International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Study on Cyber Victimization Through Identity Theft Using Fake Identities in Social Media

Arunachalam S.B, Dr. Latha S
M.Sc., Department of Criminology and Forensic science, Dr. MGR Educational and Research Institution.
Assistant Professor, Department of Criminology, University of Madras.

ABSTRACT

Cyber victimization on social media is a concerning trend, posing challenges to online safety and mental well-being, especially among adolescents and young adults. This project aims to understand how cybercriminals steal personal information and the impacts, including psychological distress and social isolation. The study combines literature review and empirical investigation to uncover tactics like phishing and malware. With social media's pervasive nature, cyber victimization becomes difficult to escape, amplifying its reach and intensity.

INTRODUCTION

Cybercrime involves illicit activities conducted through digital platforms like hacking, phishing, and identity theft. Combatting it requires evolving security measures. Cyber victimization refers to harm inflicted online, like cyberbullying, causing mental and reputational harm. Addressing it demands digital literacy and support networks. Laws on cyber victimization vary globally, with India employing legislation such as the IT Act and POCSO Act. International efforts aim for collaboration to protect against online abuse. Types of cybercrimes include cyberbullying, identity theft, phishing, and child exploitation. Prevention involves user caution and reporting suspicious activities. Fake identities on social media pose risks despite platform policies. Verification and reporting help manage these dangers. Youth use social media for socializing, identity expression, and activism. Mental health concerns and privacy issues necessitate attention from caregivers and authorities.

Social media platforms provide global connectivity, networking opportunities, quick information sharing, community development, marketing avenues, educational resources, and tools for social action. Overuse can harm mental health, cyberbullying is prevalent, misinformation spreads easily, privacy concerns arise, and social media addiction is a growing issue. Over 4.52 lakh cybercrime incidents were reported in India in 2021, with a significant increase in cases in subsequent years. The total amount siphoned off by cybercriminals was over Rs 10,300 crore, with efforts to block fraudulent transactions in progress. Anonymity, global connectivity, technological advancements, profit motive, data breaches, sophisticated criminal networks, lack of cybersecurity awareness, cyber warfare, and social engineering contribute to the prevalence of cybercrime. Education and awareness, strong passwords, two-factor authentication, regular software updates, cautious online behaviour, protection of personal information, secure Wi-Fi networks, encryption, data backups, and prompt reporting of suspicious activity are essential preventive measures. To understand cybervictimization through identity theft on social media among 18-

30-year-olds in Chennai. The study utilizes a quantitative analysis method with a simple/random sampling technique, employing a Google Form survey to collect data from 50 respondents.

Estee van der walt, J.H.P. Eloff, Jacomine Grobler (2018) conducted a study in social media platforms enable real-time sharing of thoughts, likes, and dislikes for billions, yet pose cybersecurity risks due to lack of censorship. To address identity deception, we draw insights from psychology to understand the motives behind lying, and from bot detection techniques to adapt solutions for identifying human deception. This interdisciplinary approach enhances our ability to detect and mitigate instances of identity deception in online interactions.

Madhura Vyawahare & Sharvari Govilkar (2022) conducted a study explores why criminals gravitate towards social networking sites, drawn by abundant information and vulnerable users. Exploiting platform features, they create fraudulent identities, leading to identity theft or masquerading, such as clone profile or fake profile attacks. While current methods largely target clone profile attacks, addressing fake profile attacks remains limited. This article distinguishes between fake profiles, clone profiles, and cross-site cloning, proposing an integrated framework to detect both fake profiles and instances of cross-site cloning.

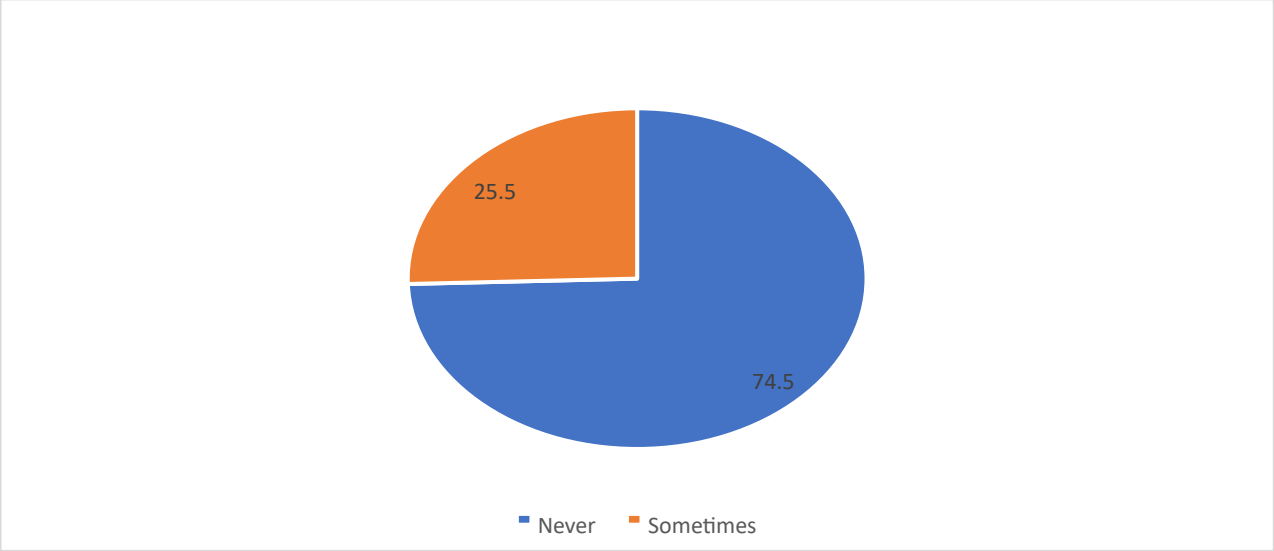
Shareen Irshad and Tariq Rahim Soomro (2019) is conducted social media's rapid evolution from basic messaging to comprehensive networking platforms like Facebook and Twitter has revolutionized online interaction. While its widespread adoption brings benefits, it also provides fertile ground for criminals, amplifying traditional crimes and fostering new ones like "Performance Crimes". Identity theft, has surged, exploiting the wealth of personal data available on social media. This study illuminates the growth of identity theft on these platforms, revealing how they have become prime targets for identity thieves.

METHODOLOGY

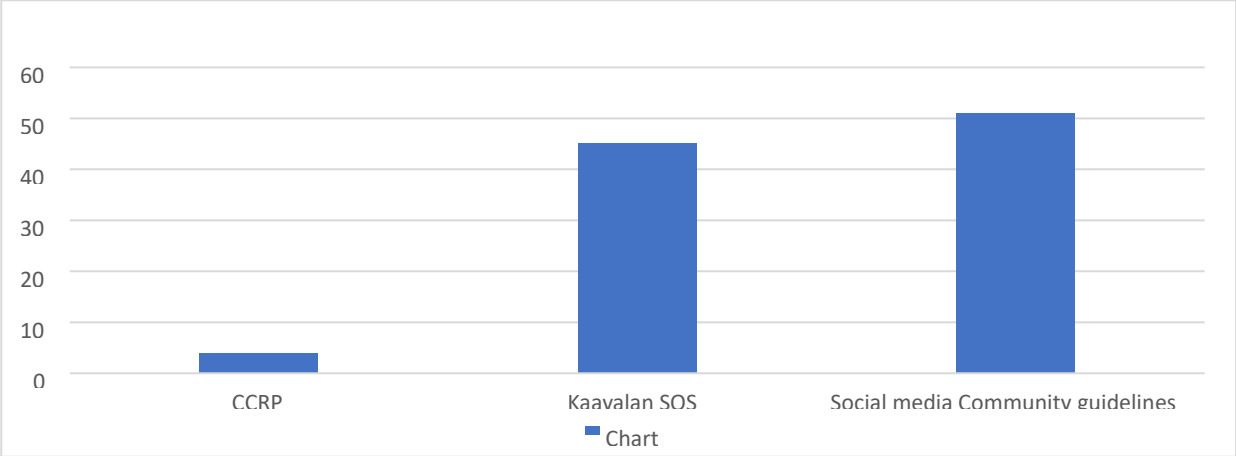
This chapter outlines the research methodology, focusing on understanding the prevalence of victimization stemming from interactions with fake identities on social media. The aim is to examine patterns, explore psychological impacts, and develop interventions to enhance awareness and protection. The study gathers data from individuals actively engaged in social media in Chennai, with a sample size of 50 responses collected via Google Forms. Statistical analysis, including the use of Microsoft Excel for generating pie charts, aids in understanding and presenting the findings effectively. The study seeks to evaluate public awareness of social media identity theft to provide guidance on preventing fraudulent identities online. The research survey indicates that most of the public is unaware in cyber victimization in social media fake identities. Out of 50 participants, only 27 individuals (52.9%) were aware of a what a social media fake identity entails, while the remaining 24 participants (47.1%) lacked this knowledge. Among the participants surveyed, 60% reported experiencing some form of cyber victimization through fake profiles on social media platforms. This included incidents of cyberbullying, identity theft, and other malicious activities perpetrated by individuals using fake identities.

RESULT AND DISCUSSION

This research investigates cyber victimization via fake profiles on social media, targeting young adults who are often victims of identity theft and fraud. Despite the benefits of social media, it has become a breeding ground for cyberbullying, harassment, and fraud through fake profiles. The study aims to understand the prevalence, patterns, and impacts of this victimization, and develop interventions for user protection. Data was collected from 50 respondents via Google Forms, covering personal details, socio-economic background, social media usage, victimization experiences, and post-victimization responses.



Navigating the challenge of gathering survey responses from the public can be tough.
Due to lack of time limit I had to collect the survey via online platform (google form).
The reliability of the data collected via Google Forms raises concerns about its authenticity, particularly when considering the diverse backgrounds and potential biases of respondents.
Respondents might withhold candid responses due to apprehensions surrounding data privacy, particularly if the survey delves into sensitive topics, thereby potentially compromising the accuracy of the data collected. Maintaining the quality and credibility of responses poses a challenge due to the scarcity of tools available for confirming respondent identities and preventing duplicate submissions from individuals, thus potentially affecting the validity of the data collected.



The pie chart shows the aware the one of the following, according to this study most of them have aware in the social media community guidelines by safe and secure usage of the social media and most of them have aware of Kavalan SOS.

CONCLUSION

This study was undertaken to examine the experiences of individuals engaged in social media who have encountered in identity theft in fake profile, the analysis indicates that individuals aged 18-20 and 22-24 are more prone to encountering such issues on social media platforms. cyber victimization through fake profiles on social media platforms represents a complex and pervasive challenge with far-reaching implications for individuals, communities, and society at large. This study has highlighted the alarming prevalence of cyberbullying, harassment, and identity theft perpetrated via fake identities, underscoring the urgent need for comprehensive strategies to address this issue. The findings underscore the importance of enhancing user awareness and digital literacy to empower individuals to recognize and respond to online threats effectively. Moreover, collaborative efforts involving platform providers, policymakers, educators, and advocacy groups are crucial in developing and implementing robust measures to safeguard user safety and well-being. By fostering a culture of online resilience, accountability, and empathy, we can create a more inclusive and secure digital environment conducive to positive social interactions and meaningful engagement. As we navigate the ever-evolving landscape of social media, it is imperative that we prioritize the protection of users' rights and dignity, ensuring that everyone can enjoy the benefits of online connectivity without fear of exploitation or harm.

REFERENCES

- Estee van der walt, J.H.P. Eloff, Jacomine Grobler (2018) Cyber security Identity deception on social media platforms, *Computers in human behaviour* volume 78, 76-89
- Mohammed ali al-garadi, kasturi dewi varathan, sri devi ravana (2016) Cybercrime detection in online communications: the experimental case of cyberbullying detection in the Twitter network, *Computers in human behaviour* volume 63, 433-443
- Hyder Ali Memon, Rashid Wassan, Jahangir Ansari (2022) Cyber-Crime
- Victimization through Social Media: An Exploratory Study of Victims in Hyderabad, Pakistan, *annals of human and social sciences*, vol 3 no. 2 453-464
- Abbas, J., Aman, J., Nurunnabi, M., & Bano, S. (2019). The impact of social media on learning behaviour for sustainable education: *Evidence of students from selected universities in Pakistan.Sustainability*,11(6), 1683
- Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime. *Paladin Capital Group.*
- Ahmed Alharbi, Hai doing, Xun Yi, Zahir tari (2021), Social Media Identity
- Deception Detection: A Survey, *AMC Computing surveys*, volume64,Issue 3,Article No.: 69pp 1–35
- Awan MJ, Khan MA, Ansari ZK, Yasin A, Shehzad HMF (2021) Fake profile recognition using big data analytics in social media platforms. *Int J Computer Appl Technology* 68:215–222
- El Yusufi Y, Zakaria E (2019) Social networks fake profiles detection using machine learning algorithms. In: the proceedings of the third international conference on smart city applications. Springer, Cham, pp 30–40

- Khaled S, Neamat E-T, Hoda MOM (2018) Detecting fake accounts on social media. In: 2018 IEEE international conference on big data (big data). *IEEE*, pp 3672–3681
- Khan, G. F., Swar, B., Lee, S. K. (2014). Social media risks and benefits: A public sector perspective. *Social Science Computer Review*, 32, 606–627
- Cassandra Cross and Rebecca Layt (2021). I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social science computer review*, Volume 40, issue 4
- Soorya Ganesh, Dhanraj Ganapathy, Keerthi Sasanka (2020), Awareness of cybercrime on social media, Vol. 26 No. 2 (2020): *The journal of contemporary issues in business and government*
- Won Kim, Ok-Ran Jeong, Sang-Won Lee, "On Social Websites", *Information Systems 35* (2010), 215-236.
- Davidson, N. and Silence, E. (2010), "It won't happen to me: promoting secure behaviour among internet users", *Computers in Human Behaviour*, Vol. 26 No. 6, pp. 1739-47.
- D. H. John Carlo Bertot, Paul T. Jaeger. The impact of polices on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly 29*, pages 30–40, (2012)
- Vieweg, S, Hughes, A, Starbird, K, and Palen, L. Micro-blogging during two natural hazards events: *What twitter may contribute to situational awareness*. In Proc. CHI, 2010.