P-ISSN: 2790-6795	Annals of Human and Social Sciences	Jul-Sep 2022,Vol. 3, No. 2
O-ISSN:2790-6809	http://doi.org/10.35484/ahss.2022(3-II)43	[453-464]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

Cyber-Crime Victimization through Social Media: An Exploratory Study of Victims in Hyderabad, Pakistan

[1]Hyder Ali Memon* [2]Rashid Wassan [3]Jahangir Ansari

1. Lecturer, Department of Criminology, University of Sindh, Jamshoro, Pakistan
2. Advocate Sindh High Court, Hyderabad, Sindh, Pakistan
3. Deputy Superintendent of Police at Girls Rescue Center, Jamshoro, Sindh, Pakistan

***Corresponding Author** hyder.memon@usindh.edu.pk

ABSTRACT

This qualitative exploratory study used data from Hyderabad, Sindh law enforcement authorities. The researcher interviewed 30 cybercrime victims, 14 females and 16 males aged 19-32, and also collected factual records of 349 social media-related cybercrimes. The study's goals were achieved using thematic analysis. The study's goals are to determine which types of cybercrime are committed on social media, which platform is most often used, and the characteristics of cyber victims. According to the findings, the most common social media cybercrimes are investment/financial scams, online job fraud, sending obscene content, harassment, defamation, religious hate content, and identity theft. Moreover, Facebook, WhatsApp, Gmail, TikTok, Messenger, Twitter, and LinkedIn are all popular cybercrime victimization sites. Interviews with cyber victims highlighted the hallmarks of online victimization, including cyber-relationship addiction, wanting attention/popularity, compulsive online purchasing, and gullibility. The accompanying research also offers practical suggestions for preventing social media cyber victimization.

Keywords: Compulsive Online Purchasing, Cyber-Criminality, Cyber-Victimization, Employment Fraud, Investment/Financial Scams, Social-Media Platforms, Victimizing Characteristics

Introduction

In the past two decades, there has been an increase in the usage of the internet and digital accessories. The development of digital technology has produced several advantages, such as e-services, speedier communication, online banking, and online social networking (Arpad, 2013). However, the development has resulted in grave consequences, such as hacking, scamming, cyberstalking, and cyber criminality (Aiken et al., 2016). All of these effects are referred to collectively as cybercrime. Electronic theft, fraud, and bullying have compromised the positive image of technology and the internet. However, the prevalent view continues to portray the internet as the sole source of global progress, prosperity, and socioeconomic advancements (Kamruzzaman et al., 2016). Cybercrime has been an essential topic of study for criminologists and an increasing concern for public policy over the past two decades. Cybercrime primarily refers to crimes conducted using computers and computer networks, but it also encompasses crimes that do not rely substantially on technology (Holt, 2017).

Meanwhile, social media platforms are crucial in incorporating digital communication into everyday life. Social media are distinguished from conventional media by accessibility, usability, originality, and longevity (Lewis et al., 2008). These platforms that allow users to log in with either real or fake identities add to the complexity of the virtual world (Karadag, 2010) & (Muzaffar, Yaseen, & Safdar, 2020). The perception of social media as a platform that provides unrestricted freedom and its unrestricted use raises several problems (Baughman, 2009; Maranto & Barton, 2010). This incident has prompted the discussion of cybercrime, cyber harassment, and cyberbullying (Lee & Cho, 2011). Social

media delivers substantial benefits, including amusement, economic engagement, and marketing advantages, following and responding to advances, freedom of speech, communication and information access, organizing, and socialization. On the other hand, it has negative characteristics such as addiction, information contamination, ethical issues, a sense of isolation, shallowness, and time loss (Kocak, 2012).

Cybercrime in Pakistan has a long history; however, it has increased since the introduction of third-generation (3G) and fourth-generation (4G) mobile networks. These are the fastest networks for connecting mobile devices or phones to the internet. These networks enable cybercriminals to assault cyberspace. Cyberspace is the virtual arena where all cyber activities occur, whereas cybercriminals use technology and cyberspace to perpetrate criminality. Cybercrime is comprised of hacking, cyber theft, cyber extortion, and cyber-terrorism. (Ullah, 2018). The internet has affected every aspect of society, including social, religious, cultural, and personal spheres. However, this influence has created a massive challenge in the form of cybercrime, particularly for a developing nation like Pakistan. It has severely threatened cyberspace's individuals, businesses, organizations, and other users. Unlike other types of crime, this threat has aggravated the stability of the entire social order. Various segments of society view cyber-engaged youth as deviants.

On the other hand, most young people pay no attention to acquiring fundamental and necessary knowledge before accessing or entering cyberspace or a platform such as social media sites and websites. This disregard has driven many youngsters into cyber chaos. Although cybercrime is not a new problem, its escalation over the previous decade pushed the Pakistani government to enact comprehensive legislation (Khan, 2016). In 2016, the government submitted a new bill known as the Pakistan Electronic Crime Act (PECA) to revise the existing cyber laws. The purpose of this bill was to punish many forms of cybercrime, including cyberterrorism and child pornography. In response to PECA, the Pakistani human rights commission (HRCP) has labeled it an infringement on the right to free speech. According to Yamin (2021), cybercrime has remained a low priority for Pakistan; hence, we lag behind other nations in preventing and limiting cyberattacks.

Most studies conducted in Pakistan are based on secondary research that examines the nature and scope of cybercrime and issues pertaining to its investigation and prosecution. However, there is a lack of primary research conducted on the characteristics of the victims and what types of cybercrimes are most commonly committed through social media. To address these challenges, the current exploratory study aims to carryout primary research to enhance the criminological understanding of cybercrimes committed through social media.

Literature Review

The internet has brought tremendous opportunities to people globally, including criminal potential (Reyns et al., 2011). The internet enables people to connect with others, communicate with family and friends, form new relationships, generate social capital, and grow their social networks. It enables non-collocated and non-face-to-face engagement (Bossler & Holt, 2009); (Muzaffar, Chohdhry, **&** Afzal, 2019). Social Media and Political Awareness in Pakistan: A Case Study of Youth**,** *Pakistan Social Sciences Review*, 3 (II), 1-13. Arguably, the internet has revolutionized the manner in which people communicate and interact to the extent that it has affected habits and lifestyles (Bossler et al., 2012). Social networking platforms such as Twitter, Instagram, and Facebook are not free from these actions that occur across the internet's many features (Reyns et al., 2012).

In terms of cyberspace victimization, various characteristics or habits of the end-user will increase their vulnerability to cyber criminals. According to Van Wilsem (2013), the availability of personal information (pictures, sexual orientation, relationship status, and gender) via an instant messenger or social media is sufficient for cybercriminals to

target potential victims. In addition, engaging in online deviant behavior (such as posting insulting comments or sending sexually explicit images) or chatting with strangers can increase the likelihood of being a victim of cybercrime (Henson et al., 2013). In addition, a study conducted by Holtfreter and Meyers (2015) revealed that end-users with a low level of self-control, a high level of engagement in remote shopping, frequent use of instant messaging, and a habit of downloading music or movies from an unreliable website are more likely to become victims of cybercrime.

According to a new Eurobarometer survey, Internet users are highly concerned about cybersecurity, and 85 percent say that the likelihood of becoming a victim of cybercrime is rising. The two most common concerns are identity theft (68%) and harmful software (66%). Since 2013, the levels of anxiety have increased, indicating that Internet users perceive the virtual environment to be growing more unpredictable and less secure (TNS Opinion & Social, 2015). Moreover, cyberbullying, cyber harassment, and cyber impersonation, to name a few, are just a few examples of the new illegal acts that the internet has facilitated.

A considerable amount of research indicates that age plays a crucial role in online fraud victimization (Arfi & Agarwal, 2013; Norris et al., 2019). Due to a lack of self-control, young adults, particularly those between the ages of 18 and 25, are more prone to become victims of online fraud (Roberts et al., 2012). According to anecdotal evidence, a lack of self-control and a high level of risk-taking are anticipated to be the fundamental causes that lead young adults to browse the dark web and purchase counterfeit goods from fake versions of trusted websites. In addition, this circumstance will undoubtedly enhance their likelihood of engaging in unauthorized financial activities, increasing their likelihood of becoming a victim of online fraud.

Pakistan also faces the hazards and dangers of cybercrime, and the Federal Investigation Agency (FIA) and Police are detaining cybercriminals from Bahawalpur and Peshawar, such as gangs and young university students (Manzar et al., 2016). Internet users in Pakistan are oblivious to cyber risks, with only a few victims emphasizing the urgency and importance of preventing them. In Pakistan, cybercriminal practices and the misuse of technology can be countered by prohibiting particular websites, channels, and sources (Ahmed & Khan, 2015; Munir & Gondal, 2017). Cybercrime in Pakistan varies from rude text message transmission to online pornography (Munir & Gondal, 2017). According to the National Response Centre for Cybercrime (NR3C) of FIA, 10% to 16% of Pakistan's population are active internet users who use the internet for social networking, online banking, internet browsing, communication, entertainment, online purchases, map directions, online learning and auction, data transmission, medical services, and computer gaming. In 2012, the police apprehended members of a Bahawalpur-based gang that had stolen millions of rupees by hacking bank accounts and credit card details and forging National Bank of Pakistan vouchers. The FIA has arrested university students in Peshawar and other locations for blackmailing women through hacking and defacement.

In addition, multiple reports of unregistered Subscriber Identity Modules (SIMs) being used to threaten and extort individuals have been reported. Only in Dera Ghazi Khan were 1415 illegally obtained mobile phone SIM cards seized. In Pakistan, even the government has been victimized. A hacker using the moniker 'Zombie_ksa' hacked and vandalized the website of the Supreme Court of Pakistan. He uploaded content critical of the judiciary and the Chief Justice and urged that pornographic websites are outlawed, and the impoverished be helped (Manzar, 2016).

The research indicates that cybercrime complaints in Pakistan increased by 83 % between 2018 and 2020. In 2018, the Cyber Crime Wing handled 16,122 complaints; by 2020, that number is expected to exceed 94,000. 60 % of the complaints were filed in the previous year, 30 percent in 2019, and 10 % in 2018. During the past three years, more than

44,000 financial fraud-related complaints were received and resolved. From 2018 to 2020, there were 22,255 harassment complaints, 15,000 hacking complaints, 10,358 defamation complaints, and 16,601 reports of bogus profiles (The News International, 2021).

In the past three years, cybercrime has surged by 83%, with financial scams leading the way. In 2020, the FIA (Federal Investigation Agency) captured approximately 30 gray trafficking entry points. Financial scams, phony profiles, harassment, hacking, and defamation are the most rapidly growing cybercrimes in the United States, according to the statistics. E-mail, WhatsApp, and Facebook are the most common cybercriminal tools. Throughout the years 2018 through 2021, Facebook remained on top with 62,357 complaints. The agency uncovered roughly 104 fraudulent transactions, primarily in the Ehsaas Programme, and initiated 95 inquiries and 10 cases, resulting in the arrest of 22 perpetrators and the recovery of approximately Rs4m.

Furthermore, the data indicates that cybercrime complaints have gradually increased in Pakistan's major cities during the previous three years. Lahore registered more than 19,000 complaints in 2020, Karachi more than 12,000, Islamabad 11,126, Rawalpindi 9,780, Multan 8,573, Faisalabad 7,273, and Gujranwala 5,323 registered complaints, respectively. These are the five cities with the highest reported cybercrime incidents during the past three years (Pakistan Observer, 2022).

Material and Methods

The data for the following study was gathered using the qualitative research approach, which involved conducting in-depth interviews with victims of social media cybercrimes. This method of collecting primary data was carried out by visiting the Law Enforcement Agency located in Hyderabad, Sindh, in November 2022, where all the details of the victims were collected, such as their contact numbers, e-mail, home addresses, detail of cases, a total of (30) victims (14) females and (16) males aging 19 to 32 were selected using random sampling technique, and later on, the researcher contacted these victims personally through phone number. When the victims agreed to share their stories, the researcher met the victims in their homes or offices to conduct detailed, in-depth interviews. All interviews were audio recorded, and the researcher avoided using questionnaires because they could interfere with the free flow of discussion in sensitive matters. Besides that, the initial interviews were conducted in Urdu; all audios were translated and transcribed into English. In addition, the researcher also gathered factual information from the agency, which facilitated it to examine the first two objectives of the study. In order to get the desired research conclusions, the researcher employed thematic analysis to analyze the collected data.

Results and Discussion

The information obtained from the Law enforcement agency, which included specifics of 349 different cases, was crucial in the establishment of the first two objectives of the study, which are 1) To identify the nature and types of cybercrimes perpetrated using social media and 2) To explore through which social media platform victims are most commonly victimized on. Following a comprehensive analysis of the data that was acquired, all of the data was then transferred into Excel to create figures to calculate the actual percentage that had been achieved in relation to the objectives.

According to the study's first objective, the findings revealed (07) of the most prevalent crimes perpetrated via social media, as depicted in (Figure 01) below.

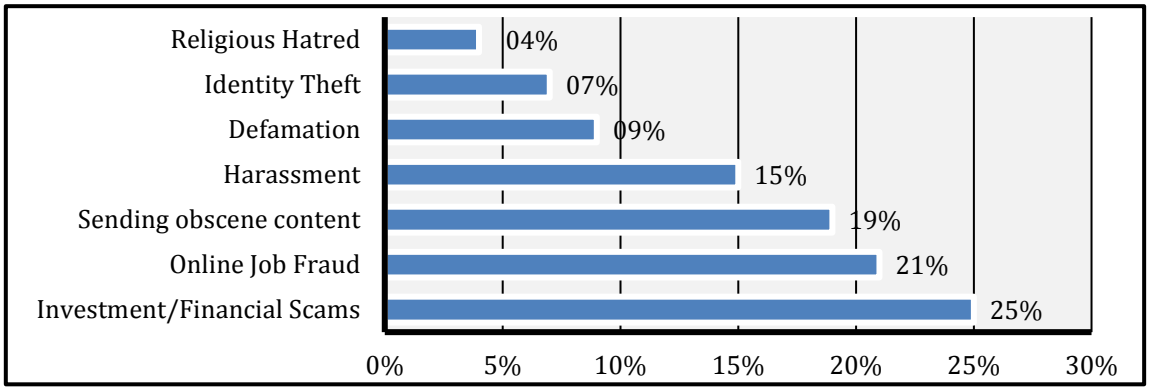

Figure 01: Common Crimes Committed via Social Media

It was discovered in the findings of the research that the most common types of cybercrime that are committed through social media are:

1) **Investment/Financial Scams** (25%) such as Crypto asset-related scams, Ponzi schemes, and Advance fee fraud.

2) **Online Job Fraud** (21%), including e-mailed fake job offers, offering money in exchange for services like typing but first requiring victims to submit a charge, and fake jobs apparently from legitimate employers or companies.

3) **Sending Obscene content** (19%), this included sending indecent or pornographic pictures, videos, audio, messages, and links to the victims.

4) **Harassment** (15%) included cyberstalking, cyberbullying, blackmailing, posting online disparaging remarks, and sending negative and offensive messages to the victims.

5) **Defamation** (09%), including distributing obscenity or other explicit content to the victim with the intent to offend, posting misleading information on the internet that portrays the victim in a bad light, and posting a false written statement about an individual on social media.

6) **Identity Theft** (07%), including creating fake social media accounts with the victim's name, information, and pictures.

7) **Religious Hatred content** (04%) included giving online hate speeches, videos, or live calls, and making fun of other people's religion through comments, chat, and posts.

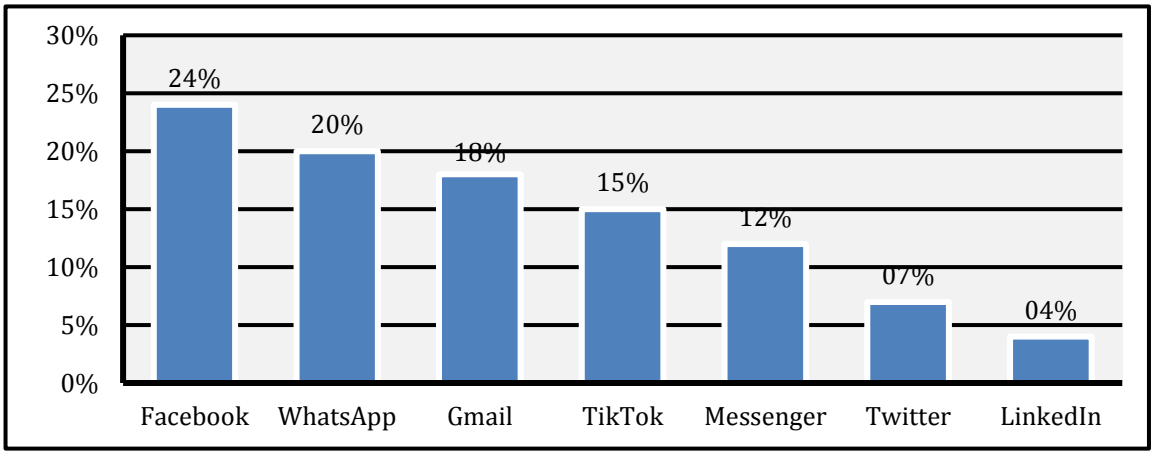

Figure 02: Common Social Media Platforms for Cybercrimes Victimization

Regarding the second purpose of the study, it was revealed that there are (07) the most prevalent social media platforms for cybercrime victimization, as depicted in the following (Figure 02) above.

According to the research findings, the social media sites where cybercrime victimization occurs most frequently are **Facebook** (24%), **WhatsApp** (20%), **Gmail** (18%), **TikTok** (15%), **Messenger** (12%), **Twitter** (07%), and **LinkedIn** (04%).

In addition, the findings of the third objective of the study, which is to determine the characteristics of victims who are typically victimized, data were gathered through interviews with a total of (30) participants, (16) of whom were male and (14) of whom were female, ranging in age from 19 to 32. After analyzing all the interviews, the researchers came up with four common traits among people who become victims of cybercrime. These characteristics are as follows: "Cyber Relationship Addiction," "Seeking Attention/Popularity," "Compulsive Online Purchasing," and "Being Gullible."

The following (Table 01) below depicts the characteristics of the victims, a description of their victimizing characteristics, and the cybercrimes they were mostly victimized of.

Table 1
Characteristics of Victims and Criminal Acts

Victims Characteristics	Description of Characteristics	Become a Victim of Criminal Acts	Male	Female
Cyber-Relationship Addiction	Forming online relationships with strangers or numerous persons simultaneously and exchanging their images and information.	Blackmailing	02	03
		Harassment	Nil	04
Seeking Attention/Popularity	Continuously upload pictures, videos, and information publicly to gain fame, attention, and likes from random people.	Identity Theft	02	01
		Cyberbullying	01	02
Compulsive Online Purchasing	Investing an excessive amount of money in internet purchases and divulging financial information	Investment/financial Scams	03	Nil
		Counterfeit merchandise	02	01
Being Gullible	Quickly become persuaded by what they see and hear on social media.	Online Job Frauds	05	03
		Cyber Theft	01	Nil

According to interviews with victims, they claimed that they became victims of cybercrime through social media by engaging in a cyber relationship(s), with (02) of males and (03) of women being victims of blackmail and (04) of women becoming victims of social media harassment.

Another characteristic of victims was their desire for popularity or attention on the internet, which led to (02) of males and (01) female becoming victims of identity theft, (01) of male and (02) of females becoming victim of cyberbullying.

Furthermore, the victims' compulsive online purchasing led to (03) of males falling victim to Investment/financial scams, while (02) of males and (01) of female fell victim to counterfeit merchandise.

Another characteristic of the victim was gullibility, which led to (05) of males and (03) of females becoming victims of online employment frauds and (01) of male becoming victim of cyber theft.

Social media has demonstrated its usefulness in various facets of life, from organizing a popular uprising against the government to bridging the gap between astronauts and scientific enthusiasts worldwide. With a large amount of data available on social networking sites, there are countless opportunities for applying big data to various fields. The popularity of social media platforms is evident in their 2.22 billion users in 2019, projected to increase to 3.02 billion by 2021 (Soomro, 2019). Social media is generating an avalanche of big data, which we might refer to as big social data, due to its enormous user base. Our data-driven culture may view this as an advantage, but it comes with various evolving issues, including volume, diversity, velocity, veracity, volatility, quality, and exposure. Alongside the obstacles, the productive applications of this vast quantity of big data are limitless in all fields. Social media is a perfect location for anyone seeking a potential customer, an employee to fill a particular position, or a victim of crimes such as burglary, identity theft, or cyberstalking. It is a valuable resource for law enforcement organizations and criminals, just as it is for other professions.

There are three research aims underlying this study. The initial purpose of the study was to determine the nature and classification of cybercrimes committed via social media. The factual data of 349 cases were collected from Federal Investigation Agency FIA in Hyderabad, Pakistan. According to the findings of the research, the most prevalent cybercrimes performed through social media are categorized into seven separate crimes with substantial connections to social media those are: Investment/financial scams, online job fraud, sending obscene content, identity theft, harassment, defamation, and posting or sharing religious hatred content. In their respective studies, Manzar et al. (2016) and lama et al. (2021) reported similar research findings.

Regarding the second purpose of the study, which was to explore through which social media platform victims are most commonly victimized, we found that there are seven most prevalent social media platforms for cybercrime victimization such as; Facebook, WhatsApp, Gmail, TikTok, Messenger, Twitter, and LinkedIn. These forums have produced the most popular communication tools for users, allowing them to share data, personal information, personal photographs, messages, video calls, and thoughts. The widespread use of social media for communication between individuals, organizations, and governments generates new concerns around social media privacy, accessibility, protection, and other personal-related issues (Munir, 2018). On social media sites, users voluntarily disclose their identity and personal information and make details about themselves accessible to the general public. Users might become victims of online harassment and abuse due to malicious activity on social media networks. It is recognized that social networks violate their users' personal rights by disseminating illicit or unauthorized content. Colak et al. (2012) found that providing information through images, home addresses, and location tags increases the likelihood of being targeted by various criminal acts. These platforms that are highly susceptible to manipulation and crime also create trust concerns, mainly owing to the potential for the creation of fraudulent profiles and fictional and suspect identities. With so many negative characteristics and risks, social media platforms are susceptible to criminality. Consequently, the great majority of cybercrime occurs on social media platforms (Erdogdu et al., 2021).

Furthermore, the findings of the third objective of the study, which is to determine the characteristics of victims who are typically victimized, the research found that there are specific characteristics of victims that make them vulnerable to criminals. These qualities include being addicted to online relationships, seeking attention or popularity online, making compulsive purchases online, and having a gullible nature. In the research findings, it was concluded that victims who are addicted to pursuing online relationships with multiple people, some of whom are often unknown or strangers, are frequently victimized by crimes such as blackmailing and harassment and that females are more frequently victimized online by crimes such as harassment and blackmailing than males. These findings

are similar to those of another study conducted in Pakistan by Farid et al. (2018). It was asserted that social media had encouraged generational deviance and that many crimes, including pornography, blackmail, and online harassment, are committed via social networks. It also revealed that these sites are responsible for 56.6% of online harassment and that most victims are females.

According to a second feature of victims, which is seeking attention or popularity through social media platforms, it was revealed that victims are frequently victims of cyberbullying and identity theft owing to their negligence. In order to acquire online fame, these victims do not care about sharing their photographs and information, and as a result, many cybercriminals take advantage of this irresponsible behavior. Some may steal personal information and use it for other unlawful purposes, while others may engage in persistent cyberbullying. According to research conducted by Rafi (2019) in Pakistan, the most common causes of cyberbullying are the victims' careless and naive usage of social media platforms and offline confrontations.

The research found that another behavior that makes victims susceptible to crimes such as investment fraud and counterfeit goods is a propensity for compulsive online shopping and excessive financial investment. The extensive use of social media for shopping provides fraudsters with several opportunities to interact with individuals and commit fraud using various methods. Scammers are constantly devising novel and innovative techniques to rob victims of their money or personally identifiable information that may be used for financial gain. These scams can cause customers significant financial loss, emotional distress, and loss of confidence. According to research by Abbas et al. (2018), the majority of investment frauds in Pakistan occur on sites such as Facebook marketplace, where fraudsters pose as legal online traders. Consumers acquire fraudulent items (e.g., counterfeit clothing or gift cards) or inferior quality (e.g., faulty or substandard). Sometimes, victims pay in advance for things that never arrive. It further stated that in investment fraud, fraudsters offer an investment opportunity that is "too good to be true," but when consumers are enticed to invest, they may lose all of their money.

The last victim attribute discovered in the research was gullibility and the propensity to be readily convinced by what they see and hear on social media; this trait frequently led victims to crimes such as online employment fraud and cyber theft. Online recruitment fraud is a fraudulent practice in which job seekers are tricked into applying for false positions in order to obtain their sensitive information. The repercussions can range from little financial loss to severe identity theft. One of the primary channels for these fraudsters is social networking platforms, and another is online recruitment portals, where a job advertisement can be easily deceived into believing it is genuine. In fact, it is a forgery intended to defraud desperate job searchers (Mahbub et al., 2022). A secondary analysis of the 2014 U.S. "Caught in the Scammers' Net," a national survey of online victimization (N = 1,539), reveals that individuals with low self-control and those who engage in online activities are more inclined to disclose personal information online. As a result, these individuals are more likely to be targeted by fraudulent employment offers (Dodel et al., 2018).

Cybercrime Prevention and Protection Mechanisms in Social Media

- In the same manner that criminals utilize social media to commit crimes, technological innovations can be used to manage, dissuade, protect, and prosecute illegal activity.
- While criminals might use social networking sites to discover potential victims, law enforcement agencies could utilize similar platforms to pursue criminal charges.
- It is urged that all social media users, whether they are individuals or business people, should exercise caution and vigilance while posting personal information that could be exploited against them by criminals.

- Some techniques for managing cyber-crimes include keeping all software up-to-date, knowing friends well, employing current anti-virus software, learning basic security precautions, never disclosing critical information, and utilizing protected and unique passwords.
- Utilize anti-virus, firewall, anti-malware, perfusion framework spam filter, intrusion, and anti-malware software to prevent assaults and respond appropriately. A framework for securing data from social media attacks must be established as a matter of urgency.
- People should verify their bank account and credit card information regularly, not carry all identifying credentials at all times, and not discusses personal information with others to prevent identity theft.
- Understand the security settings of each social media platform and ask for guidance. This will ensure that privacy and settings are appropriately configured.
- Before signing up, social media site developers may provide training videos to social media users. All new users must watch a short video addressing Internet security, personally identifiable information, and network privacy settings when registering for an account. The submit account option should not appear until after viewing the video.

Conclusion

The internet has given people worldwide enormous options, including criminal potential. In the meantime, social media platforms play a vital role in integrating digital communication into daily life. The perception of social media as a platform that allows limitless freedom and its uncontrolled use creates several issues. These platforms, which permit users to log in with either a real or a phony identity, increase the complexity of the virtual world. Social media provides enormous benefits, including entertainment, marketing advantages, freedom of expression, communication, and access to information. On the other side, it has negative attributes such as addiction, information pollution, ethical concerns, a sense of isolation, shallowness, and time loss, as well as cyber harassment, identity theft, and cyberbullying. Most studies in Pakistan on cybercrime are based on secondary research that examines the nature, scope, and prevalence of cybercrime. However, there is a lack of primary research on the characteristics of the victims and the types of cybercrimes that are most frequently committed through social media. In order to address these issues, the current study conducted primary research for a better criminological understanding of cybercrimes perpetrated via social media, using agency data. The data includes information on 349 cases of cybercrime; 30 interviews with cybercrime victims were conducted to acquire additional data. The research findings concluded that cybercrime mainly occurs through social media; Investment/financial Scams, Online Job Fraud, Sending Obscene Content, Harassment, Defamation, Religious Hatred Content, and Identity Theft. It also revealed that social media sites where cybercrime victimization occurs most frequently are Facebook, WhatsApp, Gmail, TikTok, Messenger, Twitter, and LinkedIn. In addition, the data collected through interviews with cyber victims highlighted the four most significant features of online victimization, including cyber-relationship addiction, attention/popularity seeking, compulsive online shopping, and gullibility. In the outcome, the research offered some helpful recommendations for avoiding cyber-victimization. As it was indicated that social media users must grasp the security settings of each social media platform and seek help, social media users must understand the security settings of each social media platform. This will ensure that privacy and settings are correctly set up, and all social media users are asked to exercise caution and awareness when sharing personal information that could be used against them.

References

Abbas, J., Aman, J., Nurunnabi, M., & Bano, S. (2019). The impact of social media on learning behavior for sustainable education: Evidence of students from selected universities in Pakistan. *Sustainability*, *11*(6), 1683.

Abbasi, K. (2021, August 28). Cybercrime increases by 83pc in three years. *The News International*

Ahmed, A., & Khan, D. S. (2015). Cyber Security Issues and Ethical Hacking in Pakistan. *Department of Computer Science Karachi University*.

Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime. *Paladin Capital Group*.

Almadhoor, L. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 2972-2981.

Arfi, N., & Agarwal, S. (2013). Knowledge of cybercrime among elderly. *International Journal of Scientific & Engineering Research*, *4*(7), 1463-1468.

Árpád, I. (2013). A greater involvement of education in the fight against cybercrime. *Procedia-Social and Behavioral Sciences*, *83*, 371-377.

Baughman, L. L. (2009). Friend Request or Foe-Confirming the Misuses of Internet and Social Networking Sites by Domestic Violence Perpetrators. *Widener LJ*, *19*, 933.

Bhatti, N. (2022, June 06). Increasing cybercrimes in Pakistan. *Pakistan Observer*.

Bossler, A. M., & Holt, T. J. (2009). Online activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

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

ERDOĞDU, M., & KOÇYİĞİT, M. (2021). The correlation between social media use and cyber victimization: A research on generation Z in Turkey. *Connectist: Istanbul University Journal of Communication Sciences*, (61), 101-125.

Habiba, U., Farid, N., & Saud, M. (2018). Social networking sites and deviance among youth in Islamabad, Pakistan. *European Journal of Behavioral Sciences*, *1*(1), 48-58.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Does gender matter in the virtual world? Examining the effect of gender on the link between online social network activity, security and interpersonal victimization. *Security Journal*, *26*(4), 315-330.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge.

Holtfreter, K., & Meyers, T. J. (2015). Challenges for cybercrime theory, research, and policy. *The Norwich Review of International and Transnational Crime*, 54.

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

Karadağ, L. (2010). İnternet sizi bekliyor. *İstanbul: Mess Yay., Aralık*.

Khan, R. (2016). Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried. Dawn. *Livingstone, S., Ólafsson, K., & Staksrud, E.(2013). Risky social networking practices among "underage" users: lessons for evidence-based policy. Journal of Computer-Mediated Communication*, *18*(3), 303-320.

Koçak, N. G., & Oyman, M. (2012). Social media usage behaviors of individuals: An application in Eskişehir. *International Journal of Business and Social Science*, *3*(22), 177-188.

Lee, S., & Cho, M. (2011). Social media use in a mobile broadband environment: Examination of determinants of Twitter and Facebook use. *International Journal of Mobile Marketing*, *6*(2), 71-87.

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & Christakis, N. (2008). Tastes, ties, and time: A new social network dataset using Facebook. com. *Social networks*, *30*(4), 330-342.

Mahbub, S., Pardede, E., & Kayes, A. S. M. (2022). Online Recruitment Fraud Detection: A Study on Contextual Features in Australian Job Industries. *IEEE Access*, *10*, 82776-82787.

Manzar, U., Tanveer, S., & Jamal, S. (2016). The incidence of cybercrime in Pakistan.

Maranto, G., & Barton, M. (2010). Paradox and promise: MySpace, Facebook, and the sociopolitics of social networking in the writing classroom. *Computers and Composition*, *27*(1), 36-47.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356-1371.

Munir, A., & Gondal, M. T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition*, *10*(2), 1-23.

Munir, A., & Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review (GPR)*, *3*, 84-97.

Muzaffar, M., Chohdhry, S., **&** Afzal, N. (2019). Social Media and Political Awareness in Pakistan: A Case Study of Youth**,** *Pakistan Social Sciences Review*, 3 (II), 1-13

Muzaffar, M., Yaseen, Z., Safdar, S. (2020). Role of Social Media in Political Campaigns in Pakistan: A Case of Study of 2018 Elections*, Journal of Political Studies, 27* (2), 141-151

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Rafi, M. S. (2019). Cyberbullying in Pakistan: Positioning the aggressor, victim, and bystander. *Pakistan Journal of Psychological Research*, *34*(3), 601-620.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, *38*(11), 1149-1169.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant behavior*, *33*(1), 1-25.

Roberts, J. A., & Manolis, C. (2012). Cooking up a recipe for self-control: The three ingredients of self-control and its impact on impulse buying. *Journal of Marketing Theory and Practice*, *20*(2), 173-188.

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Appl. Comput. Syst.*, *24*(1), 9-17.

TNS Opinion & Social (2015). Special Eurobarometer 423. *Cyber security report.* http://ec.europa.eu/pub lic_opinion/archives/ebs/ebs_423_en.pdf

Ullah, F. (2018). Socio-psychological impacts of cybercrime on youth: A case study of Peshawar. *Khyber Pakhtunkhwa [Unpublished Master of Philosophy dissertation] University of Peshawar*.

Van Wilsem, J. (2013). 'Bought it, but never got it'assessing risk factors for online consumer fraud victimization. *European sociological review, 29*(2), 168-178.

Yamin, D. (2021). Cyberspace Management in Pakistan. *Governance and Management Review*, *3*(1), 46-61.

Yavanoğlu, U., SAĞIROĞLU, S., & ÇOLAK, İ. (2012). Information security threats in social networks and precautions to be taken. *Journal of Polytechnic* , *15* (1), 15-27.