International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Interlinked Relationship between Cybercrime & Digital Media

Md. Golam Rabbani Sarker

Assistant Professor, Department of Sociology, Begum Rokeya University, Rangpur, Bangladesh.
grabbi27@gmail.com

ABSTRACT

Today, the internet has become so interwoven in our lives that it is difficult to fathom life without it. Technology advancements have led to the emergence of digital media as a significant aspect of our lives, the growing use of mobile information, and social media, which provide platforms for easy global interaction. Technology has many advantages, but it also puts people at risk. As the amount of crimes committed online has multiplied, digital media has become a haven for crooks. The advantages of the internet are no longer a mystery to anyone, and the most recent social media platform is open to anyone. The anonymity it offers and the creation of a genuine atmosphere where users may connect, swap photos, meet others, play games, fall in love, argue, etc. without ever having met in person are the main draws of social media. The exploitation of a victim's name, residence, location, and other personal information by criminals is now, however, all too typical, particularly in situations involving women. Due to the confidentiality and fakeness that are present in social media, as well as jurisdictional concerns, cybercrime has become more prevalent among people of all ages and is now a global problem. The study describes and discusses the effects of digital media on young people as well as the reasons behind the increase in cybercrime on social media. The study addresses the common types of cybercrime that happen there as well as the role of the law in dealing with and preventing it on social media. The research makes numerous recommendations for completely and sufficiently teaching the nation's children about the dangers of cybercriminals.

Keywords: Digital media, Cybercrime, Legislation, Confidentiality, Cyber Protection

INTRODUCTION

Digital media, whether it be utilized by a government institution or any other commercial company, has profoundly changed how data is used and exchanged among individuals. It has also become a crucial component of every organization [1]. It provides users with a platform to quickly exchange ideas and information with a sizeable portion of the public without using traditional media outlets. Social media has been having a big impact on how individuals think and what they believe. Data from social networking sites can be used to study, among other things, the flow of ideas, attitudes, and opinions. It is incredibly valuable to know how frequently data is shared, who is sharing it, and what the information is about. This can be useful in many ways, such as providing billions of people with information on any catastrophe. The transmission of information regarding the lockdown protocols used during the pandemic serves as a recent example. Social media has instead developed into an important political media platform; yet, it is not often utilised to share news or any other public problems.

When used effectively, digital media can inform viewers about any event happening around the world and raise awareness of it. Social media is the software's success story of the previous 10 years in terms of users. The increasing popularity of social media may be seen in Facebook's expansion from 2.45 billion monthly users in 2020 [2] to 2.75 billion monthly active users by July 2021, an increase of 14% over the previous year. These websites are popular, which draws cybercriminals to them like a bee to nectar. Digital media, one of the best and most powerful technologies, has recently become a haven for criminal behavior. With the increase of internet users over the past ten years [3], cybercrimes have increased. Cybercrimes are misdeeds committed using a computer. Alternatively, cybercrime is any illegal doing involving a computer or computer network. Cybercriminals may access our personal information on social networking sites, shopping websites, and other online services with ease. They can also employ advanced methods like malware to assault our social media identities. Another method is creating a false online identity in order to slander someone or to steal credit card information and other data that may be easily obtained through online shopping sites. Two more serious types include attacks against adolescents and attacks related to gender. Due to the privacy of the criminal, child pornography is on the rise in cyberspace, with mothers and young children as its primary targets. Children are also victims of such criminals in the online world who are mislead by false social media communications and identities. It continues after these since there have been recent revelations about schoolchildren planning to rape a young girl on social media [4,5]. As per report Bangladesh's cybercrime rate is 28.31% [6].

IMPACT OF SOCIAL MEDIA

Digital media offers a stairway that connects humans to the rest of the globe via the internet, voice and online conversations, chat rooms, and a host of different features. Children may easily and conveniently join up to become members of any social media platform because the process is so simple. A person must register with their personal information in order to join any social media platform. Once logged in, they can browse the platform's material and share facts, images, or information with other users of that network. Popular social media sites with young people include Facebook, Twitter, Instagram, WhatsApp, Snapchat, and others.

However, digital media also contributes to society isolation because face-to-face contact has decreased significantly during pandemics. This, in turn, has an impact on people's mental, emotional, and psychological health and results in anxiety, FOMO, sadness, and several other problems. These days, people are concerned about their privacy. The third party engages in cyber bullying and cyber theft against teenagers by using the individuals' private information. The youth are more susceptible to these things because of the prevalence of offensive content on social media. They waste their days away in internet chat rooms. Additionally, inaccurate information spreads more quickly than accurate information, which can be done for any reason, including fostering animosity between diverse ethnic and religious groups or deceiving humans, which makes virtual hate crimes worse.

Social media is widely used to keep people in touch, yet it can also cause social loneliness. Social media platforms have reduced face-to-face communication to a minimum. Numerous studies and pieces of research have shown that young people who experience social loneliness might experience a range of negative impacts on their worry, hopelessness, and dread of being left out, as well as their intellectual, moral, bodily, and psychosocial factors. Additionally, teenagers frequently engage in cyber bullying and online thievery on social media. Due to social media's lack of security, there is very much likelihood that

a third party may misuse a people's private information [7]. Another aspect of this is how young people waste time on these platforms by conversing online rather than doing anything useful. In addition to children, young teens are also preyed upon by hackers. There have been instances where teens have discussed raping a minor on a social networking platform. Additionally, while digital media, on another hand, disseminates details, it also facilitates the propagation of false statistics. The main platform for spreading fake information is WhatsApp, and the fact that some people still believe it is worrisome. Spreading such rumors might be done to incite conflict and hostility amongst diverse group Children may be the most affected by internet media because they are the most open group and willing to adopt such cutting-edge inventions. The concepts of engagement and communication have changed as a result of the expansion of such online media. According to studies, computer crimes have increased recently during COVID [8].

The fact remains that digital media has become a part of our culture and that it dominates most people's lives. Although digital media is a useful platform of people's details, it occasionally contains falsehoods and misinformation. Our lives are missing face-to-face interactions and physical encounters since we can get anything via the network on a portable device.

TYPES OF CYBER CRIMES

According to the One Cyber Crime Reporting Portal [9], 5 cybercrimes are highlighted –

Email scam and Phishing – Phishing is a form of online fraud that occurs when a fake email purporting to be from a specific company requests sensitive personal and financial information**.** Consequently it tricks the user into disclosing their personal information and then using it to their advantage [10]. The nation's federal cybersecurity office received a report on a bogus email campaign in May 2020 that threatened to reveal a user's private footage if a cryptocurrency ransom was reimbursed [11].

Identity Theft – Social networking have made this a much similar occurrence. In this kind of crime, the perpetrator uses social media platforms to get the victim's personal information [12]. This is done so that the victim's information can be used to apply for credit, loans, or other forms of financial aid. It also involves obtaining sensitive statistics to get acquire to bank balances or maybe using it to defraud people or a violation under the victim's identity.

Obscene content – Obscene is defined as "offensive to modesty or decency; vulgar, dirty, and unpleasant" by the Supreme Court in one of the key cases [14]. The Supreme Court also made a distinction between obscenity and pornography. Additionally, criminals alter social media images, produce pornographic content, and distribute it online with disregard for the victim. According to the Hindustan Times, a man who was producing, distributing, and posting photographs was detained of Hindu deities figures on digital media [15].

Online scam or fraud – Online fraud and scams have gained attention in the era of the internet where everything is accessible. Another fraudulent online behavior is the cloning of a person's account in order to obtain personal information. The perpetrators create a new account using photos and pictures, and then entice friendship and family too divulges bank account information or any other sensitive information. Occasionally, they will also send offensive content to foster disdain [16].

Cyberbullying – A person is forced to do something they do not want to do by bullying, which is a type of harassment. Young people and teenagers frequently experience it. This has grown to be extremely typical. Among many other things, it involves making fictitious websites about people, making comments, posting offensive words about people, spreading pointless images or videos of people, and more. In a research conducted in Delhi by the NGO Children Rights and society, over 9.3 percent of 632 teenagers reported seeing cyber harassment and 50% of them did not report it to their guardians, instructors, families, or any relevant digital media companies [17].

CONCLUSION

Social media has proven to be effective in many facets of life, from using the populace to topple our government to bridging the gap between astronauts and scientific aficionados throughout the world. A study by Aljazeera claims that social media sites like Facebook, Twitter, and others are crucial for protest organizers. There are numerous opportunities for the use of massive amounts of data in numerous industries due to the tremendous volume of information that is available on social networking sites. Marketers can utilize social networking sites to comprehend consumer behavior and design effective marketing campaigns.

The British government started monitoring Facebook, Instagram, Twitter, and blog feeds on social media. The study's summary and some key findings are described here, along with the author's suggestions for how to stop such crimes. The lack of an absolute law anywhere on the globe is one of the main problems with cybercrime. The issue worsens as a result of the disproportional growth ratio of all internet-and cyber-related regulations. The Information Technology Act and the IPC changes represent a positive beginning, yet cybercrime challenges and difficulties still exist.

The British government started keeping an eye on social media feeds from Facebook, Instagram, Twitter, and blogs. This section summarises the study's main findings and offers some recommendations for how to prevent similar crimes. One of the primary issues with cybercrime is the absence of an absolute law anyplace in the world. The problem gets worse because all internet- and cyber-related rules are growing at an unbalanced rate. In light of the aforementioned facts and the current situation in our nation, it is frequently claimed that modifications to the Information Technology Act are necessary to prevent cybercrime. Bangladesh should also possess the necessary technology to completely defeat cybercriminals.

References

1. Prashant Sharma, 'Core Characteristics of Web 2.0 Services' (Tech Pluto Staff, 28 Nov. 2008) accessed 23 February 2013
2. Menlo Park, Facebook Reports Second Quarter 2021 Results, FACEBOOK INVESTOR RELATIONS (July 30,2021), https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter2021-Results/default.aspx
3. RESEARCH Gate, May 2019, Digital Media-Related Cybercrimes and Techniques for Their Prevention, Tariq Rahim Sumro & Mumtaz Hussain, https://www.researchgate.net/publication/333944511

4. Suchetana Ray and Anirban Ghoshal, Every sixth cybercrime in India committed through social media: NIA, HINDUSTAN TIMES (Aug 25, 2019, 00:51 IST), https://www.hindustantimes.com/india-news/every-sixth-cybercrime-in-india-committed-throughsocialmediania/storKscgnwjcTZ0pzVeVaOiN6M.html#:~:text=are%20growing%20exponentiallyEvery%20sixth%20cybercrime%20in%20India%20is%20committed%20through%20social%20media,annually%20between%202013%20and%202015.
5. Sandhya Keelery, Number of cybercrimes related to social media across India 2019-2020, STATISTA (Oct. 16, 2020), https://www.statista.com/statistics/875906/india-number-of-cyber-crimes-related-to-social-media/#:~:text=In%202017%2C%20there%20were%20overcrime%20reported%20in%20the%20country.
6. https://www.tbsnews.net/bangladesh/55-cybercrime-victims-failed-police-survey-476406#:~:text=In%20the%202021%20report%2C%20the%20rate%20was%2028.31%25.
7. Umarani Purusothaman, Impact of social media on youth, RESEARCH GATE (Oct. 2019), https://www.researchgate.net/publication/336716719_Impact_of_social_media_on_youth.
8. AFP, Interpol warns of 'alarming' rise in cybercrime cases during Covid-19 pandemic, DECCAN HERALD (Aug. 04 2020, 18:00 IST), https://www.deccanherald.com/international/interpol-warns-of-alarming-rise-in-cybercrim e-cases-during-covid-19-pandemic-869489.html.
9. National Cyber Crime Reporting Portal, Ministry Of Home Affairs, https://cybercrime.gov.in/Webform/More
10. Mayur Joshi, Phishing in India is becoming innovative, INDIA FORENSIC, https://indiaforensic.com/understandingphishingindia/#:~:text=Phishing%20uses%20'spoofed'%20e%2D,numbers%2C%20account%20usernames%20and%20passwords.&text=Phishing%20mails%20take%20you%20to%20 fraudulent%20websites.
11. PTI, Fake ransom seeking email scam prowling in Indian cyberspace, THE ECONOMIC TIMES, https://cio.economictimes.indiatimes.com/news/digital-security/fake-ransom-seeking-email-scamprowling-in-indian-cyberspace/75503847.
12. https://bdnews24.com/bangladesh/cybercrime-cases-rise-in-bangladesh-but-suspects-are-mostly-acquitted.
13. ET Bureau, 4 in 10 Indians have experienced identity theft: Report, THE ECONOMIC TIMES (Apr. 07, 2020, 05:51 PM IST), https://economictimes.indiatimes.com/tech/internet/4-in-10-indians-have-experienced-identitytheft-report/articleshow/75029916.cms?from=mdr.
14. Ranjit D. Udeshi vs. State of Maharashtra, AIR 1965 SC 881, Para 7, p. 885
15. https://www.dhakatribune.com/op-ed/2022/09/19/bangladesh-is-at-serious-risk-of-cyber-crimes#:~:text=Spam%20has%20been%20identified%20as,the%20total%20daily%20email%20volume.
16. https://archive.dhakatribune.com/cybersecurity/2019/04/20/3-conviction-rate-of-cybercrime-in-bangladesh
17. Rhea Maheshwari, In one year alone, cyberbullying of Indian women and teenagers rose by 36%, SCROLL.IN, https://scroll.in/article/956085/in-one-year-alone-cyberbullying-of-indian-womenand-teenagers-rose-by-36