related to family income" (Hindelang, et al., 1978, p. 4). Therefore, income level can be identified as a determinant of cybercrime victimization among youth.

What about the capable guardian, computer literacy, digital literacy and awareness? As discussed in the literature review, a person who is more knowledgeable with the technical capabilities and is more aware about safety utilizes online risk freely. In this study it is found that younger who has considerable digital literacy skills such as recognizing cookies, spam messages etc. avoid becoming victims of cybercrimes. In other hand, it is found that the risk of becoming victims of cybercrimes is low for younger persons who has enough awareness about online security. Therefore, the capable guardianship measurements which were considered as social factors under this study are associated with cybercrime victimization. The results for computer literacy do not provide clear understanding of their relationship with the risk of cybercrime victimization. Yucedal (2010) also found under his SEM results that, individuals who have better knowledge of computer and Internet related terms are less likely to experience computer problems. Also, McQuade (2006, p. 487) asserts that a major opportunity to minimize computer crime through enhanced information security is via "public awareness, formal education, and professional training".

Using logistic regression, the researcher(s) found that a younger person who stay longer on the internet tend to have a greater risk of becoming victims of cybercrimes; duration measure risk exposure to cybercrime victimization. As routine activity theory suggests, exposure to certain places at certain times increases victimization risk (Cohen & Felson, 1979). The victimization literature has shown that risk increases when people spend more time in public places. In cybercrime victimization, the amount of time spent on the internet is believed to be a high-risk place. Further, the researcher(s) found that a youth who surf internet in purpose of education tend to have a lower risk of becoming victims of cybercrimes. Therefore, youth who is surfing internet for the purpose of communicating and entertainment tends to have a greater risk of becoming victims of cybercrimes.

Conclusion

The model chi-square (161.273) with 13 degree of freedom is significant at the 0.000 level. This indicates that the goodness of fit of the overall model is significant and it is better than a model with only an intercept. Therefore, the inclusion of the independent variables has improved the model. Based on "-2 Log likelihood" (411.084), which is significant, the overall model is good. Accuracy of the prediction of model is 77.3%. The all variables in the model explain 4.3% of the variance in victimization of Cyber-Crime. Based on previous studies and Chi-square tests of independency, all relevant independent variables are included and all irrelevant ones excluded. According to the standard residuals, there is no observations lie in between three sigma level. The minimum standard residual is -2.67798 while the maximum is 237641. Therefore, no significant outliers were occurred. Since all the standard errors are below 1, the cell sample sized was adequate. According to the correlation matrix, there are no significant correlations has found above the 0.7. Therefore, independent variables are not correlated with each other. As Hosmer and Lemeshow test, the probability value (.052) is greater than the significance level of 0.5 revealed that the linearity between Logit and independent variables is satisfied. Hence, the model is fitted adequately.

In preventing a threat, taking precautionary actions to avoid that threat is very crucial. Depending on the findings of the study, recommendations can be noted as: the awareness about online security should be empowered among young generation; maintenance of security settings and concentration about the privacy should be encouraged among youth in order to enhance online safety and privacy protection; it is important to provide information about the basic ways of keeping the computer secure and avoiding online activities that put individuals at greater victimization risk; the elders should pay more attention on youth to safeguard online behavior of youth. This has been significantly affecting the reducing victimization as mentioned above; should discourage the involvement with fake people while accessing internet in order to minimize the risk of victimization; the use of internet among youth should be improved in a more productive way. For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb cybercrime, it is recommended that there is need for them to understand both the technology and the individuals who engaged in this criminal act. Prevention of cybercrime requires the cooperation of all the citizens and not the law enforcement agencies alone. It is therefore, recommended that everyone should watch and report to law enforcement agencies, anyone who indulge in cybercrime.

The researcher(s) believes that the result of this study might be limited in terms of generalization because it concerns only the university students. Also, it may reduce the effectiveness of assessing the impact of different education level. While the field of cybercrimes is a complex phenomenon it might result some difficulties for respondents such as misunderstandings of technical terms, difficulties of distinguishing a cybercrime from an ordinary crime. Therefore, future researches have to consider these aspects too.

References

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey.* Saarbruecken, Germany: VDM Verlag.

APCERT Annual Report. (2015). APCERT.

Choi, K. (2008). Structural Equation Modeling Assessment of Key Causal Factors in Computer Crime Victimization. *Knowledge Repository @ IUP (Theses and Dissertations)* .

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* , 588-608.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society.* London: Addison Wesley.

Goodman, M., & Brenner, S. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology* , 139-223.

Hargittai, E. (2005). Survey Measures of Web-Oriented Digital Literacy. *Social Science Computer Review* , 374.

Higgins et al. (2008). *A Macro-Social Exploratory Analysis of Rate of Interstate Cyber-Victimization.* Retrieved from https://www.researchgate.net/publication/282811676_A_Macro-Social_Exploratory_Analysis_of_the_Rate_of_Interstate_Cyber-Victimization.

Hindelang, M. J., Gottfredson, M. R., & Gaffalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.

Jayasekara, A., & Rupasinghe, W. (2015). Trends and Challenges in cybercrime in Sri Lanka. *Regional Challenges to Multidisciplinary Innovation*, 760.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, Choice, and Criminal Victimization: A Test of a Theoretical Model. *Journal of Research in Crime & Delinquency*, 243-266.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures. *Criminology, 36*, 829-857.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 773-793.

Oksanen, & Keipi. (2013). Young people as victims of crime on the internet: A population-based study in Finland.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information.* New York: Wiley.

Weeramantry, C. (1998). Protecting Human Rights in the Age of Technology. *Justice Without Frontiers* .

Wilkinson, A., Roberts, J., and While, A. (2010). Construction of an instrument to measure student information and communication technology skills, experience and attitudes to e-learning. *Computers in Human Behavior* , 1369-1376.

Yucedal, B. (2010). Victimization In Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories. Kent State University.