A Study to Investigate Security Issues in Online Social Networks and Effective Prevention Strategies

Sudipta Das[1], Dr. Priya Vij[2]

[1,2]Department of Computer Science and Engineering, Kalinga University, Raipur, Chhattisgarh

ABSTRACT

The rise of OSN has made it possible for anybody, formerly a mere observer, to actively participate in the creation of content. Online virtual communities have given users a platform to voice their opinions, share knowledge, and make connections with people who share their interests. This is a concern since OSN have turned people's social networks into a platform for ads. The security and privacy of OSN users might be jeopardized by this. Data collectors, third parties, or unauthorized users might misuse the private and sensitive information that OSN service providers acquire from their consumers. Typical privacy and security concerns are detailed in this article, along with suggestions for how OSN users should safeguard their social media accounts. Identity theft, phishing, and virus dissemination are some of the primary security challenges plaguing OSNs, and this paper thoroughly analyzes them. Problems with user education, authentication, and privacy measures are some of the root causes of these vulnerabilities. This article takes a closer look at the existing safeguards and new approaches to strengthen the safety of OSN platforms by referencing current research and real-world examples.

Keywords: Security issues,Phishing, Malware, Social networking,Privacy

INTRODUCTION

With the launch of the internet in the mid-1990s, hitherto unimaginable means of information sharing became feasible. The human element was still missing from the information exchange, though. The early 2000s saw a dramatic increase in the amount of personal information shared online as a result of the proliferation of social media. You may increase the amount of time you spend interacting with other people by using social media sites like Facebook, Twitter, Instagram, LinkedIn, and many more. Both your personal and professional life can benefit from it. In this setting, people may meet new people, talk about topics that interest them, and form bonds based on common ground. It basically makes it easier for people all around the world to work together. The idea that social media platforms are simple and straightforward has persisted for quite some time. The exponential growth of social media platforms and their user engagement may be explained by this. The potential benefits of social networking on an individual's social abilities, entertainment choices, career prospects, and personal relationships are many. Facebook and Myspace are among the most widely used social networking sites. Because of the massive user bases of these platforms, advertising products and services as well as causes has become increasingly important on social media.

Consumers often fail to realize how important it is to safeguard the personal information they preserve on social networking sites because they view these platforms as a means of personal contact. Over time, people are sharing more and more information on social media in various formats, which might result in unparalleled access to personal and business data. The abundance of sensitive user data stored on social media platforms makes them a tempting target for cybercriminals. They can cause global chaos once they get their hands on this enormous data set. Additionally, marketers are discovering social media to be an excellent venue for advertising; yet, they must exercise caution lest they be vulnerable to various threats and have concerns regarding the security of their sensitive data.

Email, Usenet, blogging, IM, and online social services are just a few examples of the many new forms of online sociality that have arisen with the advent of the Internet. Of these two technical trends, social networking sites (SNSs) have emerged as the most notable in the modern day. These types of social media have seen an explosion in user numbers in the past few years. Users may find individuals with similar interests and beliefs, share and discuss material, and form communities via these online social networks. These internet networks are very beneficial to both individuals and companies. The numerous benefits of social media platforms include:

- No matter where they are, people may easily maintain connections with their peers. Students in particular may benefit from the heightened sense of self-worth that can result from the relationships formed through social networking.
- Discover and connect with others who share your interests.

- Establish a digital meeting place for novel forms of online learning, teaching, learning from one another's experiences, and building trust, including the gathering and trading of personal and company reputations.
- A social networking site (SNS) may increase a company's collective knowledge and allow many employees to participate in strategic planning when it comes to businesses.

There are many different kinds of social networks, each with its own specific purpose. There are four main types of social networks: friendship networks, professional networks, multimedia sharing networks, and debate forums. Malicious content-based phishing assaults are highlighted as a current concern. It is possible to classify many social networking sites into the categories shown in Figure 1.

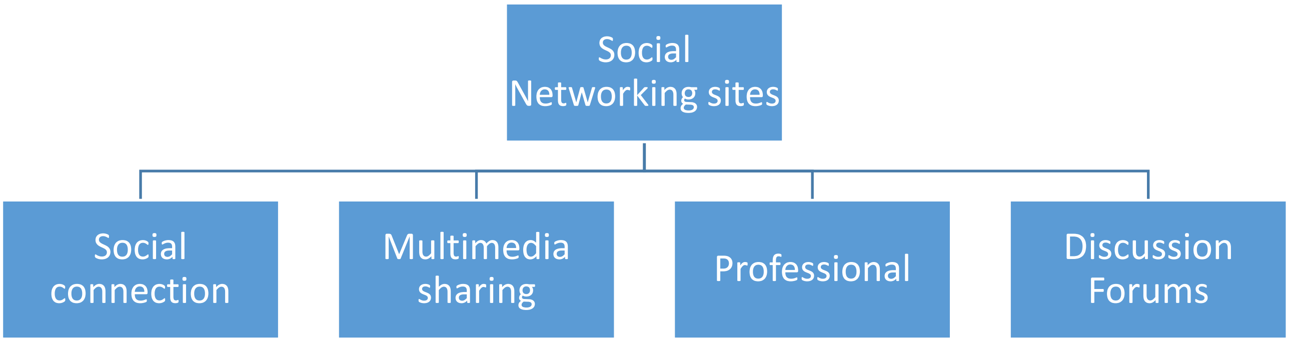

Figure 1: Types of social networking sites

Social connection
Users interact virtually with companies and each other in social connection. Despite the existence of other social media platforms, this one is quickly becoming the de facto norm. Sites like "Facebook," "Twitter," "Google+," and "Myspace" are instances of this. There are benefits to using these sites, but there are also some drawbacks. Phishing attacks can target these sites in various ways. Create a gateway that mimics the appearance of a Facebook page; an attacker may access it easily. Then they could try to trick consumers into inputting their credentials in various ways.

Multimedia sharing

Another way that material like photos, movies, and live streams can be shared online is through multimedia sharing networks. They make it possible for consumers and businesses to exchange media content online. Websites like "YouTube," "Flickr," "Instagram," and "Snapchat" fall under this group. These days, it appears like every social media site has a "inbox" feature where users may send and receive messages and have conversations with their friends. This function has now been made available on YouTube as well. The attacker has a perfect chance to phish their victim because of this. He can trick the recipient into visiting a malicious website by using a shortened URL in the message. Attackers take advantage of the fact that abbreviated URLs are difficult to discern as authentic by hiding their harmful information in them.

Professional
Users can find job possibilities on professional social networks. Depending on the website's purpose, it could offer a broad forum or cater to certain interests or professions. Professional social networking sites include; "LinkedIn," "Classroom2.0," and "Pinterest," among others. An attacker may send a target a tailored email because to the wealth of professional information available on social media platforms, including email addresses. These emails could look like prize money claims but instead include a malicious link.

Discussion forums
The same holds true in online discussion forums, where users exchange ideas and information. These networks, which are among the first types of social media, offer a goldmine of information for market researchers. "Reddit," "Quora," and "Digg" are wonderful instances of wildly popular discussion boards. To help other users learn more about a certain subject, members of these forums often offer links to resources they've found useful in their own study. In order to lure unsuspecting visitors to phishing websites, some dishonest people distribute harmful links. This is another method that online discussion boards may be used for phishing.

Websites that facilitate human connection are known as online social networks. They make it easy for people to connect with one another, stay in contact, and exchange ideas, emotions, and stories. They are all based on the same principle, which is that the user establishes a network of connections connected by a trust factor. The next step is for the user to make material for their friends, which they may then access. This material can contain a wide variety of items, such as images from vacations, links to interesting websites, commentary, opinions, and status updates on current events.

In recent years, the number of people using online social networks has increased at an exponential rate. Social media has many different applications. They have several potential uses, including but not limited to: traditional social networking with friends and family, professional networking and job searches, increasing sales income, and public awareness of current events. One case in point is In August 2011, the India Against Corruption (IAC) campaign, spearheaded by Anna Hazare, used Facebook and other social media to rally the people against corruption in India. Similarly, in February 2011, the Egyptian revolution made significant use of online social media. These recent events proved that online social networking is strong and popular in our traditional culture.

REVIEW OF RELATED STUDY

Shah, Akash et al., (2024) Online social network (OSN) platforms are becoming an integral part of almost everyone's daily life. Online social networks (OSNs) allow a large portion of our society to communicate with one another and spread news and views. The ease and speed with which information may be transmitted on OSN platforms makes them a prime target for cybercriminals attempting to steal private information. When people exchange information, particularly private media like videos, photos, and audio files, several privacy and security concerns arise. Anyone with access to the data might potentially use it for malicious purposes. We need to take a close look at the privacy and security threats that OSN platforms represent, even those that have so far eluded detection and prevention efforts. It is critical to categorize these risks so that scholars and researchers can better understand the motivations behind cyberattacks. In order to make sure that people using OSNs are secure, researchers studying various privacy and security issues should provide their datasets to the public. So yet, no one in that sector has made that move. This project aims to fill these gaps by researching the dynamic nature of threats, categorizing them into three types (conventional, advanced persistent, and targeted), and locating pertinent datasets that academics can utilize to create strong protections for OSN users. Furthermore, the article summarizes several security methods to guarantee the safe and secure usage of OSN platforms and discusses present research problems in the area of OSN. Ali, Shaukat et al., (2018) Anyone, who was formerly just able to watch, can now take part in making content thanks to the proliferation of OSN. Online virtual communities have given users a platform to voice their opinions, share knowledge, and make connections with people who share their interests. This is a concern since OSN have turned people's social networks into a platform for ads. This may put OSN users' privacy and security at risk. The personal and sensitive information that OSN service providers obtain from their customers might be misused by those who aren't allowed to access the data, as well as other parties. This article provides guidance on how OSN users should safeguard their social media accounts and covers typical privacy and security concerns.

Almutairi, Abeer et al., (2016) Online social networking (OSN) services provide a simple means for individuals to maintain online relationships. Their significance in the development of the web is rapidly growing. The web's capacity to facilitate these networking abilities is becoming increasingly robust as the need for connection among governments, organizations, and individuals remains consistent. On top of that, they offer a digital platform where users may share their every action and interest with everyone, whether it's close friends and family or total strangers. With the use of this brilliant technology, cybercriminals have figured out how to easily steal personal and company information from social media sites. Concerns about personal information security on social networking sites have increased dramatically since the introduction of the internet. Improving security measures to ward off hackers is the starting point for this analysis's complexity level. In this essay, we will go over a few of these aspects of social media site security and safety. Kumar, Senthil et al., (2016) Social media has become an integral part of people's daily lives. Media (including current events and related images), education (including course materials, quizzes, and workshops), business (including online surveys, marketing, and customer targeting), and entertainment (including songs, videos, and jokes) are some of the areas where people are starting to share more than just text, photos, and messages. The sheer variety of ways in which individuals use social networking sites has led even the most cynical among us to conclude that they define contemporary Internet culture. Sharing content on social media might be entertaining, but it also raises serious privacy and security issues. Users' personal information ought to be kept private.

Gao, Hongyu et al., (2011) This essay gives a thorough review of the current state of security problems and different protection solutions, with an emphasis on popular online social networks. Several dangers are discussed, along with possible solutions if they are available. Viral marketing, viral attacks, network structural attacks, and privacy breaches are the ways these assaults are categorized by the writers, who place a focus on privacy concerns. After a comprehensive review of each category, they move on to investigate the relationships between the various security issues.

ONLINE SOCIAL NETWORK SECURITY ISSUES

Users' Anonymity

The vast majority of people who use social media apps online use their own name. Because of this, individuals' identities are accessible to the public on social media, and search engines may access all of these platforms. People are missing out on career prospects because employers now look at a candidate's OSN profile. The perpetrator will be sent to the specific user profile when they enter the victim's name into the search engine. By breaking into a victim's social media accounts, hackers can have access to all of their personal data.

Profile and Personal Information

All of the personal information (full name, phone number, email, date of birth, relationship status, etc.) of almost every social media user is readily available, educational background, and employment history posted on their page. The availability of such sensitive data on social media platforms gives hackers all the knowledge they need. Everyone who uses a social networking web app has access to these fundamental and personal details. In terms of privacy settings, the majority of users have them set to public. Because no one knows to look on their profile for the privacy settings, every user's private and sensitive data is accessible to everyone.

Even with the privacy settings set to private, hackers can still get the data through several approaches. People who use social media websites often download third-party apps. Users must provide the third-party app access to their personal data when they utilize it to access their social media accounts more conveniently. This means that the user's data is being sent to an external application domain.

Image Tagging

Online social network users have the option to include their complete name, email address, and even a link to their profile when they tag photographs. The public, friends of friends, and even complete strangers can view this tagged photograph. So, hackers may exploit this picture tagging to do annoying things as it gives other users information about the user.

Image Hacking

Each user's profile is updated daily with several actual photographs. Due to a lack of information regarding Regardless of the settings for privacy, the public can view some of the photographs. Most of the real images will only be seen to those in your tight circle. The following are some of the many ways these actual photos might be compromised:

- **Dragging the image:**Any time someone posts a picture on social media, hackers may easily grab it and store it somewhere. The perpetrator just needs to drag the picture to the spot where they want to save it. Pictures shared on social media platforms are not encrypted in any way.

- **Right Click and save as image:**Any image will display the context menu when you right-click on it. When you right-click on a picture, a menu with choices to save the image appears. The criminal may easily save the snapshot to their computer by using this option. The fact that this right-click option is available on every social media platform demonstrates that users' uploaded photos are not protected.

- **Snipping tool in windows OS:**A function called the snipping tool is included in the advanced edition of Windows OS. You may use this application to crop and save any image that is now shown on your computer screen. With this program, you may easily crop and save photographs from social media.

- **Print Preview and save:**As soon as the picture appears on the social media website, the perpetrator might use the print preview feature to steal it. To get a preview of the current page in print format, just click the print preview button. You may find the "save as pdf" option on the preview page. By selecting this option, the hacker may save the page as a PDF and then edit the picture to their liking by cropping it.

- **Combination of keys:**Pressing a shortcut key, such Ctrl+A, will select the full current page. Once the attacker has picked the full site, they may simply copy and paste it to their preferred place. Then, they can divide the picture. Similarly, you may save the document to any place on the client system by using Ctrl+S. All of the current page's content is accessible in the saved folder after the page is saved. If a hacker gains access to the stored folder, they can simply steal the image.
- **Temporary Internet Folder:**A "temporary internet folder" exists on every computer. The multimedia elements of a website are saved in the temporary internet folder upon initial page load. The webpage is retrieved from the temporary internet folder every time it is reloaded. The server alone loads the new page content to the client PC. The contents are not temporarily stored in this folder. All of the contents of this folder will remain accessible within it unless the user explicitly deletes them. Inside the temporary internet folder, you may find all of the users' photographs from social media. With the photo in the hands of hackers, it might be used for anything.

- **Print Screen:**The ability to print one's screen is standard on all computer systems. Clicking this button allows the user to save the current web app to their preferred location. Consequently, the print screen option makes it easy for hackers to breach social media sites' picture galleries.

Photo sharing on social media platforms is thus not secure. Real user photographs are easy for hackers to steal, and then those photos may be exploited for all sorts of annoying purposes.

Fake Profile

It is easy for hackers to gain facts when a user's complete personal information and genuine photograph are available on social media. The hacker will construct a false profile using the stolen sensitive information and photographs. False profiles can ruin the reputation of the original person, putting them in legal hot water indefinitely. The perpetrator can gain access to sensitive information and add the victim's acquaintances to their own circle using this phony profile.

Social Phishing

The goal of social phishing attacks is to get victims to provide personal information. The hacker will create a phony website that mimics the appearance of a legitimate one in this type of attack. The perpetrator will notify the target via messaging that the profile will be removed until the victim verifies their identity. The victim's personal information, including their login and password, will be requested when they visit the specific fraudulent website. The majority of the time, the victim's lack of awareness allows the assailant to succeed.

E-Mail Spam Attack

By obtaining the victim's email address, the hacker may launch this kind of attack and start flooding their inbox with spam. The majority of users leave their email addresses visible on social media, making them easy targets for attackers. Even if the user's email is set to private, it may still be guesstimated using the victim's first and last name. You can find someone on most social networking sites by just sending them an email. Using these tools that social media sites provide, an attacker may readily get personal information.

Malware Attack

The prevalence of malware attacks has grown in the eyes of social media users. The malicious code will be sent to the victim's profile by the attacker. Malware will publish bogus information on the victim's wall the moment the user clicks on the URL. Malware can also take the form of URL redirects that, when clicked, take the visitor to a phony website that requests personal information. In a similar vein, the victim's PC will be infected with client-side code that can steal data when they click on the malicious URL.

Sharing Day to Day activities

Sharing mundane details of one's day with friends and family is a common practice among social media users. Think about the following post as an example. Hello, I am relocating the beauty parlor by myself. The kidnappers can use this type of publication to their advantage. The kidnapper will then have complete knowledge of the victim's whereabouts and the others accompanying them. A security risk to users, particularly women, will result from these types of sharing current actions occurring online.

Gathering Social Data

By keeping tabs on the victim on social media, the perpetrator can learn about the victim's interests and likes. Marketing advertisements and shopping offers will be sent to the victim based on the information collected from their profile. The level of user privacy is severely compromised here.

Deleting the User Account

The abuser might find out what the victim is into by following them on social media. Based on the victim's personal information, marketing ads and shopping offers will be delivered to them. There is a serious breach of user privacy occurring here.

Physical Threat

A person's home address, phone number, and email address are among the personally identifiable information that frequent social media users provide online. The perpetrators may then use this information to contact the victim by phone or send spam to their email account, revealing their physical identity. Forever, the victim will be in danger physically.

REASONS BEHIND ONLINE SOCIAL NETWORK SECURITY ISSUES

One of the most unique, unstructured, and uncontrolled datasets in the modern world has emerged as a result of the fast globalization of social media. Every single day, millions upon millions of people across the world use social media to exchange multimedia content like photos and movies. Digital risk monitoring solutions have grown in popularity as a consequence of this. Customers (representatives, clients, and partners) are in the path of the attacker due to new security needs caused by the emergence of web-based media. Attackers now assume victim identification is simple due to the social network's status as a new digital standard. In terms of danger to the safety of the authorities, it is now among the top priorities. Here are three reasons why cybercriminals can influence social media:

The scale of social media
Because social media is used by so many individuals for so many diverse purposes, an attack may easily go viral. Hackers can use trending topics, clickbait, and hashtags to spread malware that targets either everyone or a specialized group. Security personnel have a formidable physical challenge in this area.

Trusted nature of social media
Criminals take advantage of people's naiveté on social media. From time to time, individuals will accept a friend request from an unknown sender just because they share ties with them. They carelessly click on the link their pals shared, completely oblivious to the risk of a security breach. Online platforms are perfect for gaining a target's trust, as almost one-third of social media users accept friend requests from strangers.

Invisibility to security team
There are a lot of different kinds of social media, and most people throughout the world use them often. Because of limitations in their visibility, security teams are unable to keep tabs on the vast majority of employees in the social media sphere, where they are extremely vulnerable to intrusion.

STRATEGIES TO PREVENT SECURITY THREATS IN ONLINE SOCIAL NETWORKS

To protect one's privacy and data from potential dangers posed by social media sites, there are a number of things one may do. In order to mitigate security risks associated with social media platforms, it is recommended to follow these guidelines, which are based on the security issues mentioned before.

Don’t be overly social online
Sharing too much personal information on social media could have negative consequences. Some cybercriminals actively seek out people to commit identity theft by perusing their Facebook and Myspace pages. Unless you've taken the necessary precautions, it's not a good idea to make your location, address, birthday, or any other personal information public on social media. Just provide us the data we need for the task at hand. For instance, when signing up for a dating site, it's not necessary to provide the precise date of birth; simply providing your age will do.

Security and privacy setting on Social Networks
Check that your social media profile cannot be viewed by unauthorized users by adjusting the platform's privacy and security settings. Prior to making a final decision, make sure you thoroughly examine the social networking site's security and privacy settings.

Use Applications and games provided by Social Network consciously
Before you participate in a quiz, survey, poll, game, or any other program that uses your personal information, be sure you read and understand how it will be used and shared. Before you choose the game or software, be sure you're ready.

Have a strong and unique password
Strong passwords include a mix of uppercase and lowercase letters, digits, and symbols and are 8-10 characters long. Regularly change your password. Another crucial security measure is to use unique login credentials for each account. This way, even if a hacker manages to get access to one of your accounts, they won't be able to access the others. Have many e-mail accounts on various clients for these reasons, as most sites now let you use your email as a username.

Look for Secure gateways to avoid loss of credit card information
Always look for indicators of a safe and encrypted service whenever a game or other program requests money online, whether it's through a social network or not. To provide encrypted communication and secure server identification, a secure page requires an HTTPS connection, which employs SSL or TLS. To further illustrate the site's security policies and settings, browsers also show a "lock" icon. Before moving forward with a transaction, be sure you've checked for the same. Be wary of sites that imitate the lock icon and display it in the banner at the top of loaded pages; be sure the lock is on the browser window and not the page itself.

Add only people you trust to your contact list
Make sure you trust the individual making the request and that they have good intentions before you provide them access to your data. Make sure you never click on a suspicious link offered to you by a new friend on social media; instead, use a dedicated email address for establishing friends.

Get reliable Antivirus Software and keep firewall on
Phishing emails, spam, and harmful websites may all be detected and warned against by antivirus software. Worms and viruses are kept at bay by it. Trojans that secretly log your keystrokes and gather information that might be utilized to impersonate you are extremely harmful. Trojan horses typically propagate via infected websites, e-mail attachments, and faulty software. Be cautious to run an antivirus scan on the downloaded file before opening it. In addition to keeping your antivirus software up-to-date, you should always use a firewall on your computer.

Learn to Identify Phishing E-mails

Be very wary of clicking on links in emails that request personal information, passwords, or financial details. Typically, a trustworthy website would use a secure page that supports SSL to request this information rather than emailing it. Make verify the sender's email address is real before opening any attachments.

Keep your Browser updated

Keep your browser up-to-date at all times; developers release updates often to patch security issues. Make sure the browser's security settings are set to the level you like. In order to make the browser more secure, the High Security settings block features like Java Script and Active-X. If that's what you like, you're free to go with it.

Use Online Social Network Usage policy

Organizations may need to establish regulations regarding workers' use of online social networks in order to avoid any negative impact on their professional reputation. While businesses can take precautions to protect their customers' personal information by banning social media, they risk losing out on a powerful marketing and sales tool in the process. It is possible to choose a midway ground. The rules for using these websites can be found in their use policies. In the event that an employee does not adhere to the usage regulations, the policy includes punishment measures. The SANS Institute for System Administration, Networking, and Security offers a customizable policy template to meet the culture and HR requirements of any organization.

Ask yourself again

If you want to keep your personal information private on social media, the golden rule is to think about whether you would have told your friends the same thing over the phone or in person before putting anything online. We shouldn't ever publish the update if the response is no.

CONCLUSION

In today's globally interconnected society, online social networks play an essential role. The paradigm change has made it possible for social networks to interact with people every single day. Because of the meteoric rise in social media use, there is an increasing need to inform consumers about the hazards, threats, attacks, and privacy issues connected with these platforms. As a result of developments in technology, social media has developed into several distinct platforms. Connecting with one another may happen in a variety of ways. Through a plethora of professional sites, discussion forums, multimedia sharing networks, and more, netizens may achieve the pinnacle of connectivity. Unfortunately, a number of cyberattacks might be launched using social media since consumers aren't well-informed about security and privacy.

There is now no viable option for academics to implement the innovative solutions they have proposed for the issue of social media security, despite their best efforts. In light of this, it is crucial to repeatedly and regularly assess social network security vulnerabilities in order to keep up with technology. Along with taking precautions, parents should monitor their children closely when they are on OSNs.

REFERENCES

[1]. Shah, Akash & Varshney, Sapna & Mehrotra, Monica. (2024). Threats on online social network platforms: classification, detection, and prevention techniques. Multimedia Tools and Applications. 84(16). 17083-17115. 10.1007/s11042-024-19724-5.

[2]. Shah, S. Varshney, and M. Mehrotra, “Threats on online social network platforms: classification, detection, and prevention techniques,” Multimedia Tools and Applications, vol. 84, no. 16, pp. 17083–17115, 2024.

[3]. N. Nawaz, K. Ishaq, U. Farooq, A. Khalil, S. Rasheed, A. Abid, and F. Rosdi, “A comprehensive review of security threats and solutions for the online social networks industry,” PeerJ Computer Science, vol. 9, no. 1, pp. 1–36, 2023.

[4]. Shabani and I. Gashi, “Social and privacy threats in social networks, challenges and the most critical issues,” International Journal of Health Sciences, vol. 6, no. S8, pp. 5578–5586, 2022.

[5]. M. Singh, C. Verma, and P. Juneja, “Social media security threats investigation and mitigation methods: A preliminary review,” Journal of Physics: Conference Series, vol. 1706, no. 1, pp. 1–10, 2020.

[6]. Ali, Shaukat & Islam, Naveed & Rauf, Azhar & Ud Din, Ikram &Guizani, Mohsen & Rodrigues, Joel. (2018). Privacy and Security Issues in Online Social Networks. Future Internet. 10(12). 10.3390/fi10120114.

[7]. S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, “Social network security: Issues, challenges, threats, and solutions,” Information Sciences, vol. 421, no. 2, pp. 43–69, 2017.

[8]. D. Hiatt and Y. B. Choi, “Role of security in social networking,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, pp. 12–15, 2016.

[9]. Almutairi, Abeer & Hassan, M. & Al-Sharif, N. & Hemalatha, M. (2016). Security issues in social networking sites. 11(12). 7672-7675.

[10]. Kumar, Senthil & Kandasamy, Saravanakumar & K, Deepa. (2016). On Privacy and Security in Social Media – A Comprehensive Study. Procedia Computer Science. 78(2). 114-119. 10.1016/j.procs.2016.02.019.

[11]. M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: Threats and solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014.

[12]. Obiniyi, O. Oyelade, and P. Obiniyi, “Social network and security issues: Mitigating threat through reliable security model,” International Journal of Computer Applications, vol. 103, no. 9, pp. 1–7, 2014.

[13]. M. M. Joe and B. Ramakrishnan, “Enhancing security module to prevent data hacking in online social networks,” Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 2, pp. 184–191, May 2014.

[14]. M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: Threats and solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 2019–2036, 2014.

[15]. S. K. G. K. R. S. A. Kumar, “Social networking sites and their security issues,” International Journal of Scientific and Research Publications, vol. 3, no. 4, p. 5, 2013.

[16]. R. Goyal and N. R. Dholakia, “Online privacy concerns and trust in social networking sites: An empirical study of Indian consumers,” Journal of Retailing and Consumer Services, vol. 20, no. 5, pp. 441–449, 2013.

[17]. O. Al-Mushayt, “Threats and anti-threats strategies for social networking websites,” International Journal of Computer Networks & Communications, vol. 5, no. 4, pp. 53–61, 2013.

[18]. K. D. Verma and S. Khan, “Privacy and security: Online social networking,” Association of Computer Communication Education for National Triumph (ACCENT), vol. 3, no. 8, pp. 310–315, 2013.

[19]. W. Gharibi and M. Shaabi, “Cyber threats in social networking websites,” International Journal of Distributed and Parallel Systems, vol. 3, no. 1, pp. 1–8, 2012.

[20]. S. A. O. W. N. J. Shafi’i and M. Abdulhamid, “Privacy and national security issues in social networks: The challenges,” International Journal of the Computer, the Internet and Management, vol. 19, no. 3, p. 7, 2011.

[21]. Gao, Hongyu & Hu, Jun & Huang, Tuo & Wang, Jingnan& Chen, Yan. (2011). Social Network Security Security Issues in Online Social Networks. Internet Computing, IEEE. 15(4). 56 - 63. 10.1109/MIC.2011.50.

[22]. A. Hasib, “Threats of online social networks,” IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 11, pp. 288–293, 2009.

[23]. G. Hogben, “Security issues and recommendations for online social networks,” ENISA Position Paper, vol. 1, no. 1, pp. 1–36, 2007.