Journal of Social Sciences and Media Studies (JOSSAMS) Volume 7, Issue 2, 2023
ISSN: 2518-8046

Response and Reporting of Cybercrimes in Pakistan – Mass Media as a Mean of Awareness, Prevention, and Protection

Syeda Afsheen Sohail[1], Dr. Fouzia Naz[2]
[1]PhD Scholar, Department of Mass Communication, University of Karachi.
[2]Associate Professor, Department of Mass Communication, University of Karachi.
Corresponding Author: Syeda Afsheen. Email: afsh601@hotmail.com

Abstract

The escalating popularity of the internet has contributed to the augmented rate of cybercrimes across the globe. From financial fraud to cyber bullying, nations, organizations, and individuals are commonly confronting the threats of cybercrimes. Pakistan has also recorded a substantial upsurge in the reported cases of cybercrimes during the last few years. The cybercrime cell working under the Federal investigation Agency is not only providing awareness to internet users about identifying and reporting cybercrimes, but it also takes legal action against the people involved in such activities. Despite these efforts, there is insufficient awareness among the public about their cyber rights. This research paper focuses on the issue of cybercrimes and the response of internet users in Pakistan toward these acts. The data for the study has been collected through a survey conducted online among 250 internet users belonging to Pakistan. The data provide a picture of the current level of awareness among internet users about the reporting procedure for cybercrime and punishments for different crimes determined by the law. The paper also highlights various factors that discourage users from reporting crimes and the response of users toward several types of cybercrimes. The discussion also underlines the role of traditional and new media in this context. The paper also proposes a communication plan to raise awareness and encourage cybercrime reporting in the country to abridge the pervasiveness of such acts.

Keywords: Cybercrime, Cyber Crime Cell, Response and Reporting, Awareness, Crime Prevention

Introduction

The popularity of the internet across the globe is providing a wide array of benefits to individuals and societies (Herath, Khanna & Ahmed, 2022). However, this popularity is also bringing some challenges and threats to the users that comes under the umbrella term ‘cybercrime’ (Appel, Marker & Gnambs, 2020). Cybercrimes could perhaps be considered as the most complicated and most challenging problem that the modern-day encounters in cyber space. Cybercrime is a rapidly growing threat in today's interconnected world, affecting individuals, organizations, and societies alike. Cybercrime can have far-reaching consequences for individuals and organizations, affecting their finances, personal and business operations, reputation, and mental health. There are strong evidence from literature showing the severity and long-term effects of encountering cybercrimes upon the psychological wellbeing of individuals resulting in constant stress, anxiety and even depression. Hence, a healthy functioning society should be aware of the consequences of cybercrimes and need to adopt a proactive approach to prevent the frequent occurrence of such cases (Nikhat et al, 2021).
Pakistan, like many other countries of the world is experiencing massive hike in the numbers of internet users. As the presence of people on online platforms is increasing, the incidents of cybercrimes are also increasing including cyber-attacks, identity theft and financial scams. Although the prevalence of cybercrimes is increasing with each passing day, the level of understanding regarding the nature and extent of cybercrimes is still very limited among the internet users. Moreover, there is insufficient awareness about the reporting mechanism to follow in case of encountering any cybercrime (Bányai, et al. 2019). Consequently, the numbers of cybercrimes reported each year are substantially increasing in Pakistan (Soomro & Hussain, 2019). The meeting of Standing Committee on Information Technology and Telecommunication, Government of Pakistan, held in September 2022 revealed that a rise of 83% in cybercrime cases has been recorded in last three years (Daily Times, 2022). Such incidents are not limited to individuals and organizations, but some government official accounts and websites and military institution’s websites were also hacked causing damage and leakage of sensitive data and information (Munir & Shabir, 2018).

The government of Pakistan has been taking several measures to addressing the rising issue of cybercrimes. Over the last few years, legislation has also been formulated to deal with these issues. Additionally, the government also established a cybercrime2 response and reporting cell that works under FIA. However, most of the experts do not appreciate these efforts and consider them insufficient and ineffective. Lack of adequate resources, sound technology infrastructure and absence of professional training slackens the capability of law enforcement agencies to prevent and deal with cybercrime cases. The low level of awareness among the internet users is also an important issue that is adding to the severity of the problem. It has been observed that most internet users are not completely aware of the rights that the law grants them on cyber space. This is because they usually don’t have adequate and enough information about the cyber crimes and the procedure that they are supposed to follow to register their complaint against cybercrime (Omar, 2021). This research paper is an attempt to display the current situation of cybercrime awareness among the internet users of Pakistan and their usually response towards any such activity. In addition, the research paper suggests some ways through which mass media can effectively be used as tool of creating awareness regarding cybercrimes and the reporting mechanism.

Media and Awareness Regarding Cybercrimes

The review of relevant and recent literature shows that there are several research studies conducted to discuss the potential of media as tool of creating awareness regarding cybercrimes. Some of the researchers like Dadkhah, Lagzian & Borchardt (2020); Fire & Elovici (2020); Patel et al., (2021); Humayun et al, (2020) and Craig, et al, (2020) suggested that raising awareness about cybercrimes is very important in present times. This awareness can best be created using mass media including both traditional and new media. Despite the widespread popularity of digital media, the effectiveness of traditional media is still very important in this context because of their wider reach and popularity. The coverage of online frauds and scams on TV programs and news can make people more careful during their online activities to avoid and prevent cybercrimes. Donalds & Osei-Bryson (2019) observed that preventing cybercrimes and making people aware about the steps that they need to take in such cases, is easier to on digital platforms. The social media communities can play a very helpful role in raising awareness and convincing people to take appropriate actions to highlight and confront the culprits. These platforms also provide support to the victims as they can share their experience with others to seek advice. Humayun, et al, (2020) also view the role of media very important in this context. The researchers believe that media must be used to encourage the victims of cybercrimes to report the issues to the authorities instead of hiding and minimizing the time that they use to spend online. This encouragement is also necessary to assure that the users will not feel prey to blackmailing activities instead they will contact the authorities to get the criminal arrested. Digital media campaigns can significantly help in this regard through community action and engagement. (Kok, Azween & Jhanjhi 2020). Many other researchers (e.g. Sulaiman & Sreeya, 2019; Longobardi, Settanni, Fabris & Marengo, 2020; Milani, Caneppele & Burkhardt, 2020; Nikhat et al, 2021) also authenticate the effectiveness and usability of media to make people aware about cybercrimes and adopt the attitude of breaking salience and make habit of reporting the incidents to the relevant authorities.

Bele et al (2019) emphasized upon the importance of educating the internet users to identify and prevent criminal activities on cyber space. The researchers proposed that technological advancements are bringing new avenues for interaction. These avenues are increasing the risks of cybercrimes but at the same time, there is great potential in these platforms to be used as tools of raising awareness. The researcher suggested the use of digital media platforms for cybercrime awareness and proposed the creation of LMS system E-Campuses where the children, students of different levels and their parents can access comprehensive information and guidance to prevent cybercrimes. It implies that educating internet users of all ages is very critical for cybercrime prevention and digital platforms can help in spreading this awareness and information efficiently. Buono (2021) stressed upon the importance of raising awareness for cybercrime prevention and suggested that the government and related agencies must launch publicity campaign through mass media that can reach people and explain them the ways to avoid being victim of cybercrimes. The government should create awareness through sustained media campaigns, advertisements on electronic media and messages through emails, websites, and social media platforms. If the authorities will not make effective use of media for raising awareness, there are chances that the prevalence of cybercrime will increase multiple fold due to lack of awareness among internet users. While literature insisted upon the importance of using media as tool of creating awareness relating to cybercrimes; there is limited evidence found in literature examining the role that media is currently playing in this context. It implies that there is a need for further investigation in this area to implement and then evaluate the role of media strategies to combat cybercrime.

Theoretical Perspective

The diffusion of innovation theory presented by Everett Rogers explain the process of innovation including ideas and technology spread within a society (Barnett & Vishwanath, 2017). In this research study, the innovation refers to the information, awareness and preventive mechanism required to deal with the incidents of cybercrime. The study proposes that the mass Media tends to become the channel for dissemination of this innovation i.e. the knowledge and ideas about cybercrime prevention. Mass Media can significantly help in diffusion the awareness messages and techniques to identify, report and prevent cybercrimes.

Methods

The research is based on quantitative approach and the method selected for data collection is online survey. The survey has been administered to a sample of 200 internet users of Pakistan. The questionnaire was created on Google forms and the link was distributed through various social media platforms over the time of one month during which the required number of responses (n=200) were collected. Descriptive statistics are used to analyze the collected data, including measures of central tendency (mean, median, mode). The results are presented in charts and tabular form to provide a quick glimpse of outcomes. The participants were informed of the purpose of the study and were requested to give their informed consent. Data is collected and stored securely, and confidentiality is maintained throughout the study. The personal information of the respondents is not collected to maintain their comfort level while sharing the incidents they have encountered on cyber space. The demographic characteristics of the survey participants are shown in Table 1.

Table 1.
Demographic Characteristics of the Respondents

	Frequency	Percentage%
Gender		
Male	82	59
Female	118	42
Age		
18 Years and Below	12	6
19-30 Years	106	58
31-42 Years	28	14
43-64 Years	24	12
Occupation		
Working Professional	88	44
Student	132	66

Results

The data for this research study has been collected through an online survey. The survey asked the respondents about their awareness levels regarding different types of cybercrimes, their response towards such incidents and their current level of understanding and practice related with cybercrime reporting. In the first section of the survey, the respondents were asked to inform if they consider several activities under cybercrime or not. The results collected from this question are presented in Table 2.

Table 2.
Awareness Regarding different types of Cyber crimes

Statement	Responses (%)		
	Yes	No	Not Sure
Share other's personal data	80	12.5	7.5
Promote harmful substances	74.5	15.5	10
Support terrorist organizations	70.5	15	14.5
Direct users to illegal sites	78	10	12
Sharing copyrighted works	60.5	19.5	20
Using insulting expressions	47.5	35	17.5
Bullying	60.5	24.5	15
Sharing violent images	80.5	10	9.5
Spreading fake news	62.5	17.5	20
Share of unlicensed software	59.5	20	20.5
Sharing pictures /videos without permission	78	11	11
Creating fake identities	72.5	16	11.5
Sharing racist messages	80	10.5	9.5
Average Score for All cybercrimes	69.6	16.7	13.7

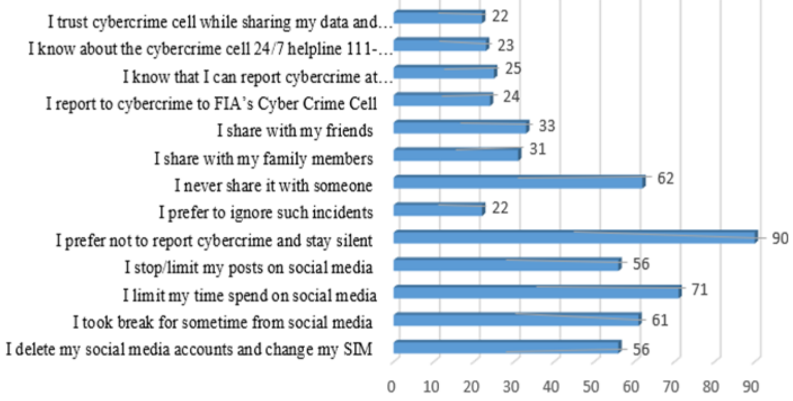
Along with estimating the level of awareness of Pakistani internet users regarding cybercrimes, the survey also collected the data to find out the occurrence of various types of cybercrimes with the respondents. Table 3 shows the prevalence of different types of cybercrimes as encountered by the internet users in Pakistan.

Table 3.
Response of Users when they encounter cybercrime.

Cybercrimes faced by Respondents	Responses
	(%)
Account hacked	45
Email ID hacked	41
Identity stole	23
Cyber bullying	81
Harassment	36
Threatened	24
Sexual content message	62
Personal data leaked	21
Blackmailing	18
Got Violent material	56
Self-harm messages	61
financial fraud	72
Scammed during shopping online	78
Bank account hacked	21
Someone posted false negative reviews about me	18
Someone tried to ruin my reputation online	20
Some give me life threats as we share different opinions	32
Average Cybercrime Encounter	41.7

An important objective of this research study was to find out the reaction of the internet users whenever they experience any type of cybercrime. For this purpose, the respondents were asked to choose from various types of possible reactions towards the cybercrimes. The data also shows the ratio of people sharing and reporting cybercrimes and their knowledge about the mechanism of cybercrime reporting in Pakistan that currently works under FIA. The data collected from this section is presented in Figure 1.

Figure 1
Reaction to Cybercrime and reporting mechanism (%)



Discussion

The data collected from 200 internet users in Pakistan provide some insightful information about the awareness, reaction, and reporting of cybercrimes in Pakistan. The demographic features exhibited in Table 1 shows active participation of both male and female belonging to age group of 19-30 in the study. This age group is commonly found actively participating in different activities in cyberspace and hence, they are vulnerable to cybercrimes as well. Therefore, information about their awareness level and reaction towards the incidents of cybercrime is very important to collect and analyze.

Table 2 shows that even some common cybercrimes are still not perceived as cybercrimes by many of the internet users. For example, around 40% of users are either unsure or clearly deny that bullying is a cybercrime. Similarly, around 41% of the users are not aware that sharing unlicensed software comes under the category of cybercrime and 38% don't consider spreading fake news as a crime. The level of awareness about different types of cybercrimes revealed in this study affirms that there is lot of need to educate people about various types of crimes on cyber space. due to this lack of awareness, they can not only become victims of such crimes but can also get involved in any of such activities. The current social media scene also confirms this low level of awareness among the users. Every day uncountable number of fake news are circulated across social media and many people took active part in spreading this news without even realizing that they are committing a crime (Appel, Marker & Gnambs, 2020). The common practice of bullying people on their posts and making insulting comments is also an indicator of lack of awareness among the masses about the boundaries of cybercrimes. These findings indicate that creating awareness among the internet users is critically important now otherwise it would become difficult to control the prevalence of cybercrimes in the country.

Many factors account for this low level of awareness including lack of education and awareness programs, poor media coverage, and underestimation of risks associated with cybercrimes. Since smartphones have become popular in Pakistan, even less educated and less aware people are actively participating in online activities but due to lack of formal education and awareness programs about cybercrime they are not completely aware about the dangerous side of cyberspace. Also, limited technical knowledge makes it difficult for them to understand the intricacies of cybercrime and how to protect themselves from it. The young people specially may be naive and not fully understand the risks involved in using the media in Pakistan may not be providing sufficient coverage of cybercrime, making it difficult for young people to stay informed about the issue. Furthermore, users, especially youth often underestimate the risks involved with cybercrime, thinking that they are unlikely to be affected by it.

The data presented in Table 2 shows that all the respondents have encountered some sort of cybercrimes during their online journey. The prevalence of cyber bullying (81%), hacking of social media accounts (45%), online shopping scams (78%) and financial frauds (72%) are the most common cybercrimes that the respondents have faced in cyber space. The data clearly shows that the situation is getting very serious with each passing day. On one hand, the mental state of the internet users is at stake due to bullying and on the other hand, they are losing their money due to financial frauds and shopping scams. It is also alarming to see that the average cybercrime encounter by the respondents is 47% which is very high because people now a days spend several hours on cyber space on daily basis. Prevalence of crimes at this rapid pace can damage internet users psychologically, socially and financially (Fabris & Marengo, 2020).

Figure 1 throws light to some very important aspects related with the reaction of internet users when they become victim of any cybercrime. It is alarming to see that most people do not share such incidents with their family and friends very commonly. Just 31% of users informed that they share cybercrime incidents with their families and 33% share with their friends. There could be several reasons why internet users in Pakistan do not share incidents of cybercrime in their circles. For example, many parents may not have a good understanding of cybercrime and its effects, making them less likely to be trusted as a resource for reporting incidents. There is also a stigma associated with being a victim of cybercrime, and some users may not want to share the incident with their parents and friends for fear of being judged or blamed. The technology gap often draws lines between individuals with their parents and other family members. Some parents may not be as familiar with technology as their children and may not understand the full extent of the cybercrime incident. Additionally, some users may feel that their parents and friends would not provide adequate support or assistance in the event of a cybercrime incident (Soomro & Hussain, 2019). Eventually, there is a rising trend of ignoring such issues and rather acting, people prefer to limit their own online activities to avoid further crimes.

The cybercrime cell actively working under FIA also seems to fail in gaining trust of the internet users. Just 22% believe that they can trust FIA with their data, and this could be a reason why 24% users ever report any incident of cybercrime to FIA. It is important to note that the cybercrime cell has been functioning for several years but just around 25% of users are aware of the cybercrime helpline and the website where they can report. Lack of awareness among users about the working of cybercrime cells is an important reason behind this behavior. However, people may not trust the FIA cybercrime cell to effectively handle and investigate their cases, as they may not have the necessary expertise or resources to effectively respond to cybercrime incidents. There is also a perception of corruption within the FIA cybercrime cell, with people believing that their cases will not be handled fairly or effectively. People may not trust the FIA cybercrime cell due to a perception of inefficiency, slow response times and a lack of effective follow-up on reported cases. Most importantly, people may not trust the FIA cybercrime cell to handle their cases confidentially, as they may fear retribution or backlash from the individuals or groups responsible for the cybercrime.

The analysis and discussion of the collected data clearly indicate that the situation demands immediate and strategic actions from the policy makers. In this scenario, the media appears to be a very important weapon to win the war against the cyber criminals. There are various ways through which the media can help the country in reducing the cases of cybercrimes by creating awareness and encouraging people to report the incidents rather than hiding from everyone. The objective of this study also include finding out the ways through which media can be effectively used in this situation. For this purpose, an open-ended question was included in the survey asking people about their opinion about using media as tools. In the light of the collected opinions and literature search, the study recommends the following actions to assure that the mass media is used in its full potential to make the situation better.

- Campaigns on Digital Platforms: Digital platforms like websites, social networking sites and applications have quick and broad reach among online users. Awareness campaigns at these platforms will provide interactive opportunities to the users to know more about the issues related with cybercrimes and cyber laws.
- Use the Reach of Digital Influencers: the government agencies working to prevent cybercrimes can collaborate with popular influencers and digital storytellers to reach online users and tell them about the correct actions in case of facing any cybercrime.
- Appealing Visual and Video Messages: educational videos about the procedure of reporting process can help in creating awareness about the complaint mechanism. Such videos and visual content can make internet users more vigilant towards cybercrimes.
- Media partnership: Traditional media like TV channels, newspaper and radio have great reach and awareness messages spread through these platforms can reach many people. TV shows featuring authorities related to cybercrime cell can help in making people familiar with the mechanism.
- Awareness Sessions, Trainings, Workshops and Seminars: the authorities need to frequently organize different seminars, training sessions and awareness programs so that the internet users can understand the importance of identifying and reporting cybercrimes.
- Nationwide drives to create Awareness Drives: The government and related authorities should also make direct connection with the masses through awareness drives in different cities and towns where they can meet people and inform them about importance of reporting such offences.
- Collaboration with Law Enforcement: the law enforcement agencies that are responsible for dazzling with the cybercrime cases must also collaborate with the authorities for educating masses about different types of criminal activities that happen on cyberspace and the steps they need to take in such situations.

Practical Implication of Research

The research provides evidence about a significant gap in cybercrime prevalence and awareness among internet users. It proves that there is a critical need for creating strategies and plans to guide internet users on ways to protect themselves from being victims of cybercrimes. The study also proved that the government entities like FIA are working to combat cybercrimes, but the internet users of Pakistan are widely unaware about the reporting mechanism and the mostly they prefer not to report any incident that further harms the situation. The evidence is enough to realize that there is an urgent need to make effective strategies in this regard. The recommendations proposed in the study also possess practical value as they specifically mention some actions that can help in making the situation better.

Conclusion

The research paper presents an overview of the current situation of cybercrime prevalence and reporting trends in Pakistan. It is revealed that many of the online users in Pakistan are not aware that many activities they witness online often come under the umbrella of cybercrime. Furthermore, the study also shows the trend of not reporting any cybercrime to the authorities. People in Pakistan do not report these cases most of the times because they do not know the procedure. Even if the online user knows the procedure to complain such incident, he or she prefers not to do so due to lack of trust on the authorities. The findings of this study highlight the need for a comprehensive and coordinated response to cybercrime in Pakistan, including increased collaboration between law enforcement agencies, organizations, and the public. The study also highlights the importance of promoting public awareness about the issue, and the role that the media can play in this regard.

References

Appel, M., Marker, C., & Gnambs, T. (2020). Are social media ruining our lives? A review of meta-analytic evidence. *Review of General Psychology*, *24*(1), 60–74.

Bányai, F., Zsila, Á., Király, O., Maraz, A., Elekes, Z., Griffiths, M. D., et al. (2019). Problematic social media use: Results from a large-scale nationally representative adolescent sample. *PLoS ONE, 12*(1).

Bele, J.B., Dimc, M., Romzan, D. and Jamec, A. S. (2019). *Raising awareness of cybercrime - the use of education as a means of prevention and protection*. Conference paper: 10th International Conference Mobile Learning

Buono, L. (2021). *Fighting cybercrime through prevention, outreach and awareness raising*. ERA Forum 15, 1–8

Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., et al. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, *66*(6), S100–S108.

Dadkhah, M. Lagzian, K. and G. Borchardt (2020). Identity Theft in the Academic World Leads to Junk. *Science and Engineering Ethics*, *24* 1, 287–290

Daily Times. (2022). *FIA: Cyber Crime increases 83%* (Online) Available at https://dailytimes.com.pk/1001261/fia-cyber-crime-increases-83/ Retrieved on 29 January 2023

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403–418.

Fire, R. G., and Elovici, Y. (2020). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys & Tutorials*, *16,* 2019-2036.

Herath, T.B.G.; Khanna, P.; Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *J. Cybersecur. Priv*. ,*2*, 1-18.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *1*-19

Kok, S. H., A. Azween, and N. Z. Jhanjhi. (2020). Evaluation metric for crypto-ransomware detection using machine learning. *Journal of Information Security and* Applications *5,* 1026-46.

Longobardi, C., Settanni, M., Fabris, M. A., & Marengo, D. (2020). Follow or be followed: Exploring the links between Instagram popularity, social media addiction, cyber victimization, and subjective happiness in Italian adolescents. *Children and Youth Services Review*, *113*, 1049-55.

Milani, R., Caneppele, S., & Burkhardt, C. (2020). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*.

Munir, A. and Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review*. *3*. 84-97. 10.31703/gpr.2018(III-II).09.

Nikhat A., Bedine K., Yusuf P., Anurag T., Sheeba P. (2021). A Comprehensive Overview of Privacy and Data Security for Cloud Storage, *International Journal of Scientific Research in Science, Engineering and Technology* (IJSRSET), *8* (5), 113-152.

Omar, A. (2021). Threats and Anti-threats Strategies for Social Networking Websites. *International Journal of Computer Networks & Communications*, *5*, 53-61

Patel, P., et al. (2021). A theoretical review of social media usage by cyber-criminals. *2017 International Conference on Computer Communication and Informatics (ICCCI). IEEE.*

Soomro, T. and Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*. 24. 9-17. 10.2478/acss-2019-0002.

Sulaiman, S. and Sreeya, B. (2019). Public awareness on cyber-crime with special reference to Chennai. *International journal of innovative and exploring engineering*, *9*(1), 3362-3364.