**Cyber attacks in Social Media -A Review**

B S Panda\*

Dept. of CSE, Raghu Engineering College, Visakhapatnam, AP, India.

E-mail: bspanda.cse@gmail.com

**Abstract:** All through the phase of reconnaissance a social media or phishing operation, attackers regularly use social media groups. Social media can offer attackers with a stage to pose as well-known individuals and companies, over and above the data they need to conduct additional assaults like social media and phishing. Social engineering, site compromise, data theft or breach, brand idea and malware bug are further threats. These threats consist of various phases of data collection on individuals for extortion or holding them at ransom. Don't share too much personal information online. Alter your privacy settings and avoid using location services. Update your operating system and software programs. Use capital and lowercase letters, numbers, and special characters to create secure passwords. A firewall regulates the flow of incoming and outgoing network traffic to guard against malicious attacks and un-trusted networks. One of the most important cyber security solutions in any computer network is antivirus and anti-malware software.

**Key words:** Cyber Attacks, Social Media, Privacy, Malware, Hacker, Security.

1. **INTRODUCTION**

Internet serves as a hub for information exchange in the field of information technology. Social networks form a sizable and significant portion of so-called Web 2.0. This platform sees itself as a helpful tool for connecting with loved ones. Even when people are geographically separated, it is a cheap and useful tool for keeping in touch. A social network is, to put it simply, a network of connected individuals who have a shared interest and who may communicate with one another or share information via the services. In recent days social networking is a fantastic method to connect with people today.

In order to construct the cyber-communications required for the public to continue to exist in its fundamental nature in a cyber-communication world, social cyber security is an rising scientific area paying attention on the social media to understand, characterize and forecast cyber-communicated changes in human behavior, political, social and cultural outcomes.

Unfortunately, the platforms of social media can provide a number of major security threats and hazards to users. This chapter goes into detail about social media threats, security issues, and various attack types.

1. **CUBER THREATS IN SOCIAL MEDIA**

* Social Networking Malicious code can occasionally be introduced directly into a social networking site by hackers, including through third-party apps and adverts. Shortened URLs, which are common on Twitter, can be exploited to deceive users into accessing malicious websites that are able to steal their personal information. Due to how simple it is to retweet a message, which might finally be seen by many people, Twitter is particularly vulnerable to this technique.
* Impersonation on Twitter, several impersonators has amassed tens of thousands of followers before embarrassing or even outright humiliating the targets of their impersonations. Now, Twitter will take action against impersonators who try to defame their targets, but only in their exclusive discretion.
* Social media has been something like since before there were network of computers, and it is a favorite of slick-talking con artists everywhere. However, the growth of the Internet made it simpler for con artists and scammers to identify possible victims. Social media has increased this threat because of two factors social networking platforms encourage a dangerous amount of presumed confidence, and many people are eager than ever to divulge private information regarding themselves. The next stage is to inform your friend about your company's undisclosed project; if you merely give him the password to a file on your corporate network, he might be able to assist you with that project.



Fig1. Cyber threats in Social Media

* Applications for Mobile Inextricably related to the advanced mobile computing, which has agreed to rise a sizable business in mobile development application, is the advent of social media. People frequently download dozens of applications, as is only natural. People occasionally download more than they anticipated. Google removed more than 80 fraudulent applications from the Android Market at the beginning of March. Some of the malware was created to steal users' personal information, spread itself to other devices, delete user data, or even pretend to be the device holder.
* Progressive Advanced Threats the collecting of intelligence about persons of concern is individual of the fundamental components of “advanced persistent threats” (APT), and social networks can be a goldmine for this information. APT perpetrators utilize this information to advance their attacks, gathering more intelligence before getting access to vulnerable systems to install malware, trojans, and other malicious software.
* Trust nearly all of these risks have one thing in common: consumers place a great deal of faith in these social media platforms. People believe links, photographs, movies, and implemented when they approach from "friends," at least until they are tricked a small times, just like when email first became popular or when instant messaging became common place. Social media applications have not yet succeeded in duping enough users. The variation with social media networks is that their exclusive function is knowledge sharing, which will lead to higher price increases.
* False Cross-Site Requests (CSRF) CSRF attacks take advantage of the trust that a social media application places in a logged-in user's browser, while they aren't a specific form of threat per se; rather, they are further like a method used to spread an advanced social networking worm. Therefore, it is simple for an attack to "share" an image in a user's event stream that other users may click on to capture or spread the assault as long as the social network program isn't inspecting the referrer header.



Fig2. Security Threats in Social Media

1. **SOCIAL MEDIA ATTACKS**

**Social Engineering**

Cybercriminals carry out this kind of attack by manipulating people's minds. Through social engineering, people who aren't paying attention are persuaded to share sensitive or private information via email, social media, or other avenues of communication. The victim is frequently persuaded by the communications to divulge private information, open a malicious file, or click a harmful link by invoking urgency, fear, or other comparable feelings or interests. Due to social media's widespread use, attackers may easily find out everything they need to know about their intended victim, which makes it simpler for them to craft attack-related emails that appear authentic.

**Malicious Links and Content**

Cybercriminals typically employ harmful links instead of posting malicious content directly to social media platforms to trick a victim into clicking through to data that is hosted on third-party websites. When clicked, exploits can be disseminated on social media and exploited to take over accounts. The hijacking of the Live.com sub domain of Microsoft, which was discovered last year, serves as an example of this kind of attack.

**Fake Profile**

The methods used by cybercriminals are becoming increasingly sophisticated. They can clone a real social media profile using a false one, carrying out both small- and large-scale attacks. False profiles can be used to replicate the online personas of real prominent figures and spread phishing or malware to their followers or contacts.

Cyber attackers can also use wrong profiles to mimic the actual social media profiles of important figures within a target corporation or business. These cybercriminals, for instance, can carry out cat fishing attacks and request private or sensitive information about the company using a wrong CEO profile. Additionally, they have the power to direct an employee to take a course of action that might compromise someone's safety or interrupt normal business operations. A person named Spas Vasilev, who exploited the fictitious identity of Alexander Nikolov to defraud individuals, is one example of this type of social media attack.

**Compromised Profile**

The aim of this kind of assault is most likely verified social media profiles. Customers of a brand might be exposed to malicious content through a compromised profile. This attack, which resembles brand hijacking, can be extremely harmful because it may have a negative effect on a company's website.

Target, a major retailer, was the target of a hacked profile assault in 2018. Scammers solicited customers to send Bit coin to participate in a fraudulent contest using the brand's verified Twitter account.

**Reconnaissance**

Today's social media users are more willing to provide intimate information about themselves, making them prime candidates for a reconnaissance attack. Users' profiles, relationships, actions, hobbies, and other information can be gathered and analyzed by cyber attackers or threat actors, who can then use that data to create appealing messages and other baits.

Social media can be used passively for a reconnaissance attack, which is challenging to identify. Users are unaware that threat actors are already using their personal data to log in to or access other services or accounts, such online banking. In order to reduce the intelligence value of your personal information to possible cyber attackers, it is ideal if you restrict the quantity of personal information you disclose publicly on social media.

Cybercriminals love social media, and businesses shouldn't ignore this fact. By defending against these attacks on your social media accounts, you are also defending your clients and your company. Give social media the same priority as you would any other platform or channel you use.

Inform your staff about these frequent attacks, especially the group in charge of your social media groups. To strengthen your cyber security defenses, create a strong social media and digital brand protection strategy, and identify the finest cyber threat intelligence solutions for your company.

1. **PHASES OF CYBER ATTACKS**

Survey

Initial Development

Establish Resolution

Install Tools

Move Across

Gather, Use

& Exploit

Fig3. Phases of Cyber attacks

**Protect Privacy in Online**

* Keep your software up to date.
* Frequently take back-ups
* Save to Sharing information Less Online.
* When not using log out from the services.
* Clean Unused Mobile Apps and Browser Extensions.
* Beware phishing attacks.
* Use Unique and typical Passwords and Two-Factor Authentication (No SMS)
* Privacy Settings for Your Online Accounts should be Tighten.
* Block Search Engines from Tracking You.
* Browse Online With a Secure VPN.

1. **Conclusion**

Social media networks have been compromised by cybercrime as a result of rising usage and user numbers. Hackers hunt for ways to access users' accounts, personal information, or financial data, frequently through clicking on doubtful links or downloading dubious software. Cyber security breaches can result in identity theft and extortion attempts on an individual level, which can seriously harm that person's life. Everybody depends on the security of their data and personal information. Many businesses create software for data protection. The data is shielded by this software. Cyber security is crucial since it protects not only our systems from virus attacks but also helps to secure information.

Researchers from all over the world have up till now offered a variety of techniques to stop cyber attacks or lessen the harm they inflict. Some of the methods are now being used, while others are still being studied. This study's objectives are to examine the issues and conduct a thorough analysis of the standard advancements in cyber security in social media that has been made.

**References**

1. D. Rosenblum. What anyone can know, (2007) “The privacy risks of social networking sites”, IEEE Security and Privacy, pages 40–49.
2. Won Kim, Ok-Ran Jeong, Sang-Won Lee, (2010) "On Social Websites" , Information Systems pages 215-236.
3. Anchises M. G. de Paula, (2010) “Security Aspects and Future Trends of Social Networks", IJoFCS, 1, pp 60-79.
4. Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho, Jayme Tadeu Machado, (2010) “A Security Framework to Protect Against Social Networks Services Threats”, Fifth International Conference on Systems and Networks Communications.
5. Abdullah Al Hasib, (2009) “Threats of Online Social Networks", IJCSNS, Vol. 9, No 11.
6. W. He, (2013) "A survey of security risks of mobile social media through blog mining and an extensive literature search", *Inf. Manage. Comput. Secur.*, vol. 21, no. 2, pp. 381.
7. Quigley K., Burns C., Stallard K. (2015) ‘Cyber Gurus’: “A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection Gov.” Inf. Q., 32 (2), pp. 108-117.
8. Robinson M., Jones K., Janicke H. (2015) Cyber warfare: Issues and challenges Comput. Secur. 49, pp. 70-94.
9. Thomson J.R. (2015) “Cyber security, cyber-attack and cyber-espionage Thomson J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries”, Butterworth-Heinemann, Boston, pp. 45-53.
10. Zhao J., et al. (2020) TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data Comput. Secur., 95.
11. Tosun O.K. (2021) “Cyber-attacks and stock market activity”, Int. Rev. Financ. Anal.,76.
12. [Varga et al.,](https://www.sciencedirect.com/science/article/pii/S2352484721007289#bb73) Varga S., Brynielsson J., Franke U. (2021) “Cyber-threat perception and risk management in the Swedish financial sector” Comput. Secur. 105.