An Analytical Study of the Surge in Cyber Crimes in Digital India with Special reference to Social Media

Dr. Anjum Ajmeri Rabbani Ansari
Assistant Professor
Dr. D. Y. Patil Law College, Pune

Abstract: Social media usage and internet penetration have significantly expanded nationwide since the launch of the Digital India program, promoting social and economic development. But this digital growth has also led to a dramatic increase in cybercrimes, especially on social networking sites. In the context of Digital India, this research paper conducts an analytical analysis of the rise in cybercrimes, paying particular attention to social media abuse. It looks at the characteristics, origins, and trends of cybercrimes include financial fraud, identity theft, cyberstalking, online harassment, and the spread of false information. The paper assesses court interpretations and enforcement issues while critically analyzing the current legislative framework, particularly the Information Technology Act of 2000. It highlights the main weaknesses brought on by a lack of cybersecurity measures, a lack of digital literacy, and the ever-changing nature of cyberthreats. The study identifies weaknesses in the current regulatory and preventive systems using case studies and data analysis. In order to handle the new hazards, it also suggests extensive reforms that include technological, legal, and pedagogical measures. In order to protect the goals of the Digital India program, the results highlight the urgent need for a balanced strategy that fosters digital innovation while maintaining strong cybersecurity.

Keywords*:* Digital India, Cybercrime, Information Technology, Cybersecurity.

I. INTRODUCTION

Cybercrime is a dynamic phenomenon. Technological and societal advancements present opportunities all the time, and hackers are always coming up with new ways to take advantage of the newest browsers, e-commerce websites, and mobile computing devices. Social media is no exception. Social media platforms' ability to link people in novel ways and open up new channels for communication is what gives them their power. They open new avenues for people, businesses, and governments to connect with people, market goods, and build communities. Cybercriminals are equally drawn to social media sites. [1]

However, little is known about the widening variety of criminal threats that may be found on social media. This Article describes how the buying and selling of services, tools, and data on social media platforms, as well as the distribution of malware, are facilitating traditional crime and creating possibilities for cybercriminals. Additionally, it draws attention to the effects this is having on people and organizations, demonstrating how Cybercriminals now have an alluring potential to generate money on the web thanks to social media sites.

II. CONCEPT OF CYBER CRIME:

The laws pertaining to computers and the Internet are known as cyber laws. It goes without saying that digital technology and new communication methods have drastically altered our way of life. Nearly everyone is

[1] https://www.forbes.com/sites/jessicabaron/2019/04/30/social-media-platforms-increasingly-popular-with-cybercriminals/

impacted in the highly digitalized world of today. The way people are transacting is undergoing a transformation. Demat form is used for almost all share transactions. Nearly all businesses rely heavily on their computer networks to store their data in an electronic format, and customers use credit cards to make purchases. Most people communicate via SMS messaging, cell phones, and emails. Instead of using traditional paper documents, businesses and consumers are increasingly creating, transmitting, and storing information in electronic form using computers.

E-contracts and digital signatures are quickly taking the place of traditional commercial methods. Quality, quantity, and speed have all increased dramatically in the sector since the advent of the computer age. The lifestyle is becoming more modern. The technology is still evolving and changing, though. The human mind is the source of men's curiosity and thinking abilities, which lead to the development of contemporary science and technology. Therefore, human innovation is the process of creating knowledge to increase human potential or meet new demands and desires.

The advent of computer networking has made it easier to access and store information, removing time and distance barriers to communication. The globe has essentially become a global village because of their providing an efficient means of information exchange.

Cybercrimes are offenses that occur over the Internet or through its services. These cover a wide range of unlawful actions. Many criminal behaviours can be lumped together under the umbrella term "cybercrime." Many unsettling behaviours take place in cyberspace due to the anonymous aspect of the internet, which may allow offenders to engage in a variety of illegal activities known as cybercrimes. Since technology is the weapon used in cybercrimes, the majority of those who perpetrate these crimes are technically proficient individuals who possess in-depth knowledge of the internet and computer programs. Cyberstalking, cyberterrorism, email spoofing, bombing, cyber pornography, cyber defamation, and polymorphic viruses are a few of the recently discovered cybercrimes.
Cybercrime as defined internationally by the U.N. Congress on Prevention of Cyber Crime and Treatment of Offenders[2] comprises two categories as follows,
1. Cybercrime in its strictest definition, cybercrime refers to any illicit activity that targets the security of computer systems and the data they process and is carried out through electronic methods.
2. Cybercrime in its broadest definition, cybercrime encompasses all crimes involving computers and any unlawful activity carried out through or in connection with a computer system or network, including unlawful possession and the offering or dissemination of information via a computer system or network.

According to the Information Technology Act of 2000, cybercrime in India is defined as a deliberate and voluntary act or omission that negatively impacts a person, their property, or their computer systems and is punishable by criminal penalties.

III. Cyber Crime & Role Of Social Media In India

Through virtual communities and networks, social media are interactive computer-mediated tools that make it easier to create or share ideas, information, career interests, and other forms of expression. The wide range of integrated and standalone social media platforms currently on the market makes classification difficult, but there are several characteristics that they all share.

[2] Tenth U.N. Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.

With around 2.9 billion monthly active users[3], Facebook is the most popular social media worldwide and many companion like Facebook Messenger, TikTok, SnapChat, Instagram, Twitter, and LinkedIn are a few of the most well-known social networking platforms. YouTube, Quora, Telegram, WhatsApp, Pinterest, Reddit, Google, Zoom , Microsoft Teams, and more are some well-known platforms that are occasionally referred to as social media services depending on how it is interpreted. Numerous advantages and disadvantages of social media use have been seen by observers. Businesses, entrepreneurs, non-profit organizations, advocacy groups, political parties, and governments can all benefit from social media as a communication (or marketing) tool. It can also make people feel more connected to real or virtual communities.

IV. SOCIAL MEDIA CRIMES:

To communicate with one another in this virtual setting, people of all ages and genders are increasingly setting up profiles on online social networks. Across several profiles, some people have hundreds or thousands of friends and followers. However, there is also an increase of phony profiles at the same time. Fake personas frequently upload offensive or unlawful content to harass real users. Additionally, fake profiles are made by misrepresenting a well-known someone to annoy them.

The most conventional steered websites or apps for generating 'Fake Profiles' are as under:

1. Facebook
2. Snapchat
3. Instagram
4. Twitter
5. LinkedIn etc.

A social media service is an online platform that focuses on establishing social networks or relationships between people who might want to talk, share pictures, videos, backdrops, sports, or real-life connections. A social community service includes a profile, which is a summary of each user, together with information about their social connections and a variety of offerings. Most social community offerings are focused on the internet and provide ways for people to communicate, such as instant messaging. Even though, from a wider perspective, social community services typically explain as individual-oriented services, online network services are regarded as social network services. In contrast, online social offerings are group oriented.

People can share their thoughts, sports, events, and hobbies with their private networks on social networking websites.

The information is no longer private as soon as it is posted on a social networking website. The more information a customer posts, the more likely it is that they will be involved. Even when using high-security settings, friends or websites may unintentionally leak personal information.

One percent's personal information could be used to attack the user or their friends. The more information that is shared, the more likely it is that someone could replace the user and trick all their friends into divulging sensitive information, such as downloading malware or gaining access to websites that are blocked.

Hackers, remote location actors, commercial enterprise gamers, and predators utilize social networking websites to find people's personal information to accuse of misuse. Information gathered from social media platforms can be used to create a targeted attack that doesn't use the social media platform itself.

[3] https://datareportal.com/essential-facebook-stats

Some may want to refute the huge technological innovations that are constantly occurring within the cutting-edge world. The laptop, the internet and technological tools have appreciably changed what its method to socialize, to 'chat', and even to look at an eBook. each the merits and demerits of those varieties of improvements are obvious, and as technology attains speed so have the illegal sports of folks that aspire to take advantages of such developments. Cybercrimes have grown to be as multifaceted because the technology that allows them to be dedicated and the experience that one is at ease from the offence within the confidentiality of one's personal home should not be relied upon.

With reference to users in India, it is debatable whether cybercrime victimization on social media platforms is caused by the focus of these platforms' vulnerabilities or by their risky use. It also determines the effectiveness of mitigation strategies to limit the vulnerability introduced by social media platforms.

Websites on social media are vulnerable. The revolution in social communications has been shaped by online social media platforms[4]. However, artists were abusing their talent for evil purposes, and there were sensational forgeries in addition to growing mendacity. Social media websites are online resources designed to facilitate communication and knowledge sharing among users. Previously, knowledge is positioned on social media platforms because it is not a long-term exclusivity. The more expertise we possess, the more likely we are to become victims of cybercrimes. You or your associates may be the target of behaviour assaults using personal information you share.

The more data you share, the more likely it is that someone will pose as you and fool one of your friends into downloading malware, sharing confidential information, or giving access to restricted funds. Social media websites are trolled by predators, hackers, business rivals, and foreign kingdom agents who seek out information or people to target for exploitation. Information obtained from social media platforms might be utilized to create a specific assault that isn't supported by the typical way that social media platforms are used.

V. VULNERABILITY FREQUENTED WITH SOCIAL MEDIA CRIMES

1. Click on-jacking

hiding hyperlinks beneath legitimately clickable content that, when clicked, cause someone to inadvertently perform actions, including downloading malicious software or sending your ID to a website. "Like" and "percentage" buttons on social media platforms have been used in a number of click-jacking frauds[5]. Turn off frames and scripting in any web browser you use. Look at different methods for configuring your browser to optimize security.

2. Social Media Worms

Koobface is a social media worm that has grown to be the biggest web 2.0 botnet. Koobface is a multidimensional threat that defies the notion of a "malicious program" because it is specifically made to spread via social networks, infect new computers into its botnet, and take over more accounts in order to send more junk mail that infects other computers. all while making money with the same old botnet business, along with Russian romance services and scareware.

3. Phishing Bait

[4] https://www.sciencedirect.com/science/article/pii/S0268401220308082

[5]https://www.researchgate.net/publication/360088248_Clickjacking_A_Study_on_Existing_Websites_in_Cameroon

With the use of a URL known as the "fbaction" for the browser, the email tricked you into signing up for Facebook[6]. Even though it was only a small percentage, many Facebook users had their bills compromised. This is still a significant number when one considers that Facebook has over 350 million users. Facebook, to its credit, moved quickly to blacklist that region, but several imitation attempts followed. When you think about it, Facebook has become good at Whack-A-Mole.

4. Data Leaks

Sharing facts is the main purpose of social networks. Unfortunately, a lot of consumers overestimate the company, issue, goods, finances, organizational changes, scandals, or other sensitive information. Even spouses occasionally divulge too much about their significant other's tardiness on the Top Mystery Challenge and some of the specifics of the task. The embarrassment, the injury, and the prison are the problems that follow.

Links that have been shortened to fit long URLs into little space, people employ URL shortening services. Additionally, they obfuscate the links, which makes it less obvious to users that they might be clicking on malware rather than a CNN video[7]. These abbreviated hyperlinks are widely used and easy to use. Customers of Twitter will automatically shorten any hyperlinks so that others can view them.

5. Increase continual Threats

The gathering of information for which social networks can be a veritable gold mine of data, is one of the primary components of improving persistent threats. These data are used by criminals to advance their threats, such as establishing more extensive intelligence gathering and gaining access to sensitive infrastructure[8].

6. Forgery of Cross-Site Requests.

However, it is a specific type of technological error that is utilized to reveal a complex social media problem. CSRF attacks take advantage of the trust that social networking software has in a user's browser when they are signed in[9]. Therefore, it is simple for an attacker to post a picture in a customer's occasion movement that other customers may click on to record or disseminate the attack, provided that the social community application is not verifying the referrer header.

Elicitation communicating strategically to elicit information from others without making them feel as though they are being questioned. Understand elicitation methods and how social engineers try to obtain personal information.

7. Assertion of the problem

Over the past five years, social media's phenomenal rise in popularity has brought about a significant increase in private correspondence, both online and offline. The popularity of websites like Facebook,[10] YouTube, and Twitter has made human interaction not only easy but instantaneous, enabling users to connect and interact

[6] https://insertintelligentname.wordpress.com/2011/10/14/internet-insecurity/
[7] https://www.cmu.edu/iso/aware/dont-take-the-bait/shortened-url-security.html
[8]https://www.researchgate.net/publication/334274476_StrategicallyMotivated_Advanced_Persistent_Threat_Definition_Process_Tactics_and_a_Disinformation_Model_of_Counterattack
[9] https://www.researchgate.net/publication/380357864_Mitigating_Cross Site_Request_Forgery_CSRF_Attacks_Using_Reinforcement_Learning_and_Predictive_Analytics
[10] https://www.charleagency.com/articles/facebook-statistics/

with anyone with an internet connection in a matter of seconds but the large collection of private and business-related information found on social media websites shared by users looking for cybercrimes.

The lack of barriers between social media management's private and professional lives is a challenging task to combat this new assault method for social engineering attempts. Finding out whether or if cybercrime victims on social media platforms are the result of website vulnerabilities or risky use of websites with a particular relationship to Indian consumers is the challenge 80 researchers may find in this thesis. The increase in the number of people falling victim to social media can be attributed to the sites' weaknesses, dangerous user usage, and the difficulties users experience as a result of the shift in the next generation.

VI. Lacunas in Legal framework for combating Cyber Crimes relating to social media

Users must therefore exercise caution and be mindful of what they share online. The IT Act of 2000 was amended in 2008, and although sections 43[11], 66[12], and 67[13] penalized cybercrimes broadly, sections 66A to 66F and sections 67A to 67C made provisions for specific cybercrimes, including sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, privacy violation, cyberterrorism, etc. Like a cumbersome appendix, their revisions protrude.

Furthermore, the Bharatiya Nyay Sanhita[14] employs the word "or" to indicate that the offense could be punished with either jail or a fine, whereas the Information Technology Act 2000 considers both the imposition of a fine and imprisonment. Regarding identity theft, the most significant difference between the BNS and the IT Act is that the latter mandates that the crime be conducted with the use of a computer resource. Therefore, the IT Act and other regulations for addressing the problem are falling short.

VII. Conclusion

By using social media sites with a little awareness and mindfulness, the risk of cybercrime can be decreased. Ensuring the security of personal data from social media platforms requires a minimal effort. Sharing a password on any online forum or with friends or coworkers is safe. Social networking is a fantastic way to meet new people, make new connections, share our knowledge with others, and learn new things. However, the user needs to know other hand, be conscious of the fact that the web has its own fair share of good and bad components which pulls users to be victim of the vulnerabilities.

Regulations pertaining to cybercrime are lagging emerging technologies, and the threat presented by cybercriminals is growing rapidly worldwide. Accessing, storing, and using data is simpler than ever before, but increased connectivity also raises the possibility of illicit conduct.

Laws have not evolved to keep up with technological advancements and it is behind in race with technological developments.

[11] Penalty and compensation for damage to computer, computer system

[12] If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

[13] Punishment for publishing or transmitting obscene material in electronic form

[14] https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf