ONLINE SOCIAL NETWORKS: SECURITY AND PRIVACY ISSUES

ABUBAKAR ABBA; & MUHAMMED ABDULAZEEZ HASSAN
Department of Computer Science, Federal College of Education, Zaria

Abstract

Online social networks (OSN) have made it possible for individuals to actively participate in virtual communities and exchange information, ideas, and other forms of self-expression with people who have similar interests as they do. But as OSN has grown, the social realm has also become more commercialized, raising questions about users' security and privacy. OSN service providers frequently gather private and sensitive information from their users, which may be accessed and used improperly by unauthorized users or other parties. In order to help users stay safe when using social media, this article outlines typical security and privacy vulnerabilities pertaining to OSN, present popular online social networks with active users and also present the leading countries based on the number of Facebook users.

Keywords: Security, Privacy, Social network, Users, Threat

Introduction

Social media platforms, such as online social networks (OSN), allow for communication and the creation of virtual communities between data owners (also known as data generators) and end users. OSN are online platforms used by end users to form social connections with others who have similar interests, activities, or real-life connections. These connections, or relationships, are represented as nodes (users, organizations, groups, etc.) and edges (the relationships between the nodes) in a social graph. There are many different types of social networking services available on the internet Ikram et al. (2018).

The primary purpose of online social networks (OSNs) is to enable users to share content with as many people as possible. Examples of OSNs include Facebook, Twitter, and LinkedIn, and users often publish updates about their daily activities on these platforms. However, some of the information that is shared can be private and should not be made public. For example, users may post updates about their personal lives or share photos and videos through OSNs. Many OSN users also use smartphones to capture and share images and videos on these platforms. When users share content on online social networks (OSN), such as photographs or videos, it may contain metadata and location information. While OSN service providers may collect this data to personalize their services for users, it can also be used for commercial purposes and shared with third parties, leading to privacy breaches. This information can be exploited by malicious users to invade an individual's privacy. Information retrieval and data privacy are two important areas in computer science that serve different purposes. Information retrieval involves techniques for extracting data and providing organizations with tools for analyzing and making decisions based on this information. Data privacy, on the other hand, focuses on protecting data from unauthorized

and malicious access that could reveal, alter, attack, or destroy the data stored or shared online. Researchers in the field of information retrieval may not always consider privacy issues when developing solutions for information management, while those working on data privacy may limit information retrieval techniques in order to protect sensitive data from adversaries who seek personal information.

The rise of social media and the increasing use of online social networks (OSN) for communication has made more sensitive information about individuals available online. While not all data shared through OSNs is sensitive, some users do post personal information publicly, which can potentially lead to the disclosure of their privacy. When publicly available data can be traced and linked to a user's activities, their privacy is at greater risk as sensitive information can be mined and extracted from it. The concept of privacy can vary depending on the context and the sensitivity of the shared content. According to Mario et al. (2018), it is important to protect the value of data in order to maintain the integrity of the context in which it is shared online. While information gathered from social media for analysis purposes may not always be intentional or relevant, it can still be linked to a person's private activities, such as their religion or political affiliations (Davison et al., 2012). Therefore, it is important to consider the privacy implications of collecting and using this data.

Privacy and Security Threats in OSNs

User-generated content on social media can include a range of information, such as users' experiences, opinions, and knowledge, as well as private data such as names, gender, location, and personal photos (Taddicken et al., 2014). It is important to note that this information, once shared online, is electronically stored and can be permanent, replicable, and reshared. Online social network (OSN) users often face challenges in managing their social identity while also maintaining their social privacy. The widespread use of social media has led to an estimated of more than 2.95 billion active users worldwide by 2022 (https://www.statista.com/topics/1164/social-networks/). Figure1 shows the total number of active users on various popular social media networks.

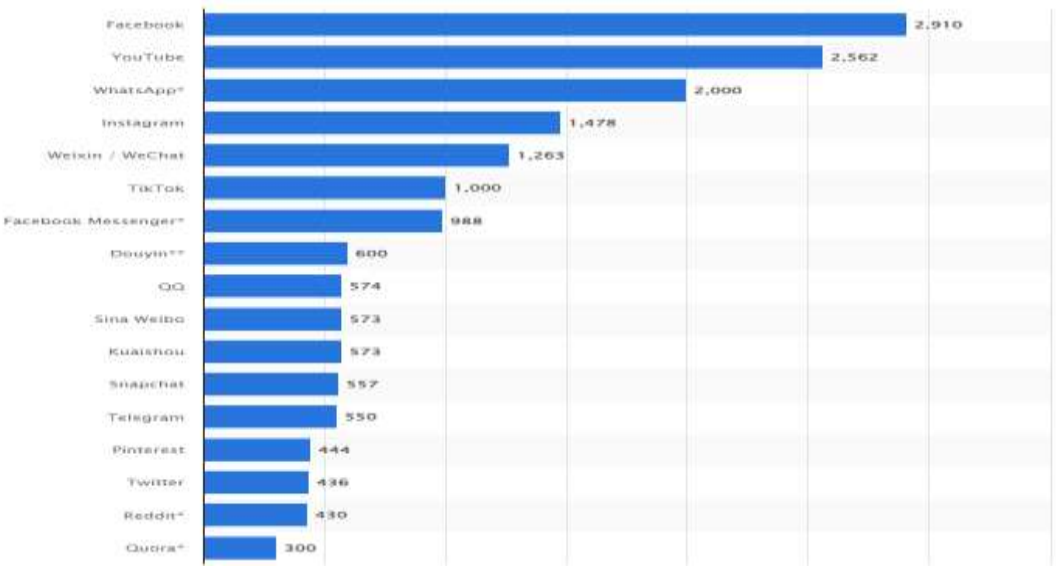

Figure 1*: Total number of active users on various popular social media networks in millions (https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/)*

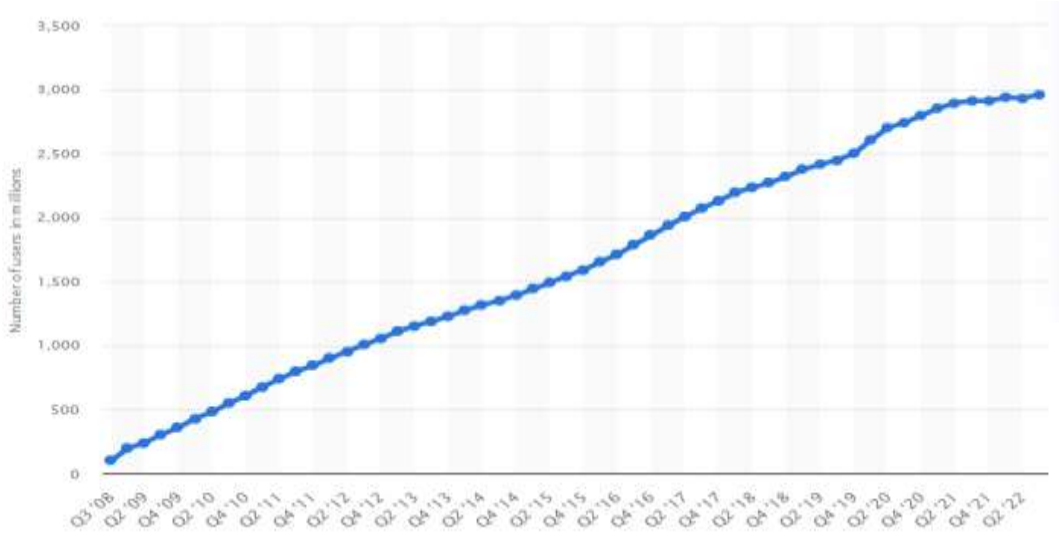

Figure 2: *Number of monthly active Facebook users worldwide as of 3rd quarter 2022 (https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/) in millions*

As of the third quarter of 2022, Facebook had over 2.96 billion monthly active users, making it the most popular online social network globally. It took the site just over 13 years to achieve two billion active users, which was reached in the second quarter of 2017. In contrast, it took 11.2 years for Instagram, owned by Meta, and little over 14 years for YouTube, owned by Google. As of January 2022, India had the largest following on Facebook, with approximately 330 million members, followed by the United States, with about 180 million users approximately and Nigeria is number 18 as shown in figure 3 below with about 26 million facebook users.

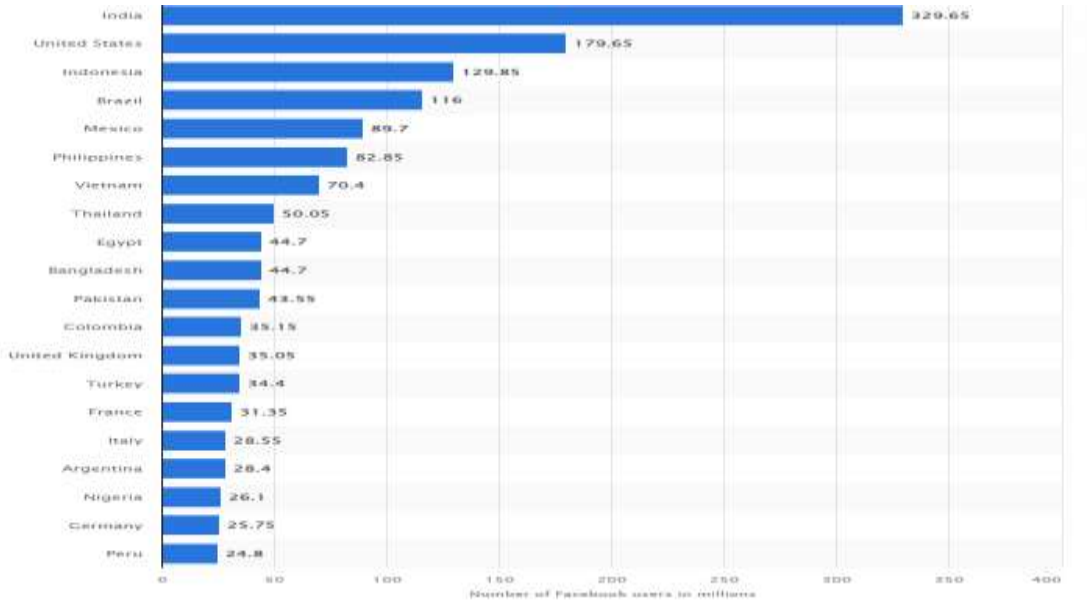

Figure 3: *Leading countries based on number of facebook users (https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/) as of january 2022 in millions.*

Given the large number of users of online social networks (OSN) globally, privacy is a significant and pressing issue. OSN can foster various privacy concerns, such as surveillance, in which the social sphere becomes commercialized and OSN service providers monitor user actions for market force access control. Standard online social networks (OSN) may share users' personal data with third parties for advertisement purposes, which can be exploited (Shaukat et al., 2018). Additionally, when users browse OSN sites, they leave digital footprints that can be used for commercial purposes and user profiling. Social networking tools have transformed the way we communicate in our personal and professional lives, but they also pose significant risks to privacy and security. These tools have become an important part of both our social and business lives, but it is important to be aware of the potential risks they may pose. Due to the high number of users who regularly access online social networks (OSN), they have become a particularly attractive target for attackers in recent years. The widespread use of social media has also made online users more vulnerable to privacy and security threats. There are two categories of threats that online social network (OSN) users face: classic threats and modern threats. Classic threats are online threats that affect not only OSN users, but also other online users who do not use OSN. The second type of threats, modern threats, are specifically related to the use of online social networks (OSN) and the potential for the OSN infrastructure to compromise user privacy and security (Fire et al., 2014). A 2016 report from NopSec, the State Vulnerability Risk Management Report (http://info.nopsec.com), found that organizations often use inadequate risk evaluation scoring systems that do not take into account the potential risks posed by social media. The report noted that social media platforms are among the top types of platforms for cybersecurity, yet they are often not included in risk evaluation scoring systems.

Classic Threats

Classic threats, such as spam (Soumya and Revathy, 2018), malware (Mohit et al., 2018), phishing (Alam et al., 2016), and cross-site scripting (XSS) attacks (Nithya et al., 2015), have been a concern since the early days of the internet. While researchers and industries have worked to address these threats, they can still spread quickly through online social networks (OSN) and be used to extract personal information from users. This can not only target the intended victims, but also their peers by using private attributes to tailor the threat.

Malware

Malware, short for malicious software, is any software that is designed to intrude on a computer and access private content. Malware attacks on social networks can be particularly effective because of the structure of online social networks (OSN) and the interactions among users. In the worst cases, malware can access users' login credentials and impersonate them in order to send messages to their peers. For example, the Koobface malware was spread through OSN platforms such as MySpace, Facebook, and Twitter, and was used to collect login credentials and turn the infected computer into a part of a botnet (Baltazar et al., 2018) Online social networks (OSN) can serve various purposes, such as marketing and entertainment, but they can also expose users to harmful activities. Fraud and the propagation of malware are criminal actions in which users are tricked into accessing a URL and running malicious code on their computer (Alghamdi et al., 2018).

Phishing Attacks

Phishing is a type of fraudulent attack in which the attacker obtains personal information from a user by pretending to be a trustworthy third party through a fake or stolen identity. For instance, in an attack attributed to the Chinese government, senior military officials from the U.K. and U.S. were tricked into becoming Facebook friends with someone impersonating U.S. Navy Admiral James Stavridis (Protalinski et al., 2018). Social media platforms have also been used by phishers posing as other people in many instances (Miller et al., Vishwanath et al., 2018).

Spam Attacks

Spam messages are unwanted messages that can come in the form of wall posts or instant messages on online social networks (OSN). Spam on OSN is more dangerous than traditional email spam because users tend to spend more time on these platforms. Spam messages often contain advertisements or malicious links that can lead to phishing or malware sites. Spam can originate from fake profiles or spam applications, and fake profiles may be created in the name of a popular person in order to spread spam (Soumya and Revathy, 2018). Spam messages can originate from compromised accounts and spamming bots (Egele et al., 2017), but most spam is spread through compromised accounts. To prevent spam from reaching its intended targets, spam-filtering approaches are used to detect malicious messages or URLs in a message and filter them out before delivery.

Modern Threats

Modern threats are typically specific to online social networks (OSN) and often involve the goal of obtaining private information about users and their friends. For example, an attacker may want to know about a user's current employer information. If a user has their privacy settings on their Facebook account set to public, their information can be easily viewed by anyone. However, if they have a customized privacy setting that only allows their friends to view their information, the attacker can create a fake Facebook profile and send a friend request to the targeted user in an attempt to gain access. Once the friendship request is accepted, the attacker can access the user's information. The attacker may also use an inference attack to collect personal information from the publicly available content of the user's friends.

Clickjacking

A user-interface redress attack, often referred to as lickjacking, is a harmful tactic that deceives web users into clicking on something other from what they intended to. Attackers that utilise clickjacking techniques on online social networks (OSN) might trick people into posting garbage on their timelines and unintentionally requesting likes on specific links. Attackers may even be able to capture a user's activity using the computer's hardware, such as the microphone and camera, in clickjacking assaults (Lundeen et al., 2018).

Fake Profiles

The establishment of false profiles is a frequent method of assault on social networks. In this kind of attack, an attacker sets up an account on a social network using fictitious information and sends messages to verified individuals. The attacker delivers spam to users who have requested to be friends with them.

Fake profiles are frequently automated or semi-automatic and made to look like real profiles. A false profile's objective is to gather confidential data from online social networks (OSN) that is only visible to friends in order to spread it as spam.

Information Leakage

The main purpose of social media is to freely share and trade information with peers. Some users voluntarily divulge their private information, including health-related information. Unfortunately, some of them divulge a little bit too much private information about goods, projects, businesses, or other types of private information. Sharing such private and delicate information could have detrimental effects on OSN users. As an illustration, an insurance provider may use OSN data to categorise users as dangerous customers (Soumya and Revathy, 2018).

Location Leakage

Data leakage is a form of threat that includes location leaking. There is a trend among users to use mobile devices to access social networks. Apps are typically used to connect a mobile device to an online source. The new privacy risk of location leakage is introduced by the use of mobile devices for online access. Users are more likely to share their location while using mobile devices for online access (Soumya and Revathy, 2018). As a result, attackers may utilise the disclosure of geographic information on social networking sites to attack users.

Features In Social-Networking Sites

All of the contemporary social networking services are web-based and run through the internet. Through a centralised access management system, content is kept on cloud storage. Anywhere with an Internet connection and a web browser can access these contents.

• Users of OSN must construct public profiles for social networking sites in accordance with their predefined formats. The main purpose of this profile information is to authenticate users entering the social networking site.

By connecting a user's profile with that of other users who have comparable profile information, almost all of the social networking platforms currently in use assist users in establishing social connections with other users.

• The fact that user-generated material is used by existing OSNs for commercial gain is an intriguing aspect of these networks.

At the moment, a large number of users use their mobile phones for social networking. Apps are typically employed for this purpose. Anybody with access to a mobile device can use any app that is loaded on it. Therefore, any app that is installed on a user's mobile device needs to be protected with a strong password.

Recommendations

Online social networks (OSNs) are websites or apps that allow users to connect with each other and share information, such as posts, photos, and videos. While these platforms can be useful for staying in touch with friends and family, they also have a number of privacy and security concerns. For example, the information that users share on OSNs could potentially end up in the wrong hands, or be combined

with other public datasets to reveal even more private information. In order to protect their privacy, OSN users should take a number of precautions, such as verifying their privacy settings, being careful about what personal information they share, keeping their location information private, installing antivirus and antispyware software, and uninstalling third-party applications. By taking these steps, users can reduce the risk of their information being misused or accessed by unauthorized parties.

Conclusions

There are many advantages to social media, but these advantages have also led to some issues, according to OSNs. Social media's primary issues centre on user data as well as security and privacy. OSN service providers, unauthorised users, or other parties who use OSN data for their business activities could be to blame for these issues. Several privacy and security issues involving OSN users, data from OSN service providers, and outside data collectors are discussed in this article. The study's main objective was to educate OSN users about these issues and provide them with advice on how to stay clear of them whenever they use social media. A significant amount of private and personal data has been produced as a result of social networks' steadily growing user base. However, as social networks have expanded, so have the security risks they face, posing a serious risk to user privacy. It's crucial to address these security threats by properly understanding the problems and having constructive discussions to come up with solutions.

References

Alarm, S.; El-Khatib, K. Phishing Susceptibility Detection through Social Media Analytics. In Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; pp. 61–64.

Alghamdi, B.; Watson, J.; Xu, Y. Toward detecting malicious links in online social networks through user behavior. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence Workshops, Omaha, NE, USA, 13–16 October 2016; pp. 5–8.

Ali, S.; Rauf, A.; Islam, N.; Farman, H.; Khan, S. User Profiling: A Privacy Issue in Online Public Network. Sindh Univ. Res. J. (Sci. Seri.) 2017, 49, 125–128.

Egele, M.; Stringhini, G.; Kruegel, C.; Vigna, G. Towards detecting compromised accounts on social networks. IEEE Trans. Dependable Secure Comput. 2017, 14, 447–460.

Baltazar, J.; Costoya, J.; Flores, R. The Real Face of Koobface: The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research. 2009. Available online: https://www.trendmicro.de/cloud-content/us/pdfs/ security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf (accessed on 21 October 2018).

Burke Winkelman, S.; Oomen-Early, J.; Walker, A.D.; Chu, L.; Yick-Flanagan, A. Exploring Cyber Harassment among Women Who Use Social Media. Univers. J. Public Health 2015, 3, 194–201.

Davison, H.K.; Maraist, C.C.; Hamilton, R.; Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. Empl. Responsib. Rights J. 2012, 24, 1–21.

Fletcher, D. How Facebook Is Redefining Privacy. Available online: http://content.time.com/time/ magazine/article/0,9171,1990798,00.html (accessed on 10 November 2018).

Fire, M.; Goldschmidt, R.; Elovici, Y. Online social networks: Threats and solutions. IEEE Commun. Surv. Tutor. 2014, 16, 2019–2036.

Gupta, S.; Gupta, B.B. Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. Int. J. Syst. Assur. Eng. Manag. 2017, 8, 512–530.

Gulyás, G.G.; Simon, B.; Imre, S. An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, 24 October 2016; pp. 1–11.

Lundeen, R.; Ou, J.; Rhodes, T. New Ways Im Going to Hack Your Web APP. Black Hat Abu Dhabi. Available online: https://www.blackhat.com/html/bh-ad-11/bh-ad-11-archives.html#Lundeen (accessed on 1 November 2018)

Mario F.; Pasquale P.; Gianluca A.; Giancarlo F. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges IEEE Internet of Things Journal, Vol. 5, no. 4, August 2018.

Mohit Sewak, Sanjay K. Sahay and Hemant R. Comparison of Deep Learning and the Classical Machine Learning Algorithm for the Malware Detection, arXiv:1809.05889v1 [cs.CR] 16 Sep 2018.

Miller, S. Sen. Grassley's Twitter Account Hacked by SOPA Protesters. Available online: https://abcnews. go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/ (accessed on 1 November 2018).

Nithya, V.; Pandian, S.L.; Malarvizhi, C. A survey on detection and prevention of cross-site scripting attack. Int. J. Secur. Appl. 2015, 9, 139–152.

Obar, J.A.; Wildman, S. Social media definition and the governance challenge: An introduction to the special issue. Telecommun. Policy 2015, 39, 745–750.

Penni, J. The future of online social networks (OSN): A measurement analysis using social media tools and application. Telemat. Inform. 2017, 34, 498–517.

Protalinski, E. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials. Available online: https: //www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/ (accessed on 21 October 2018).

Shozi, N.A.; Mtsweni, J. Big data privacy in social media sites. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, Southern Africa, 30 May–2 June 2017; pp. 1–6.

Shaukat A.; Naveed I.; Azhar R.; Ikram U.; Mohsen Guizani and Joel J. P. C. Rodrigues. Privacy and Security Issues in Online Social Networks. Future Internet 2018.

Soumya.T.R and S. Revathy. Survey on Threats in Online Social Media, International Conference on Communication and Signal Processing, April 3-5, 2018, India.

Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. J. Comput.-Mediat. Commun. 2014, 19, 248–273.

Tam, K.; Feizollah, A.; Anuar, N.B.; Salleh, R.; Cavallaro, L. The evolution of android malware and android analysis techniques. ACM Comput. Surv. 2017, 49, 76.

Torabi, S.; Beznosov, K. Privacy Aspects of Health Related Information Sharing in Online Social Networks. In Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, Washington, DC, USA, 12 August 2013.

Vishwanath, A. Getting phished on social media. Decis. Support Syst. 2017, 103, 70–81.

Wani, M.A.; Jabin, S.; Ahmad, N. A sneak into the Devil's Colony-Fake Profiles in Online Social Networks. Available online: https://arxiv.org/ftp/arxiv/papers/1705/1705.09929.pdf (accessed on 29 October 2018).

Zhang, W.; Al Amin, H. Privacy and security concern of online social networks from user perspective. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP2015), ESEO, Angers, Loire Valley, France, 9–11 February 2015; pp. 246–253.