Research Journal for Societal Issues

Vol 2 No 1 (2020): 96-106

Factors Affecting Online Attacks of Malicious Code among University Students in Khyber Pakhtunkhwa Province of Pakistan

Asghar Ullah Khan[1] Muhammad Imran Khan[2] ShakilaYaqoob[3]

[1],[2]Department of Communication and Media Studies, Gomal University, Dera Ismail Khan, KPK Pakistan

[3]Folks Grammar Higher Secondary School, Worker Welfare Board, KPK, Pakistan

Corresponding author: asgharullahadvocate@gmail.com

Keywords: *Malicious Code, Target Suitability, Routine Activity Theory*

Article History

Date of Submission: 12-02-2020

Date of Acceptance: 22-04-2020

Date of Publication: 31-12-2020

How to cite? Khan A.U., Khan M.I., Yaqoob S., (2020). Factors Affecting Online Attacks of Malicious Code Among University Students in Khyber Pakhtunkhwa Province of Pakistan. *Research Journal for Societal Issues.* 2(1), 96-105

This paper focused to measure the relationship of online target suitability with the chances of encountering malicious code i.e. hacking and viruses. Particularly, young students are prone to online attacks due to their excessive use of online spaces. The concept of target suitability was adopted from Routine Activity Theory (RAT). The study is a descriptive survey in nature. The population of the study was all university students of KP. 800 students were selected from the six top-ranked universities of KP. Multiple regression analysis was used to analyze the data. The findings of the study revealed that the target suitability in online activities of young adults increases the likelihood to face attacks in form of hacking and viruses. More careful use of the internet is recommended to avoid hacking and virus attacks during online communication.

Introduction

In contemporary world, with wide spread accessibility to smart phones and internet, malicious software are becoming major threat during online communication (Qbeitah & Aldwairi, 2018). Malicious code are software with harmful effects particularly designed to meet the desires of online offenders (Egele, et al., 2012). It can be transferred in different types of computer files like PDF, macros or document files, which then spread across the online world using online means of communication like emails (Palmer, 2018). These malicious codes are programs which cause harmful changes, delete or destroy files in computer or the whole system, which is one of the major online criminal activity where data files are destroyed using these programs (Qbeitah & Aldwairi, 2018). Through the uses of these malicious code, online attackers hack e-mail accounts, disrupt networks, gain access to and delete or corrupt valuable files, and can also be used to damage software and hardware (Taylor, et al., 2014). In most cases victims of such attacks remain unaware of the attack which poses even bigger problem (Palmer, 2018).

These viruses and hacking software are intended to interrupt modern communication technologies, access and stealing private data without victim's knowledge, which threaten users privacy, and the integrity of hosting sites (Sikorski & Honig, 2012). Malicious codes or programs includes "worms, Trojan horses, viruses, backdoors, time-bombs etc.*"*(Kienzle & Elder, 2003; McGraw & Morrisett, 2000). In light of the previous studies, the researcher divided all these forms of malicious codes into two categories of hacking and viruses. Previous studies applied Routine Activity Theory (RAT) to study hacking (Wilsem, 2013) and computer viruses (Holt & Bossler, 2013), but with limited scope.

Due to the pervasive nature, and widespread effects, it is important to study how these hacking and viruses' software affect the young users of internet; particularly this study focuses on the conditions which makes young university students suitable targets for such attacks. Findings of the study hopefully could lead to better understanding of the danger posed by these software as well as finding ways to counter the threat. In this regard, some understanding of hacking and viruses is beneficial for the study.

This study focused on the objective, "To measure the relationship of online openness (target suitability) with the chances of malicious code i.e., hacking and viruses that students face".

Hacking

Hacking is unauthorized access to online accounts, data, computer network with malicious intent (Mshana, 2015). Through hacking, online offenders bypass the security systems security systems and gain access to victim's computer, Smartphone of a whole online network(Marcum, et al., 2014; Wilsem, 2013). Usually, users of internet, particularly of Social Networking Sites do not take adequate measures to

protect their data and valuable personal information from hacking (Martens & De Wolf, 2018). One study shows that about 1.2 to 5.8% of the world population fall victim to hacking every year (Reep-van den Bergh & Junger, 2018). Study also shows that hacking is major problem in Pakistan as well, and one such study identified that 42.5% of university going students fall prey to hacking with criminal intent from the offender (Manzar, et al., 2016).

Viruses

Computer Virus has become major threat to computer systems and online communications of individuals (Chauhan, 2013). Virus is a kind of malicious software that causes disruption in normal functioning of computer system (Martens & De Wolf, 2018). These viruses commonly attack the data files and corrupt them by making alterations or sometimes completely delete important files (Chauhan, 2013). A study showed that 82.20% of the participants were attacked through viruses, 58.47% of them realized the risk of that virus attack, 71.18% of them were victimized repeatedly, at least twice, 62.25% were attacked thrice and 56.77% of participants were attacked through viruses for more than three times (Kamruzzaman et al., 2016). Viruses are more frequently transmitted through downloading games online (51.55%) and by clicking fake online ads(19.59%)(Kamruzzaman et al., 2016). The phenomenon of virus attacks is global in nature. Symantec in 2010 reported that globally, 51% of adult internet users face the effects of Computer viruses and malwares, while in New Zealand the rate is even higher at 61%, in Brazil it is 62% and in China 65% feel the effects of virus attacks (Symantec, 2010).

Theoretical Framework

Routine Activity Theory (RAT) developed by Cohen and Felson (1979) identified that presence of motivated offender, a suitable target and the lack of a capable guardian increases the chances of victimization. The present study focuses on suitable target which means in this case, the online users who use internet and social media carelessly and do not adopt security measures. Such users use internet with their real identities or do not object in providing or discussing personal information with other online users.

Over the years, scholars have used RAT theory to explain the factors behind online criminal activities; therefore, this theory provides theoretical ground for this study because the theory has proved as useful in explaining online victimization of various types. The theory suggests that there should be an opportunity of victimization as without presence of such opportunity it is less likely that people will be victimized (Felson & Clarke, 1998). Previous literature on online victimization suggests that certain online behavioural patterns are related with the chances of being victimized during online presence. Those behaviour patterns include a) the behaviour of clicking online links carelessly (Choi, 2008) amount of time spent on using social networking sites (Holt & Bossler, 2009; Wilsem, 2013), and sharing personal information online

(Reyns & Henson, 2016). These studies showed that with increased exposure, chances of online victimization also increases and also the physical location where users use internet also have effects on being victimized (Marcum, et al., 2010). This study focuses on what are the traits of university students that make them suitable targets for online attacks through malicious codes of hacking and viruses.

Methodology

This study utilizes the cross-sectional survey research design for collecting fresh data for the study. Students enrolled in the six leading universities of Khyber Pakhtunkhwa province of Pakistan makes the population of the present study, and the individual student is the unit of analysis for this study. Student data was obtained from their respective universities. A closed-ended questionnaire was used to collect relevant data from the university students. Items and questions for the questionnaire were selected as a result of rigorous literature review on the subject. At the time of data collection, the information collected from the respected universities revealed that in total there were 51887 students enrolled in the six leading universities of KPK, with 38991 male students and 12896 female students. The sample of 800 students was selected using stratified sampling method. To ensure that respondents fill the questionnaire appropriately, each questionnaire was administered separately and the respondent was requested to fill the questionnaire at spot so that if any problem they face during the process, the researcher will help them to sort it out.

The variable of malicious code was operationalized by distributing various types of malicious software into two categories of hacking and viruses. For hacking, seven (7) statements were formulated, while for measuring of virus attack six (6) statements were deduced from literature. A likert scale with five categories was provided for each statement of both the sub-constructs of malicious code. The five categories were labeled as; 1 means never, 2 means rarely, 3 means sometimes, 4 means often and 5 means very often. Answers for both the sub-constructs were separately calculated and the cumulative mean score of each was treated as individual's score of how often they were victimized through hacking or virus threats.

Hypothesis

Students who provide more information in online communication are suitable targets and are likely to face significantly higher rate of malicious code.

Results

Multiple regression tests are used to analyse the data. There was no collinearity between the independent variables. The alpha level was set at .05. In total, four tables were generated using SPSS. The first two tables present the results of multiple regression tests for predicting chances of hacking viruses respectively from posting personal information on social media. The last two tables predict chances of online

hacking and facing viruses respectively sharing personal information online contacts during interaction.

According to table no 1, multiple regression test was used to predict the effect of posting personal information in social media sites on hacking. F (12, 787), = 9.562, *p*= .000 predicts statistically significant relationship between different types of Adjusted R^2 = 0.114 suggested that the overall model explains 11.4% of the variation in the hacking due to age, phone number, family conflicts and audio. While gender, picture, school information, extracurricular activities, goals, emotional distresses, description of your-self, and video variables in the model has insignificant relationship with hacking. One unit increase in using to age, will increase hacking by 0.12 unit, phone number will increase hacking by 0.22 unit, family conflicts will increase hacking by .14 unit, and audio will increase hacking by 0.09 unit.

Table No 1: Posting personal information on social media and its effects on chances of hacking

Sharing personal information on SNS	Mean	SD	SE	B
Age	2.61	1.25	.04	.12*
Gender	3.01	1.33	.03	.06
Picture	3.14	1.20	.03	.01
Phone number	2.16	1.26	.03	.22***
School information	2.78	1.20	.03	.06
Extracurricular activities	2.72	1.25	.03	.01
Goals	2.56	1.24	.03	.02
Emotional distresses	2.13	1.16	.03	.01
Family conflicts	1.55	.93	.04	.14***
Description of yourself	2.39	1.22	.03	.06
Audio	2.00	1.06	.03	.09*
Video	2.43	1.19	.03	.04
Adjusted R^2= .11				
F= 9.56				
p= .000				

N=800; *p<.05; **p<.01; ***p<.001

According to table no 2, multiple regression was performed to predict the effect of sharing personal information in social media sites on viruses. F (12, 787), = 12.888, *p*= .000 shows significant relationship between the variables. Adjusted R^2 = .151 suggested that the overall model explains 15.1% of the variation in the viruses due to emotional distresses, description of yourself and video.

While age, gender, picture, and school information, extracurricular activities, goals, family conflicts and audio variables in the model have insignificant relationship with viruses. One unit increase in using to emotional distresses will increase viruses by .17 unit, description of yourself will increase viruses by .13 unit and video will increase viruses by .18 unit.

According to table no 3, multiple regression was performed to predict the effect of providing personal information to online contact on hacking. F (12, 787), = 10.445, *p*= .000 shows significant relationship between the variables. Adjusted R^2 = .124 suggested that the overall model explains 12.4% of the variation in the hacking due to gender, phone number, family conflicts and description of yourself. While age, picture, school information, extracurricular activities, goals, emotional distresses, audio and video variables in the model have insignificant relationship with hacking.

Table No 2: Multiple regression analysis of posting personal information on social networking sites and its effects on virus

Sharing personal information on SNS	Mean	SD	SE	B
Age	2.61	1.25	.04	.07
Gender	3.01	1.33	.03	.03
Picture	3.14	1.20	.03	.01
Phone number	2.16	1.26	.03	.04
School information	2.78	1.20	.03	.08
Extracurricular activities	2.71	1.25	.03	.05
Goals	2.56	1.24	.03	.05
Emotional distresses	2.13	1.16	.03	.17***
Family conflicts	1.55	.93	.04	.02
Description of yourself	2.39	1.22	.03	.13**
Audio	2.00	1.06	.03	.01
Video	2.43	1.19	.03	.18***
Adjusted R^2= .15				
F= 12.89				
p= .000				

N=800; *p<.05; **p<.01; ***p<.001

One unit increase in using to gender, will increase hacking by .16 unit, phone number will increase hacking by .15 unit, family conflicts will increase hacking by .25 unit and description of yourself will increase hacking by .14 unit.

According to table no 4, Multiple regression was performed to predict the effect of providing personal information to online contact on viruses. F (12, 787), = 11.989, *p*= .000 shows significant relationship between the variables. Adjusted R^2 = .142 suggested that the overall model explains 14.2% of the variation in the viruses due to emotional distresses, description of yourself, audio and video. While age, gender, picture, phone number, school information, extracurricular activities, goals and family conflicts variables in the model has insignificant relationship with viruses. One unit increase in using to emotional distresses, will increase viruses by .12 unit, description of yourself will increase viruses by .23 unit, audio will increase viruses by .12 unit and video will increase viruses by .12 unit.

Table No 3: Multiple regression analysis of providing personal information to any one among the online contacts and its effects on hacking

Providing personal information to anyone of your online contact	Mean	SD	SE	B
Age	2.47	1.22	.04	.02
Gender	2.82	1.27	.03	.16**
Picture	2.77	1.14	.04	.08
Phone number	2.41	1.09	.03	.15***
School information	2.62	1.20	.03	.02
Extracurricular activities	2.59	1.26	.04	.07
Goals	2.48	1.24	.03	.08
Emotional distresses	2.08	1.13	.04	.02
Family conflicts	1.53	.87	.04	.25***
Description of yourself	2.34	1.26	.03	.14**
Audio	2.15	1.08	.04	.08
Video	2.29	1.16	.04	.02
Adjusted R^2= .12				
F= 10.44				
p= .000				

N=800; *p<.05; **p<.01; ***p<.001

Table No 4: Multiple regression analysis of providing personal information to any one among the online contacts and its effects on viruses

Providing personal information to anyone of your online contact	Mean	SD	SE	β
Age	2.47	1.22	.04	.08
Gender	2.82	1.27	.04	.06
Picture	2.77	1.14	.04	.09
Phone number	2.41	1.09	.03	.07
School information	2.62	1.20	.04	.05

Extracurricular activities	2.59	1.26	.04	.06
Goals	2.48	1.24	.03	.037
Emotional distresses	2.08	1.13	.04	.12**
Family conflicts	1.53	.87	.04	.05
Description of yourself	2.34	1.26	.03	.23***
Audio	2.15	1.08	.04	.12*
Video	2.28	1.16	.04	.12*
Adjusted R^2= .14				
F= 11.99				
p= .000				

N=800; *p<.05; **p<.01; ***p<.001

Discussion and Conclusion

Literature on Routine Activity theory suggests that using internet excessively could lead to higher levels of online victimization in form of hacking and virus attacks (Bossler, et al., 2012; Hinduja & Patchin, 2008; Marcum et al., 2010).This study supports the findings of these previous studies and findings revealed that while communicating online, providing personal information increases chances of facing malicious codes in form of hacking and virus software. Result accepted the research hypothesis, "Students who provide more information in online communication are suitable targets and are likely to face significantly higher rate of malicious code i.e., hacking and viruses". Findings of this study also provided support to the previous study of Peluchette et al. (2015) and suggests that posting careless SNS content is an important determinant of making students suitable targets for hacking and virus attacks. Another study by Avais et al. in (2014) revealed that half of the respondents have faced hacking in different ways like, hacking of email id, facebook account etc. Study conducted by Kamruzzaman et al. (2016) showed that more than eighty percent respondents were victimized by virus attack and approximately seventy percent respondents were victimized for second or third time (Kamruzzaman et al., 2016). As RAT theory suggests and supported by findings of this study, careless use of internet makes individuals attractive target, and may provide an opportunity for online offenders to attack through hacking and virus software. Also as previous studies(Staksrud, Ólafsson, & Livingstone, 2013)found, this study suggests that as the number of friends in online social spaces increases, the risk of online victimization also increases as there may be more potential perpetrators among the friends list. Other studies found self-disclosure as a significant predictor of online victimization (Dredge, et al., 2014; Kokkinos & Saripanidis, 2017). Findings of this study support these findings, which highlights that pattern of using online spaces could attract potential offenders which is also consistent with the Routine Activity Theory.

Policy implications and research suggestions

From the knowledge gained through this study, hopefully more effective policies and programs can be introduced to educate internet user about protecting themselves while online. Internet is often used for educational, information, entertainment purposes, and many young people use the Internet to socialize and connect with others. It would be more effective to educate adolescents on the threats present online so they are aware of the potential victimization. Awareness raising seminars should be held on a regular basis to inform internet users about what is available for them to deal with malicious code and how they can access it.

For future researchers, it is suggested that causes and prevention mechanisms of other types of malicious code should also be investigated. As this study was limited to few universities of KP Province of Pakistan, studies with same variables can be carried out in different geographical areas, which would add to the knowledge base. Research is necessary to identify the prevalence of malicious code in other age groups. Studies among even younger students of schools and colleges could add new information in our knowledge of the phenomenon that how this age group is impacted by malicious code, and what coping strategies could be utilized.

Note: This research paper is part of Ph.D. thesis of Dr. Asghar Ullah Khan.

References

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500-523.

Chauhan, A. (2013). Evolution and Development of Cyber Law-A Study with Special Reference to India. *Available at SSRN 2195557*.

Choi, K.-s. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308.

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

Dredge, R., Gleeson, J., & De la Piedad Garcia, X. (2014). Presentation on Facebook and risk of cyberbullying victimisation. *Computers in Human Behavior, 40*, 16-22.

Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. *ACM computing surveys (CSUR), 44*(2), 6.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police research series, paper, 98*(1-36), 21-25.

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of adolescence, 31*(1), 125-146.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant behavior*, *30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), 22-28.

Kienzle, D. M., & Elder, M. C. (2003). *Recent worms: a survey and trends.* Paper presented at the Proceedings of the 2003 ACM workshop on Rapid malcode.

Kokkinos, C. M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter? *Computers in Human Behavior*, *74*, 235-245.

Manzar, U., Tanveer, S., & Jamal, S. (2016). The incidence of cybercrime in pakistan.1-89

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

Martens, M., & De Wolf, R. (2018). Measuring the cost and impact of cybercrime in Belgium (BCC): D3. 1.2 Risk perception monitor report (2 nd wave, 2017).

McGraw, G., & Morrisett, G. (2000). Attacking malicious code: A report to the Infosec Research Council. *IEEE software*, *17*(5), 33-41.

Mshana, J. A. (2015). Cybercrime: An Empirical Study of its Impact in the Society-A Case Study of Tanzania. *Huria: Journal of the Open University of Tanzania*, *19*(1), 72-87.

Palmer, D. (2018). What is malware? Everything you need to know about viruses, trojans and malicious software. Retrieved June 5, 2018, from https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior*, *52*, 424-435.

Qbeitah, M. A., & Aldwairi, M. (2018, April). Dynamic malware analysis of phishing emails. In *2018 9th International Conference on Information and Communication Systems (ICICS)* (pp. 18-24). IEEE.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, *7*(1), 5-15.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine

activity theory. *International journal of offender therapy and comparative criminology, 60*(10), 1119-1139.
Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*: no starch press.
Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*(1), 40-50.
Symantec. (2010). Norton cybercrime report: The human impact.
Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*: Prentice Hall Press.
Wilsem, J. v. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453.