How to Cite:
Shabani, A., & Gashi, I. (2022). Social and privacy threats in social networks, challenges and the most critical issues. *International Journal of Health Sciences*, *6*(S8), 5578–5586. https://doi.org/10.53730/ijhs.v6nS8.13545

Social and privacy threats in social networks, challenges and the most critical issues

Amet Shabani
Colleg Biznesi, Prishtine, Kosovo
Email: ametshabani@gmail.com

Ilir Gashi
Colleg Biznesi, Prishtine, Kosovo
Corresponding author email: ilir_gashi2002@hotmail.com

***Abstract*---**Online social networks are permeating every aspect of our daily lives. With their incomparable popularity, social networks have evolved from platforms for news distribution and communication and social interaction to essential tools for online content distribution, professional networking, social recommendations, marketing, and more. Due to their heterogeneous nature and complexity, there are many technical and social challenges that need to be addressed. Specifically, security and privacy are among the most critical issues in online social networks. This paper identifies the characteristic features of social networks and the impact they have on their users. The main objective is to contribute to the discussion about privacy and security by identifying potential threats and challenges in this dimension of cyberspace.

***Keywords*---**social network, threat, privacy, architecture, security.

Introduction

Information and communication technology has evolved rapidly over the past 15-20 years, thanks to the proliferation of media and social networks. Social networks serve as tools to unite groups of people with common interests. They are enabled to interact with each other by building a community and sharing information. This consequently caused the number of users to be beyond any expectation. The sharing of personal information on popular platforms such as Facebook, Instagram, twitter has become a social trend, causing users to be more open and share more and more personal information online in front of a wide audience, without thinking about the implications of their safety. This revolutionary phase is also producing its evils by targeting the users of these

platforms to attackers who aim to access their digital identity and their data as a whole for various reasons.

Given the heterogeneous nature and the large volume of data they handle, social networks become a potential vector to be exploited by attackers, therefore a balance must be maintained between online disclosures of personal information and privacy. It is also very important that users of social networks develop technical skills and knowledge to protect their privacy online. This paper presents a systematic and in-depth study from the origins of social networks to the threats and security issues we face today. The main objective of this paper is to identify issues and challenges related to privacy and security in social networks by analysing them in different dimensions

Problem statement

The evolution to Web 2.0 and broadband Internet followed with a huge proliferation and development of social networks and user-generated content. The penetration rate of social networks is increasing every day, thanks to the continuous advancements as well as the fulfilment of user requirements. Social networks can be seen as graphs with nodes representing groups, organizations and individuals. Edges represent the relationships and interactivity between these entities. When we analyse the structure of the social network, how information spreads and the increasing role of social networks in our lives, we are convinced that it is essential to preserve privacy and improve security. [1]

According to A. Salama et al. , web 2.0 and social networks in general due to their functionality are very easy targets for attacks as they allow users to upload different types of content. Also, the heavy use of social networks also adds new threats every day. [2] The first social networks in the world such as: Six Degrees, Classmate, Live Journal, etc. were developed during the second half of the 1990s. But it can be considered that the biggest explosion of social networks occurred after 2001, as a result of an experiment in Britain where broadband Internet connection was tested for the first time, which enabled a network data transmission speed tens of times greater as well as offering a much higher level of interactivity.[3]

In parallel with other countries around the world, Kosovo was also involved in this wave of the spread of the Internet, specifically social networks. According to IPSOS, it is reported in the Media Journal that Kosovo has one of the largest internet penetration rates in the region with 86.49%. Statistically, mobile phone users exceed 96% of the population and inevitably social networks play a critical role. [4]

The use of personal information on social networks raises new privacy concerns and requires awareness of security issues. According to Ahn, Shehab and Squicciarini in general, the issue of privacy and security in social networks is associated with the identifiability and connection of information available in this social environment, its possible recipients and its possible uses.[5] Attacks can be of the most different across social networks, among them as the most frequent we

can count: Social network infrastructure attacks, malware attacks, phishing attacks, identity theft attacks, cyberbullying.[6]

We also have the analysis of Jain, Sahoo and Kaubiyal in which they divided the threats related to privacy and security into three categories: conventional threats, modern threats and targeted threats. Conventional threats include threats that users have experienced since the beginning of the social network. Modern threats are attacks that use advanced techniques to compromise user accounts and targeted attacks are attacks that target a specific user that can be carried out by any user for various personal revenges. [7]

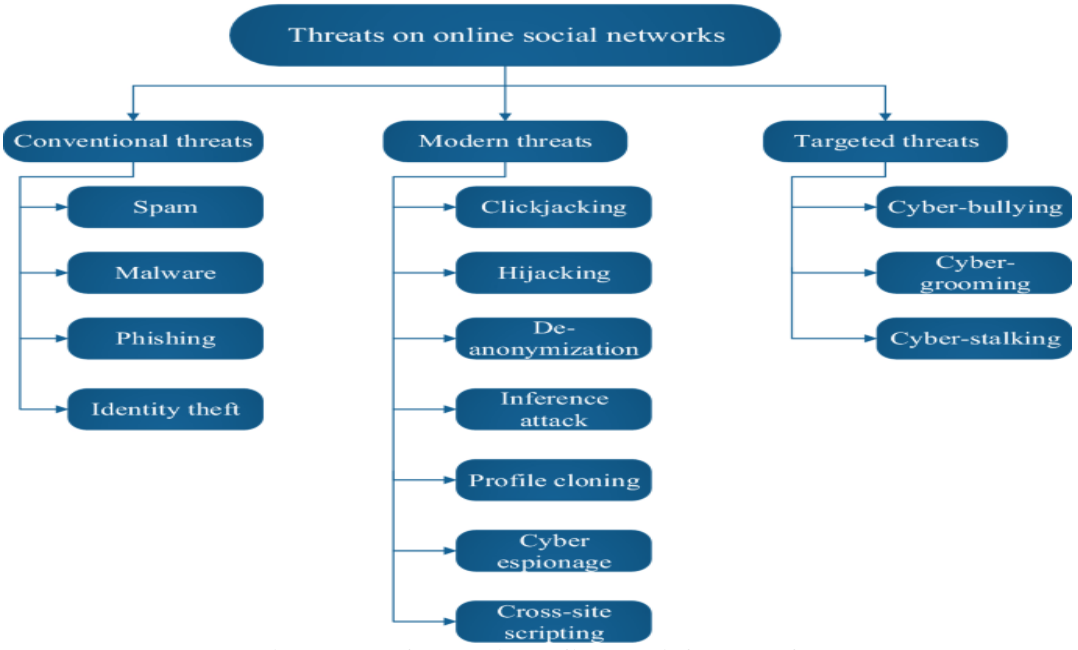

Figure 1 . Threats in online social networks

On the other hand in Barkworth et al.'s research, threats were categorized into three main groups:

- Account-based threats: Account-based threats are typically related to user authentication and access controls.
- URL-based threats: URL-based threats are caused by external sources, including posts that contain external URLs.
- Content-based threats: Content-based threats are based on shared content, eg, hate speech. [10]

Threat	Account	URL	Contents
Phishing and Social Engineering	✓	✓	
Fraud and Spam Posts	✓	✓	✓
Malware Propagation		✓	
Cross Site Scripting		✓	
Clickjacking	✓	✓	
Identity Theft	✓		
Data Leakage	✓		✓
Cyberbullying	✓		✓
Malicious links		✓	
Hate Crimes			✓
Cyberterrorist	✓	✓	✓
Revenge Porn	✓		✓
Inappropriate Contents		✓	✓

Table 1 . Classification of threats in social networks

Security and privacy threats in social network

Social networks can bring new threats to their users due to the functionality of generating a large amount of personal information from the users themselves. Various assets are prone to attack in social networks including digital identity, private information, intellectual property, financial assets, etc. In this section we analyse some of the most common attacks on social networks.

Scams

Scams are everywhere and of course even on social networks. Some of them are easily identifiable and social networks are making progress in eliminating such links. But attackers nevertheless use new approaches once an old technique of theirs is targeted and eliminated. One way is through the friends you have on social networks. This happens when you click on scam links distributed by virtual friends. A recent scam is when attackers are creating profiles using photos and information of legitimate accounts, then sending friend requests to real people, followed by posting scam articles and even sending private messages [8].

Mistakes from lack of information

Often times social networks can be quite complex when we are not informed enough. Training or information about social networks is also very important, as a result of the possible risks that can be presented for anything confidential. Participants should be informed which links they can click, who to add to their friends list. And also be informed about privacy and security settings so that features that don't need to be transparent aren't available to everyone[9].

A concrete example is the Locky ransomware case. Through it, files were encrypted where the malware code was inserted through images posted on social networks, and when users clicked on them, Locky (malware virus) was downloaded and installed on their devices. [11].

Figure 1. Safety

Hacking is one of the most popular security issues because it happens so often. This broad term includes all attempts to access information or damage a system without being authorized. While there are countless hacking tactics, social media accounts are typically accessed in one of two ways. The first method involves waiting for the user to fail after a malware has been sent to his computer. A real case is the one that happened in 2017, where the streaming service VEVO detected a massive breach of confidential data, after one of its employees fell prey to a Linkedin phishing campaign. In this way, the way was opened for hackers who undermined the LinkedIn network by presenting themselves as authentic profiles, and then seeking to connect with other users. Once the connection was accepted, the hackers had full access to the victim's account. [12]

The second method is known as psychological hacking, this involves the act of a person knowingly handing over important information to someone posing as another person. An example of this type of issue is the case of the SONY hack in 2011, causing losses of up to $171 million. Hackers were able to get into Sony's headquarters by posing as staff after they stole the computer password of one of the system administrators and then planted malware across the network. This is how passwords for very important files were discovered and stolen. [12]

Application interconnection

The convenience that social networks are offering with the possibility of connecting them to each other has created a security problem for users on the other hand. When using third-party applications, they are given the opportunity to log in through an existing account on another platform, such as Google or Facebook. If one particular account is hacked then all fall like dominoes.

We have the concrete case in 2017 with the Twitter social network, where McDonald's account was accessed in an unauthorized manner and someone posted inflammatory comments about the US president. After adequate investigations, officials found that hackers intervened by gaining access through a third-party application [12].

Clickjacking

"Clickjacking" refers to the act of hiding links behind legitimate clickable content, where through this technique the user is tricked into clicking on a different content compared to what they perceive. [15]In this way, confidential information can be disclosed or control over the user's device can be gained. And we have Facebook's version of click-jacking called Like-jacking, in which a malicious code is linked to a fake like button.

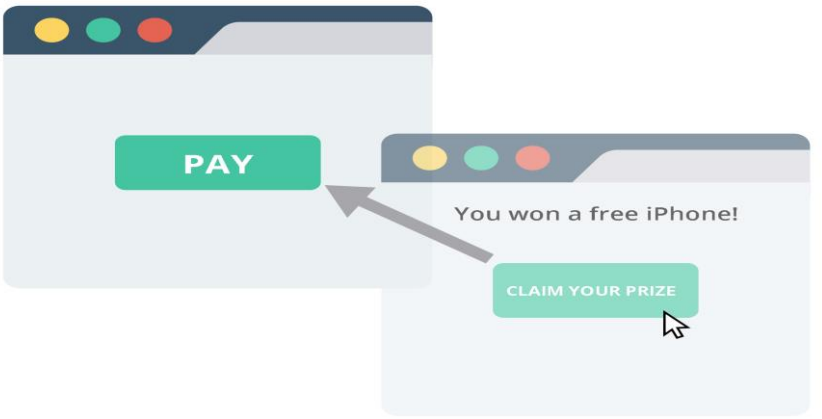

Figure 2. Clickjacking attack

Fishing

A type of social engineering that includes the act of sending a fraudulent message in order to reveal sensitive information (such as name, password, bank card details) to installing software on the user's infrastructure by masquerading as a real entity in a facebook or twitter message. Example: The social network Twitter - on this platform there were rumors that a service known as "Twitviewer" will allow users to see who is viewing their posts without following them. To access the service, the user name and password of the account had to be provided, thus the account was compromised and used for promotional messages and other purposes. [13]Also, in August 2019, a massive phishing campaign targeted Instagram users by posing as a two-factor authentication system, prompting users to log in to a fake Instagram page. [14]

Data mining

Data mining is essentially a powerful tool in the hands of researchers to uncover valuable insights from large volumes of data. Although information collected from

social networks using data mining techniques can be a useful resource to evaluate online social networks and improve the quality of services, it can also be used by attackers to extract knowledge that can endanger the privacy of users.

Botnet attacks

Social media bots are automated accounts that automatically create posts or follow new people whenever a certain term is mentioned. A large group of robots/bots can form a network known as a botnet. Bots and botnets are widespread on social networks and are used to steal data, send spam, and launch attacks that help cybercriminals gain access to people's devices and networks [14].

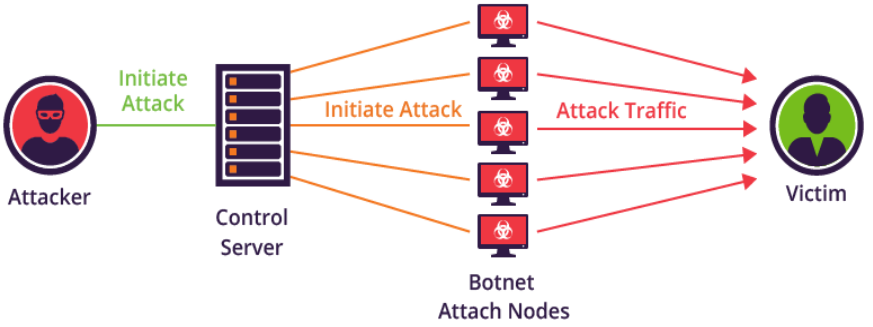

Figure 3. Botnet attack

Danger from connecting to public Wi-Fi networks

Accessing social networks through public Wi-Fi networks makes us more exposed and protecting privacy becomes more difficult across these networks. In these cases, the packets that we generate in the traffic can be decrypted and access to our sensitive data can be gained. If we cannot avoid using these public networks then protecting the traffic and therefore the privacy with a VPN comes into play. The latter encrypts all your traffic, so even if the packets are intercepted it is practically impossible to decode

Social network best practices on critical issues

The modern network is getting richer every day with services and social networks. Given all the information we generate online, our online security and privacy is at risk. Therefore, it is essential to take countermeasures to operate safely and protect privacy online.

Below are some of the best practices you can follow to be safe:

- Always configure your account privacy settings across social networks and configure data recovery security responses
- To be more secure, configure your profile settings by making the account private

- Be careful what information you are making public and regulate access to it by modifying your privacy settings accordingly
- Use unique and strong passwords that contain letters, numbers and characters. And change them from time to time to be more secure.
- Download applications from official sources
- Make sure the people you follow as friends and communicate with are known to you
- Enable two-factor security (two-factor authentication) options for email and social networks.
- Limit location sharing.
- Make sure that the pages visited contain the https authentication protocol. [16]
- Never click on suspicious ads.

Conclusion

Social networks have become an integral part of everyday life. Interaction, communication and entertainment as among the basic features of social networks are causing us to get lost in the use of platforms, without thinking carefully about the implications of privacy and security caused by the generation of content through them. The spread, the number of users as well as the diversity of social networks is increasing in parallel with the number of threats and attacks, in these circumstances it is vital that security measures increase in number, speed and complexity.

Taking everything into account, a critical role in the protection of information in social networks is directly played by users, being responsible for the content they upload to their accounts. So there is a possibility that everyone can protect themselves to some extent. Some recommendations that simulate more sustainable management are listed below:

- Be careful when clicking on links.
- Make sure you manage your privacy settings effectively.
- Turn off the GPS feature on your phone's camera to keep your exact location private.
- Change your passwords often and choose strong passwords at least eight characters long and with a combination of numbers, letters and symbols.
- Never disclose personal information to a source you do not trust or know, etc.

Although there are ways to help users improve privacy and security on social networks, we must always be aware that the Internet is open and it is very difficult to achieve complete privacy and security online.

References

1. "How Secure is Social Media Really?," DIGITAL INFORMATION WORLD, 2018. [Online]. Available: https://www.digitalinformationworld.com/2018/09/how-secure-is-social-media-really.html. [Accessed 17 May 2022].

2. "Key Social Media Privacy Issues for 2020," 2020. [Online]. Available: https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020. [Accessed May 2022].
3. "Preventing XSS with Content Security Policy," MST Solutions, 2021. [Online]. Available: https://www.mstsolutions.com/technical/preventing-xss-with-%E2%80%8Bcontent-security-policy/. [Accessed 10 May 2022].
4. "Security Weak Points: Social Media," 9 Nov. 2017. [Online]. Available: https://www.n-able.com/blog/security-weak-points-social-media. [Accessed 28 May 2022].
5. "Social Media Security Threats," December 2015. [Online]. Available: https://en.paperblog.com/social-media-security-threats-infographic-1369843/. [Accessed May 2022].
6. "Synopsys- Clickjacking," [Online]. Available: https://www.synopsys.com/glossary/what-is-clickjacking.html#:~:text=Clickjacking%20is%20an%20attack%20that,describes%20what%20is%20going%20on. [Accessed 2022].
7. "The Emerging Need for Social Media Security, KING University," 11 September 2018. [Online]. Available: https://online.king.edu/news/social-media-security/. [Accessed 2022].
8. A. Barkworth, L. McDonald, S. Khosravi, MIU Haq and AhmedAbueletta, Security and Privacy in Online Social Networks, 2021.
9. A. Hoxha, MEDIA LANDSCAPE IN KOSOVO, SEENPM, Tirana, Peace Institute, Ljubljana and Kosovo 2.0, Prishtina, 2020.
10. AK Jain, SR Sahoo and J. Kaubiyal, "Online social networks security and privacy: comprehensive review," in Complex & Intelligent Systems , 2021.
11. C. Zhang, J. Sun, X. Zhu and Y. Fang, "Privacy and Security for Online Social: Challenges and Opportunities," [Online]. Available: http://www.diit.unict.it/users/spalazzo/materiale/05510913.pdf. [Accessed 2022].
12. G.-J. Ahn, M. Shehab and A. Squicciarini, Security and Privacy in Social Networks, IEEE Internet Computing, 2011.
13. M. Salama, M. Panda, Y. Elbarawy, AE Hassanien and a. A. Abraham, Computational Social Networks: Security and Privacy, Series in Computer Communications and Networks, 2012.
14. Mr. e. K. pt D. e. Information, "PRIVACY AND SECURITY OF PERSONAL DATA," 2016. [Online]. Available: https://www.idp.al/wp-content/uploads/2017/02/Studimi_privatesia_dhe_siguria_e_te_dhenave_botim_2016.pdf. [Accessed May 2022].
15. NS Kumar, K. Saravanakumar and K. Deepa, "On Privacy and Security in Social Media – A Comprehensive Study," in International Conference on Information Security & Privacy , India, 2016.
16. Social media and their use by Albanian media, Albanian Media Institute, 2015.