Asia Pacific Journal of Information System and Digital Transformation
2023, Vol 1 No 01, Research Article

Understanding The Phenomenon and Risks of Identity Theft and Fraud on Social Media

Ahmad Rafi Ilzan
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
rafiilzan@student.telkomuniversity.ac.id

Reihaini Fikria Bunga Oktaviani
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
reihainifbo@student.telkomuniversity.ac.id

Farhan Muzammil Yusuf
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
farhanmuzam@student.telkomuniversity.ac.id

Dirk Jan Wegman
School of Building, Business and Technology, Saxion University of Applied Sciences, Netherlands
d.j.wegman@saxion.nl

Nazwa Yaqzhania Imtiyaz
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
nazwayaqzhania@student.telkomuniversity.ac.id

DedenWitarsyah
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
dedenw@telkomuniversity.ac.id

Abstract

The use of social media platforms has created new opportunities for people to connect and share information with one another. However, this has also increased the risk of identity theft and fraud. The purpose of this paper is to provide an overview of the phenomenon of identity theft and fraud on social media by exploring the various methods used by perpetrators to gain access to personal information, the ways in which they utilize this information to commit fraud, and the impact that these crimes can have on the victim's privacy. This paper will also examine the various strategies that individuals and organizations can use to protect their privacy on the internet from identity theft and fraud on social media. Ultimately, this paper aims to increase understanding of the risks of social media use and to provide practical recommendations for minimizing these risks.

Keywords: Privacy, Identity theft, Fraud, Social media, Internet.

1. Introduction

In this era where everything is digitalized, social media platforms have become an integral part of our daily life providing us with a platform to connect with others and share information including personal ones. However, the privacy concerns of its use are alarming as the widespread use of social media platforms has opened up new opportunities for identity theft and fraud, posing a serious threat to individuals' privacy and security. In recent years, there have been numerous reports of social media users falling victim to scams and fraudulent activities, resulting in financial losses and damage to their reputations. Despite the growing awareness of these risks, many people still underestimate the potential dangers of sharing personal information online and fail to take adequate measures to protect themselves.

This paper aims to provide a comprehensive understanding of the phenomenon and risks of identity theft and fraud on social media, including the methods used by cybercriminals to target victims, the types of personal information that are most vulnerable to theft, and the impact of these crimes on individuals and society as a whole. By examining case studies and analyzing existing research on this topic, we can gain insights into the underlying factors that contribute to these crimes and identify effective strategies for preventing and responding to them.

2. Literature Review

A. Privacy

Privacy is the process of an individual controlling when, how, and to what extent their information is communicated to others (Van De Garde-Perik et al., 2008). Privacy is also a dynamic construction, driven by context (Bélanger & Crossler, 2011; Crossler, 2010; Hong & Thong, 2013; Raschke et al., 2014; Xu et al., 2008), and multi-dimensional. Altman suggests that privacy includes interpersonal and social aspects and varies according to life experiences (Altman, 1975).

B. Identity Theft

1. "Identity theft happens when someone knowingly and without permission uses another person's identifying information (e.g., name, Social Security number, driver's license, bank account) to commit fraud or other crimes" (Copes & Vieraitis, 2009).
2. "While identity theft is not a new crime, the scope of the problem has grown in tandem with society's increasing reliance on electronic transfer and storage of personal

information in all forms of commerce and services. Identity theft affected over 10% of US people in 2016, up from 7% in 2012" (Harrell, 2019).

From the two opinions above, identity theft is a growing public health problem that has been exacerbated by society's increasing reliance on electronic storage and transfer of personal information. This crime occurs when someone intentionally uses another person's identity information without permission, such as their name, Social Security number, or bank account, for fraudulent purposes or other criminal activities. The prevalence of identity theft has been on the rise, necessitating heightened awareness and preventative measures to protect individuals from the financial and reputational damage caused by this crime.

C. Social Media

1. Social media is social interaction between humans in producing, sharing, and exchanging information, ideas, and various content in virtual communities (Ahlqvist, 2008).
2. Social media is a collection of internet-based applications built on the basic ideology and web technology version 2.0 which allows the creation of interactive websites (Kaplan & Haenlein, 2010).

From these two opinions above, it can be concluded that social media is social interaction from a group of internet-based applications whose function is to produce, share, and exchange information.

D. Fraud

1. Fraud is unlawful acts that are carried out intentionally for a specific purpose by people from within or outside the organization to gain personal or group benefits that indirectly disserve other parties (ACFE Indonesia Chapter #111, 2016).
2. Fraud is defined as all kinds that can be thought of by humans, and which are attempted by someone to gain an advantage over others by wrong advice or insistence of truth, and includes all ways that are unexpected, full of deception or hidden stratagems, and any unnatural ways that cause others to be deceived (Peak Indonesia, 2003)

From these two opinions above, it can be concluded that fraud is an act that is thought of by the human mindset to gain benefits from other people for himself personally or in a group in a cunning way that causes other parties to feel loss or be deceived.

E. Internet

The Internet is a system that global computer network via telecommunications such as telephone radio, satellites, and more. The Internet is a connection between various types of

computers and networks in the world with different operating systems as well the application that takes advantage of advances in communication media that use the standard protocol for communicating (Vitria, 2021).

3. Methodologies

The methodologies employed in this paper involves conducting a comprehensive literature study to get an understanding of the phenomenon of identity theft and fraud on social media. The primary method used is a systematic review of existing scholarly articles, books, and relevant research studies. This approach enables the collection, analysis, and synthesis of a wide range of literature, providing a holistic understanding of the topic. A literature review is an academic piece of writing that exhibits knowledge and understanding of the academic literature on a certain topic in context (*Literature Review | The University of Edinburgh*, n.d.).

Additionally, the inclusion of peer-reviewed sources ensures the reliability and credibility of the information gathered. This methodology ensures that the paper is based on a rigorous analysis of the existing body of knowledge, offering valuable insights and a solid foundation for further research and discussion on the topic of identity theft and fraud on social media.

4. Result and Finding

The results section of this paper presents key findings derived from the analysis of the literature and research conducted on understanding the phenomenon and risks of identity theft and fraud on social media.

The results presented in this section highlight the importance of understanding the phenomenon and risks of identity theft and fraud on social media, emphasizing the need for proactive measures to combat these threats. These findings contribute to a comprehensive understanding of the topic, providing valuable insights for individuals, organizations, and policymakers to develop effective strategies and countermeasures against identity theft and fraud on social media.

A. Overview of Identity Theft and Fraud on Social Media.

Firstly, the overview of identity theft and fraud on social media reveals that these malicious activities have become increasingly prevalent.

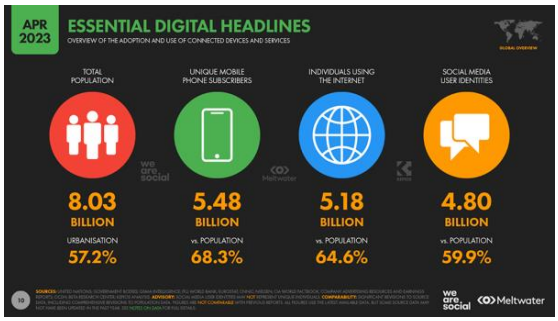

Figure. 1. Essential digital headlines (April 2023)

As per the global overview conducted by Datareportal on April 2023, we can see that social media users growth has increased there are as 4.80 billion people or 59.9% of the world population who now use it, and millions of new users within the last year (Kemp, 2023). This means that more people are going online and using social media over the years.

As the number of users on social media platforms continues to grow at an unprecedented rate, so does the risk of identity theft. The widespread adoption of social media has created a vast pool of personal information that can be exploited by malicious actors. With each new user account created, more personal details such as names, dates of birth, addresses, and even financial information are being shared online. These platforms, while providing valuable connections and opportunities for individuals, also attract cybercriminals who are constantly seeking to exploit vulnerabilities and gain unauthorized access to sensitive information (Rahim Soomro & Irshad, 2018).

The crimes themselves on social media include the following (Brindha et al., 2018).

1. Cyberbullying, stalking, and online threats:

   A highly common offense in which the perpetrator is unaware that he or she is committing a crime.

2. Uploading criminal activities videos and photos:

   Criminals are enticed to post and upload their criminal deeds to these networks for the public to view as smartphone technology and social media improve.

3. Identity theft and identity theft

   Logging into someone else's account for the aim of intentionally misusing it has grown increasingly widespread in recent years, as has identity theft, in which phony accounts or accounts for impersonation are created specifically for the goal of fraud.

4. Spying on Business

   The fraudster can simply impersonate a firm employee by starting a Facebook profile and inviting other employees to join.

B. Factors Contributing to Identity Theft and Fraud on Social Media

Secondly, factors contributing to identity theft and fraud on social media are multifaceted. Social engineering tactics play a crucial role, in exploiting human vulnerabilities and manipulating victims into divulging sensitive information. Additionally, weaknesses in privacy and security settings on social media platforms create opportunities for unauthorized access and data breaches, enabling fraudsters to perpetrate identity theft and fraud.

In Indonesia, there have been numerous examples of cybercrime, ranging from identity fraud to frightening debt bills that were never generated. Many of these cybercrimes are committed over social media platforms such as Facebook, WhatsApp, Instagram, and others. To address this, M Novel Ariyadi, Director of Cybersecurity BDO in Indonesia and Co-Founder of the Indonesia Cyber Security Forum (ICSF), outlined the primary elements that generate cybercrime and separate it from other crimes. According to a media clinic titled The Role of Secure Digital Identity in Increasing Trust in Fintech, the three causes that induce cybercrime are as follows:

1. User identification

   Users with malicious intent frequently employ features that make it easy to influence completeness on social media. Furthermore, other users' data is easily stolen. This facilitates cybercriminals' manipulation of victims.

2. Information asset multiplication

   Users can readily copy information assets on social media. This is due to the lack of a delete option, sometimes known as a 'delete button' on the internet.

3. Location

   Another element that can lead to cybercrime attacks is when a user's location is recognized on social media. Similarly, it is simple to forge or conceal. Furthermore, the government serves as a guarantee and source of identity from person to person offline.

To secure identity verification and electronic signatures, the government must work with identity suppliers, as opposed to the internet sphere. At the very least, politicians, electronic system administrators, and internet users must work together to secure digital identities against cybercrime.

C. Impacts of Identity Theft and Fraud on Individuals and Society

The impacts of identity theft and fraud on individuals and society are substantial. Victims often face severe financial consequences, including unauthorized transactions, stolen funds, and compromised credit. The emotional and psychological toll cannot be overlooked, as victims may experience feelings of violation, fear, and loss of trust. Furthermore, the damage to one's reputation and social standing can have long-lasting implications, affecting personal and professional relationships.

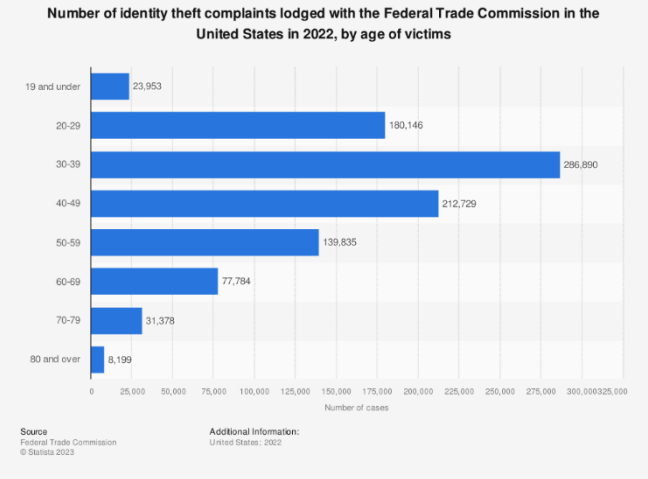

Figure. 2. Identity theft reports by age of victims (2022)

Based on the identity theft cases reported to the FTC in the US, 30-39 year olds were the most targeted ages for identity theft, and persons aged 40 to 49 were the second most targeted age group in 2022, (*Number of Identity Theft Complaints, by Age of Victims U.S. 2022 | Statista*, n.d.).

According to one study, in the United States, elder Black victims are more likely to have had more money stolen and to be affected by the crime than older White victims. The most vulnerable seniors, those living at or below the federal poverty level, were far more likely to face overhead costs. The length of time information was exploited, following financial troubles and problems with friends or family, and the hours spent resolving identity theft were all connected with increased distress in their emotional well-being. Age was not substantially connected with losses or emotional suffering among people aged 65 and above (DeLiema et al., 2021).

According to research, identity theft victims with unresolved cases were more likely to have clinically elevated scores than those with settled cases when compared to a normative sample. Victims used coping techniques that were quite comparable. According to the findings of this

study, victims of identity theft have heightened psychological and physical anguish, and discomfort persists over time for those whose cases go unsolved (Sharp et al., 2004).

D. Emerging Trends and Techniques in Identity Theft and Fraud on Social Media

Media pose extra threats. To deceive people, fraudsters constantly alter their techniques, employing modern technology such as deep fakes and AI-generated content. Manipulation of algorithms and social media features increases the efficiency of their fraudulent actions, making it more difficult to detect and prevent such incidents. Currently, identity data theft in Indonesia occurs more frequently within the scope of fintech or companies engaged in the financial sector, especially online loans. According to Press Release data No. 1399/SK-ADV-PMU/XII/2018, The Jakarta Legal Aid Institute has 1330 complaints of victims of online loan funds and 14 violations of human rights experienced by victims. Among the customer-related breaches of data theft are; 1). Threats, slander, and sexual insults, 2). Distribution of personal data, 3). Dissemination of photos and loan information on cell phone purchases, 4). KTP data is used by online loan application providers to apply for loans in other applications (Nurdiani, 2020). These online loan companies will usually ask for the victim's personal data and information such as KTP, KK, and photos as a condition for making loans where there are still many ordinary people who do not understand then submit their data voluntarily without looking at the causes and consequences of online loan applications. Unknowingly, this data is often misused by debtors to take actions that are detrimental to their victims.

E. Preventive Measures and Mitigation Strategies

Preventive Measures and Mitigation Strategies:

1. Education and awareness campaigns, play a significant role in alerting users about the hazards connected with disclosing personal information and restraining safe online conduct;
2. Improve privacy and security settings on social media platforms to protect personal data from cyber-attacks;
3. Implement multi-factor authentication and robust identity verification measures;
4. Accelerate ratification of the personal data protection bill, and
5. Applying severe penalties to dissuade criminals.

6. Conclusion

This study concludes that the widespread use of social media has led to an abundance of personal information that can be exploited by cybercriminals. Factors contributing to identity theft and fraud on these platforms include social engineering tactics and vulnerabilities in privacy and security settings. The consequences of these crimes are significant, ranging from financial losses to emotional distress and damage to one's reputation. Emerging trends, such as deep fakes and AI-generated content, pose additional challenges in detection and prevention. To address these risks, the paper suggests preventive measures such as education campaigns, improving privacy settings, implementing strong authentication methods, and enacting legislation for personal data protection. Additionally, strict sanctions against perpetrators are recommended as a deterrent. Overall, the findings contribute valuable insights for individuals, organizations, and policymakers to develop effective strategies against identity theft and fraud on social media.

References

1. ACFE Indonesia Chapter #111. (2016). *Survai Fraud Indonesia*. https://acfe-indonesia.or.id/wp-content/uploads/2017/07/SURVAI-FRAUD-INDONESIA-2016.pdf
2. Ahlqvist, T. (2008). *Social media roadmaps : exploring the futures triggered by social media*. 78.
3. Altman, I. (1975). The Environment and Social Behavior. *Environment And Behavior*, *20*(4), 34–61. https://books.google.com/books/about/The_Environment_and_Social_Behavior.html?hl=id&id=GLBPAAAAMAAJ
4. Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly: Management Information Systems*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971
5. Brindha, S., Swetha, K., Professor, A., & Kavitha, : R. (2018). Identity Theft (Emerging Trends in Security Issues in Information Security). *International Journal of Engineering Research & Technology*. https://doi.org/10.17577/IJERTCONV6IS14060
6. Copes, H., & Vieraitis, L. M. (2009). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*(3), 329–349. https://doi.org/10.1177/0734016808330589
7. Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2010.311
8. DeLiema, M., Burnes, D., & Langton, L. (2021). The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging*, *5*(4), 1–11. https://doi.org/10.1093/GERONI/IGAB043
9. Harrell, E. (2019). *Victims of Identity Theft, 2016*. Bureau of Justice Statistics. https://bjs.ojp.gov/library/publications/victims-identity-theft-2016

10. Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly: Management Information Systems*, *37*(1), 275–298. https://doi.org/10.25300/MISQ/2013/37.1.12
11. Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/J.BUSHOR.2009.09.003
12. Kemp, S. (2023, April 27). *Digital 2023 April Global Statshot Report — DataReportal – Global Digital Insights*. https://datareportal.com/reports/digital-2023-april-global-statshot
13. *Literature review | The University of Edinburgh*. (n.d.). Retrieved June 5, 2023, from https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review#
14. *Number of identity theft complaints, by age of victims U.S. 2022 | Statista*. (n.d.). Retrieved June 9, 2023, from https://www.statista.com/statistics/587677/identity-theft-complaints-victims-age-in-the-us/
15. Nurdiani, I. P. (2020). Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime. *Jurnal Kriminologi Indonesia*, *16*(2), 1–10. http://www.jurnalkesos.ui.ac.id/index.php/jki/article/viewFile/12571/67546786
16. Rahim Soomro, T., & Irshad, S. (2018). Identity Theft and Social Media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1), 43. https://www.researchgate.net/publication/323185128
17. Raschke, R. L., Krishen, A. S., & Kachroo, P. (2014). Understanding the Components of Information Privacy Threats for Location-Based Services. *JOURNAL OF INFORMATION SYSTEMS American Accounting Association*, *28*(1). https://doi.org/10.2308/isys-50696
18. Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004). Exploring the Psychological and Somatic Impact of Identity Theft. *Journal of Forensic Sciences*, *49*(1). https://doi.org/10.1520/JFS2003178
19. Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, *26*(1), 20–43. https://doi.org/10.1177/0894439307307682
20. Vitria, N. (2021). PENGARUH INTERNET BAGI SISWA-SISWI SMA NEGERI 3 PADANG. *Science, Engineering, Education, and Development Studies (SEEDS): Conference Series*, *4*(2). https://doi.org/10.20961/SEEDS.V4I2.56700
21. Xu, H., Dinev, T., Jeff Smith, H., Hart, P., & Jeff, H. (2008). *Association for Information Systems AIS Electronic Library (AISeL) Examining the Formation of Individual' s Privacy Concerns: Toward an Integrative View Recommended Citation*. http://aisel.aisnet.org/icis2008/6

DOI: https://doi.org/10.61973/apjisdt.v101.3