IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime On Social Media Platform And Its Challenge

Researcher- shefali bajpai (p.k. university,shivpuri)

Supervisor -Dr. Jitendra k.malik professor deptt. Of law P. K. university ,shivpuri

Dr. Hardayveer assistant professor (h.o.d)deptt.of law P.K. university ,shivpuri

Abstract- Social media is a weapon that is capable of construction as well as destruction. The real power of the prevailing social media platforms becomes evident by witnessing the influence created by these platforms on a large scale. It plays a significant role in everyday life. The rising popularity due to its ability to make people attached with kith and kin have paved the way for the world to share photos, feelings, videos, which bears a high-security concern. However, most social media users do not know the underlying security level(s) of the respective account(s), including which features of these social media have to be considered if there is a risky situation. Hence, this would help the police to identify the type of people who would create more crimes. These results would help the police to narrow down their search on criminals for better surveillance. The police must focus on those with these factors while monitoring social media.

Key words- social media, cyber crime ,cyber criminals

Introduction -Social media has become an integral part of our daily lives, connecting individuals, businesses, and organizations globally. However, as the influence of social media continues to grow, so does the dark side associated with it. Cybercrimes on popular social media platforms have become a pervasive issue, posing threats to individuals, organizations, and even national security. In this article, we delve into the multifaceted aspects of cybercrimes on social media.

What Is Social Media Social media are websites and programmes that help people talk to each other, get involved, share information, and work together. People use social media to stay in touch with their friends, family, and neighbours. Social media is a computer technology that allows people to share ideas, views, and information through networks and online communities. People use software or web apps on their computers, tablets, or phones to use social networks. Social media on the Internet facilitates the rapid and electronic sharing of personal information, documents, movies, and photos.

Understanding Social Media as a Platform for Cybercrimes

Social media platforms serve as a virtual world where billions interact, share information, and build connections. The sheer volume of personal data exchanged on these platforms makes them attractive targets for cybercriminals. Understanding social media as a platform for cybercrimes involves recognizing the vulnerabilities in these virtual spaces.

1. Inadequate Security Measures

While social media platforms implement security measures to protect user data, these measures are not foolproof. Cybercriminals exploit vulnerabilities in platform security, often through sophisticated techniques, to gain unauthorized access to user accounts, compromising personal information.

2. Rapid Increase in the Number of Fake Profiles and Impersonation

The ease of creating fake profiles on social media platforms facilitates impersonation which is a common tactic used by cybercriminals. These fraudulent accounts can be employed for various malicious activities, including spreading misinformation, engaging in social engineering attacks, and even committing financial fraud.

Dangers Of Cybercrimes On Social Media for Individuals and Organizations

The consequences of cybercrimes on social media extend beyond the individual level, impacting organizations and their stakeholders. The interconnected nature of social media makes it vulnerable to all types of threats that can harm both personal and professional lives.

1. Reputational Damage

For businesses and organizations, maintaining a positive online reputation is crucial. Cybercriminals exploit social media platforms to break down the image of companies through tactics such as spreading false information, defaming key figures, or creating fraudulent accounts in the organization’s name.

2. Financial Loss and Identity Theft

Individuals are vulnerable to financial losses and identity theft through cybercrimes on social media. Phishing attacks, for instance, can trick users into revealing sensitive information, leading to unauthorized access to bank accounts, credit cards, or other personal assets.

Impact of Social Media on Cybercrime

The dynamic landscape of social media serves as a breeding ground for cybercrimes and influences the overall trends in cybercriminal activities.

1. Amplification of Traditional Cybercrimes

Social media platforms amplify traditional cybercrimes by providing a vast and interconnected user base. Crimes such as phishing, identity theft, and financial fraud increase when it’s done on social media due to the sheer volume of potential targets.

2. Rapid Spread of Malicious Content

The virality of content on social media contributes to the rapid spread of malicious content, including malware, ransomware, and other harmful software. Cybercriminals leverage social engineering techniques to influence users into clicking on infected links, leading to widespread compromise of personal and organizational data.

Social Media Platforms as Malware Distribution Centers

One of the lesser-known aspects of cybercrimes on social media is the role these platforms play as distribution centers for malware. Malicious actors utilize various strategies to spread harmful software, exploiting the trust users place in these platforms.

1. Infected Advertisements

Malware-laden advertisements often find their way onto users' timelines through targeted advertising. Clicking on such ads may lead to the inadvertent download of malware, compromising the user's device and potentially spreading the infection to others within their network.

2. Compromised Third-Party Apps

The integration of third-party applications with social media platforms introduces additional vulnerabilities. Cybercriminals create fake apps or exploit security loopholes in legitimate ones, leading to the installation of malware on users' devices when these apps are downloaded and used.

Common Cybercrime Methods on Social Media

Understanding the common attack methods employed by cybercriminals on social media is essential for users and organizations to bolster their defenses against these threats.

1. Phishing Attacks

Phishing remains a prevalent method of cyberattack on social media. Cybercriminals create fake login pages or send deceptive messages, tricking users into revealing their login credentials or other sensitive information.

2. Account Takeovers

Account takeovers involve cybercriminals gaining unauthorized access to user accounts by exploiting weak passwords, utilizing leaked credentials, or employing social engineering tactics. Once in control, attackers can manipulate account content, impersonate the user, or conduct further malicious activities.

3. Social Engineering

Social engineering attacks manipulate human psychology to deceive individuals into divulging confidential information. Cybercriminals leverage social media platforms to gather information about their targets, making these attacks highly personalized and difficult to detect.

Emerging Threats to Social Media Users and the Businesses that Employ Them

As technology evolves, so do the tactics employed by cybercriminals. Emerging threats pose new challenges to social media users and organizations that rely on these platforms for communication and marketing.

1. Deepfake Technology

Deepfake technology, powered by artificial intelligence, enables the creation of highly convincing fake videos or audio recordings. Social media can be exploited to disseminate deepfake content, potentially causing reputational damage, spreading misinformation, or even manipulating public opinion.

2. Cyber Extortion and Ransomware

Cyber extortion on social media involves threats of revealing sensitive information, manipulating private data, or disrupting online activities unless a ransom is paid. Ransomwareattacks which encrypt user data until a ransom is paid, can also target individuals and organizations through social media channels.

3. Data Privacy Concerns

The increasing emphasis on data privacy brings forth new challenges for social media platforms. As regulations tighten, cybercriminals may focus on exploiting gaps in compliance or targeting users directly to gain unauthorized access to sensitive personal information.

Strategies for Mitigating Social Media Cybercrimes

In combating the dark side of social media, it is imperative to adopt proactive strategies that address the evolving nature of cyber threats. Individuals, organizations, and social media platforms must work collaboratively to mitigate the risks and enhance the overall security posture of the digital landscape.

1. User Education and Awareness

User education is a fundamental pillar in the fight against social media cybercrimes. By educating users about the various attack methods, the importance of strong passwords, and the risks associated with sharing sensitive information, individuals can become more resilient against cyber threats. Social media platforms should play an active role in promoting digital literacy through tutorials, webinars, and in-app notifications.

Without question, technology can safeguard your data to a significant degree, but humans remain one of the weakest points in the chain where cybercrime can take place. However, it would be best if you didn’t worry because UniSense Advisory will take care of this for you.

UniSense Advisory combines everything, from analyzing the risks of cybercrime to creating a culture of digital security. The tools required to combat cybercriminals include risk analysis and management organizational training,

2. Two-Factor Authentication (2FA)

Enabling two-factor authentication adds an additional layer of security to user accounts, requiring a second form of verification beyond the password. This significantly reduces the likelihood of unauthorized access, even if login credentials are compromised. Social media platforms should encourage and facilitate the adoption of 2FA to enhance user account security.

3. Strengthening Platform Security

Social media platforms bear a significant responsibility in ensuring the security and privacy of their users. Regular security audits, prompt patching of vulnerabilities, and investing in advanced security measures, such as machine learning algorithms for anomaly detection, can bolster platform security. Timely communication with users about security updates and ongoing threats is crucial for maintaining a vigilant user base.

4. Collaboration with Law Enforcement

Cooperation between social media platforms and law enforcement agencies is essential in addressing cybercrimes effectively. Timely sharing of information, joint investigations, and the pursuit of legal actions against cyber criminals can serve as deterrents and contribute to the overall reduction of cyber threats on social media.

5. Implementing Strict Content Policies

Social media platforms should enforce stringent content policies to combat the dissemination of malicious content, deepfakes, and other harmful material. Automated content moderation tools, combined with human oversight, can help swiftly identify and remove inappropriate or dangerous content.

Case Studies of Social Media Cybercrimes

Examining real-world case studies provides valuable insights into cybercrimes' varied nature and impact on social media. Analyzing past incidents helps individuals and organizations understand the tactics employed by cybercriminals and reinforces the importance of robust cybersecurity measures.

1. The 2018 Facebook Data Breach

In 2018, Facebook faced a massive data breach that affected nearly 87 million users. The breach, orchestrated by Cambridge Analytica, involved illegally harvesting personal data for political purposes. This incident highlighted the vulnerabilities in social media platforms regarding user data and sparked a global conversation about privacy and data protection.

2. Twitter Bitcoin Scam

In July 2020, a high-profile Twitter hack targeted several prominent accounts, including those of Barack Obama, Elon Musk, and Bill Gates. The attackers used compromised accounts to promote a Bitcoin scam, urging followers to send cryptocurrency to a specified address. This incident underscored the potential financial implications of social media cybercrimes and emphasized the need for improved account security.

3. Instagram Phishing Attacks

Instagram has been a hotbed for phishing attacks, with cybercriminals creating fake login pages to trick users into revealing their account credentials. These attacks often involve fraudulent messages or emails posing as official Instagram communications. The frequency of such incidents emphasizes the ongoing challenges of maintaining secure user accounts on popular social media platforms.

Future Trends and Challenges Of Cybercrimes On Social Media

Looking ahead, it is crucial to anticipate future trends and challenges in the realm of social media cybercrimes. The evolving landscape of technology introduces new opportunities for cybercriminals, necessitating continuous adaptation and innovation in cybersecurity measures.

1. AI-Powered Attacks

As artificial intelligence advances, cybercriminals may leverage AI-driven techniques to conduct more sophisticated and targeted attacks. AI-powered chatbots and deep learning algorithms could be used to enhance the effectiveness of social engineering attacks, making it increasingly challenging to distinguish between legitimate and malicious interactions.

2. Quantum Computing Threats

The development of quantum computing poses both opportunities and challenges for cybersecurity. While quantum computing has the potential to break existing encryption algorithms, it also opens avenues for developing quantum-resistant cryptographic methods. Social media platforms must stay ahead of the curve in adopting quantum-safe encryption to protect user data in the post-quantum computing era.

3. Increased Focus on Social Media Regulations

As the impact of social media on society becomes more evident, governments and regulatory bodies are likely to increase their focus on implementing and enforcing regulations. Stricter data protection laws, enhanced privacy measures, and penalties for non-compliance may reshape the way social media platforms operate, impacting both users and cyber criminals.

Conclusion

In conclusion, the dark side of social media manifested through cybercrimes on popular platforms, is a multifaceted challenge that demands collective and adaptive solutions. As individuals, organizations, and social media platforms work together to fortify defenses and raise awareness, the digital landscape can become more resilient against the ever-evolving tactics of cybercriminals. The capacity of the human mind is immeasurable. It is not possible to remove cybercriminals from cyberspace. It is entirely possible to test them. History is witness that no law has succeeded in eliminating crime from the planet. The only measure that can be done is to make people aware of their rights and obligations (denunciation of crimes is a collective obligation to society) and tighten the application of the law to control crime. Without a doubt, France is a historic step forward in the cyber world. Furthermore, I do not deny that it is necessary to change the Information Technology Act to make it more effective in the fight against cybercrime. I would like to close with a warning to the pro-law school to remember that the provisions of cyber law are not implemented so strictly that they can stifle industry growth and backfire. Various media have been used to create awareness and knowledge about it. And that gave birth to the concept of social cognitive communication. Social awareness communication can be defined as an important strategy for informing the public about social concerns and keeping important social issues on the public agenda.

ReferencesJenifer Stella, S., and S. Ambika Kumari. "Cyber Space-A Critical Analysis On The Feminine Facet." (2022).
2. Mambi, Adam J. ICT law book: A source book for information and communication technologies & cyber law in Tanzania & East African community. African Books Collective, 2010.
3. Sahoo, Ms Deepali Rani, and Pooja Kapoor. "An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India." Computers in Human Behavior 25.5: 1089-1101.
4. Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber crime and cyber laws of India." International Research Journal of Engineering and Technology (IRJET) 4.6 (2017): 1633-1640.
5. Brenner, Susan W. "US cybercrime law: Defining offenses." Information Systems Frontiers 6.2 (2004): 115.
6. Karnika Seth, Computer, internet and new technology laws, (2016), Lexis Nexis, New Delhi.
7. Castañeda, J. Alberto, Francisco J. Montoso, and Teodoro Luque. & quot;The dimensionality of
8. customer privacy concern on the internet.& quot; Online Information Review (2007).
9. Shilpa Dongre (2015), Cyber law and its applications, Current Publication, Mumbai
Jenifer Stella, S., and S. Ambika Kumari. "Cyber Space-A Critical Analysis On The Feminine Facet." (2022).
2. Mambi, Adam J. ICT law book: A source book for information and communication technologies & cyber law in Tanzania & East African community. African Books Collective, 2010.
3. Sahoo, Ms Deepali Rani, and Pooja Kapoor. "An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India." Computers in Human Behavior 25.5: 1089-1101.
4. Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber crime and cyber laws of India." International Research Journal of Engineering and Technology (IRJET) 4.6 (2017): 1633-1640.
5. Brenner, Susan W. "US cybercrime law: Defining offenses." Information Systems Frontiers 6.2 (2004): 115.
6. Karnika Seth, Computer, internet and new technology laws, (2016), Lexis Nexis, New Delhi.
7. Castañeda, J. Alberto, Francisco J. Montoso, and Teodoro Luque. & quot;The dimensionality of
8. customer privacy concern on the internet.& quot; Online Information Review (2007).
9. Shilpa Dongre (2015), Cyber law and its applications, Current Publication, Mumbai

References

1.Jenifer Stella, S., and S. Ambika Kumari. "Cyber Space-A Critical Analysis On The Feminine Facet." (2022).

2. Mambi, Adam J. ICT law book: A source book for information and communication technologies & cyber law in Tanzania & East African community. African Books Collective, 2010.

3. Sahoo, Ms Deepali Rani, and Pooja Kapoor. "An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India." Computers in Human Behavior 25.5: 1089- 1101.

4. Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber crime and cyber laws of India." International Research Journal of Engineering and Technology (IRJET) 4.6 (2017): 1633-1640

. 5. Brenner, Susan W. "US cybercrime law: Defining offenses." Information Systems Frontiers 6.2 (2004): 115.

6. Karnika Seth, Computer, internet and new technology laws, (2016), Lexis Nexis, New Delhi.

7. Shilpa Dongre (2015), Cyber law and its applications, Current Publication, Mumbai.

8. https://www.thelawcodes.com/cyber-crime-social-media-and- information-technologyact/
9.https://economictimes.indiatimes.com/definition/social-media.