IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Proliferation of Cyber Crime via Social Media

Under the Supervision of

Dr. (Prof.) Ritesh Dwivedi

AMITY BUSINESS SCHOOL

AMITY UNIVERSITY UTTAR PRADESH

SUBMITTED BY

Debdutta Mitra

A0102222048

MBA (Marketing & Sales)

Section-A

ABSTRACT

This study investigates the alarming rise of cybercrime facilitated by social media platforms in India. With the country boasting one of the world's largest internet user bases, social media has become a breeding ground for criminal activity. The paper explores how these platforms' inherent features, coupled with a lack of digital literacy and robust legal frameworks, contribute to the proliferation of cybercrime.

Particular emphasis is placed on the vulnerability of two key demographics: youth and women. The paper examines how young people's inherent trust and openness online make them prime targets for cyberbullying, sextortion and online predation. Furthermore, the research explores the unique challenges faced by women on social media, including harassment stalking and the misuse of personal information.

The paper adopts a multi-pronged approach, analysing data on reported cybercrimes in India and examines the limitations of existing legislation and explores potential solutions. These solutions may include promoting digital literacy campaigns, strengthening legal frameworks and fostering greater collaboration between law enforcement agencies and social media platforms.

By delving into the specific risks posed to young people and women, this paper aims to provide valuable insights for policymakers, educators and social media companies. Ultimately, it seeks to contribute to a safer online environment for all Indian citizens.

Keywords: Cybercrime, Cyber security, Social Media, Online, Youth, Women, Crimes, Indiaan crimes, Crimes in India, Cyber crime trends

Chapter I - Introduction

According to a general definition, Cyber law is a legal system that deals with the internet, computer systems, cyberspace, and all matters related to cyberspace or information technology.

Cybercrimes in India have been a pressing issue in recent years as a result of increasing prevalence and usage of social media. If looked upon, various sources attribute several factors for the rise of cybercrimes in India (Vilks, 2019). These factors include the rapid development of technology and the internet, the availability of Internet technologies to a wide population, weak control and distribution of pornographic material, lack of awareness and education about online security and privacy, and the absence of stringent laws and regulations to combat cybercrimes. Furthermore, the anonymity provided by social media platforms makes it easier for criminals to carry out their activities without easily being traced.

While it is evident that the landscape of cybercrimes in India is complex and multifaceted, requiring a comprehensive approach to address the myriad of challenges. the rapid proliferation of technology and the internet has undoubtedly played a significant role in the escalation of cybercrimes. With the widespread availability of Internet technologies to a vast population, the potential for criminal activities to take place has expanded exponentially.

Also, the lack of stringent laws and regulations to combat cybercrimes has created a conducive environment for malicious actors to exploit vulnerabilities in the digital realm. the absence of robust legal frameworks. (Roy, 2012) has emboldened cyber criminals, making it imperative for the Indian authorities to enact and enforce effective legislation to deter and prosecute offenders.

Additionally, the proliferation of pornographic material and lack of awareness and education about online security and privacy have exacerbated the susceptibility of individuals to fall victim to cybercrimes. it is crucial for authorities to prioritize cybersecurity education and awareness initiatives to equip the populace with the knowledge and tools to protect themselves in the digital sphere.

(Vij, 2013) cites that the anonymity provided by social media platforms presents a significant challenge in tracing and apprehending cyber criminals. Addressing this issue requires leveraging advanced technological solutions and international collaboration to enhance cyber forensic capabilities and strengthen investigative efforts. The evolving nature of cybercrimes in India necessitates a holistic approach that encompasses not only legal and technical aspects but also social and educational measures. it is crucial for authorities to engage in proactive measures such as enhancing law enforcement capabilities, fostering collaboration between the public and private sectors and promoting responsible online behaviour via educational campaigns and outreach programs.

With the increasing popularity and usage of social media platforms in India, cyber criminals have targeted the youth demographic through various techniques. According to (Datta et al, 2020), the youth population in India is often targeted more via social media due to several factors. First young people are more active and engaged on social media platforms, making them easier targets for cyber criminals. They are more likely to share personal information, photos and details of their daily lives, which can be exploited by individuals with malicious intent.

Furthermore, (Sehgal & Dhaarna, 2021) cite that the lack of awareness and understanding of online risks among the youth population makes them vulnerable to cybercrimes via social media. Many young people may not fully comprehend the potential consequences of sharing sensitive information online, making them easy targets for scams, phishing and identity theft.

(Batra, 2013) adds that the youth's reliance on social media for social interaction and networking makes them more susceptible to manipulation and grooming by cyber criminals. Online predators often exploit the trust and naivety of young individuals, leading them to dangerous situation. Moreover, the rapid technological advancements and the constant emergence of new social media platforms create a challenging environment for young people to navigate safely. With the ever-changing landscape of social media, youth are often the first to adopt new platforms, making them more susceptible to privacy breaches and unfamiliar threats

Furthermore, the rapid digitization of various sectors in India has introduced new vulnerabilities and attack surfaces, leading to an increased risk of cyber threats. it is imperative for organizations and individuals to prioritize cybersecurity measures, including robust risk management strategies, regular security assessments and the implementation of industry best practices to safeguard against potential cyber-attacks. According to (Siddique et al., 2014) cite that overall, the combination of youthful naivety, trust in social media and lack of awareness about online risks makes the youth population in India a prime target for cyber criminals operating via social media channels. It is imperative to educate and empower young individuals with the knowledge and skills to protect themselves in the digital world

In addition, the emergence of new technologies such as Artificial Intelligence, Blockchain and Internet of Things (IoT) (Varma and Khan, 2017) brings both opportunities and challenges in the realm of cybersecurity. While these technologies have the potential to revolutionize various industries, they also introduce new vectors for cyber-attacks. Therefore, it is essential for India to invest in research and development to stay ahead of cyber threats and harness the potential of these technologies while mitigating associated risks.

To effectively combat cybercrimes, it is essential for India to strengthen international cooperation and information sharing mechanisms to address transnational cyber threats. by fostering partnerships with other countries and international organizations, India can bolster its cyber defence capabilities and collectively combat cybercrime on a global scale.

While the concerns about the rise in cybercrimes in India are valid, it is important to consider he potential drawbacks and limitations presented by overly stringent laws and regulations to combat cybercrimes. Some experts argue that overregulation of the digital space could hamper innovation and stifle free flow of information (Bamrara, 2012). They suggest that instead of solely focusing on imposing stringent laws, there should also be a balance that allows for the continued growth and development of the digital economy while addressing the challenges of cybercrimes.

Furthermore, critics of prioritizing cybersecurity education and awareness initiatives argue that while these efforts are important, there may not be sufficient laws that protect individuals falling victim to cybercrimes. They emphasize the need for greater investment in technological solutions and law enforcement capabilities to actively combat cybercrimes rather than solely relying on educating the populace.

Another perspective to consider is that while international collaboration is essential in addressing cybercrimes, it may lead to concerns about potential infringements on national sovereignty and privacy. Striking a balance between international cooperation and protecting national interests is a delicate matter that requires careful consideration.

(Singh, 2015) suggests the following steps to mitigate cybercrimes on social media:

Update Passwords Regularly: Many social media and email users prefer easy passwords for convenience, but regularly changing them can significantly reduce the risk of internet crime. Complex passwords incorporating not only letters but numbers and special characters should also be used for all types of accounts. Also, the secret question facility should have a challenging answer for making personal data more secure.

Avoid Disclosing Home Address: particularly relevant to women, especially those in prominent business roles, it is the practice of refraining from revealing home address. Instead, opting for a work address or a rented private mailbox can help deter stalkers in social media. Furthermore, minimizing personal information uploaded online can prevent easy access by unauthorised individuals

Maintain Limited Social Circles: While the allure of a large social media following is enticing, it’s advisable to limit one's connections to a manageable number, ideally around 150 individuals with whom genuine social relationships can be maintained. This practice ensures that personal information is shared only with that one truly knows, minimizing exposure to unknown entities.

Conduct Awareness Campaigns: Grassroots awareness campaigns, starting from schools and colleges, are essential for educating individuals about various cybercrimes such as stalking, cheating, defamation and cyber harassment. These initiatives serve to empower people with the knowledge necessary to recognize and combat online threats effectively.

Guard Against Unsolicited Communications: Women should exercise caution regarding unsolicited phone calls and messages, as these could potentially be used for monitoring purposes. Persistent harassment should be documented, with phone calls recorded and reported to the authorities. Downloading applications from trusted sources and confiding in trusted individuals can also provide additional support.

Understand Privacy Settings: It's crucial to familiarize oneself with the privacy policies and settings of social networks and online platforms. By adopting appropriate privacy settings, individuals can minimize their exposure to risks and protect themselves from potential online harm.

Regularly Monitor Accounts: Regularly checking email, blog and website accounts helps individuals stay informed about their online activities and reduces the likelihood of hacking or stalking incidents. Neglecting to monitor accounts can leave individuals vulnerable to exploitation, emphasizing the importance of staying vigilant.

Hence, addressing the complexities of cybercrimes in India requires a concerted effort from government entities, law enforcement agencies, businesses and individuals. By prioritizing cybersecurity at both national and individual levels, India can effectively mitigate the risks posed by cybercrimes and create a safer digital environment for its citizens.

It is clear that the landscape of cybercrimes in India is complex, and there are differing opinions on the most effective strategies to address these challenges. As India, continues to grapple with the escalation of cybercrimes, it is crucial to consider a range of viewpoints and engage in constructive dialogue to develop comprehensive and effective solutions.

Chapter II - Literature Review

(Kumar, 2016) cites that with the advent of internet and the widespread use of social media platforms have transformed the way people communicate, share information and conduct business. As a result, social media has become essential tool for cybercriminals to carry out their illicit activities, including cybercrime.

According to (Koops, 2012), cybercrime refers to criminal activities that are conducted through digital networks or involve the use of computer technology. Numerous studies have highlighted the role of social media in the proliferation of cybercrime in India. These studies reveal that social media platforms such as Facebook, Twitter and WhatsApp are commonly used by cybercriminals to target unsuspecting individuals and organisations. They utilize various tactics, such as phishing, malware distribution and identity theft to exploit vulnerabilities and gain unauthorized access to personal information and financial resources.

Moreover, the anonymity provided by social media platforms makes it challenging to trace cybercriminals, further facilitating the proliferation of cybercrime. Adding to that, the growing popularity and accessibility of social media platforms have also led to an increase in online scams and fraud.

These scams often involve enticing individuals with false promises of financial gain or other benefits, leading them to disclose personal and sensitive information. This information is then used by cybercriminals for fraudulent activities such as identity theft and financial fraud. Additionally, social media platforms have also become breeding grounds for cyberbullying and harassment with individuals misusing it to target and harass others, spread hate speech and engage in online harassment.

Overall, the literature suggests that social media plays a significant role in the proliferation of cybercrime in India (Arshey & Viji, 2021). The misuse of social media platforms and the increasing number of cybercrime incidents have raised concerns among policymakers and law enforcement agencies. Efforts are being made to tackle cybercrime, including raising awareness among users about online safety, implementing stronger security measures on social media platforms and collaborating with international agencies to track and apprehend cybercriminals.

The research study emphasizes the role of social media in the proliferation of cybercrime in India, highlighting how cybercriminals exploit various tactics through platforms such as Facebook, Twitter and WhatsApp to carry out their illegal activities.

The study also underscores the challenges in tracing cybercriminals due to the anonymity provided by social media platforms (Singh et al, 2020). The impact of social media on cybercrime in India goes beyond the technical aspects of illicit activities. its influence extends to the societal and psychological realm. The ease of reaching a wide audience through social media makes it an attractive platform for cybercriminals. Moreover, the anonymity and lack of physical confrontation make it easier for perpetrators to carry out their illegal activities without fear of immediate consequences.

The psychological impact of victims can't also be overlooked as cyberbullying and online harassment can cause severe emotional stress and mental health issues for the affected individuals. Moreover, the financial implications of falling victim to online scams and fraud can be devastating, leading to financial instability and distrust in digital platforms. Furthermore, the role of social media in shaping public perception and spreading misinformation adds another layer of complexity to the proliferation of cybercrime (Imran, 2016). The rapid spread of false information and propaganda on social media can be utilised by cybercriminals to manipulate public opinion and carry out coordinated cyber-attacks.

Understanding the multi-faceted role of social media in the proliferation of cybercrime in India is crucial in developing comprehensive strategies to address this issue. in addition to technological solutions, there is a need for greater emphasis on digital literacy, mental health support for victims and collaboration between various agencies to combat cybercrime effectively. The literature review highlights that such acts of cybercrime is greatly influenced by the role of social media platforms.

These platforms provide a convenient and accessible space for cybercriminals to carry out their illicit activities, exploit vulnerabilities and target unsuspecting individuals. they also play a significant role in the dissemination of misinformation and manipulation of public perception, further fuelling cybercrime activities. the review emphasizes the need for stiffer and uniform mitigation mechanism backed by international laws to combat cyber threats. the increasing participation of people in social media and the lack of adequate measures to protect personal data contribute to the vulnerability to cyber-attacks.

Additionally, the review highlights that certain demographic, such as children and young adults, are particularly vulnerable to cybercrime in India (Vilks, 2019). The lack of maturity and understanding of online risks makes them easy target of cyberbullies and scammers.

In conclusion, the literature review underscores the significant role of social media in the proliferation of cybercrime in India. The misuse of social media platforms has facilitated cybercriminals in carrying out illicit activities such as phishing, malware, distribution, identity theft, online scams and fraud. Furthermore, social media has also become a breeding ground for cyberbullying and harassment, exacerbating the psychological impact on victims.

(Datta et al, 2020) emphasizes the need for comprehensive strategies to address the multifaceted issues associated with the role of social media in cybercrime proliferation. it is crucial to not only focus on technological solutions but also to prioritize digital literacy, mental health support for victims and collaborative efforts between international and domestic organisations to effectively combat cybercrime.

Their study highlights the vulnerability of certain demographics, such as children and young adults to cybercrime, emphasizing the need for targeted protection and education for these groups. Overall, understanding the influential role of social media in cybercrime proliferation is essential for developing and implementing mitigation mechanisms and international laws to combat cyber treats effectively in India. (Dubey and Pateriya, 2023) have studied the extent of awareness regarding cybercrime across different social media platforms among Indian users. It delves into how various sociodemographic factors such as age, family come, usage frequency, urban or rural setting and education level influence the awareness levels among youth concerning fraudulent activities on social media.

(Iqbal and Beigh, 2017) have studied on how India has embarked on several bilateral agreements, such as cyber agreement with Russia, a framework agreement with the US and a recent visit by PM Narendra Modi to Israel to sign the Indo-Israel cyber framework aimed at countering cybercrime. however, these bilateral agreements are deemed to have limited scope and efficacy in addressing cybercrime. However, the authors felt that India requires a multilateral treaty to synchronize its laws under an unified criminal policy and facilitate international cooperation in combating cybercrimes on a global scale. This treaty should aid in the formulation of effective legislation and the development of robust investigative techniques, fostering international collaboration to effectively combat cybercrime. (Malar, 2012) studies the safety and security of users, with special focus on protecting vulnerable group like girls who are often targeted by online sexual predators. The author delves int other impacts of cybercrime, especially within social networking sites, on these victims and how it alters their social networking behaviours. Such cybercrimes leave deep emotional scars, reshaping users' communication patterns within social networks and sometimes compelling them to withdraw entirely from such platforms.

(Hamsa et al., 2018) have conducted research on various prevalent cybercrimes encountered by individuals and assessed the overall awareness levels among young people in a broad conceptual framework. Ther findings revealed that despite endeavours to enhance awareness of information security, there is lack of substantial research on the efficacy of different methods for delivering information security awareness. (Kandpal and Singh, 2013) have researched on cybercrime, analysing its trends and the challenges encountered by Indian users. The authors explored ways to mitigate cybercrimes through the implementation of robust cybercrime laws in India. They also delved into Indian cybercrime statistics, the existence of cybercrime cells nationwide, and other recent developments. National-level agencies are encouraged to devise security protocols and policies aimed at safeguarding internet users from cybercrimes.

(Thuraisingham, 2020) has studied to explore the impact of AI and cyber security on social media platforms, highlighting the advantages of AI and the importance of safeguarding these systems. The author notes that the increasing presence of AI technologies and sophisticated machine learning methods, coupled with the rise of cyber threats, are reshaping how people interact with social media platforms.

(Aggarwal and Kamboj, 2023) delve into the Indian government's endeavours aimed at safeguarding cyberspace and mitigating cybercrimes alongside suggesting preventive measures individuals can adopt to shield themselves from falling victim to cyber criminals. Despite these efforts, the authors highlight a persistent rise in cybercrime rate annually. Therefore, they emphasize the indispensable need for collaborative endeavours between the government and citizens to address the challenge effectively. the government must focus on bridging the divide between policy formulation and execution, while individuals are urged to exercise caution in cyberspace and adhere to guidelines issues by relevant government agencies.

(Shah, 2019) cites that with newly emerging cybercrimes are occurring for the first time, lacking any prior history, their growth rate is remarkably high. To effectively address such incidents, it's imperative for the Indian government and cyber officers to remain updated and prepared to combat any novel cybercrime that may arise at any point in any given year. According to (Sankwar et al, 2023) women are frequently targeted by numerous cybercriminals and fraudsters, making them vulnerable in cyberspace. This insecurity experienced by women underscores the imperative to delve deeper into our comprehension and data regarding cybercrimes targeting women in India.

(Bhat and Ahmad, 2022) study the actualities of cybercrimes against women in practice - assessing the efficacy of Indian laws in safeguarding women (and girls) and fostering a conducive environment for their secure internet usage. The authors cite that social media companies ought to proactively combat online-gender-based abuse online and advocate for the creation of safe spaces for women. They also found out that Instagram doesn't include gendered abuse as a reason for reporting a profile on the platform and by implementing a specific mechanism, a woman's sense of online security can be enhanced.

(Nagarwal, 2019) studies the aspects of cyber harassment and gender-based discrimination on social media platforms. it emphasizes the importance of launching and perpetuating an awareness campaign aimed at addressing gender-related harassment. Suchi initiatives are vital to ensuring that women's grievances are acknowledged, particularly in cases where they encounter online abuse from trolls or violations of their privacy. The author also adds that the judiciary must actively engage in enforcing stricter laws to combat cybercrime effectively. This entails regular review of the regulatory framework overseeing social networking sites. (Singh, 2015) emphasizes that within the realm of cybercrime, its crucial to recognize that violence against women stems from gender discrimination and unequal power dynamics. The author underscores the need to shift mindsets regarding women and cultivate a sense of solidarity, as fostering equality begins with individual attitudes and behaviour

According to (Sankhwar and Chaturvedi, 2018), major cybercrimes that affect women include cyber stalking, defamation, morphing, cyberpornography, email spoofing, phishing and trolling. The authors also added that the underreporting of cyber harassment and related crimes against women and children persists largely due to stigma and parents' reluctance to engage law enforcement in these cases. The reporting process for cybercrimes against women must be streamlined, and the identities of the complainants involved must be safeguarded to prevent these crimes from going unreported. The authors also proposed a Cyber Crime prevention Model, built on three pillars: - Education, Empowerment and Legal Recourse.

Education: - It emphasizes on bolstering the education system within the context of digital India where girls should receive capacity-building classes or workshops starting from the school-level itself

Empowerment: - It motivates women to speak out against cybercrime, fostering an environment conducive to achieving quality across all spheres (i.e. socially, economically, politically and mentally)

Legal Recourse: - This will establish a connection between women and law enforcement. A digital portal can be established, enabling women to report their issues online, facilitating a swift and secure path towards resolution with minimal time and effort.

Chapter III - Research Methodology

The research aims to investigate the connection between social media and the rise of cybercrime in India. This research aims to investigate the proliferation of cybercrimes perpetrated via social media platforms in India. Here, we outline the methodological approach to achieve this objective. The research will employ mixed-methods approach, combining quantitative and qualitative data collection techniques.

This allows for a comprehensive understanding of the phenomenon. The quantitative aspect will focus on the prevalence and nature of cybercrimes committed via social media. The qualitative aspect will focus on the prevalence and nature of cybercrimes committed via social media. The qualitative aspect will delve deeper into the experiences of victims, perpetrators and social media platforms themselves.

Data from official sources like the NCRB will be analysed to understand reported cybercrimes. This data will be examined for trends in cybercrimes linked to social media platforms over a specific period. Reports from cybersecurity agencies and social media platforms themselves can also be valuable sources.

An online survey will also be conducted among social media users to understand their experiences on social media usage, including the usage of platforms and the way it is impacting them. The survey will be target towards a demographically representative sample of the Indian population to ensure generalizability.

Data will also explore experiences in detail, including the tactics used by the criminals and the emotional and financial impact of the crime and any corrective interaction.

The research will also look into social media users to understand their perceptions of cybercrime risks These discussions will explore user awareness of cyber threats, their security practices and their trust in social media platforms to address cybercrime.

In-depth case studies will be conducted on high-profile cybercrimes that have occurred via social media in India. This will provide a richer understanding of the criminal modus operandi, the vulnerabilities exploited and the societal impact of such crimes.

The findings from both quantitative and qualitative data will be triangulated to create a more holistic understanding of the phenomenon. This will further involve identifying areas of convergence and divergence between the different data sources.

Also, informed consent will be obtained from all participants in the study before data collection begins. This will ensure participants understand the purpose of the study, how their data will be used, and their right to withdraw at any point. Any anonymity and confidentiality of participants, if requested, will be maintained through the research process. Data will be anonymized during analysis and reporting, and no personally identifiable information will be shared.

Chapter IV – Data Analysis

According to the NCRB's latest report for 2022, there were a total of 65,893 cases registered for cybercrimes, indicating a 24.4% surge in registrations compared to 2021 (52,974 cases). The crime rate in this category escalated from 3.9 in 2021 to 4.8 in 2022, notably, during 2022, the majority of cyber-crime cases, accounting for 64.8% were motivated by fraud (42,710 cases), followed by extortion with 5.5% (3648 cases) and sexual exploitation with 5.2% (3434 cases).

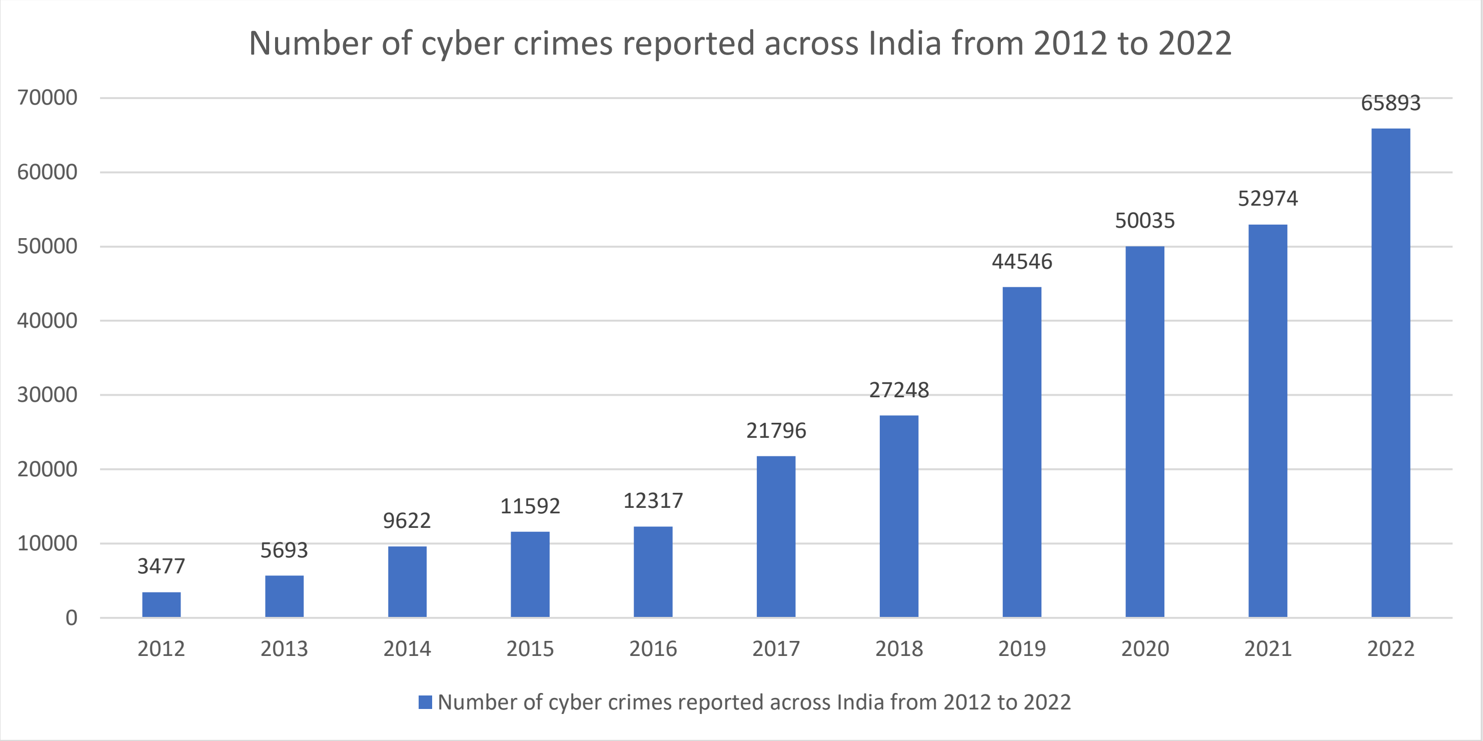
According to another report released the same year, 24,420 registered cases (i.e. 37.06% out of these total) came from top 19 metro cities, marking a significant surge of 42.7% from the previous year's count of 17,115 cases. The cybercrime rate also escalated from 15% in 2021 to 21.4 in 2022. Among the various types of cybercrimes, Computer Related Offences under Section 66 of the IT Act accounted or the highest number of cases, totalling 12,213 cases, constituting 50% of all cybercrimes reported during 2022.

According to (Vij, 2024), recent figures from the Indian Cyber Crime Coordination Centre (I4C) indicate there has been a significant increase in cybercrime via social media in India, particularly targeting the youth demographic. Data indicates that there has been a 63% rise in cyber offenses related to social media platforms, with a staggering 70% of the victims being individuals under the age of 25. Statistics from the Internet and Mobile Association of India reveal that the proliferation of cybercrime via social media has been a 45% increase in cases of online fraud, identity theft and harassment specifically targeting young users. According to a report by National Crime Records Bureau, cybercrimes related to social media in India have shown a concerning upward trend in recent years. The report highlights that there has been a 55% surge in cases of online harassment, cyberbullying and stalking with a significant portion of the victims falling within the age group of 18-24.

According to a report by National Crime Records Bureau, cybercrimes related to social media in India have shown a concerning upward trend in recent years. The report highlights that there has been a 55% surge in cases of online harassment, cyberbullying and stalking with a significant portion of the victims falling within the age group of 18-24.

According to (Scamley, 2018), data from the Indian Computer Emergency Response Team indicates a sharp rise in incidents of social media account hacking and unauthorized access, with a staggering 68% increase in such cases reported in the past year alone. According to an Economic Times report, between 2018 and 2020, India witnessed a surge in cybercrimes targeting women. Instances of posting sexually explicit content online surged by 110%, with reported cases rising from 3076 to 6308.

According to (Basuroy, 2023), in 2022, India witnessed a significant surge in reported cybercrimes compared to the previous year with over 65 thousand incidents recorded. Karnataka and Telangana emerged as the regions with the highest share of such incidents during that period. Uttar Pradesh a northern state, reported the highest number of cybercrimes nationwide in 2018, totalling over six thousand cases and following closely behind was tech-hub Karnataka. A majority of these cases were filed under the IT Act, often involving motives of fraud or sexual exploitation of victims. (Fig 1.1) will show the spike in total number of cybercrimes in India

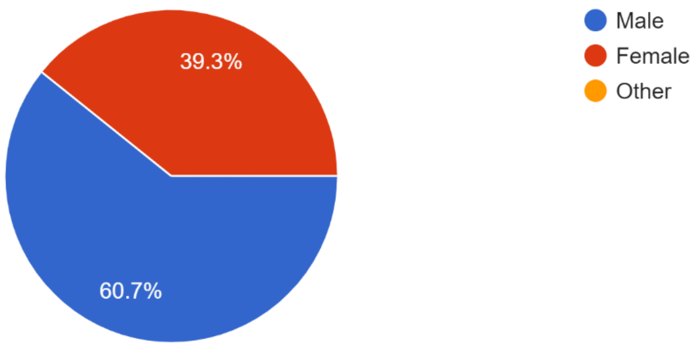


Estimates suggest that in 2017, Indian consumers collectively suffered losses exceeding Rs 1.17 lakh crore due to cybercrimes. However, these figures may be considered conservative, due to chances of underreporting attributed to insufficient awareness about cybercrimes or inadequate reporting mechanisms. Recent governmental initiatives, including the introduction of dedicated online portals for reporting cybercrimes, may have contributed to the notable increase in reported incidents since 2017. The author cites that more than 25,000 men faced arrests for cybercrimes throughout India, in contrast to 541 women apprehended out of which legal proceedings were initiated against all men and 522 women for cybercrime violations across the country.

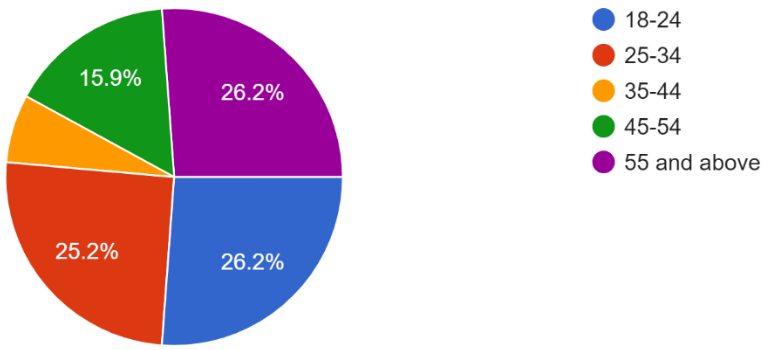
According to a PTI report in 2014, MHA statistics revealed that there were 71,780 reported cyber frauds in 2013, compared to 22,060 in 2012. As of June 2014, there were 63,189 incidents of the same.

Coming to recent figures, data from CERT-In (Indian Computer Emergency Response Team), India's nodal agency for cyber security threats under the Union IT Ministry, indicates that the first two months of 2022 saw more cybercrimes than the entirety of 2018, which indicates a major spike in cases of cybercrime. In 2018, the country reported 2,08,456 cases, followed by 3,94,499 in 2019, 11.5 lakhs in 2020, 14.02 lakhs in 2021 and 2.12 lakhs in the first months of 2022. Hence, this indicates a nearly sevenfold increase in cybercrimes between 2018 and 2021, with a sharper rise during the pandemic.

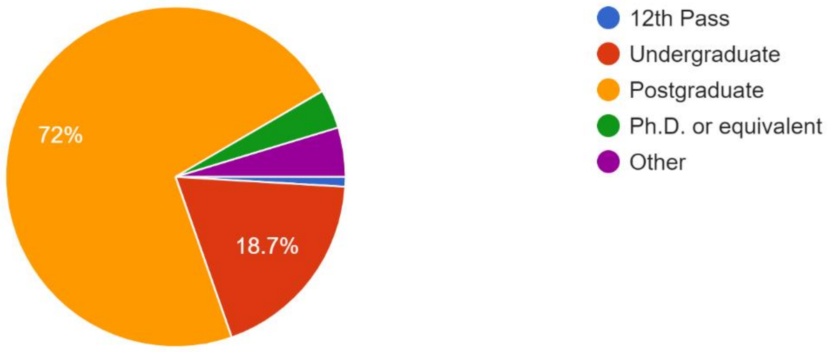
Gender
107 responses



Age Group
107 responses

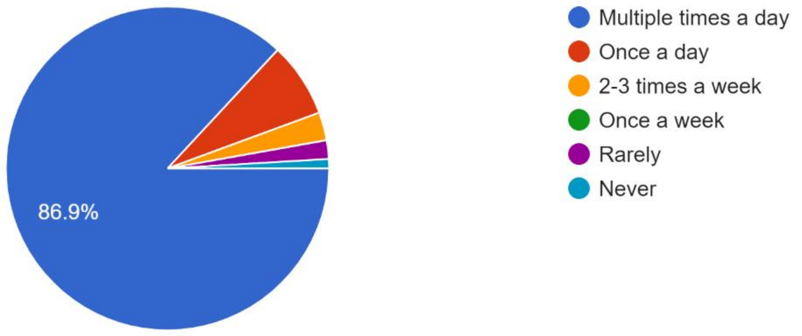


Educational Background
107 responses



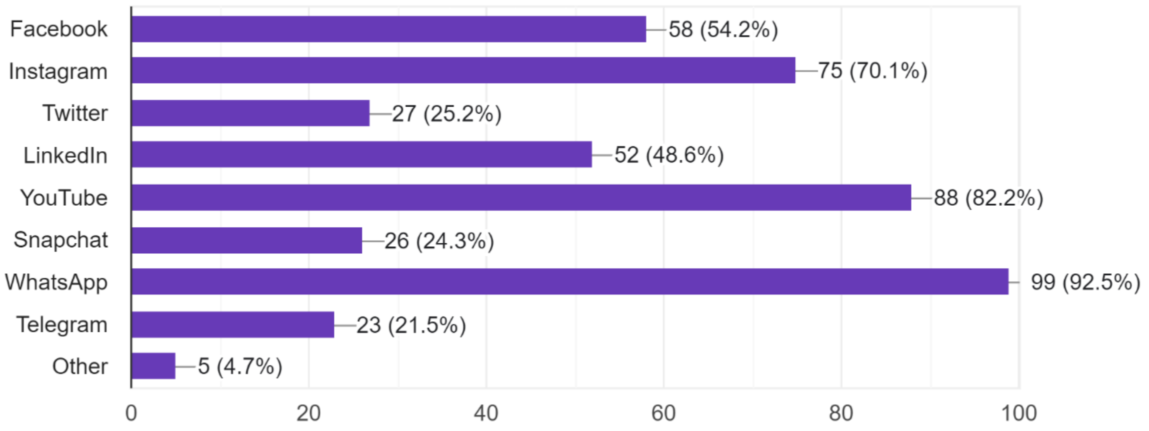
How frequently do you use social media platforms?

107 responses



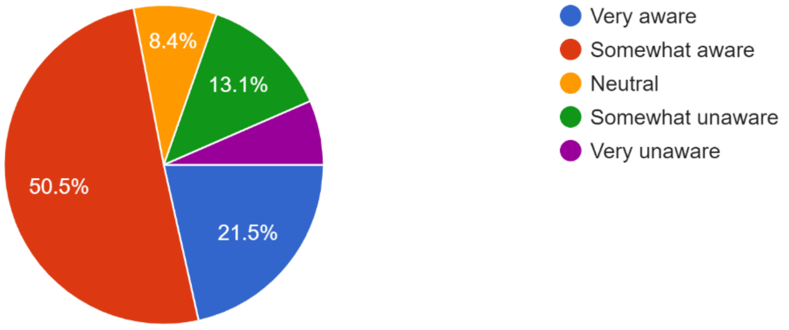
List the social media platforms you use regularly

107 responses



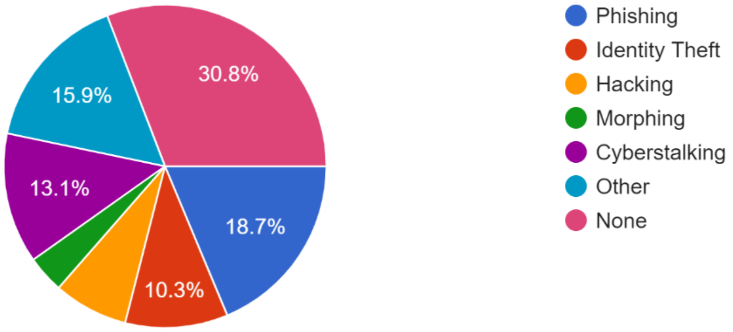
In your opinion, how aware are people of the potential cyber threats associated with social media usage?

107 responses



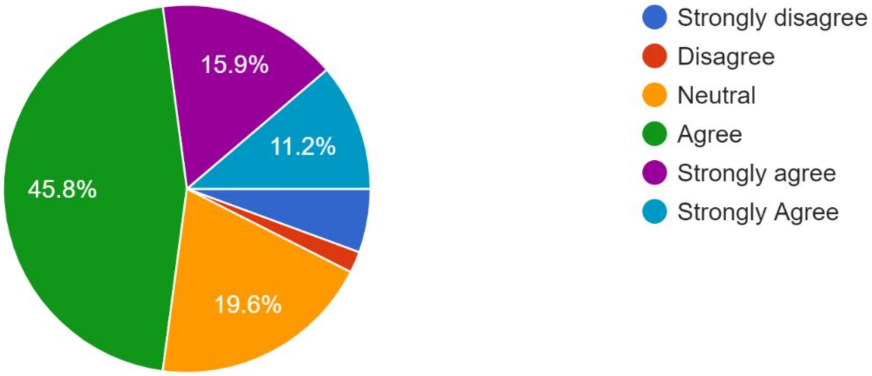
If you have personally experienced any form of cybercrime through social media, what type of crime was it?

107 responses



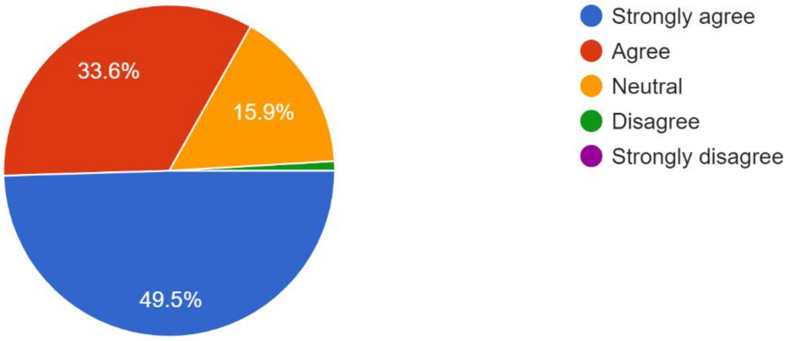
Social media platforms contribute to the proliferation of cybercrime

107 responses



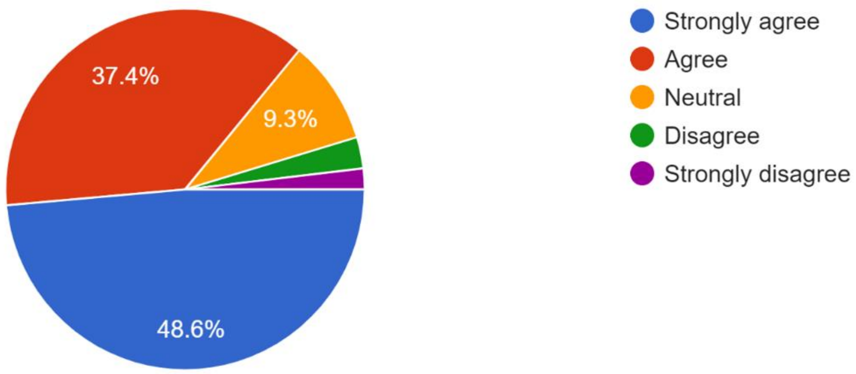
One should update his/her passwords on social media platforms regularly in 1-3 months

107 responses



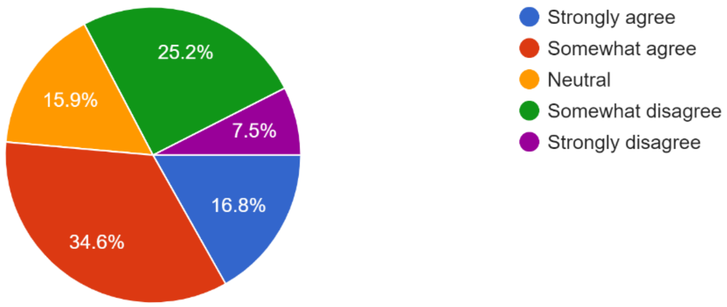
Two-factor authentication on your social media accounts is the need of the hour

107 responses



Do you think social media platforms provide sufficient information and tools to educate users about cybersecurity?

107 responses



This section explores factors associated with cybercrime victimization using a regression analysis. The analysis examines how age group and gender influence the likelihood of experiencing cybercrime.

Model and Variables:

Dependent Variable: Cybercrime Victimization (likelihood of being a victim)

Independent Variables:

Age Group (categorical, representing different age ranges)

Gender (categorical, representing male or female)

Regression Coefficients:

β_0 (intercept)

β_1 (coefficient for Age Group)

β_2 (coefficient for Gender)

ε (error term)

Results and Discussion:

The analysis revealed statistically significant relationships ($p < 0.05$) between both age group and gender and cybercrime victimization.

Age Group: Individuals in two specific age ranges - 55 and above, and 25 to 34 - were found to be more susceptible to cybercrime victimization compared to other age groups.

Gender: The analysis indicated a higher prevalence of cybercrime victimization among females compared to males.

These findings highlight the vulnerability of certain demographic groups, particularly those within the identified age ranges, and emphasize the need for gender-specific strategies when developing cybersecurity measures. Understanding these factors can inform policymakers and cybersecurity professionals in creating targeted interventions to mitigate cyber threats for these vulnerable populations.

Cybercrime has emerged as a significant threat in the digital age, affecting individuals and organizations alike. Understanding the patterns and characteristics of cybercrime victimization is crucial for devising effective preventive measures and interventions. This chapter analyzes the results of a survey conducted to explore the prevalence of cybercrime victimization among respondents, along with the demographic and modus operandi-related patterns associated with such victimization.

Prevalence of Cybercrime Victimization

The survey garnered responses from 107 individuals, revealing that a substantial portion, 74 respondents (69.15 per cent), reported being victims of cybercrime. This finding underscores the pervasive nature of cyber threats and highlights the need for enhanced cybersecurity measures.

Demographic Analysis

Age Group: Analysis by age group revealed distinct patterns in cybercrime victimization. The age groups of 55 and above, and 25 to 34, exhibited the highest incidence rates, with each group comprising 24.3% of the total cases. Notably, the younger age group of 18-24 accounted for 22.9% of the cases, indicating that cybercrime affects individuals across various age demographics. Conversely, the age group of 35 to 44 demonstrated the lowest incidence rate at 9.4%. These findings suggest that individuals of all age groups are susceptible to cyber threats, with younger and older demographics being particularly vulnerable.

Gender: Gender-based analysis revealed that while 40.54% of cybercrime victims were female, the majority, constituting 59.5%, were male. This distribution highlights a potential gender disparity in cybercrime victimization, warranting further investigation into underlying factors contributing to this phenomenon.

Modus Operandi Analysis

Phishing: Phishing emerged as the most prevalent modus operandi among cybercrime victims, accounting for 18.7% of the cases. This finding underscores the effectiveness of phishing attacks in deceiving individuals and compromising their sensitive information.

Identity Theft: Identity theft constituted 10.3% of the reported cases, indicating a significant threat to personal and financial security. The prevalence of identity theft underscores the need for robust identity protection measures to mitigate the risks associated with unauthorized access to personal information.

Cyberstalking, Hacking, and Morphing: Cyberstalking, hacking, and morphing accounted for 13.1%, 7.5%, and 3.7% of the cases, respectively. These findings highlight the diverse range of cyber threats faced by individuals, necessitating multifaceted approaches to cybersecurity.

Other Cybercrimes: Additionally, 15.9% of respondents reported experiencing other forms of cybercrime, reflecting the evolving nature of cyber threats and the need for continuous adaptation of cybersecurity strategies.

CHAPTER V- RESULTS AND DISCUSSION

On the basis of the survey conducted, I had 107 respondents. It was found out that 74 (69.15%) of these respondents have been victim to a certain type of cybercrime such as phishing, hacking, identity theft, morphing, cyberstalking and other types of cybercrime.

In terms of age-group, most cybercrime victims came from age groups of 55 and above and 25 to 34 with 18 cases (24.3%) for each. While the age group 18-24 accounted for 17 (i.e. 22.9%) cases, samples between the age group 45 to 54 accounted for 14 (18.9%) of the cases. The least-affected group (i.e. 35 to 44) had 7 cases (9.4%) to their tally.

In terms of gender, while 30 respondents (40.54%) were found to be females who have been victims of cybercrimes, while the remaining 59.5% were males. While phishing was the most common modus operandi among the victims (accounting for 18.7% of the cases), 11 (10.3%) accounted for identity theft. Cyberstalking accounted for 14 (13.1%), hacking & morphing accounted for 8 (7.5%) & 4 (3.7%) cases respectively and 17 (15.9%) respondents have faced other sorts of cybercrime as victims.

CHAPTER VI- FINDINGS AND SUGGESTION

Following analysis of the results from the survey conducted to understand the literacy of cybercrime, it has been found out that there is a substantial proportion of respondents (i.e. 74) who have reported being victims of cybercrime. This highlights the pervasiveness of cyber threats on social media platforms in India. it is crucial to raise awareness and implement preventive measures to mitigate these risks.

The survey also identified interesting trends regarding age and cybercrime victimization. individuals aged 55 and above, followed by those aged 25-34, emerged as the most susceptible demographics (24.3% each). This suggests a need for targeted interventions catering to these age groups.

There can only be two possible explanations for such findings: - a lack of familiarity with technology and online safety practices might leave them vulnerable to social engineering tactics for the age group of 55 and above. on the other hand, the 25-34 age group might be more active on social media, increasing their exposure to online threats.

Unlike common perception that women are more exposed to cybercrimes, the survey indicated a higher prevalence of cybercrime victims among men (59.5%) though a significant number of women are also affected (40.54%). This emphasizes the need for cybersecurity awareness campaigns tailored for each gender.

Phishing scams emerged as the most dominant modus operandi (18.7% of cases). This aligns with national and international trends highlighting the effectiveness of social engineering tactics in luring victims. Social media platforms can play a crucial role in combating phishing by implementing stricter content moderation policies and user education initiatives.

The survey also identified a concerning prevalence of identity theft (10.3% of cases) and cyberstalking (13.1%). These crimes can have severe consequences for victims, causing financial loss and reputational damage. Additionally, the presence of hacking (7.5%), morphing and other cybercrimes underscores the diverse treats users face on social media.

There are also some limitations to this study. The survey distribution was based on convenience sampling method and as a result, most of the respondents ended up from two specific age groups (i.e. 18-24 and 55 and above). If the survey was primarily shard through social media channels or online forums, it may have reached younger demographics (18-24) more easily.

Additionally, limited access to detailed demographic data on cybercrimes from the records of NCRB (National Crime Records Bureau) also hindered the ability to compare the survey findings with national trends.

CHAPTER VII- CONCLUSION

The findings from the survey underscore the pervasive nature of cybercrime in today's digital landscape. With 69.15 per cent of respondents reporting victimization, it's evident that a significant portion of the population has been affected by various forms of cyber threats. The distribution of victims across different age groups highlights the universal vulnerability to cybercrime, with individuals of all ages being potential targets. Additionally, the gender disparity in victimization rates suggests the need for tailored cybersecurity awareness and protection measures.

Phishing emerged as the most prevalent modus operandi, followed by identity theft, cyberstalking, hacking, and morphing. These findings provide valuable insights into the tactics used by cybercriminals to exploit individuals and organizations. Understanding these patterns is essential for developing effective preventive strategies and enhancing cybersecurity resilience.

Learning Outcomes

- Understanding the prevalence and impact of cybercrime on individuals and society.
- Recognizing the demographic patterns associated with cybercrime victimization, including age and gender disparities.
- Identifying common modus operandi employed by cybercriminals, such as phishing, identity theft, and cyberstalking.
- Appreciating the diverse nature of cyber threats and the need for multifaceted approaches to cybersecurity.
- Acknowledging the importance of continuous awareness and education in mitigating cyber risks and protecting against cybercrime.

Recommendations

- Strengthen cybersecurity education and awareness programs targeting individuals of all age groups, with a focus on recognizing and mitigating common cyber threats.
- Enhance collaboration between government agencies, law enforcement, and private sector stakeholders to combat cybercrime effectively.
- Implement robust identity protection measures, such as multi-factor authentication and encryption, to safeguard personal and financial information.
- Encourage the adoption of cybersecurity best practices, such as regular software updates, secure password management, and cautious online behaviour.
- Foster a culture of cybersecurity resilience within organisations through employee training, incident response planning, and regular security assessments.

By implementing these recommendations and fostering a proactive approach to cybersecurity, individuals and organizations can better defend against cyber threats and minimize the impact of cybercrime on society as a whole.

CHAPTER VIII – INDUSTRY IMPLICATION

This chapter explores the implications of cybercrime proliferation via social media in India for various industries. While this research indicates a higher prevalence among men aged 55 and above falling victim to phishing scams, the threat landscape is constantly evolving. industries that rely heavily on social media engagement or cater to these demographics eed to be particularly vigilant

Financial Services and E-Commerce

Phishing Concerns: The dominance of phishing scams highlights the vulnerability of online financial transactions. Financial institutions and e-commerce platforms must invest in robust security measures, including multi-factor authentication and user education on phishing tactics.

Targeted Scams: Social media allows criminals to tailor phishing attacks to specific demographics. Financial institutions and e-commerce platforms can leverage data analytics to identify high-risk user profiles and implement targeted security warnings and educational campaigns

Reputation Management: Data breaches and financial scams can severely damage an institution's reputation. Strong cybersecurity practices and transparent communication in the event of a breach are crucial for maintaining user trust.

Social Media Platforms

Content Moderation: Social Media platforms have a responsibility to actively combat phishing attempts and other forms of cybercrime. implementing stricter content moderation policies that identify and remove malicious content can significantly reduce the attack surface.

User Education: Social media platforms can play a vital role in educating users about cyber safety practices. This can include interactive tutorials, pop-up warnings and collaborations with cybersecurity experts to create informative content.

User Verification: Implementing stricter user verification processes can help reduce the anonymity that allows cybercriminals to operate. This could include requiring government-issued ID verification or two-step verification for high-risk actions.

Demographic-focused Solutions

Targeted Awareness Campaigns: The research finding that individuals over 55 are more susceptible to phishing scams necessitates targeted awareness campaigns. Financial institutions, social media platforms and even community centres can organize workshops and seminars specifically focused on educating seniors about online safety practices.

Intergenerational Support: Encouraging younger family members to assist older adults in navigating social media can be a valuable strategy. Helping seniors understand privacy settings recognizing phishing attempts and setting up secure online accounts can significantly reduce their risk.

Technological Solutions: Developing user-friendly interfaces and functionalities that prioritize security for seniors and can be a valuable step. features like clear warnings before financial transactions or one-click reporting of suspicious content can empower seniors to navigate social media more safely.

Hence cybercrimes perpetrated via social media pose a significant threat to various industries in India. By understanding the evolving tactics and most vulnerable demographics, can take proactive measures to mitigate these risks. Collaboration between social media platforms, financial institutions, government agencies and user awareness initiatives s crucial to create a safer online environment for everyone. This multi-dimensional approach can help foster a thriving digital economy in India without compromising user safety.

REFERENCES

Vilks, Andrejs. "Cybercrime and sexual exploitation of children in e-environment in the context of strengthening urban and rural security." SHS Web of Conferences. Vol. 68. EDP Sciences, 2019.

AK Roy, "Role of cyber law and its usefulness in Indian IT industry," 2012 1st International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 2012, pp. 143-147

Bamrara, Dr Atul. "The Challenge of Cyber Crime in India: The Role of Government." Pakistan Journal of Criminology 3.3 (2012): 127-134.

Varma, Dr TN, and D. A. Khan. "Curbing Cyber Crimes by Indian Law." Available at SSRN 2922365 (2017).

Kumar, PN Vijaya. "Growing cyber crimes in India: A survey." 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE). IEEE, 2016.

Koops, Bert-Jaap. "Criminal law and Cyberspace as a Challenge for Legal Research." SCRIPTed 9 (2012): 354.

Arshey, M., and KS Angel Viji. "Thwarting cyber crime and phishing attacks with machine learning: a study." 2021 7th international conference on advanced computing and communication systems (ICACCS). Vol. 1. IEEE, 2021.

Singh, Mandeep, Chaman Verma, and Pamela Juneja. "Social media security threats investigation and mitigation methods: A preliminary review." Journal of Physics: Conference Series. Vol. 1706. No. 1. IOP Publishing, 2020.

Imran, Mohd. "Emerging Trends in Cyber Crimes in India: An Over View." Available at SSRN 2818402 (2016).

Datta, Priyanka, et al. "A technical review report on cyber crimes in India." 2020 International conference on emerging smart computing and informatics (ESCI). IEEE, 2020.

Dubey, Pushkar, and Srijan Pateriya. "Social Media and Cybercrime: A Sociodemographic Study of Awareness Level Among Indian Youth." Cybercrime in Social Media. Chapman and Hall/CRC 23-40.

N. Singh and S. K. Sharma, "Review of Machine Learning methods for Identification of Cyberbullying in Social Media," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 284-288

Batra, Mukta. "Cyber-Bullying in India: The Search for a Solution-Why the Current Law Is Ill-Equipped in the Face of Cyber-Bullying." Available at SSRN 2396568 (2013).

Iqbal, Juneed, and Bilal Maqbool Beigh. "Cybercrime in India: trends and challenges." International Journal of Innovations & Advancement in Computer Science 6.12 (2017): 187-196.

Venkatesha, Sushruth, K. Rahul Reddy, and B. R. Chandavarkar. "Social engineering attacks during the COVID-19 pandemic." SN computer science 2 (2021): 1-9.

Agarwal, Chandni, and Akshath Singhal. "Securing our digital natives: A study of commonly experience internet safety issues and a one-stop solution." Proceedings of the 10th international conference on theory and practice of electronic governance. 2017.

Vivek Tripathi (2017) Youth Violence and Social Media, Journal of Social Sciences, 52:1-3, 1-7

Harper, Ness et al. "Gray Hat Hacking : The Ethical Hacker's Handbook" (75-157)

Shaikh, Anjum N., Antesar M. Shabut, and M. Alamgir Hossain. "A literature review on phishing crime, prevention review and investigation of gaps." 2016 10th international conference on software, knowledge, information management & applications (SKIMA). IEEE, 2016.

Halder, Debarati, and K. Jaishankar. "Cyber victimization in India." A baseline survey report. Tirunnelveli, Tamil Nadu, India. Centre for Cyber Victim Counselling (2010).

P, Navitha & Jegadeeshwaran, Dr. (2023). An Empirical Study on Cyber Crimes Against Women and Children in India. International Journal of Advanced Research in Science, Communication and Technology. 141-149. 10.48175/IJARSCT-11327.

Malar, M. Neela. "Impact of cyber crimes on social networking pattern of girls." international Journal of Internet of Things 1.1 (2012): 9-15.

Issac, Biju, Raymond Chiong, and Seibu Mary Jacob. "Analysis of phishing attacks and countermeasures." arXiv preprint arXiv:1410.4672 (2014).

Muhammed T, Sadiq, and Saji K. Mathew. "The disaster of misinformation: a review of research in social media." International journal of data science and analytics 13.4 (2022): 271-285.

Siddiqui, Faizia, Mohammed Iftikhar Alam, and Roshan Lal Raina. "From Facebook to WhatsApp: The changing mood of social networking in India." International Journal of Civic Engagement and Social Change (IJCESC) 1.2 (2014): 23-36.

Nee, Rebecca C. "Youthquakes in a post-truth era: Exploring social media news use and information verification actions among global teens and young adults." Journalism & Mass Communication Educator 74.2 (2019): 171-184.

Hamsa, Sajeesh, Archana Singh, and Nehajoan Panackal. "Study on Effect of Social Networking Sites on the Young World of Cyber Crime." Annual Research Journal of SCMS, Pune 6 (2018): 68-79.

Kandpal, Vineet, and R. K. Singh. "Latest face of cybercrime and its prevention in India." International Journal of Basic and Applied Sciences 2.4 (2013): 150-156.

Kaur, Manpreet, and Munish Saini. "Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions." Education and Information Technologies 28.1 (2023): 581-615.

Meel, Priyanka, and Dinesh Kumar Vishwakarma. "Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities." Expert Systems with Applications 153 (2020): 112986.

Bose, Indranil, and Alvin Chung Man Leung. "Unveiling the mask of phishing: Threats, preventive measures, and responsibilities." Communications of the Association for Information Systems 19.1 (2007): 24.

Thuraisingham, Bhavani. "The role of artificial intelligence and cyber security for social media." 2020 IEEE international parallel and distributed processing symposium workshops (IPDPSW). IEEE, 2020.

Sathisha, H. K., and G. S. Sowmya. "Detecting Financial Fraud in the Digital Age: The AI and ML Revolution."

Aggarwal, Rachna, & Kamboj, Deepmala (2023). AN ANALYSIS OF CYBER CRIME IN INDIA: TRENDS, GOVERNMENT INITIATIVES AND PREVENTIVE MEASURES; Volume -12 , Special Issue-5(Part-A) : Page: 1094 – 1101

Shah, Riddhi. "Cyber Crimes in India: Trends and Prevention." International Journal of Research and Analytical Reviews (IJRAR) 6.1 (2019).

"India is the 80th most targeted country worldwide in cybercrime", NCIS, 24 February 2024

Bhat, Rashid Manzoor, and Peer Amir Ahmad. "Social Media and the Cyber Crimes Against Women-A Study." Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN (2022): 2815-0953.

Saha, Tanaya, and Akancha Srivastava. "Indian women at risk in the cyber space: A conceptual model of reasons of victimization." International Journal of Cyber Criminology 8.1 (2014).

Sehgal, Dhaarna. "Millennials on Social Media and Cyber Security." *Law Essentials J.* 2 (2021): 74.

Rajinder Kumar Vij. "Cybercrime: A Rising Threat to Internal Security. " Centre for Research on Strategic and Security Issues (February 2024)

Rahul Tripathi, ET Bureau. "Cases targeting women with explicit content double in 3 years." The Economic Times (6th January, 2022)

Nagarwal, Narender. "Social Media Crime in Digital World-A Critique through Law, Policy and Practice." Indian JL & Just. 10 (2019): 34.

Singh, Jaspreet. "Violence against women in cyber world: a special reference to India." International Journal of Advanced Research in Management and Social Sciences 4.1 (2015): 60-76.