Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

# Preventive Measures for the Impacts of Social Media Networks in Security and Privacy - A Review

**B.Vivekanandam[1], Midhunchakkaravarthy[2]**

[1,2]Associate Professor, Faculty of computer science and Multimedia, Lincoln University College, Malaysia

**E-mail:** [1]vivekresearch2014@gmail.com, [2]midhun.research@gmail.com

## Abstract

Recently, smartphones have made it simpler than ever, to access social networking sites, which have become an integral part of our daily lives. However, safety and privacy are still major concerns. User-shared material, such as images, movies, and audio recordings may provide several safety and privacy concerns. Especially when the user uploads sensitive content, the attacker has the ability to misuse the information. If minors are targeted, the dangers are significantly greater. This study examines how data breaches or leaks impact the community and how security and privacy are compromised. Administrative authority, private service keys, private employee information, and publicly available databases have all been reported to be subjected to mass data leak. This study investigates the potential dangers, steps to avoid them, and remedies that could be found. Finally, this study provides merits and demerits of using social network sites through modern threat cases. Numerous case studies have been carried out to understand what may go wrong with online social networks.

**Keywords:** Network security, social media, preventive measure, modern threat, phishing

## 1. Introduction

Nowadays, it's almost difficult to go about your daily routine without being a member of various social media networks like Facebook and Instagram. Social networks provide a wide range of features and options to its members. Many of these are useful, but a couple may expose user data to hackers and attackers, which might be dangerous. When it comes to social networking, many believe they are safe, but this is a myth. As new technology advancements are introduced on a daily basis, existing levels of protection become more insufficient and insecure. In this article, we'll look at ways to deal with security risks and


*DOI: https://doi.org/10.36548/ jismac.2021.4.001*
*Received: 21.02.2022, received in revised form: 10.03.2022, accepted: 26.03.2022, published: 07.04.2022*

flaws in social media networks. Data breach, unauthorised access, insecure protocol, and attack method are only a few of the serious security concerns that are now being investigated [1-5]. Figure 1 shows purposes of visiting social media.

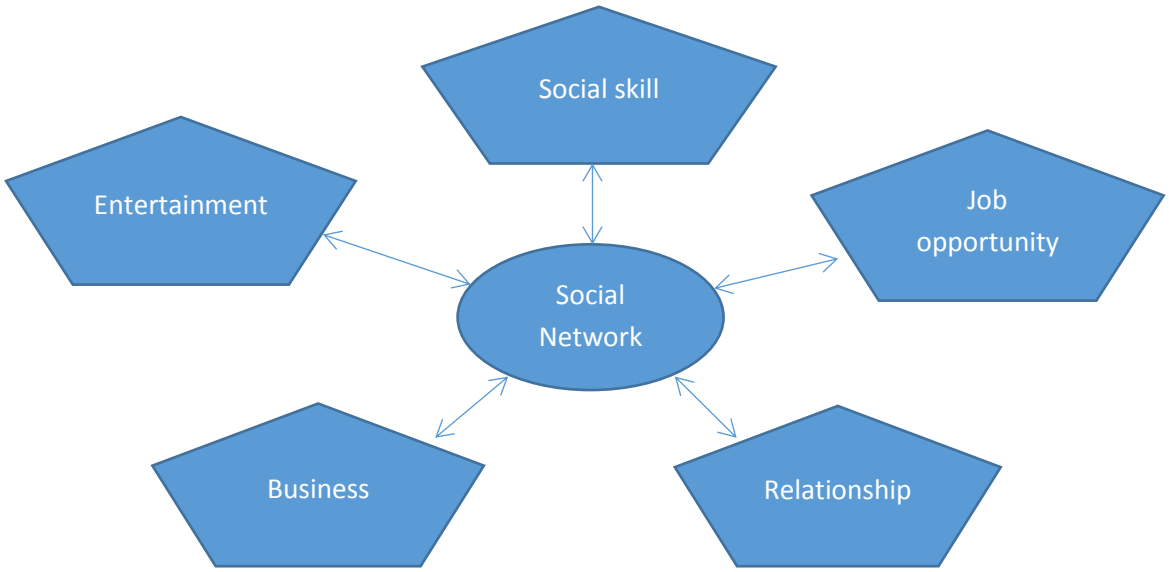


**Figure 1.** Purposes of visiting social networking sites

It's easy to overlook the significance of protecting the data you save on social networking sites like Facebook and Twitter since you use them for personal communication. However, as more and more information is shared on social media, it is becoming possible to get unparalleled access to private information about individuals and businesses. The sheer volume of information that can be gleaned, they have the power to wreak devastation throughout the globe. Furthermore, social media has evolved into a powerful tool for brand promotion.

A lack of attention to security on social media may leave individuals open to a wide range of dangers and expose their private information [6-8]. Social networks may be divided into a variety of sorts depending on the purposes for which they are intended. The four primary categories of social networks are:

1. "Social connections,"
2. "Multimedia sharing,"
3. "Professional,"
4. "Discussion forums"

Various kinds of social networking sites and their vulnerabilities, as well as phishing attacks that have targeted them, are discussed in this section. Malicious content-based phishing assaults are highlighted as current issues [9, 10].

Since the dawn of time, people have been using social media to connect with one another. With over 2.3 billion individuals using mobile social networks, the mobile Internet has taken this to a whole new level. This transformation in how individuals find and share information and material is a result of social media. Monologues (one to one) have been replaced by dialogues (one to many) (many to many). People's everyday lives have been intertwined with their use of social media. When some individuals switch on their cell phones, the first thing they do is check their social media newsfeeds.

An 84 percent of the world's internet population has access to Facebook and Twitter, with 271 million users on Twitter alone. As smartphones and ubiquitous Internet connections continue to grow, social networking is now much more accessible to mobile users, allowing them to stay connected to friends and family across the globe as well as receive messages from them no matter where they are [11-15].

This article consists of several sections as follows. Introduction of social media networks is addressed in Section 1. Section 2 consists of the contents of threats in the social media networks. Section 3 provides the details of preventive measures, and discusses the limitation and advantages of the social media networks. Finally, the conclusion has been briefed in section 4.

## 2. Threats

### 2.1 Conventional Threats

#### 2.1.1 Spam attack

Unwanted electronic communications in large quantities are referred to as "spam". Even though email is the most popular technique for distributing spam, social networking sites are much more successful. For example, a user's messages may be easily gathered from the company's website, blog, or newsgroup. As a result, persuading the intended customer to read spam communications and have faith that they would be safe is not difficult. While most spam is commercial, it may also gather personal information from consumers or be infected with malicious software such as viruses and malware.

### 2.1.2 Phishing

Using phoney websites and emails that seem to be from a reputable source, an attacker may get a victim's personal and secret information, such as their login, password, and credit card number, via what is known as a phishing assault [16, 17].

### 2.1.3 Identity theft

For example, a thief may use someone else's social security or cell phone numbers or address to carry out an assault without their authorization. With these details, an attacker may access a victim's friend list and demand personal information from them.

## 2.2 Modern threats

### 2.2.1 Profile cloning attack

Recently, the cybercriminals can create an exact copy online identity of a natural person to fool their real-life pals into thinking they are the natural person. Then, the attacker may use the victim's trust to steal personal information about the victim's acquaintances or commit online fraud [18 – 20].

### 2.2.2 Hijacking

To commit online fraud, an adversary hijacks a user's account and takes control of it. Phishing may collect credentials from sites without multifactor authentication and charges with weak passwords.

### 2.2.3 Inference attack

When a person posts statistics on a social networking site, an inference attack might infer sensitive information about the user that the user may not wish to share. For example, the user's buddy list and network architecture may be analysed using data mining techniques. Using this method, an attacker may get access to an organization's confidential information, as well as geographic and educational data [21 – 23].

### 2.2.4 Sybil attack

During a Sybil attack, a single node assumes the identity of numerous other nodes in the network. Platforms like Facebook and Twitter, which have a large number of users connected through a peer-to-peer network, may suffer as a result. There is no need for a

central server since computers connected over the internet are known as "peers," and they may transfer data directly amongst themselves.

### 2.2.5 Clickjacking

A technique called clickjacking is used to trick a person into clicking on a website that is not what he expected. The "User Interface Redress Attack" is another name for it. This attack is carried out by an attacker who takes advantage of a flaw in the browser. Another page is shown as a translucent overlay on top of the page the user wishes to see [24].

### 2.2.6 De-anonymization attack

A person's genuine identity may be protected on numerous social networking platforms, such as Twitter and Facebook, by adopting an alias or fake name. It is possible, however, for a third party to discover the true essence of a person by just tying together the information that these social networking sites provide. These assaults are typically utilised as part of military activities or as a form of criminal intimidation. They are motivated by a desire for money.

## 2.3 Reasons behind online social media security issues

One of the most distinctive, unstructured, and uncontrolled datasets in the modern world is being addressed by social media, and this scenario is rapidly emerging throughout the world. Many individuals post their images and other multimedia material to social media every day so that they may share it with their friends and family. This has sparked the creation of digital risk assessment.

# 3. Preventive Measures

## 3.1 Data breach

All sectors have been the target of cyberattacks and data leaks in the last several years. Data breach prevention is becoming a top priority for a wide range of businesses. Training and awareness may help prevent this from happening.

## 3.2 SQL injection

Before making any assumptions about the security of an application's code, run it through a vulnerability scanner to look for things like SQL injection. Security rules, password strength, encryption of secret data, real usage by administrators of admin passwords, filtered

SQL queries and changing code to utilise prepared statements or stored procedures may be used to avoid this kind of attack.

### 3.3 Spyware

Hackers are increasingly relying on spyware to get access to private information. This means that individuals must be taught about spyware, such as not clicking on strange links in emails from unknown senders, not downloading files from unauthorised sites, and not clicking on popup adverts from unknown sources; these are all crucial.

### 3.4 Downgraded server version

The majority of reduced server versions are susceptible to zero-day vulnerabilities and may be readily exploited by criminals. As a result, it is critical to keep server versions up-to-date or only employ the most recent ones. Furthermore, it protects data from such intrusions.

### 3.5 Phishing

To avoid becoming a victim of a phishing scam, it's important to educate people about the many forms of phishing assaults and how to recognise legitimate online apps on social networking sites. For further protection, users should be aware of the security and privacy options accessible to them on social networking sites [25, 26].

### 3.6 Clickjacking

Hackers use clickjacking to generate false dummy websites that resemble the actual ones in a significant amount of cases. Verify the website's source and IP address to ensure if it's legit. Verify the legitimacy of any social networking site before disclosing your login credentials or any other personal information.

### 3.7 Identity clone attacks

To avoid identity clone attacks, only trusted sources and friends should have access to a user's profile. Accepting friend requests from strangers is discouraged. Even if you know the person you're talking to, don't give out any personal information on social media since they might be cloned.

### 3.8 Insecure networks

Insecure networks are being exploited by hackers these days. Free Wi-Fi is a common method of connecting to unsecured networks, but this is dangerous since it invites hackers to steal your data. So, check to see whether the network we're utilising is secure. Using a public or free wireless network is not recommended.

### 3.9 Hypertext Transfer Protocol (HTTP)

For this reason, if you're on a social networking site that uses Hypertext Transfer Protocol Secure (HTTPS), it should ensure that all of the data is encrypted before it's sent to the server. Users' data cannot be decrypted by hackers even if they deploy a man-in-the-middle attack. Based on conventional and modern threats, it is found that many impacts of social media networks for preventive measures. Primarily, social networking websites are targeted by a variety of different sorts of attackers. People's decisions may serve a variety of reasons, as seen in Figure 1. As indicated in Table 1, the continual use of social networking sites or apps allows for the observation of both advantages and catastrophes.

**Table 1.** Merits and demerits of social network usage

| S.No | Various Sections | Merits | Demerits |
|---|---|---|---|
| 1 | Health Sector | Good in approach | Frequent Health problems |
| 2 | Technical Sector | Technological literacy | Attracts attention |
| 3 | Business / Bank Sector | Opportunity to widen business | Distraction and it leads to failure |
| 4 | Relationship Sector | Bringing people together | Relationship problems |

## 4. Conclusion

A cyber-attack might include fraud, a compromise of personal information, or cyber bullying. To avoid these assaults, it is essential to educate individuals about their own safety and security. It's also important to educate children about the most common hacker assaults and the implications they might have. This article examines how data breaches and leaks influence the community as a whole, and how this affects the security and privacy of individuals. Besides, the preventive measures for data confidentiality and safety are proposed, which in turn serve to improve security. Online social networks have been studied extensively to identify possible dangers and weaknesses. When submitting information to social media, users must exercise caution and ensure that their data is secure. In the future,

discussion forum users will also need to be protected. As more people fall for phishing scams on discussion boards, their faith in these venues is eroding. URL detection and filtering may be used to keep a user safe from harmful behaviour on these forums. However, implementing parsers to read external links on every forum would be prohibitively expensive despite the fact that such instances often notify users when they leave the parent site. Incentives may be devised to reward websites that scan external connections.

## References

[1] Benson V, Saridakis G, Tennakoon H, Ezingeard JN (2015) The role of security notices and online consumer behaviour: an empirical study of social networking users. Int J Hum Comput Stud 80:36–44

[2] Fosso Wamba S, Akter S (2016) Impact of perceived connectivity on intention to use social media: modelling the moderation effects of perceived risk and security. pp 219–227.

[3] Sahoo SR, Gupta BB (2020) Fake profile detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3):303–331.

[4] Ahmed M, Mahmood AN, Hu J (2016) A survey of network anomaly detection techniques. J Netw Comput Appl 60:19–31

[5] Mislove A, Viswanath B, Gummadi KP, Druschel P (2010) You are who you know. In: Proceedings of the third ACM international conference on Web search and data mining—WSDM ’10, p 251

[6] Sahoo SR, Gupta BB (2021) Multiple features based approach for automatic fake news detection on social networks using deep learning. Appl Soft Comput 100:106983

[7] Jain AK, Gupta BB (2018) Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417.

[8] M. Fire, R. Goldschmidt and Y. Elovici, "Online Social Networks: Threats and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019-2036, Fourthquarter 2014. doi: 10.1109/COMST.2014.2321628

[9] S. Kairam, M. Brzozowski, D. Huffaker, and E. Chi, “Talking in Circles: Selective Sharing in Google+.” In proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems, pp. 1065-1074. May, 2012.

[10] Andreas M. Kaplan, and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media," Business horizons, Vol. 53(1), pp. 59-68, 2010.

[11] Aggarwal A, Rajadesingan A, Kumaraguru P (2012) PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime pp 1–12

[12] Rathore S, Loia V, Park JH (2018) SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook. Appl Soft Comput 67:920–932.

[13] Michalopoulos D, Mavridis I, Jankovic M (2014) GARS: Realtime system for identification, assessment and control of cyber grooming attacks. Comput Secur 42:177–190

[14] Balduzzi M, Egele M, Kirda E, Balzarotti D, Kruegel C (2010) A solution for the automated detection of clickjacking attacks. Asiaccs 4(2):135

[15] Sahoo SR, Gupta BB (2020) Popularity-based detection of malicious content in facebook using machine learning approach. In: First international conference on sustainable technologies for computational intelligence. Springer, Singapore, pp 163–176.

[16] Wolniewicz CA, Tiamiyu MF, Weeks JW, Elhai JD (2018) Problematic smartphone use and relations with negative affect, fear of missing out, and fear of negative and positive evaluation. Psychiatry Res 262:618–623.

[17] Faris H et al (2019) An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks. Inf Fusion 48:67–83

[18] Munene, Assa Gakui, and Ycliffe Misuko Nyaribo. "Effect of social media pertication in the workplace on employee productivity." *International Journal of Advances in Management and Economics* 2, no. 2 (2013): 141-150.

[19] de Vries L, Gensler S, Leeflang PSH (2012) Popularity of brand posts on brand fan pages: an investigation of the effects of social media marketing. J Interact Mark 26(2):83–91

[20] Colicev A, Malshe A, Pauwels K, O'Connor P (2018) Improving consumer mindset metrics and shareholder value through social media: the different roles of owned and earned media. J Mark 82(1):37–56.

[21] Liu F, Xu D (2018) Social roles and consequences in using social media in disasters: a structurational perspective. Inf Syst Front 20(4):693–711.

[22] R. Vijayanandh and Dr. G. Balakrishnan, Performance Analysis of Human Skin Region Detection Techniques with Face Detection Application, International Journal of Modeling and Optimization, Vol. 1, No. 3, August 2011.

[23] Ruben Tous and Jaime Delgado, A LEGO-like Metadata Architecture for Image Search & Retrieval, 20th International Workshop on Database and Expert Systems Application, 2009.

[24] Bei-bei Liu and Jing-yang Su and Zhe-ming Lu and Zhen Li, Pornographic Images Detection Based on CBIR and Skin analysis, Fourth International Conference on Semantics, Knowledge and Grid, 2008.

[25] Tarek M. Mahmoud, A New Fast Skin Color Detection Technique, World Academy of Science, Engineering and Technology, 43, 2008.

[26] Paul Alvarez, Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis, International Journal of Digital Evidence Winter, Volume 2, Issue 3, 2004.

## Author's biography

**B. Vivekanadam** is an Associate Professor in the Department of Computer Science and Multimedia at Lincoln University College in Malaysia. His major area of research are machine learning, neural network algorithms, image processing, video and signal processing, cloud computing, deep learning, artificial intelligence, object recognition, complex feature extraction and vision graphics.

**Midhunchakkaravarthy** is working as an Associate Professor in the Department of Computer Science and Multimedia at Lincoln University College in Malaysia. His area of interest includes Big Data, Web Text Mining, Machine Learning, GPU Security, NLP.