Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0048

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

Safeguarding Personal Details on Social Media Platform at the Backdrop of Social Media Frenzy

***Dr. Vyankati Nagargoje**
Assistant Professor in Marathi
Orange City College of Social Work, Nagpur
Mob.: 9423454443
E-Mail ID: drvyankati7@gmail.com

Abstract: With the increase of internet-connected devices and the growing digitisation of financial transactions, the threat landscape has expanded, requiring proactive measures to mitigate risks. With the rise of digital currencies and online investment platforms, securing digital assets and investments has become a priority for investors. The growing number of people joining social media sites has led to increased security breaches as attackers seek to take advantage of vulnerabilities. Some of the prominent security concerns associated with the use of social media platforms include identity theft, spam attacks, malware attacks, social phishing, impersonation, hijacking, and fake requests (Zhang & Gupta, 2016). Fogues et al. (2015) explained that the benefits of using social media networks are now rapidly overshadowed due to growing concerns over user security threats. Security concerns related to social media also pose a growing threat to businesses. By guarding your digital footprint, limiting the personal details you disclose, adjusting privacy settings, being cautious of accepting requests, and using strong passwords, you can mitigate potential threats and protect yourself from identity theft, privacy invasion, and social engineering attacks.

Introduction: In an era of digitalisation and interconnectedness, protecting personal and financial information has become increasingly critical. As individuals and businesses rely more on digital platforms and technologies to manage their wealth, the risk of cyber threats and attacks has escalated. Cyber threats, such as data breaches, identity theft, ransomware attacks, and phishing scams, pose significant financial security risks to individuals and businesses. Hackers and cybercriminals continuously exploit digital system and network vulnerabilities to access sensitive information and exploit financial assets. With the increase of internet-connected devices and the growing digitisation of financial transactions, the threat landscape has expanded, requiring proactive measures to mitigate risks. With the rise of digital currencies and online investment platforms, securing digital assets and investments has become a priority for investors **HMW Group, (2024).**

According to a recent survey, 81% of Americans say they're concerned about their privacy on social networking sites. Yet, the privacy risks of using social media are a nightmare that most users choose to ignore — until it becomes a reality. That's what happened to families in Arizona, when a local man used location data on Snapchat to stalk and spy on young girls in the area. Even worse, data protection issues and privacy loopholes mean that you (or your kids) are likely **sharing personal data** without your knowledge. But how much danger are you putting yourself in just by using social media? And is there a way to stay social and safe at the same time? Social media privacy refers to the personal and sensitive information that people can find

out about you from your accounts. This information can be purposefully shared (such as in public profiles and posts) or unknowingly shared (such as the data sites share with other companies and social media marketing agencies). But while most people are concerned about what companies know about them, the bigger danger is what scammers and fraudsters know — and how they can use that information.

Many people unknowingly post personal information that could give hackers clues to their passwords or security questions — for example, posting about your hometown, pets, elementary school, or extended family. Scammers either use this information to try and brute-force their way **into your account** or employ **social engineering attacks** to trick you into providing your password. In many cases, scammers don't even need to trick you into giving up your passwords or account information. Leaked social media account information sells on the **Dark Web** for as little as $25. If your social media accounts aren't set to private, you can receive messages from anyone — even scammers trying to get you to click on malicious links. Last year, 12% of all clicks to fake phishing websites originated on social media. Fraudsters also regularly use social media to run romance scams and investment fraud schemes. In the past few years, the brutally-named "**pig butchering scam**" has run rampant on social media, costing victims over $10 billion. Fraudsters create fake social media profiles to try and lure you into **fake online relationships** — and then ask you for cash, gift cards, or personal information. Romance scammers on social media can use your personal information to craft the perfect scam designed to ensnare you **Jory MacKay (2023).**

Identity Theft and Fraud: Sharing personal information, such as your full name, date of birth, or home address, on social media puts you at risk of identity theft. Cybercriminals can exploit this information to impersonate you, open fraudulent accounts, or carry out financial fraud. Limit the personal details you disclose on social media to minimize the chances of falling victim to identity theft or fraud. By oversharing on social media, you may inadvertently expose yourself to privacy invasion. Posting pictures of your home, workplace, or daily routines can provide unwanted insights to potential criminals. Consider carefully what you share and ensure your privacy settings are set to limit the visibility of your posts and personal information to trusted connections only. Social Engineering Attacks: Cyber attackers often gather information from social media profiles to execute social engineering attacks. By analyzing your posts, comments, and interactions, they can tailor phishing attempts or scams specifically designed to exploit your interests, relationships, or preferences. Be cautious about accepting friend requests or engaging with strangers who may have ulterior motives. When sharing your location or check-ins on social media, you expose yourself to potential physical risks. Broadcasting your whereabouts in real-time can make you an easy target for stalkers or burglars. Exercise caution when sharing your location information and consider disabling location services for social media apps unless necessary. The content you share on social media can have long-lasting consequences on your personal and professional life. Inappropriate posts, offensive comments, or compromising pictures can harm your reputation, jeopardize job opportunities, or strain personal relationships **Hernan Popper (2023)**.

Discussion and Analysis: The growing number of people joining social media sites has led to increased security breaches as attackers seek to take advantage of vulnerabilities. Some of the prominent security concerns associated with the use of social media platforms include identity theft, spam attacks, malware attacks, social phishing, impersonation, hijacking, and fake requests (Zhang & Gupta, 2016). Fogues et al. (2015) explained that the benefits of using social media networks are now rapidly overshadowed due to growing concerns over user security threats. Security concerns related to social media also pose a growing threat to businesses. As companies become increasingly connected with consumers via social media, another exchange occurs when consumers share their personal information within social media networks due to a lack of understanding privacy policies, making users vulnerable to security hacks when it comes to the information they share (Fox & Royne, 2018). Alba et al. (1997) noted that while social media provides consumers with access to a vast amount of company information to enable better, more efficient decision-making, consumers are vulnerable when it comes to the information they share. There is often uncertainty about how information is collected, stored, shared, and potentially misused by both public and private businesses (Buchannan et al., 2006). To address security concerns associated with social media, Carminati et al. (2011) proposed that enhanced access control systems for social network sites are a recommended first step for addressing the security and privacy threats. Similarly, Zhang and Gupta (2016) argue that it is up to social media sites to establish security and trustworthiness within their platforms by studying user's actions and treat them as a means of establishing credible, safe, and lasting social platforms that provide secure infrastructure with regular security updates and notices to users. There are Security Concerns Construct/Component retained all its five designated items/factors, indicating that the component. Prominently, the five items retained are security concerns about regarding 1) identity theft - attacker stealing users' personal information, 2) impersonation/social phishing - attacker impersonating a real person through a fake website to steal users' data, including login credentials and credit card numbers, etc., 3) hijacking - attacker taking control over users' profile, 4) image retrieval and analysis - attacker using face and image recognition software to find more information about users and their linked profiles, and 5) malware attacks - attacker sending malware injected scripts or malicious software to perform activities on users' device without their knowledge.

The users' integrity trust – social media sites being trustworthy, users' benevolence trust – social media sites keeping users' best interests and well-being in mind, and competence trust – social media sites being competent in protecting and safeguarding users' personal information indicate that the component was empirically validated to be reliable and interpretable among all its three items/factors. The users' awareness of potential security threats and risks and their negative consequences, users' consequences, and users' awareness of the potential for harm/loss associated with their security and privacy **Alex Koohang, et. Al. (2021)**.

Securing financial accounts and transactions is paramount in wealth protection. Individuals should implement robust authentication measures, such as multi-factor authentication (MFA) and strong, unique passwords, to prevent unauthorised access to their accounts. Additionally, encrypting sensitive financial data and using secure connections (e.g., HTTPS) when conducting

online transactions can enhance security and protect against interception by malicious actors. Protecting personal and business information is essential for preventing identity theft and financial fraud. Individuals should exercise caution when sharing personal information online and be wary of phishing emails, fraudulent websites, and unsolicited requests for sensitive data. Employing reputable antivirus and anti-malware software, regularly updating software and security patches, and implementing firewalls and intrusion detection systems can help fortify defenses against cyber threats.

Suggestions and Recommendations: Utilising reputable cryptocurrency wallets and exchanges with robust security features, such as cold storage and multi-signature authentication, can safeguard digital assets from theft and unauthorised access. Similarly, exercising due diligence when selecting investment platforms and conducting thorough research on their security protocols can mitigate risks associated with online investing. Educating oneself and staying informed about emerging cyber threats and best practices is crucial in cybersecurity and wealth protection. Individuals should remain vigilant, keep abreast of cybersecurity news and trends, and participate in cybersecurity awareness training programs to enhance their knowledge and skills. While risk remains, fostering a cybersecurity awareness and resilient culture can allow individuals and businesses to better identify and respond to potential threats, reducing the likelihood of financial losses and reputational damage. Cybersecurity plays a fundamental role in wealth protection in an increasingly digitised world. By adopting proactive cybersecurity measures and adhering to best practices, individuals and businesses can safeguard their digital assets, financial information, and investments from cyber threats and attacks. Whether securing financial accounts, protecting personal information, or mitigating risks associated with digital assets, prioritising cybersecurity is essential for preserving financial security and peace of mind in the digital age.

Conclusion: Think twice before posting anything that could have negative repercussions in the future. Sharing personal information on social media can inadvertently provide cybercriminals with clues for cracking your passwords. Birthdays, pet names, or favorite sports teams are often used as security questions or password hints. Avoid sharing such information and use strong, unique passwords for your accounts to minimize the risk of unauthorized access.While social media offers a platform for connection and self-expression, it is essential to be mindful of the risks associated with sharing personal information. By guarding your digital footprint, limiting the personal details you disclose, adjusting privacy settings, being cautious of accepting requests, and using strong passwords, you can mitigate potential threats and protect yourself from identity theft, privacy invasion, and social engineering attacks. Let's maintain control over our digital lives and enjoy the benefits of social media without compromising our privacy and security

Reference:

1. Koohang, Alex. et. al. "Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument" . *Issues in Information System vol.2, no.2 pp. 133-145 2021*
2. MacKay, Jory, "Social Media Privacy: What are the Risks? (How to Stay Safe)" *Aura*, 10 July, 2023 https://www.aura.com/learn/social-media-privacy-risks#:~:text=Data%20mining%20leading%20to%20identity%20theft,-Scammers%20need%20surprisingly&text=And%20often%2C%20the%20starting%20point,sale%20on%20the%20Dark%20Web.
3. Popper, Hernan. "Guarding Your Digital Footprint: The Risks of Sharing Personal Information on Social Media". *Linkden.com* 11 July, 2013 https://www.linkedin.com/pulse/guarding-your-digital-footprint-risks-sharing-social-hernan/
4. "Why does size matter? (In a Bussiness), *HMW Group*, 2024 https://hmwgroup.com.au/blog/2025/02/20/why-does-size-matter-in-a-business/