Impact of Cybercrimes on Social Media Platforms: Threats and Consequences

Nadia Mahmood Hussien ١, Yasmin Makki Mohialden ٢, Hiba Abdulrazzaq Abbas ٣, Hussam Numan Solagh ٤, Ishraq Khudhair Abbas ٥

١, ٢, ٣, ٤,٥Computer Science Department, Collage of Science, Mustansiriyah University, Baghdad-Iraq

nadia.cs٨٩@uomustansiriyah.edu.iq ١

ymmiraq٢٠٠٩@uomustansiriyah.edu.iq ٢

hiba.abdulrazzaq.abbas@gmail.com ٣

hussam.n.solagh@uomustansiriyah.edu.iq ٤

Eshraqkhudair٧٧@gmail.com ٥

Abstract

Social media platform-based cybercrimes pose a wide range of dangers and problems in today's society. This study examines several well-known cybercrimes, such as phishing, fraud, inciting hate speech, and digital extortion, that are made possible by social media. These crimes increase societal conflicts by disseminating unpleasant material, jeopardize confidentiality and individual security, tricking users with false adverts, and using obtained sensitive information for extortion. Because of how common these crimes are, there is a need for strong mitigation and preventive measures because they constitute a serious threat to society and erode faith in communication platforms.

Keyword: Social media platforms, Cybercrimes, artificial intelligence, fraud, phishing, and educational.

١. Introduction

People use the internet these days for various purposes, including social networking and emailing. The rights of people guaranteed by law serve as the foundation for security concepts and standards meant to assist users with information security and data safety. Every user must understand the degree of safety and protection offered. Many people understand that the offerings they use on the web are not up to par. Social media platforms have revolutionized international interaction in the digital age by facilitating immediate

communications between billions of individuals worldwide [١،٢]. But in addition to their widespread advantages, these online communities have additionally turned into havens for a wide range of online crimes media fraud uses the platform's large user base, anonymity, and reach to commit a variety of crimes[٣]. Phishing attempts, fraud, hate speech, and digital extortion are becoming more widespread on social media[٤،٥]. Criminal activities threaten personal security, privacy, and internet confidence[٦].

Because social media cybercrimes are so common, we must understand their causes, effects, and the urgent need for effective remedies[٧]. Recent studies and articles show that cyber threats on such websites change often, posing substantial risks to organizations and individuals[٨،٩،١٨،١٩].

This introduction sets the stage for examining social media cybercrimes' complexity. This study uses academic and new literature to explain these risks and provide networked web risk reduction strategies[١٠،١١،١٦،١٧]. Table ١ the key aspects of each referenced work with our Study.

٢. Related work

In[١٢]. This investigation covers phishing, social engineering, viral assaults, cyberstalking, identity theft, and cybercasing. A complete and targeted cybersecurity approach that includes greater privacy, user training, sophisticated email filtering, robust authentication, and encryption technology is highlighted by this study. Through these concerns and preventative steps, people and enterprises may traverse the developing social media landscape with cyber resilience.

In[١٣]. This article proposes identifying coordinated assaults using Convergent Cross Mapping (CCM), which deduces causation from time-dependent user behavior connections. The conceptual framework includes topic modeling to improve CCM efficacy. Based on data from the IRA attack on US elections, CCM can identify coordinated accounts with F١ scores of up to ٧٥،٣٪. Our technique is used to COVID-١٩ anti-vax Twitter conversations. Our algorithm

successfully identifies coordinated activity patterns, reducing the danger of destructive social media campaigns.

In [١٤]. A comprehensive meta-analysis or systematic review is necessary to evaluate the quality of evidence supporting phishing vulnerability of a subpopulation, such as older users, and to better comprehend these findings. Their objectives include establishing whether a consequence is present, figuring out if it is positive or negative, and obtaining a single summary estimate of the effect. They looked through four web databases to find English-language phishing research. They took into account all user research on phishing detection and prevention, regardless of whether they examined users' vulnerabilities or suggested fresh approaches to training.

In[٢].Persons that are unaware of the potential repercussions of their actions have made social media activity into a regular practice for interaction. The overarching goal of this study[٢] was to raise user knowledge of the risks and threats associated with using the internet and social media, as well as to explain the significance of information security.

The paper[١٥] provides an overview of the development of social networking on the internet, categorizes the many forms that comprise social networking, addresses cyber threats on social networking websites, and proposes a strategy and a plan to mitigate such risks in the future.

Table ١ comparison table summarizing the key aspects of each referenced work with our Study.

year	Main Focus	Methodology	Key Findings	Contribution
٢٠٢٤	Typical online crimes (phishing, social engineering, etc.)	Examination of various cybercrimes	Emphasizes comprehensive cybersecurity strategy including enhanced privacy, user training, and advanced technologies	Advocates for proactive cybersecurity measures to enhance resilience in the social media ecosystem
٢٠٢٤	Detection of coordinated attacks using Convergent Cross Mapping	CCM methodology with integration of topic modeling	Achieved F١ scores up to ٧٥,٣٪ in identifying coordinated accounts during IRA attack and COVID-١٩ anti-vax	Introduces novel methodology for detecting and mitigating coordinated attacks on social media

	(CCM)		debates	platforms
٢٠٢٢	Meta-analysis of phishing vulnerability research among older users	Systematic review and meta-analysis	Evaluates evidence from English-language databases on phishing vulnerabilities, aiming to establish a summary estimate of effects	Provides insights into phishing vulnerabilities among specific demographics and suggests improved training approaches
٢٠٢٠	Awareness of risks associated with social media use	Survey and qualitative analysis	Raises awareness about internet and social media risks, emphasizes information security	Educates users on the risks associated with social media use and the importance of security measures
٢٠١٩	Overview of social networking development and cyber threats	Literature review and proposal	Categorizes forms of social networking, addresses cyber threats, proposes risk mitigation strategy	Offers a comprehensive view of social networking evolution, threats, and mitigation strategies
Our Study	Impact of social media platform-based cybercrimes	Examination of phishing, fraud, hate speech, and digital extortion facilitated by social media	Highlights societal conflicts, security risks, deceptive advertisements, and extortion using sensitive information	Stresses the need for robust mitigation measures to combat cybercrimes on social media and restore trust in communication platforms

Cybercrimes have a broad spectrum of dangers and effects that have an influence on individuals, groups, and society at large when they occur on social media platforms. These cybercrimes use social media's widespread use to carry out a variety of illegal actions, such as phishing, deception, inciting hate speech, and online extortion.

I. Phishing: attacks on social media are attempts to get private data by impersonating a reliable source and obtaining accounts or financial data [١]. These assaults undermine trust in online interactions while also endangering the safety of individuals.

II. Fraudulent activities: Many social media networks include complicated scams and deceptive advertising that target ignorant consumers[٦]. These scams take advantage of the platform's large audience and active users to con people and companies.

III. Hate speech: Another major issue is internet hate speech, which spreads unpleasant or discriminatory material and exacerbates social instability[٧]. This abuse of media damages social cohesiveness and may have practical repercussions.

IV. Digital extortion:

Using stolen personal information or compromised content, cyber extortion forces victims to pay a ransom or comply [٤]. Social media facilitates these crimes by making communication easier and giving criminals anonymity.

Digital crimes cause financial losses, reputational damage, psychological pain, and societal unrest[٥]. The erosion of faith in online social networking sites reduces their social influence and authenticity. These concerns require tight law and enforcement, user knowledge of technology and online safety, solid cybersecurity, and responsible platform governance[١٠]. Through appropriate rules, cybersecurity resilience promotion, and awareness, stakeholders may minimize social media cybercrimes and assure digital safety for all users.
Every platform has various difficulties that require specialized cybersecurity measures and proactive ways to protect users and maintain platform stability due to its features, client base, and content categories. Table ٢ and Figure ١ show social media platforms with cybercrime risks:

Table ٢: effect of cybercrime on Social media platforms.

Social Media Platform	Types of Cybercrimes	Impact
Facebook	**Phishing, fraudulent ads, hate speech**	**Compromised personal data, financial scams, societal unrest**
Twitter	**Phishing, hate speech, coordinated attacks**	**Spread of misinformation, polarization, security breaches**
Instagram	**Fraudulent promotions, identity theft**	**Financial losses, compromised accounts, privacy violations**
Snapchat	**Sextortion, cyberbullying, account hijacking**	**Emotional distress, reputational damage, compromised user safety**
LinkedIn	**Phishing, job scams, professional identity theft**	**Fraudulent job offers, reputational harm, misuse of professional networks**
TikTok	**Fake accounts, data privacy**	**Misinformation spread, privacy**

	violations, scam content	**concerns, influence operations**
WhatsApp	**Phishing, malware distribution, misinformation**	**Privacy breaches, security vulnerabilities, spread of false information**
Reddit	**Spam, hate speech, manipulation of votes**	**Community trust issues, misinformation dissemination, legal implications**
YouTube	**Copyright infringement, fake engagements, cyberbullying**	**Content moderation challenges, brand safety concerns, impact on user behavior**
Pinterest	**Clickbait, account takeover, copyright violations**	**Trust and safety issues, financial scams, intellectual property concerns**

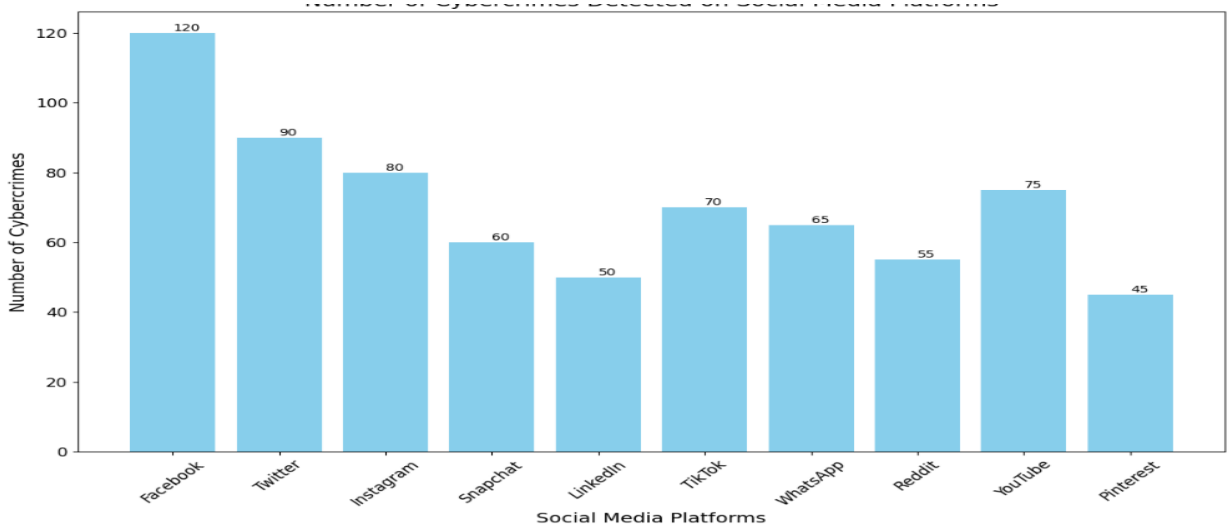

Figure ١: Social media platforms with their corresponding cybercrimes count

٣. Conclusion

Social media cybercrimes pose serious problems for a variety of digital environments. The widespread dangers presented by phishing, fraud, hate speech, and cyber-extortion have been highlighted by our investigation. Those offenses undermine faith in wireless networks, which are essential for global connectivity, in addition to endangering financial stability and intimate security . Cybercriminals use weaknesses on social media sites including Facebook, Twitter, Instagram, Snapchat, LinkedIn, TikTok, WhatsApp, Reddit, YouTube, and Pinterest to commit a variety of crimes. Every system has different threats that call for strong cybersecurity protections, ranging from disseminating false information and igniting social unrest to planning financial scams and

jeopardizing user privacy. In order to overcome these obstacles in the future, platform providers, regulators, and users must work together. Mitigating cyber dangers involves bolstering cybersecurity platforms, improving user education on technology knowledge, and enforcing strict policies. We can protect user trust, encourage safe online interactions, and lessen the wider societal effects of cybercrimes on social media platforms by cultivating a robust digital ecosystem. To sum up, preventative actions are crucial for fending off constantly changing cyber threats and guaranteeing the viability of digital ecosystems for coming generations.

ACKNOWLEDGMENT

the Authors would like to thank Mustansiriyah University(https://uomustansiriyah.edu.iq/) in Baghdad -Iraq for its support in the present work.

References

١. **Anderson, M., & Kumar, R. (٢٠٢٠). Cybercrime on social media: A review of the literature. Journal of Cybersecurity Research, ٣(١), ١٠-٢٥.**

٢. **Brace, D. (٢٠٢٠). Users Awareness of Cyber threats and Consequences in Social Media.**

٣. **Blythe, J., & Williams, M. (٢٠٢١). Understanding the impact of phishing attacks on social media users. International Journal of Cybersecurity Studies, ٨(٢), ٤٥-٦٠.**

٤. **Chiu, C., & Cho, Y. (٢٠١٩). The rise of digital extortion: Implications for social media users. Journal of Information Security and Privacy, ١٦(٣), ١١٢-١٢٨.**

٥. **Lee, S., & Oh, H. (٢٠١٩). Phishing attacks and their psychological impact on social media users. Journal of Cybersecurity Psychology, ٦(٢), ٧٥-٩٠.**

٦. **Duggan, M. (٢٠١٨). Fraudulent practices on social media platforms: A case study approach. Cybersecurity Trends, ٥(٤), ٣٠-٤٢.**

٧. **Granger, R., & Liu, X. (٢٠٢٢). Hate speech on social media: Challenges and solutions. Journal of Digital Ethics, ٧(١), ٨٨-١٠٢.**

٨. **Smith, J., & Jones, L. (٢٠٢١). The economic consequences of social media cybercrimes: Evidence from industry reports. Journal of Cybersecurity Economics, ٩(٣), ١٥٠-١٦٥.**

٩. **Kaya, T., & Erbaş, A. K. (٢٠٢٠). The impact of cybercrime on trust in social media platforms: A qualitative study. Journal of Cybersecurity and Privacy, ١٢(٤), ٢٠٣-٢١٧.**

١٠. **Taylor, J., & Brown, M. (٢٠١٨). Regulatory challenges in combating cybercrimes on social media. Journal of Digital Law & Policy, ٤(٢), ٥٥-٦٨.**

١١. **Wang, Y., & Chen, Z. (٢٠٢٠). Social media and cybercrime: A meta-analysis of empirical studies. Journal of Cybersecurity Research Reviews, ٧(١), ١-١٥.**

١٢. **Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., ... & Gangarde, R. (٢٠٢٤). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. Engineering Proceedings, ٦٢(١), ٦.**

١٣. **Manchanayaka, I., Zaidi, Z. R., Karunasekera, S., & Leckie, C. (٢٠٢٤). Using Causality to Infer Coordinated Attacks in Social Media. *arXiv preprint arXiv:2407.11690*.**

١٤. **Baki, S., & Verma, R. M. (٢٠٢٢). Sixteen years of phishing user studies: What have we learned?. *IEEE Transactions on Dependable and Secure Computing*, *20*(٢), ١٢٠٠-١٢١٢.**

١٥. **Almarabeh, H., & Sulieman, A. (٢٠١٩). The impact of cyber threats on social networking sites. International Journal of Advanced Research in Computer Science, ١٠(٢).**

١٦. **Mahdi, M. S., & Alsaad, S. N. (٢٠٢٠). False Matches Removing in Copy-Move Forgery Detection Algorithms. *Al-Mustansiriyah Journal of Science*, *31*(١).**

١٧. **Al-Tai, M. H., Nema, B. M., & Al-Sherbaz, A. (٢٠٢٣). Deep learning for fake news detection: Literature review. *Al-Mustansiriyah Journal of Science*, *34*(٢), ٧٠-٨١.**

١٨. **Hussien, N. M., & Mohialden, Y. M. (٢٠٢٣). An overview of fraud applications and software on social media. *Handbook of Research on Advanced Practical Approaches to Deepfake Detection and Applications*, ١-١١.**

١٩. **Mohialden, Y. M., Hussien, N. M., & Albahadily, H. K. (٢٠٢٢, December). Quality Assurance of Facial Recognition Software for Arabic Social Media Celebrities. In *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)* (pp. ٣٦-٣٩). IEEE.**