IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11364

SOCIAL MEDIA SECURITY AND PRIVACY: A Complete Review and Analysis

[1]Aakash Choudhary, [2]Navdeep Kandpal, [3]Niraj Gusain, [4]Pranshu Singh and

[5]Dr. Urvashi Chugh

[1, 2,3,4,5]Computer Science and Engineering, Inderprastha Engineering College, Ghaziabad

Abstract: With rapidly growing technology social media has now become a part of everyone’s daily life. From sharing the data like our personal information, text and many other things. We have also started sharing news articles and related pictures on social media platforms, different advertisements, marketing techniques, surveys, jokes, videos in the Entertainment domain. It provides a platform for users to connect with their family, friends, and other people globally. The information shared in social networks spread so fast, that makes it very comfortable for attackers to get access to the user’s information. While enjoying the content available on Social Media, secrecy and privacy of Social media need to be maintained from various possible areas. There are various security and privacy issues when a user shares his information like uploading personal data such as photos, videos, and audio. The information that is to be kept confidential, must be made private.

To resolve these problems, we are writing this paper which reflects a thorough review of different security and privacy threats and the possible solutions that can be proved beneficial in providing full-fledged security to social network users. In addition to this, we have also discussed some other defensive approaches to Social media security.

I. INTRODUCTION

a. SOCIAL MEDIA SECURITY

An organization's brand and advertising are becoming increasingly reliant on social media. To carry out attacks, attackers take advantage of the inherent trust and public nature of these platforms. On social media, protecting brands, executives, workers, and customers is vital for the modern business topic.

- **Cyberstalking**

There has always been the existence of stalking and harassment over social media, but with the advancement of technology, it has become easier for attackers who try to get access to people’s accounts. These kinds of activities that are not appropriate and undesirable lead to discomfort and sadness and worst can affect a person’s mental health.

They can either be strangers or known people and they can have different goals which cannot be noticed by common people. The more determination or obsession of an attacker, the more chances of changing the platform from one account to another until he /she gets complete control over your account. They usually try to steal your information from your online personal details, financial affairs, personal relationships, private life and the location that you entered.

- **Identity Theft**

Identity theft, also known as identity fraud, is a crime in which an attacker obtains personally identifiable information (PII), such as Social Security or driver's license numbers, to imitate other identities.

The two categories of identity theft are:

1. **True-name identity theft**:

It means the attacker uses PII to open new accounts. The attacker might open a new credit card account, build a mobile phone service or open a new checking account to obtain blank checks.

2. **Account-takeover identity theft**:

It is when the attacker uses PII to get access to the person's existing accounts. He can change the mailing address on an account and run up a bill before the victim realizes there is a problem.

b. Active Users' Favorite Top Social Media Sites and Apps

The below graph depicts the different social networking sites and apps and the total number of people accessing them.

DOI: 10.17148/IJARCCE.2022.11364

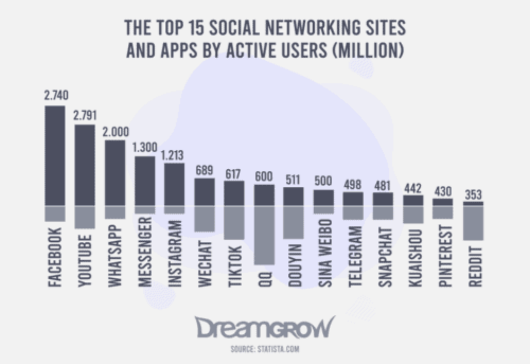

Fig. 3-1: Active users (in millions) per social networking site.[6]

1. Facebook

It is used by 2.74 Billion Active users and has been proved to be the best social media app.

2. YouTube

It has been used by 2.291 Billion Active Users and is the second most popular social media app.

3. WhatsApp

It has been used by 2.0 Billion+ Active Users. It was founded in 2009. The initial thinking behind the idea wasn't to be an instant messaging network at first, but rather to just display "statuses" next to each user's name.

4. Facebook Messenger

It has been used by 1.3 Billion Active Users. It talks more about the power of Facebook that service with their main platform reached the number four spot on this prestigious list.

5. Instagram

It has been used by 1.221 Billion Active Users. It is the world's most popular photo-sharing app which comes at number 5.

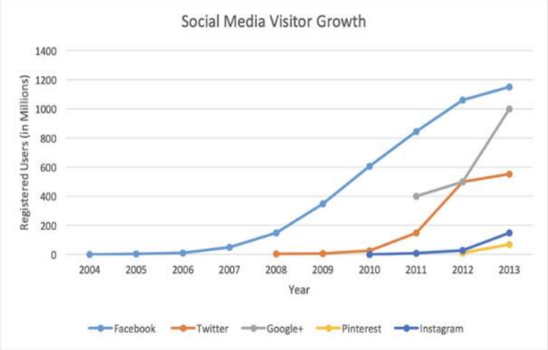

Fig. 3-2: Social media visitor growth (User in millions vs year).[7]

II. METHODOLOGY: SOME PREVENTION TECHNIQUES

a. Authentication Mechanism:

Several OSNs employ authentication techniques such as CAPTCHA, multi-factor authentication, and photos-of-friend identification to ensure that only a viable user is logged-in or enrolled in a social network and not a socialbot. There are many modern ways and one of them is to use 2-way Authentication principle, where initially password and then a code is verified to log-in user. This reduces the danger of an account being hacked and prevents a genuine account from being hijacked and bad information being posted.

b. Profile Security and Privacy Settings:

Some social media additionally provides customizable privacy and security settings, which can be altered as per the user choices and enables the customer to protect their personal data from unwanted access by other parties or apps. For Example, In Meta applications or platforms clients may change their security settings and choose who in the network can view their personal information, photos, posts, and other sensitive data.

DOI: 10.17148/IJARCCE.2022.11364

c. Phishing Detection:

The amount of questionable e-mails submitted to the security staff is one metric for phishing detection. This metric is used to determine how many employees followed the correct protocol for reporting questionable communications. As phishing assaults become increasingly common in online social networking sites, researchers have proposed specific solutions for phishing attacks in social networking environments. As an example, Aggarwal et al. put up the PhishAri technique for real-time identification of phishing attacks occurring on Twitter. It used Twitter data such as the number of followers and account age to determine if a tweet was phishing or not [16].

d. Fake Profile Detection:

In Ref. [17], the author proposes one methodology for identifying fraudulent accounts and profiles. They collected some user profile material from the LinkedIn site and processed it to extract various attributes. Following the main component preprocessing of profiles, a training set is formed in a neural network using the robust backpropagation technique. For profile characterization, Support Vector Machines (SVMs) are used. In Ref. [18], the author suggested an adaptive multilayered-based machine learning technique for detecting botnets. The suggested study developed a decision tree-based bot detection system for detecting P2P botnets.

III. RESULTS

a. Threats and Privacy Concerns in Social Networking Sites

There are certain possible advantages and disadvantages of using social media networks.

1. Initially it seems to provide full fledge security to the users but they keep us in dark by making us uninformed about the demerits of their apps.
2. It was discovered that if personal information is not used appropriately, privacy may be compromised in a variety of ways.
3. It has been estimated that privacy intrusion can likely happen as optional utilization where information or data gathered for one design is utilized to meet different purposes.

4. Nevertheless, if the appropriate steps and practices are taken by people with control over the revelation of their data, protection concerns can be intervened.

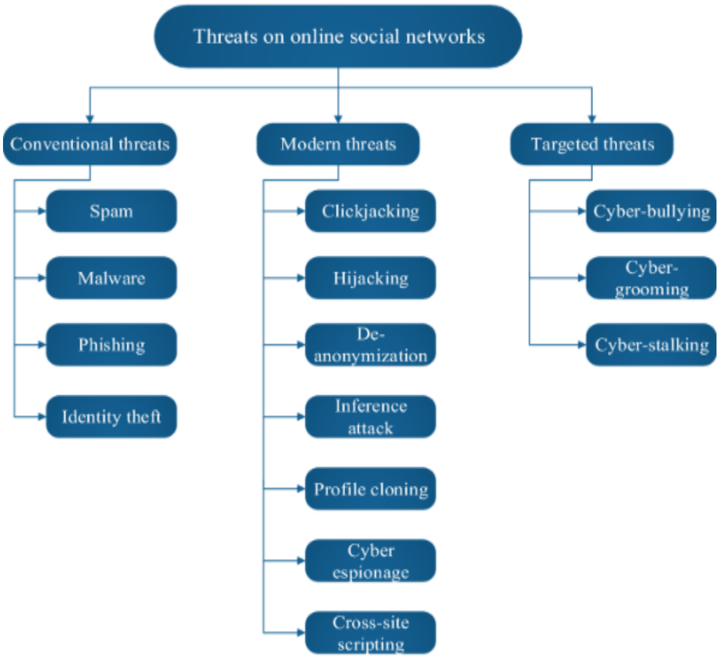

Fig. 4-1: Types of threats.[2]

b. Efficacious Effects of Social Media on Society:

There are a number of advantages to using social media:

1. Making Friends on Social Media is Easier

The rise of smartphones helped change this, connecting people in a new way, but then social media bring up and the whole idea of friendship changed again.

DOI: 10.17148/IJARCCE.2022.11364

2. Social Media Makes it Possible to Communicate Quickly

Our time is being squeezed by work and family duties to the point of weariness. But social networking sites offer a chance to communicate speedily and efficiently.

3. Social Media Shrinks the World

Now it isn't just your inner circle of close friends and even closer family members that social networking sites allow you to communicate with easily and effectively.

4. Relationships are Easier to Form with Social Media

There is no doubt that having social networking in our lives can lead to relationships breaking up.

5. Social Media Helps News Travel Faster

New lines of communication have opened the world up in a big way. No more so than when it comes to news, which can make its way around the world and back again with seconds.

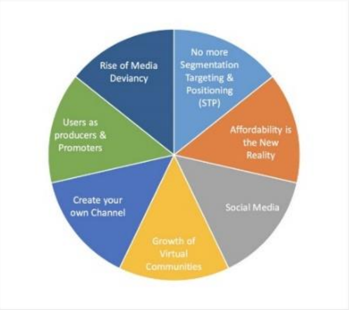

Fig. 4-2: Social Media Impact on Marketing.[7]

IV. Discussion

There are a few social networking safety precautions that you should constantly remember:

1. Manage your privacy settings - They help you control who sees what you post and manage your online experience positively.
2. Keep personal info personal. - The more information you provide, the easier it will be for someone to steal your identity, gain access to your data, or perform other crimes like stalking.
3. Protect your computer- Install Antivirus software. Maintain the most recent versions of your operating system, web browser, and other applications.
4. Use strong passwords. Make sure your password is at least eight characters long and has a unique mix of letters, numbers, and special characters (such as +, @, #, or $). [10]
5. Practice good account hygiene – We should be careful while linking our emails to social media. This will help minimize the risk of attackers gaining access to a user's account through compromised social media account credentials.

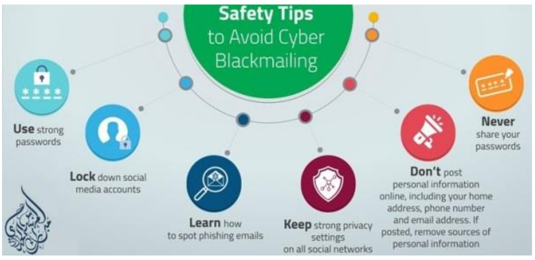
Safety Tips to Avoid Cyber Blackmailing
Use strong passwords
Lock down social media accounts
Learn how to spot phishing emails
Keep strong privacy settings on all social networks
Don't post personal information online, including your home address, phone number and email address. If posted, remove sources of personal information
Never share your passwords

Fig. 5-1: Safety tips to Avoid Cyber Blackmailing.[13]

V. CONCLUSION

It has been observed that privacy concerns are very sensitive in the social networking sites and the users attempt to make adequate changes on their social media privacy is lower than other modes of security operations. We had discussed the causes of the glitches and formulated the changes to take over the privacy concerns. If we would go for implementing a set of policies for social media, like, a strong password, awareness of changing passwords often, awareness of information disclosure, the purpose of antivirus or related software, and proprietary software etc., we'd protect social media networks against new threats and weaknesses.

DOI: 10.17148/IJARCCE.2022.11364

As we know different functions and features make some applications more appropriate for one brand than another. At the same time, different legacies and cultures also attract audiences of particular areas.

VI. REFERENCES

[1]. https://www.sciencedirect.com/science/article/pii/S1877050916000211
[2]. https://link.springer.com/article/10.1007/s40747-021-00409-7
[3]. https://www.researchgate.net/publication/301234158_On_Privacy_and_Security_in_Social_Media_-_A_Comprehensive_Study
[4]. https://www.zerofox.com/social-media-security/
[5]. https://www.getsafeonline.org/personal/articles/cyberstalking/
[6]. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/
[7]. https://www.jagsheth.com/marketing-theory/how-social-media-will-impact-marketing-media/
[8]. https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html
[9]. https://www.makeuseof.com/tag/positive-impact-social-networking-sites-society-opinion/
[10]. https://www.technology.pitt.edu/security/best-practices-safe-social-networking
[11]. https://www.trendmicro.com/en_us/research/21/f/best-practices-for-social-media-security.html
[12]. https://www.techtarget.com/searchsecurity/definition/identity-theft
[13]. https://www.mubarak.om/social-media-protection-checklist/
[14]. https://www.researchgate.net/publication/301234158_On_Privacy_and_Security_in_Social_Media_-_A_Comprehensive_Study
[15]. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/
[16]. Aggarwal A, Rajadesingan A, Kumaraguru P (2012) PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime pp 1–12.
[17]. Ramalingam D, Chinnaiah V (2018) Fake profile detection techniques in large-scale online social networks: a comprehensive review. Comput Electr Eng 65(3):165–177.
[18]. Khan RU, Zhang X, Kumar R, Sharif A, Golilarz NA, Alazab M (2019) An adaptive multi-layer botnet detection technique using machine learning classifiers. Appl Sci 9(11):2375