Research Journal for Societal Issues

Vol 1 No 1 (2019): 23-32

Target Suitability as a Determinant of Online Identity Theft: Case of University Students in Khyber Pakhtunkhwa Province of Pakistan

Asghar Ullah Khan[1] Muhammad Imran Khan[2] Shakila Yaqoob[3]

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

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

Corresponding author:asgharullahadvocate@gmail.com

Key words: *Online Identity Theft, Target Suitability, Routine Activity Theory*

Article History

Date of Submission: 14-07-2019

Date of Acceptance: 16-09-2019

Date of Publication: 31-12-2019

How to cite? A.U., Khan, Khan M.I., Yaqoob S., (2019). Depression Target Suitability as a Determinant of Online Identity Theft: Case of University Students in Khyber Pakhtunkhwa Province of Pakistan. *Research Journal for Societal Issues.* 1(1), 23-32.

This research study aimed to measure the relationship of online target suitability with the chances of online identity theft (OIT) faced by the university students of Khyber Pakhtunkhwa (KP). The concept of target suitability was adopted from Routine Activity Theory (RAT). A descriptive survey research approach was adopted in this study. University-going students of KP formed the population of this study. 800 students were selected from the 6 universities of KP. The data were analyzed using multiple regression techniques. The results reveal that the target suitability in online activities of young adults increases the likelihood of OIT.

Introduction

New communication technologies users release personal information and pictures online without realizing that their actions may lead to increased vulnerability to online identity theft (OIT) and so on (Choe, 2018; Shin, 2010). OIT, are the threats where an offender access to the personal information of other persons without the consent of those persons and uses that information for different purposes such as harassment, blackmailing, deception, fraud or economic gain (Justice, 2018). OIT affects all ranges of targets including individual user, businesses, and government institutions (Thomas, 2018).

Modern communication technologies make OIT easier for perpetrators and with the help of these technologies, perpetrators do not need to be physically present at the place of data, rather they virtually access the data, due to which it is possible that in less time they can commit OIT against several people (Rafique, 2017). Online threats are on the rise and affect individuals around the globe (Reyns & Henson, 2016). Apart from possible economic damages to the individuals, online theft of personal information, particularly on social media platforms of greater concern due to threats to individual's self-image and public identity (Gross & Acquisti, 2005). Losing personal information could cause socially irreversible damages, that may include, discloser of confidential information, embarrassment in social circles and or implying wrong impression (Tuunainen, et al., 2009). These threats are socially embracing and damaging because they the audience of such leak information are the people with whole the victim interact on frequently in real world (Sowmya & Chatterjee, 2018). Therefore, the social consequences and embracement due to online theft of information could have severe consequences for the victims, more than the loss of credit card number (Fire, et al., 2014).Similarly the survey respondents reported that, nearly twenty percent of the total population individually experienced negative effects of social media, such as personal information theft (Debatin, et al., 2009). In United Kingdom, twenty percent of the 770 respondents (aged 11 to 19 years old), ten percent reported feeling uncomfortable by a picture that someone stolen from online profile (Subrahmanyam & Greenfield, 2008). Research study by Dreßing, et al., (2014) found that 49.6% published respondent's private information on the social media sites without his/her knowledge, 25.6% published genuine private/intimate images/videos, 13.0% downloaded data from respondent's computer without his/her knowledge and 6.5% published respondent's images/data on porno web sites without his/her consent. Similarly, complaint reported by Srivastava and Yadav (2014) in his study that a 26 year old woman filed a complaint against her colleague for downloading her photos from a social networking site and was circulated to friends without the complainant knowledge.

Study conducted by Kamruzzaman et al., (2016) showed that the threat of OIT victimization is 58.47% in South Asia, where in reality it is 20.33%. OIT bring hazard for the real account holder and perpetrator can easily misuse the information or can use it for illicit activity. For that reason the impact of that threat bring the 58.47% sensitivity for OIT (Kamruzzaman, 2015). OIT is affected by giving information to unauthorized sites (58.33%) and person (41.67%). Young people easily give their personal information over internet to download or see software, porn, game, photos and likewise, post personal information on social media for self-identification (Kamruzzaman et al., 2016). Age, income level and gender are important determinants of victims of online information theft than the other demographic factors

(Reyns & Henson, 2016). This study is concerned with micro-level online identity theft, which means that it will only include those instances of identity theft where personal information of individual internet users are used by other people without their knowledge or permission.

Theoretical framework

The Routine Activity Theory (RAT) developed by Cohen and Felson (1979),provides a good theoretical foundation for this study. This theory has been used to explain criminal offences, deviant behaviors, fear of victimization and criminal victimization (Reyns, 2015). This theory states that a crime is more likely to occur when 1) there are motivated offenders, 2) there is an accessible target, and 3) there is an absence of capable guardians to guard against a violation (Cohen & Felson, 1979). At the time of the theory's development, this intersection between the three major conditions was usually spatial, meaning that victims and offenders converged at a physical location at the same time, however, Reyns (2015) have pointed out that this physical convergence is lacking in instances of online victimization and that modern communication technology networks can facilitate the intersection of victims and offenders regardless of physical location or time.

Previous studies have often used measures of economic value to reflect the concept of target suitability (e.g., Messner, et al., 2007), but in online environment other characteristics could also prove attractive for the rationale offenders (Reyns & Henson, 2016). Visiting risky or unprotected websites, readily providing personal information online, or availability of personal information publicly could make an individual an easier targets for online offenders (Reyns & Henson, 2016). Most of the victimization occurs at social media and instant messaging platforms however, disclosing less personal information online reduce adolescents' risk of online victimization (Hafeez, 2014). The type of information that youth provide while using social network sites and their means of communication (i.e., chat rooms, messenger or e-mail) may make them suitable targets for OIT victimization. Several studies reported that some online behaviours increase the risk of OIT victimization e.g. a) risk taking, such as the tendency to easily click on links, being related to general online victimization (Choi, 2008) time spent online and on social media being related online harassment victimization (Holt & Bossler, 2009; Wilsem, 2013), placing personal information online(Reyns & Henson, 2016). In each of these studies increased exposure was associated with increased chances of OIT victimization. The clicking on pop-up messages, downloading games or music or even opening unknown email attachments increases exceedingly the likelihood of OIT victimization.

This study focuses on micro level of RAT and measure the reasons of individual victimization in online space. As the physical crimes take place in real life, therefore, this study focuses only on social threats which can also be carried out using internet. It is clear that previous routine activity research and online victimization findings underscore the importance of further investigating target suitability as a person-based concept. Therefore, the present study uses the previously discussed rationale to assess the effects of target suitability on OITs victimization among university students. So, this study investigates the effect of target suitability on individual victims of OIT of six top ranked universities (i.e., Khyber Medical University Peshawar, University of Peshawar, University of Agriculture, Peshawar, Abdul Wali Khan University Mardan, University of Engineering and Technology Peshawar and Gomal University, Dera Ismail Khan) students of Khyber Pakhtunkhwa (KPK), Pakistan by applying RAT.

Significance of the study

OITs in Pakistan are usually prevalent among the students. This previous studies on OITs are mostly conducted by experts and academicians in the fields of information technology and criminology. One significant contribution of this study is to add perspective on the issue from the field of Communication studies. It may help the students and academicians who are interested in media laws and ethics. It may also help to develop the understanding of and literature on OITs as well as encouraging further discussion on how to prevent such crimes from harming individuals. Common internet users, particularly students, can get benefits from this study by knowing the way of securing themselves and avoiding potential online offenders. They may be more informed about the ways through which they can guard from online victimization. This adds more importance to exploring the possible outcomes of using social media carelessly. Not only should the individuals be more cautious about which personal information to share but also, the SNS companies need to find discrete solutions to protect their users. The results are also significant for the law enforcement personnel by knowing the causes and consequences of online threat and they better equipped for coping with the threat.

Objective of the study

1. To measure the relationship of online openness (target suitability) with the chances of online identity theft students face.

Methodology

This study utilizes the cross-sectional survey research design for collecting fresh data from the Universities of Khyber Pakhtunkhwa (KPK), in which students are the unit of analysis. All the students of six top ranking Khyber Pakhtunkhwa (KPK) universities were included in the population of the present study. Student data was obtained from their respective universities through well-structured closed-ended questionnaire which was prepared with the support of different studies and articles. The total number of population for this study is 51887 with 38991 male students and 12896 female students (Mahmood, et al., 2017). 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.

In this study, online identity theft is operationalized through nine (9) statements, using five-point Likert scale. The mean score of all these 9 questions were treated the score of an individual's online identity theft that he/she faced. Cronbach Alpha=.86. For operationalization of Target suitability, this study include two questions (In line with study of Marcum et al. (2010). The questions are measured at ordinal level. It included questions about how often do you post your personal information on social networking website? And how often do you provide your personal information to any one of your online contacts? The questions were further provided with list of personal information and each item in the list has Likert scale answer category, where 1 means never, 2 means rarely, 3 means sometimes, 4 means often and 5 means very often.

Results

The data was analysed by using statistical procedure in order to understand the online identity theft faced by internet users in Pakistan, particularly the university students in Khyber Pakhtunkhwa province. The results of the analysis are provided in an organized manner in order to give better understanding of the findings of the study. To test the hypothesis, multiple regression was used separately for online identity theft victimization. No collinearity was found between the independent variables. The alpha level is .05. The results are presented in two separate tables. First tables show the data about posting of personal information on social networking sites and its effect on online identity theft. The second table is about sharing personal information with any one in online interaction and effects of this on the same online identity theft.

Table No1: Multiple regression analysis of posting personal information on social networking sites and its effects on online identity theft

Sharing personal information on SNS	Mean	SD	SE	β
Age	2.61	1.25	.03	.13*
Gender	3.01	1.33	.03	.03
Picture	3.14	1.20	.03	.04***
Phone number	2.16	1.26	.02	.22
School information	2.78	1.20	.03	.03
Extracurricular activities	2.71	1.25	.03	.05
Goals	2.56	1.24	.03	.01
Emotional distresses	2.13	1.16	.03	.07
Family conflicts	1.55	.93	.03	.16***
Description of yourself	2.39	1.22	.03	.02
Audio	2.00	1.06	.03	.01
Video	2.43	1.19	.03	.04
Adjusted R^2= .10				
F= 8.46				
p= .000				

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

Multiple regression was performed to predict the effect of posting personal information on social media sites on online identity theft. F (12, 787), = 8.457, p= .000 shows significant relationship between the variables. Adjusted R^2= .101 suggested that the overall model explains 10.1% of the variation in the online identity theft due to age, picture and family conflicts. While gender, phone number, school information, extracurricular activities, goals, emotional distresses, description of yourself, audio and video variables in the model has insignificant relationship with online identity theft. One unit increase in using to age, will increase online identity

theft by 0.13-unit, picture will increase online identity theft by .04 unit, while, family conflicts will increase online identity theft by .16 unit.

Multiple linear regression was performed to predict the effect of providing personal information to online contact on online identity theft. F (12, 787), = 9.678, *p*= .000 shows significant relationship between the variables. Adjusted R^2 = .115 suggested that the overall model explains 11.5% of the variation in the online identity theft due to phone number, family conflict and description of yourself. While age, gender, picture, school information, extracurricular activities, goals, emotional distresses,

Table No 2: Multiple regression analysis of providing personal information to any one among the online contacts and its effects on online identity theft

Providing personal information to anyone of your online contact	Mean	SD	SE	B
Age	2.47	1.22	.03	.10
Gender	2.82	1.27	.03	.08
Picture	2.77	1.14	.03	.09
Phone number	2.41	1.09	.03	.15**
School information	2.62	1.20	.03	.03
Extracurricular activities	2.59	1.26	.03	.02
Goals	2.48	1.24	.03	.07
Emotional distresses	2.08	1.13	.03	.03
Family conflicts	1.53	.870	.03	.29***
Description of yourself	2.34	1.26	.03	.10**
Audio	2.15	1.08	.03	.01
Video	2.28	1.16	.03	.05
Adjusted R^2= .12				
F= 9.68				
p= .000				

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

audio and video variables in the model have insignificant relationship with online identity theft. One unit increase in using to phone number will increase online identity theft by .15-unit, family conflict will increase online identity theft by .29 unit and description of yourself will increase online identity theft by .10 unit.

Discussion

Those who post personal information online are at a higher risk of experiencing online victimization because this act gives prospective harassers information about their target. In addition, individuals who willingly provide such information are suitable target of experiencing online identity theft (Bossler, et al., 2012; Hinduja & Patchin, 2008; Marcum, et al., 2010).In this study careless posting and providing personal information like; age, picture, family conflicts, phone number, family conflicts and description of yourself to online contact through different platform of SNS were related to online identity theft while gender, school information, extracurricular activities, goals and emotional distresses were insignificant. According

to this study, as well as to previous ones (Peluchette, e al., 2015) posting indiscreet SNS content was found as an important determinant of online victimization. Consistent with the RAT, it appears that individuals who post indiscreet information about themselves fit into the profile of an "attractive target", as posting and sharing SNS content of an indiscreet nature may provide an opportunity for others to offend someone. Moreover, in accordance with previous findings (Staksrud, et al., 2013) increasing the number of SNS friends may increase the risk of OIT victimization as there may be more potential perpetrators among these friends. In line with relevant studies (Dredge, et al., 2014; Kokkinos & Saripanidis, 2017) self-disclosure was also found to be a significant predictor of OIT victimization. This highlights the importance of the victim's role to OIT victimization as it is this information that the perpetrators may later use to harm or humiliate the victim. Furthermore, in accordance to previous studies (Kokkinos & Saripanidis, 2017; Peluchette, et al., 2015) self-disclosure has been positively associated to the risk of being victimized. This is also consistent with the RAT and highlights the role of an active victim whose behaviour could trigger the OIT victimization mechanism, possibly by providing the suitable information to the perpetrator.

Conclusion

Sharing of personal information on social media sites and provision of personal information to online contact have been explored in relation to the routine activities theory (RAT) which predicts higher levels of OCTs victimisation among those with greater exposure to risk through their activities. With regard to online behaviour, sharing of personal information online and providing information to online contact has significant relationship with chances of facing online identity theft victimization. Result also accepted the research hypothesis that "students who provide more information in online communication are suitable targets and are likely to face significantly higher rate of online identity theft". This study indicated that communicating with people online and providing personal information to online contacts increased the likelihood of online identity theft victimization measured in the current study.

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. Use of the Internet is often vital for educational, information, entertainment purposes, and many young people use the Internet to socialize and connect with others. Rather than encouraging adolescence to discontinue socializing on the Internet, it would be more effective to educate adolescence on the threats present online so they are aware of the potential for victimization. Youths using the Internet should be educated to only—participate in online communication with peoples they know and trust. If youths limit their online communication to peoples they know, the risk of victimization should be lower. Awareness raising seminars should be held on a regular basis to inform internet users about what is available for them to deal with online threats and how they can access it. Educational institutions should introduce a separate office to stop online victimization of users. There is a need for more discussion and education about Internet rights, surveillance, privacy, and other issues commonly addressed in Internet law. Pakistan has online protection laws, but it is needed that people should be informed about those laws as well the

mechanism through which they can sought relief. Also it is important to remove ambiguities, if any, in the legal structure and to improve the ability of the organizations who are responsible for implementation of online laws.

For future researchers, it is suggested that causes and prevention mechanisms of other types of online threats which are related to institution and organizations should also be investigated. In order to establish causal relationship between various independent variables used in this study and OIT victimization, it is suggested that future researchers should adopt longitudinal methods of research. As this study was limited to few universities of Khyber Pakhtunkhwa province of Pakistan, studies with same variables can be carried out in other areas of the country. There is a sufficient opportunities for future study in this area. Surveying a wider age range of young people, also those in different geographical areas, would add to the knowledge base. Research is necessary to identify the prevalence of OIT in other age groups as well. Particularly, study about younger generation studying in schools and colleges could add new information in our knowledge of the phenomenon that how this age group is impacted by online victimization, and what coping strategies are utilized. OIT is especially relevant for this age group.

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.

Choe, J. (2018). *A Lifestyle-Routine Activity Theory (LRAT) Approach to Cybercrime Victimization: Empirical Assessment of SNS Lifestyle Exposure Activities. 4*(2), 200-215.

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

Clarke, R. V. G., & Webb, B. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods* (Vol. 112): Citeseer.

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

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

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.

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking, 17*(2), 61-67.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials, 16*(4), 2019-2036.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks.* Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Hafeez, E. (2014). Cyber Harassment and Its Implications on Youth in Pakistan. *New Horizons, 8*(2), 29.

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. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant behavior*.
Justice, D. o. (2018). Idenitity theft. Retrieved June 21, 2018, from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
Kamruzzaman, M. (2015). Dowry related Violence against Rural Women in Bangladesh. *Age (years), 15*(4), 3.7.
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.
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.
Mahmood, M. T., Farooq, M. M., Anwar, M. M., Ali, M. H., Ahmad, M. T., Khan, M. S., . . . Aftab, M. H. (2017). Development Statistics of Khyber Pakhtunkhwa Retrieved October 26, 2017, from http://www.pndkp.gov.pk/wp-content/uploads/2017/07/development statistics of Khyber Pakhtunkhwa-2017.pdf
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.
Messner, S. F., Lu, Z., Zhang, L., & Liu, J. (2007). Risks of criminal victimization in contemporary urban China: An application of lifestyle/routine activities theory. *Justice Quarterly, 24*(3), 496-522.
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.
Pires, S., & Clarke, R. V. (2012). Are parrots CRAVED? An analysis of parrot poaching in Mexico. *Journal of Research in Crime and Delinquency, 49*(1), 122-146.
Rafique, G. M. (2017). Personal Information Sharing Behavior of University Students via Online Social Networks. *Library Philosophy & Practice*.
Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396-411.
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.
Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.
Sowmya, P., & Chatterjee, M. (2018). Comparative study of threats and solutions in online social networks. *International Journal of Advanced Research in Computer Science, 9*(1), 760-764.
Srivastava, A., & Yadav, S. (2014). Cyber Stalking: A Nuisance to the Information Technology. *International Journal of Advanced Research in Computer Science, 5*(8).
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.
Subrahmanyam, K., & Greenfield, P. (2008). Online communication and adolescent relationships. *The future of children*, 119-146.

Thomas, J.E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management, 12*(3), 1-23.

Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites-case Facebook. *Bled 2009 Proceedings*, 42.

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.

Note: This research article is based on the Ph.D. thesis of Mr. Asghar Ullah Khan from Department of Communication and Media Studies, Gomal University, Dera Ismail Khan (KP) Pakistan. This article is not funded by any other organization or institution. The researchers have no conflicts of interest to declare.