Pak. j. life soc. Sci. (2025), 23(1): 7527-7536 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.00584

RESEARCH ARTICLE

Victimizing the Youth: Measuring Online Victimization of Higher Secondary School's Students in Khyber Pakhtunkhwa

Asghar Ullah Khan[1], Sook Fern Yeo[2*], Kah Boon Lim[3]

[1,2,3] Faculty of Business, Multimedia University, 75450 Bukit Beruang, Melaka, Malaysia

[2] Department of Business Administration, Daffodil International University, Dhaka, Bangladesh.

ARTICLE INFO

Received: Dec 29, 2024

Accepted: Feb 17, 2025

Keywords

Online Exposure

Target Suitability

Online Victimization

Routine Activity Theory

***Corresponding Author:**

yeo.sook.fern@mmu.edu.my

ABSTRACT

Online victimization is a persistent threat to free speech over the internet, previously studied from legal and socio-psychological perspectives. Scholars stressed the need to study it from the perspective of human communication. This study provides perspective from the field of communication into the issue of online victimization with reference to the teenage internet users in Pakistan. Routine Activity Theory (RAT) provides a theoretical foundation for this study. This study focused on the concept of target suitability in RAT and its effects on online victimization. Additionally, online exposure of students to internet and various social media platforms with online victimization was also studied. This is a cross-sectional survey study, where the researcher interviewed 800 students of sixteen Higher Secondary Schools students of Khyber Pakhtunkhwa one of the four province of Pakistan, through a closed ended questionnaire. Results revealed that the overall relationship of student's exposure to internet and various social media platforms is a significant factor of online victimization. With regard to online behavior, posting of personal information and providing personal information to online contacts is also significant contributor to online victimization.

INTRODUCTION

With the surge in use of virtual spaces, physical distances in human communication are constantly diminishing. This effect of media was once called as "Global Village" by Marshal McLuhan (McLuhan 1966). To some scholars, internet is another universe altogether, independent of time and space restrictions that differentiate it from the physical world that we live in. Therefore, with the changed nature of time and space, the nature of crimes is also different from the crimes of our physical world. The online crimes include but not limited to spamming, e-mail espionage, identity theft, spreading of virus, credit card fraud, intimidating messages and receiving unpleasant e-mails or text messages, unauthorized use of personal photographs to cause defamation and humiliation of individuals (Özdemir 2014) and also sending computer viruses, spams, malware, and so on, which affects personal privacy and cause great discomfort to online users (Khan, Ali et al. 2021), collectively called as online victimization.

Among many theoretical approaches regarding criminal activities, one theory The Routine Activity Theory (RAT) developed by Cohen and Felson (1979) has been widely 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), an accessible target, and 3), an absence of capable guardians to guard against a crime (Cohen and Felson 1979). The theory suggests that individuals who can be victimized easily are suitable targets for such online crimes. Therefore, routine activity theory presumes a rational offender, easier targets may also be more suitable or attractive targets (Reyns and Henson 2016). A persons who visit risky, unprotected websites, provide personal information, or have personal information publicly available online may be easier targets for online motivated offenders (Reyns and Henson 2016). The more time that youth spend on the Internet, especially using SNS, may increase their likelihood of being exposed

to a motivated offender. The type of information that youth provide while using SNS and their means of communication (i.e., chat rooms, messenger or e-mail) may make them suitable targets for online victimization. This study focused on target suitability as a determinant of online victimization. For this purpose, the study focused on students of higher secondary schools of Khyber Pakhtunkhwa province of Pakistan. This study treats online spaces as places for human communication and tried to measure through the use of Routine Activity Theory that how careless use of these online spaces can affect the chances of individuals being victimized online. The primary objective of this study is to examine the relationship between the online exposure of Higher Secondary School students in KP and the online victimization they encounter. Additionally, the study seeks to evaluate how online openness influences the likelihood of these students experiencing online victimization.

Significance of the study

Communication is indispensable part of social life, and with the introduction of new technologies, new players emerged that can affect the human communication and consequently, their social lives profoundly. Instead of traditional face to face mode of communication, online communication poses many threats for individual's privacy as well as relationships with others. But with the increasing number of people, particularly the younger generations, turning to the internet and online spaces for fulfilling the need for social interaction and connectivity, the importance of this mode of communication and the related dangers cannot be ignored. Young teenagers are more prone to careless use of internet and hence, more open to online victimization. Keeping in view this significance and currency of the issue, this study focused on this much needed perspective of human communication about online victimization. The major contribution of this study is to analyze the cybercrime phenomenon from human communication perspective. Earlier researches mostly focused on victimization of adults or preteens. This research enhances our understanding about teenage students. The results of this research could possibly help the potential victims in the said age group, as well as the academicians and scholars of media laws and ethics, because it helps in understanding how pattern of internet use can affect the level of online victimization of the teenagers. The finding of this study can also educate the young internet users about effective techniques of protecting themselves from online victimization, as well as it also helps in educating parents about their guardianship responsibilities. This research hopefully, contributes in enhancing the knowledge level of law enforcement personnel about identifying and controlling the potential offenders of online crimes.

LITERATURE REVIEW

Today's young generation spending extensive amounts of time online are also placing themselves at risk for an increased likelihood of victimization. Some scholars have conducted studies to ascertain the spread of online victimization. In a study it was found that nearly forty percent of students have faced online victimization in their lives (Reyns, Henson et al. 2012). During the year 2015, nearly ten percent of students from age of 8 to 15 years faced some type of unpleased and offensive behavior online (Ofcom 2016a). Another study conducted in four developed countries: Finland, Germany, UK and USA with total sample of 3506 students revealed that the rate of online victimization among the age group of 15 to 30 years is as low as 6.5 percent compared to students of other age groups (Näsi, Oksanen et al. 2015). The same study found that some major factors of online victimization which include, adolescent, male gender, urban dwelling, immigrant background, living alone not with parents, less active offline social life and joblessness (Näsi, Oksanen et al. 2015).

Online victimization in Pakistan

Pakistan like the rest of the world is neither unfamiliar nor immune from the phenomenon of online victimization. In Pakistan, various public and private organizations work to register complaints about online crimes. In 2021 Federal Investigation Agency (FIA) Pakistan Cyber Crime Wing received 95,567 complaints from all around Pakistan. This year the number of online victimizations in Pakistan has risen significantly compared to 84,764 complaints received in 2020. The major categories of complaints pertain to online blackmailing, financial fraud, and defamation, harassment, hate speech and child pornography. In 2021, nearly 20% of the total complaints relate to online harassment and blackmailing and 267 FIRs were registered and 185 arrested with regards to online blackmailing, while 199 FIRs were registered and 187 arrested concerning online harassment over social networking platform (Aslam and Wahab 2022). The Digital Rights Foundation (DRF) Cyber

Harassment Helpline Report in 2020 states that 3,298 cases were registered of online victimization. The report further stated that, 33% of the cases were related to extortion and blackmailing, while 23% cases related to hacking of social media and WhatsApp accounts along with financial fraud (Ali 2021). In 2019, DRF cyber harassment helpline reported 2,023 cases or 146 calls every month. The report highlighted that social networking sites are becoming ground for online victimization. "Most of the complaints related to online victimization in Pakistan-bullying were reported on WhatsApp (855), while 29% of callers reported victimization on Facebook." Online victimization may include stalking, threats, online impersonation, hacking, trolling, hate crime and revenge porn (Jamal, 2020). The data shows that, 40% of the online users faced some type of victimization during online interactions (Avais, Wassan et al. 2014), and most of the online crimes reported are related to online blackmailing, defamation and harassment, followed by financial frauds, threat calls, spoofing and email hacking etc. (Zahid, Luavut et al. 2017).

Target suitability

According to RAT one important factor of higher victimization risks is the target suitability. But defining a target's suitability is difficult as it depends on the purpose and motivation of offender which is not easy to gage (Yar 2005, Khan 2020). (Choi 2015) identified that initially, offenders try to access the digital record and information of an organization or individual of a potential target. When someone connects to the internet, the danger is that they become potential targets for online offenders (Cohen and Felson 1979, Choi 2008). Then such targets can face wide range of online crimes like, harassment, unauthorized trespassing, identity theft or damages and theft of data (Choi 2015).

Previous studies of Routine Activity Theory measured target suitability through monetary values, which means individuals and organization having higher financial resources are more likely to become suitable targets that those having less resources (Messner, Lu et al. 2007, Khan 2020). Along with the monetary factor, the theory also considers those people as suitable candidates for victimization who are simple and easier to target (Reyns and Henson 2016). In online environment, those people can become suitable targets who visit insecure websites, provide personal information, or whose private information available on public forums (Reyns and Henson 2016). Social media and instant messengers are major platforms for online victimization, but protecting personal information on internet can minimize the risks of online victimization, particularly of younger internet users (Hafeez 2014, Khan, Ali et al. 2021).

RESEARCH METHODOLOGY

In Mass Media research, survey methods are considered as effective tools to study attitudes and behaviours of media users (Hinkin 1998). A quantitative survey method with cross-sectional research design is adopted and a closed ended questionnaire is used for the purpose of collecting data. This study focused on the young students of various Government Higher Secondary Schools (GHSS) in the province of Khyber Pakhtunkhwa (KP), Pakistan. These students form the population of the study. The KP province is comprised of thirty five districts and seven divisions. According to recent statistics, there are some 3.9 million students studying in Elementary and Secondary schools of the province (both male and female). The total number of schools owned and run by the government in the province is 2800. In these school only sixteen higher secondary schools of male (i.e., 1- Govt. Higher Secondary School (GHSS) Sherpao, Charsadda 2- GHSS, Bandi Dhundan, Abbottabad 3- GHSS, Takhat Bhai,Mardan 4- GHSS Kot, Malakand 5- GHSS, Mingora (Haji Baba), Swat 6- GHSS No.1, Kohat 7- Bannu Model School & College, Bannu and 8- University WENSAM College, DIKhan) and female (i.e., 1- Govt. Girls Comprehensive Higher Secondary School, Peshawar 2- Govt. Girls Centennial Model Secondary School No.1, Abbottabad 3- Govt. Girls Higher Secondary School (GGHSS), Hathian, Mardan 4- GGHSS Kot 5- GGHSS No. 1, Saidu Sharif Swat 6- GGHSS, Behzadi Chikar Kot, Kohat 7- GGHSS Ghoriwala, Bannu and 8- Working Folks Grammar Higher Secondary School, D.I.Khan-I Female) whose students obtained higher marks in the Board of Intermediate & Secondary Education (BISE) (I,e., 1- BISE, Peshawar 2- BISE, Abbottabad 3- BISE, Mardan 4- BISE, Malakand 5- BISE, Saidu Sharif Swat 6- BISE, Kohat 7- BISE, Bannu and 8- BISE, Dera Ismail Khan) annual exams are selected as representative sample through multi stage sampling method on equal proportion so that, the sample becomes more representative of the population. The sample for this study was comprised of 800 students; 400 male and 400 female students.

Measures of concepts

Online exposure has two questions. The first question aim to measure the frequency of using internet while the other question is to measure the frequency of using different social media platforms like, Facebook, Instagram, Twitter, WhatsApp, YouTube, E-mail and Messenger. Likert scale containing five categories from 1 to 5 was provided to answer both the questions, where 1= never, 2 = rarely, 3 = sometimes, 4 = frequently, and 5 = very frequently.

Target suitability is measured through two questions. The aim of these two questions was to measure how often students post their personal information on social media and how often they provide such information to their online contacts. Personal information was measured through 12 items containing different types of personal information that students can potentially share or post online. Likert scale containing five categories from 1 to 5 was provided to answer both the questions, where 1= never, 2 = rarely, 3 = sometimes, 4 = often, and 5 = very often.

While online victimization is measured through forty-six (46) statements, which includes statements about online harassment, online identity theft, receiving online uninvited material, viruses and hacking. The mean score of all these forty-six (46) statements is treated score of an individual online victimization. Cronbach Alpha=0.911. The statements of online victimization were answered through using five-point Likert scale, where 1 means never, 2 means rarely, 3 means sometimes, 4 means often and 5, means very often.

Hypotheses

H1: Online exposure of students has statistically significant relationship with their chances of online victimization.

H2: It is more likely that students who share their personal information on their social media accounts are likely to face significantly higher rate of online victimization.

H3: It is more likely that students who provide information to online contacts are suitable targets and are likely to face significantly higher rate of online victimization.

RESULTS OF THE STUDY

To test these hypotheses, multiple regression was used for online victimization. Multi-collinearity test was used to assess the interdependency of independent variables. The test revealed that there was no collinearity among the independent variables. The alpha level was fixed .05.

Effects of online exposure on online victimization

Table no. 01 shows the results for multiple regression performed to predict the effects of internet use and various social media platforms on online victimization. F (8, 791), = 385.44, p= .000 shows significant relationship between the variables. Adjusted R2=.79 suggested that the overall model explains 79% of the variation in the online victimization due to Internet, Facebook, Instagram, Twitter, WhatsApp and Messenger. While YouTube and Email in the model has no significant relationship with online victimization. One unit increase in internet use will increase online victimization by .17 units (M=3.69; SD=.97; β=.17 and p=.000), using Facebook will increase online victimization by.50 units (M=2.34; SD=.85; β=.50 and p=.000), using Instagram will increase online victimization by .23 units (M=2.08 ; SD=.95 ; β=.23 and p=.000), using Twitter will increase online victimization by .04 units (M=2.30; SD=1.40; β=.04 and p=.014), and WhatsApp will increase online victimization by .16 units (M=2.56; SD=.92; β=.16 and p=.000). While using Messenger will increase online victimization by .09 units (M=2.58; SD=1.10; β=.09 and p= .000). These results show that social media use can lead to online victimization of young students. YouTube is a video sharing platform, where direct interaction among the users of the platform is very scars. Most commonly the comments are related to videos shared. Therefore, it is understandable why YouTube is not associated with online victimization. Though previous literature suggested that Email services are major source of one or the other kind of online victimization, nevertheless, use of email system among young school going children is very minimal.

Table 1: Multiple regression analysis for effects of online exposure on online victimization

	Mean	Std. Deviation	Std. Error	β	Sig.
Internet	3.69	.97	.01	.17	.000
Facebook	2.34	.85	.02	.50	.000
Instagram	2.08	.95	.01	.23	.000
Twitter	2.30	1.40	.01	.04	.014
WhatsApp	2.56	.92	.01	.16	.000
YouTube	3.68	1.21	.01	-.02	.377
Email	1.26	.61	.02	.01	.654
Messenger	2.58	1.10	.01	.09	.000
Adjusted R^2=.79 F=385.44 *P*=.000					

Effects of online openness on victimization

Table no. 02 shows the results of multiple regression performed to predict the effect of posting personal information on social media sites on online victimization. F (12, 787), = 263.11, p= .000 shows significant relationship between the variables. Adjusted R2=.80 suggested that the overall model explains 80% of the variation in online victimization due to gender, photograph, contact number, school information, co-curricular activities, emotional distresses, family disputes and video. While personal aims & objectives and audio variables in the model has no significant relationship with online victimization. One unit increase in using to gender will increase online victimization by .08 units (M=2.33; SD=.95; β=.08 and p= .000), photograph will increase online victimization by .07 units (M=2.24; SD=.99; β=.07 and p= .000), contact number will increase online victimization by .09 units (M=1.97; SD=.93; β=.09 and p= .000), school information will increase online victimization by .07 units (M=2.28; SD=.99; β=.07 and p= .000), co-curricular activities will increase online victimization by .16 units (M=2.18; SD=.88; β=.16 and p= .000), emotional distresses will increase online victimization by .245 units (M=2.01; SD=.81; β=.25 and p= .000), family disputes will increase online victimization by .23 units (M=1.92; SD=.87; β=.23 and p= .000), while, video will increase online victimization by .30 units (M=2.05; SD=.85; β=.30 and p= .000). However, there are few unusual results as well in these findings. For example, Age and description of oneself predicted negative relationship with the online victimization of young students. Which means that the more students share their age and describe their selves, less will be the victimization, which is against the current literature and common wisdom. The answer to this novelty might be explained partially by looking at the standard deviation of these variables. Compared to other variables that have significant relationship with the online victimization, age and description of oneself has higher standard deviation values (1.25 and 1.11 respectively) which show higher spread of data along the measurement scale. This discrepancy could have led the result towards negative side. However, further research must look into this and ascertain the relationship between the variables.

Table 2: Sharing personal information on social media as a determinant of online victimization

	Mean	Std. Deviation	Std. Error	β	Sig.
Age	2.60	1.25	.09	-.06	.001
Gender	2.33	.95	.01	.08	.000
Photograph	2.24	.99	.01	.07	.000
Contact number	1.97	.93	.01	.09	.000
School information	2.28	.99	.01	.07	.000
Co-curricular activities	2.18	.88	.01	.16	.000
Personal aims & objectives	2.56	1.24	.01	.01	.544
Emotional distresses	2.01	.81	.02	.25	.000
Family disputes	1.92	.87	.01	.23	.000
Self-Description	2.05	1.11	.01	-.09	.000
Audio	2.00	1.06	.01	-.02	.325
Video	2.05	.85	.02	.30	.000

Adjusted R^2= .80 **F= 63.11** ***P*= .000**					

Providing personal information and victimization

Multiple regression was performed to predict the effect of providing personal information to online contact on social media sites on online victimization. F (12, 787), = 235.43, p= .000 shows significant relationship between the variables. Adjusted R2=. 78 suggested that the overall model explains 78% of the variation in online victimization due to gender, Photograph, contact number, school information, co-curricular activities, emotional distresses, family disputes and video. While personal aims & objectives and Self-Description variables in the model have no significant relationship with online victimization. One unit increase in using to gender will increase online victimization by .12 unit (M=2.24 ; SD=.96 ; β=.12 and p= .000), photograph will increase online victimization by .16 unit (M=2.14 ; SD=.92 ; β=.16 and p= .000), contact number will increase online victimization by .30 unit (M=2.30 ; SD=.87 ; β=.30 and p= .000), school information will increase online victimization by .16 unit (M=2.41; SD=.93; β=.16 and p= .000), co-curricular activities will increase online victimization by .08 unit (M=2.35; SD=.92; β=.08 and p= .000), emotional distresses will increase online victimization t by .160 unit (M=2.30; SD=.97; β=.16 and p= .000), family disputes will increase online victimization by .21 unit (M=2.23; SD=.97; β=.21 and p= .000), while, video will increase online victimization by .05 unit (M=2.47 ; SD=1.08; β=.05 and p= .006). The results for age and audio are negative related with the online victimization. As explained in the previous table, the higher standard deviation is responsible for such novel results.

Table 3: Providing personal information to online contacts as a determinant of online victimization

	Mean	Std. Deviation	Std. Error	β	Sig.
Age	2.47	1.22	.01	-.08	.000
Gender	2.24	.96	.01	.12	.000
Photograph	2.14	.92	.01	.16	.000
Contact number	2.30	.87	.02	.30	.000
School information	2.41	.93	.02	.17	.000
Co-curricular activities	2.35	.92	.02	.08	.000
Personal aims & objectives	2.48	1.24	.01	-.01	.550
Emotional distresses	2.30	.97	.01	.16	.000
Family disputes	2.23	.97	.01	.21	.000
Self-Description	2.11	1.19	.01	-.03	.158
Audio	2.15	1.08	.01	-.04	.024
Video	2.47	1.08	.01	.05	.006
Adjusted R^2=.78 **F=235.43** ***P*=.000**					

DISCUSSIONS

According to Álvarez-García, Pérez et al. (2015), technological variables such as frequency of use and use of various social media platforms are significant risk factors for online victimisation. Both factors increase the likelihood of online victimisation. This study found that people who use internet and social media become a more "suitable target". This study identified a significant relationship between internet use and online victimization of the students. Furthermore, consistent with earlier research (Hinduja and Patchin 2008), the findings indicated that the higher exposure to social media may increase the threats of online victimization, these results are in line with the earlier studies (Bossler and Holt 2009, Ngo and Paternoster 2011, Wilsem 2013). Reyns, Henson et al. (2011) discovered that four online exposure variables: number of social media updates, variety of social media, photos on social media, and instant messenger are statistically significant predictors of online victimisation. This study also yielded nearly identical results to the previous study conducted by Reyns, Henson et al. (2011). Confirming the current study's findings is the Zhou, Tang et al. (2013) study, which found that social media sites increase the likelihood of online victimisation. Specifically, social media sites that are commonly used for entertainment, instant messaging, information searches, and the sharing

of information. Social media sites, in particular, which are frequently used for entertainment, instant messaging, information searches, and the sharing of personal information, are more likely to be victimised online. According to a 2013 survey, the most likely sources of online victimisation were ask.fm, facebook, and twitter (Butterly 2013). Instagram was the most popular platform for online victimisation in 2017. (Wakefield 2017). The majority of respondents experienced online victimisation on Instagram (42%), Facebook (37%), and Snapchat (31%). (Grigonis 2017). According to the current study in the United States, chatrooms and social media platforms have served as a breeding ground for online victimisation (Mesch 2009). More than 70% of survey respondents said social networking sites are not effective to prevent online victimisation (Grigonis 2017). Social media platforms, like in other parts of the world, are also prevalent in Pakistan. Most of Pakistani teenagers frequently use social media platforms, and this number is likely to increase. Individuals posting private information are more likely to face online victimisation because the act provides information about the target to the potential assailant. Those who willingly provide such personal information are also a suitable target, and they are victims of online victimisation (Hinduja and Patchin 2008, Marcum, Higgins et al. 2010, Bossler, Holt et al. 2012). According to this and previous studies (Peluchette, Karl et al. 2015), careless posting of content on social networking sites was identified as an important factor in online victimisation. According to the Routine Activity Theory, people who post data about themselves fit the profile of an "attractive target," because posting and sharing inappropriate content on social networking sites gives others the opportunity to offend someone. Moreover, consistent with earlier research (Staksrud, Ólafsson et al. 2013) increasing the number of social media friends may enhance the risk of online victimization, because there is a high probability of potential offenders among these contacts. Self-disclosure was also found to be an important predictor of online victimisation in earlier studies (Dredge, Gleeson et al. 2014, Kokkinos and Saripanidis 2017). This emphasizes the victim's role in online victimisation because it is this data that the offenders use. Moreover, in accordance to earlier research (Peluchette, Karl et al. 2015, Kokkinos and Saripanidis 2017) self-disclosure has been positively associated with the threat of being victimized. This is also in line with the Routine Activity Theory and emphasize the role of an active victim, whose behavior could provoke online victimization mechanism, possibly by providing fit data to the perpetrator.

CONCLUSION

The young generation is familiar with the use of online available opportunities, and they spend extensive amounts of time online. This study focused on studying effects of using internet and social media platforms on the chances of online vicitimization of school going children in Pakistan and analyzed the factors responsible for making these students into suitable targets. The study suggested significant relationship of student's internet and social media use with online victimization. As a result, the null hypothesis is not accepted, and the research hypothesis (H1) is supported which stated that “online exposure of students has statistically significant relationship with their chances of online victimization ".

Sharing and providing private information in online spaces and to online links have been investigated in the context of routine activity theory. The results predicts that careless posting and sharing of private information is associated with higher levels of online victimization. In terms of online behaviour, sharing/posting of personal information online like; gender, photograph, contact number, school information, co-curricular activities, emotional distresses, family disputes and video has significant relationship with chances of facing online victimization. While personal aims & objectives and audio has insignificant relationship with online victimization. Result also accepted the research hypothesis (H2) that “It is more likely that students who share their personal information on their social media accounts are likely to face significantly higher rate of online victimization ". This study specified that posting of personal information increased the likelihood of victimization measured in the current study. With regard to providing of personal information to online contact like; gender, photograph, contact number, school information, co-curricular activities, emotional distresses, family disputes and video has significant relationship with chances of facing online victimization. While personal aims & objectives and Self-Description has insignificant relationship with online victimization. Thus the null hypothesis is not accepted, and the research hypothesis (H3) is supported which stated that “It is more likely that students who provide information to online contacts are suitable targets and are likely to face significantly higher rate of online victimization". The current

study suggested that providing personal information to online links increased the probability of victimization measured in this study.

IMPLICATIONS OF THE STUDY

The present research provides valuable insights into the relationships among variables within a specific context and contributes new knowledge to the existing body of research. It offers empirical, theoretical, methodological, and practical contributions, making it a significant addition to the current database. The study further provides recommendations for policymakers, particularly those associated with higher secondary education institutions in a developing nation like Pakistan, to reevaluate their education policies. Additionally, it offers suggestions for future scholars to explore the studied variables further, enabling a deeper understanding of online victimization and its implications.

To enhance online security and protect against data breaches, this study suggests several precautionary measures for internet users. Firstly, individuals should avoid oversharing personal information in public posts to minimize the risk of exposure. Secondly, users are advised to control their privacy by regularly reviewing security and privacy settings on their online accounts. Thirdly, login information should be frequently checked to detect unauthorized access, and ad tracking should be disabled to prevent social media platforms and other websites from monitoring user activity. Lastly, users are encouraged to turn off location-sharing features to maintain anonymity and avoid being targeted by online predators.

This study also outlines several recommendations for policymakers to address online victimization in Pakistan effectively. To bridge the digital divide, it emphasizes the removal of social, safety, and financial barriers that hinder equitable internet access. It advocates for training law enforcement agencies and implementing gender-responsive measures to ensure the safety of vulnerable groups. Furthermore, the government should enact comprehensive legislation on data protection and digital privacy to create a more secure online environment.

The report highlights the need to shift the national online crime-related complaints portal to a more user-friendly online platform, replacing the current cumbersome system. Adequate resources should be allocated to the Federal Investigation Agency's (FIA) National Response Centre for online crime to improve its capacity for addressing cybercrimes. Additionally, local police should be empowered to process cases of online harassment effectively. Judges should also be trained in online crime laws, internet governance, and online harassment to handle cases more efficiently.

Moreover, the study recommends introducing mechanisms to address cases involving foreign jurisdictions and decriminalizing defamation laws to align them with international human rights standards. It also calls for FIA's online crime wing to collaborate with civil society, academia, the media, and community-based organizations to raise public awareness and develop preventive measures against online victimization.

This research not only contributes to the academic understanding of online victimization but also provides actionable strategies for policymakers, law enforcement agencies, and the general public. By implementing these recommendations, stakeholders can work collectively to create a safer digital environment and reduce the prevalence of online victimization, particularly among vulnerable groups such as teenagers.

REFERENCES

Ali, K. (2021). 2020 saw 70pc increase in cyber harassment complaints: report. Dawn. Islamabad.

Álvarez-García, D., J. C. N. Pérez, A. D. González and C. R. Pérez (2015). "Risk factors associated with cybervictimization in adolescence." International Journal of clinical and health psychology 15(3): 226-235. https://doi.org/210.1016/j.ijchp.2015.1003.1002.

Aslam, S. and N. Wahab (2022). FIA received 95,567 cybercrime complaints in 2021. The News. Lahore.

Avais, M. A., A. Wassan, H. Narejo and J. Khan (2014). "Awareness regarding cyber victimization among students of University of Sindh, Jamshoro." International Journal of Asian Social Science 4(5): 632-641.

Bossler, A. M. and T. J. Holt (2009). "On-line activities, guardianship, and malware infection: An examination of routine activities theory." International Journal of Cyber Criminology 3(1).

Bossler, A. M., T. J. Holt and D. C. May (2012). "Predicting online harassment victimization among a juvenile population." Youth & Society 44(4): 500-523. https://doi.org/510.1177/0044118X1140752.

Butterly, A. (2013). "'Growing trend'of cyberbullying on social networks." BBC News, October 2.

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

Choi, K.-s. (2015). Cybercriminology and digital investigation, LFB Scholarly Publishing.

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

Dredge, R., J. Gleeson and X. De la Piedad Garcia (2014). "Presentation on Facebook and risk of cyberbullying victimisation." Computers in Human Behavior 40: 16-22. https://doi.org/10.1016/j.chb.2014.1007.1035.

Grigonis, H. (2017). "Cyberbullying happens more often on Instagram, a new survey suggests." Digital Trends.

Hafeez, E. (2014). "Cyber Harassment and Its Implications on Youth in Pakistan." Horizons 8(2): 29-48.

Hinduja, S. and J. W. Patchin (2008). "Cyberbullying: An exploratory analysis of factors related to offending and victimization." Deviant behavior 29(2): 129-156. https://doi.org/110.1080/01639620701457816.

Hinduja, S. and J. W. Patchin (2008). "Personal information of adolescents on the Internet: A quantitative content analysis of MySpace." Journal of adolescence 31(1): 125-146. https://doi.org/110.1016/j.adolescence.2007.1005.1004.

Hinkin, T. R. (1998). "A brief tutorial on the development of measures for use in survey questionnaires." Organizational research methods 1(1): 104-121. https://doi.org/110.1177/109442819800100106

Jamal, S. (2020). "Cyber harassment on the rise in Pakistan, report says." Retrieved February 19, 2022, from https://gulfnews.com/world/asia/pakistan/cyber-harassment-on-the-rise-in-pakistan-report-says-1.72354581.

Khan, A. U. (2020). Cyber Communication's Threats and Responses: A Case Study of University Students of Khyber Pakhtunkhwa, Pakistan. Doctor of Philosophy Gomal University, Dera Ismail Khan, Pakistan.

Khan, A. U., A. Ali, S. Ullah, R. Ishaq, F. Shahzad, F. Ullah, M. Z. Assadi and M. H. B. Salih (2021). "Target Suitability as a Factor of Online Harassment: Case of University Students in Khyber Pakhtunkhwa Province of Pakistan." LINGUISTICA ANTVERPIENSIA: 4788-4799.

Kokkinos, C. M. and I. Saripanidis (2017). "A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter?" Computers in Human Behavior 74: 235-245. https://doi.org/210.1016/j.chb.2017.1004.1036.

Marcum, C. D., G. E. Higgins and M. L. Ricketts (2010). "Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory." Deviant Behavior 31(5): 381-410. https://doi.org/310.1080/01639620903004903

McLuhan, H. M. (1966). "Marshall McLuhan." Information Theory: 234.

Mesch, G. S. (2009). "Parental mediation, online activities, and cyberbullying." Cyberpsychology & behavior 12(4): 387-393. https://doi.org/310.1089/cpb.2009.0068.

Messner, S. F., Z. Lu, L. Zhang and J. Liu (2007). "Risks of criminal victimization in contemporary urban China: An application of lifestyle/routine activities theory." Justice Quarterly 24(3): 496-522. https://doi.org/410.1080/07418820701485429.

Näsi, M., A. Oksanen, T. Keipi and P. Räsänen (2015). "Cybercrime victimization among young people: a multi-nation study." Journal of Scandinavian Studies in Criminology and Crime Prevention 16(2): 203-210. https://doi.org/210.1080/14043858.14042015.11046640.

Ngo, F. T. and R. Paternoster (2011). "Cybercrime victimization: An examination of individual and situational level factors." International Journal of Cyber Criminology 5(1): 773.

Ofcom. (2016a). "Children and parents: Media use and attitudes report." Retrieved October 31, 2021, from www.ofcom.org.uk/data/assets/pdf_file/0034/ 93976/ Children-Parents-Media-Use Attitudes-Report-2016.pdf.

Özdemir, Y. (2014). "Cyber victimization and adolescent self-esteem: The role of communication with parents." Asian Journal of Social Psychology 17(4): 255-263. https://doi.org/210.1111/ajsp.12070.

Peluchette, J. V., K. Karl, C. Wood and J. Williams (2015). "Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem?" Computers in Human Behavior 52: 424-435. https://doi.org/410.1016/j.chb.2015.1006.1028.

Reyns, B. W. (2015). "A routine activity perspective on online victimisation: Results from the Canadian General Social Survey." Journal of Financial Crime: https://doi.org/10.1108/JFC-1106-2014-0030.

Reyns, B. W. and B. Henson (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. https://doi.org/1110.1177/0306624X15572861.

Reyns, B. W., B. Henson and B. S. Fisher (2011). "Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization." Criminal justice and behavior 38(11): 1149-1169. https://doi.org/1110.1177/0093854811421448.

Reyns, B. W., B. Henson and B. S. Fisher (2012). "Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students." Deviant Behavior 33(1): 1-25. https://doi.org/10.1080/01639625.01632010.01538364.

Staksrud, E., K. Ólafsson and S. Livingstone (2013). "Does the use of social networking sites increase children's risk of harm?" Computers in human behavior 29(1): 40-50. https://doi.org/10.1016/j.chb.2012.1005.1026.

Wakefield, J. (2017). "Instagram tops cyber-bullying study." Retrieved October 6: 2019.

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. https://doi.org/410.1177/1043986213507402.

Yar, M. (2005). "The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory." European Journal of Criminology 2(4): 407-427. https://doi.org/410.1177/147737080556056.

Zahid, Luavut and N. Dad. (2017). " Measuring Pakistani women's experiences of online violence." Retrieved October 31, 2021, from https://digitalrightsfoundation.pk/wp -content/uploads/ 2017 /05/Hamara-Internet-Online-Harassment-Report.pdf.

Zhou, Z., H. Tang, Y. Tian, H. Wei, F. Zhang and C. M. Morrison (2013). "Cyberbullying and its risk factors among Chinese high school students." School psychology international 34(6): 630-647. https://doi.org/610.1177/0143034313479692.