CYBER ATTACKS IN SOCIAL MEDIA -A REVIEW

Abstract

All through the phase of reconnaissance a social media or phishing operation, attackers regularly use social media groups. In recent the social media may offer attackers with a stage to pose as well-known persons and companies, over and above the data they need to conduct extra assaults such as 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. Change your privacy settings and avoid using location services. Update your operating system and software programs. Make use of 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 useful and important cyber security solutions in any computer network is antivirus and anti-malware software.

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

Author

Dr. B S Panda
Department of CSE,
Raghu Engineering College,
Visakhapatnam, Andra Pradesh, India.

I. INTRODUCTION

The internet acts as a centre for the exchange of information in the field of information technology. A substantial and sizeable element of so-called social network is 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. CYBER 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 from the time when 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.
- Mobile application software the emergence of social media is inextricably linked to enhance mobile computing, which has agreed to grow a substantial company in mobile development applications. It's only natural that people regularly download dozens of applications. Sometimes people download more than they intended. At the start of May, Google deleted more than 80 bogus apps from the Android Market. Some malware was developed to propagate to other devices, destroy user data, or even pretend to be the device owner while stealing users' personal information.

- 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 increase an advanced social networking issue. 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 more as the social network program isn't inspecting the referrer header.

Figure 1: Cyber threats in Social Media

II. DEAL WITH CYBER THREATS

Here are some common ones and suggestions on how to handle them without necessarily changing the operating system:

1. **Phishing Attacks:** Phishing involves tricking users into revealing their sensitive information, such as login credentials or personal details. To handle phishing attacks:
   - Be cautious of unsolicited emails, messages, or links asking for personal information.
   - Verify the legitimacy of the source before clicking on any links or providing sensitive information.
   - Double-check the URL of the social media platform to ensure it is legitimate before logging in.

2. **Account Takeover:** In an account takeover, attackers gain unauthorized access to a user's social media account. To handle this type of attack:
   - Enable two-factor authentication (2FA) for the social media account, if available, to add an extra layer of security.
   - Regularly monitor account activity for any suspicious behavior or unauthorized access.
   - Change passwords frequently and use strong, unique passwords for each social media account.

3. **Malware Infections:** Malware can infect a user's device through malicious links or downloads, potentially compromising their social media accounts. To handle malware infections:
   - Install and regularly update a reputable antivirus or anti-malware software on the device.
   - Avoid clicking on suspicious links or downloading files from untrusted sources.
   - Scan the device for malware regularly and remove any detected threats.

4. **Impersonation and Fake Accounts:** Attackers may create fake social media accounts to impersonate someone else or deceive users. To handle impersonation and fake accounts:
   - Report any suspicious or fake accounts to the social media platform.
   - Share awareness with friends and followers about the existence of fake accounts.
   - Avoid interacting with or sharing personal information with unverified or suspicious accounts.

5. **Privacy and Data Breaches:** Privacy breaches can occur when personal information is exposed or compromised on social media. To handle privacy and data breaches:
   - Regularly review and update privacy settings on social media platforms.
   - Limit the amount of personal information shared publicly.
   - Be cautious of sharing sensitive or personal details in public posts or messages.

6. **Cyberbullying and Harassment:** Social media platforms are sometimes used for cyberbullying and harassment. To handle these situations:
   - Report and block individuals engaging in abusive or harassing behavior.
   - Document evidence of harassment, such as screenshots, for reporting purposes.
   - Seek support from trusted friends, family, or helpline resources for assistance.

Handling these attacks primarily involves being vigilant, practicing good security habits, and understanding the risks associated with social media usage. While the operating system itself may not be the primary factor in preventing these attacks, maintaining a secure and updated operating system can contribute to overall device security.

III. SOCIAL MEDIA ATTACKS

1. **Social Engineering:** Cybercriminals use mind control to carry out this type of attack. Social engineering is the practice of getting unobservant individuals to divulge private or sensitive information via email, social media, or other channels of contact. The messages usually use urgency, fear, or other similar emotions or interests to induce the victim to reveal personal information, open a malicious file, or click a hazardous link. Attackers can readily learn all they need to know about their intended victim because to social media's broad use, which makes it easier for them to create attack-related emails that seem genuine.

2. **Malicious Links and Content:** Instead of submitting malicious content directly to social media networks, cybercriminals usually use hazardous links to lure a victim into clicking during to data that is hosted on intermediary websites. Exploits can be shared on social media and used to hijack accounts when they are clicked. This type of assault is exemplified by the hijacking of Microsoft's Live.com sub domain, which was detected last year.

3. **Fake Profile:** Cybercriminals are using increasingly sophisticated techniques. They can conduct both small- and large-scale attacks by employing a phony social media profile to copy a real one. In order to distribute phishing or malware to their followers or contacts, false accounts can be developed to mimic the online personas of real well-known people.

   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.

4. **Compromised Profile:** This type of attack most likely targets verified social media profiles. Through a compromised profile, customers of a brand might be exposed to dangerous content. This attack, which mimics brand hijacking, may have a negative impact on a company's website, making it potentially very destructive.

   In 2020, a hacker attack using a fake profile was aimed at large store Target. Using the company's verified Twitter account, scammers asked customers to pay Bit coin to take part in a fake competition.

5. **Reconnaissance:** Social media users in today's world are more likely to be willing to provide personal information about them, making them excellent targets for a reconnaissance attack. Cyber attackers or threat actors may gather and analyze user profiles, relationships, behaviors, hobbies, and other information with the goal of using that information to craft enticing messages and other types of bait.

   It can be difficult to spot a passive reconnaissance attack that uses social media. Users are unaware that threat actors are already logging into or accessing other services or accounts, including online banking, using their personal information. It is best if you limit the amount of personal information you post publicly on social media in order to lower the intelligence worth of your data to potential cyber attackers.

   Social media is a favorite tool of cybercriminals, thus businesses shouldn't overlook this fact. You are defending your customers and your business by thwarting these attacks on your social media accounts. Place social media on par with any other channel or platform you use in terms of importance.

   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.

IV. PHASES OF CYBER ATTACKS

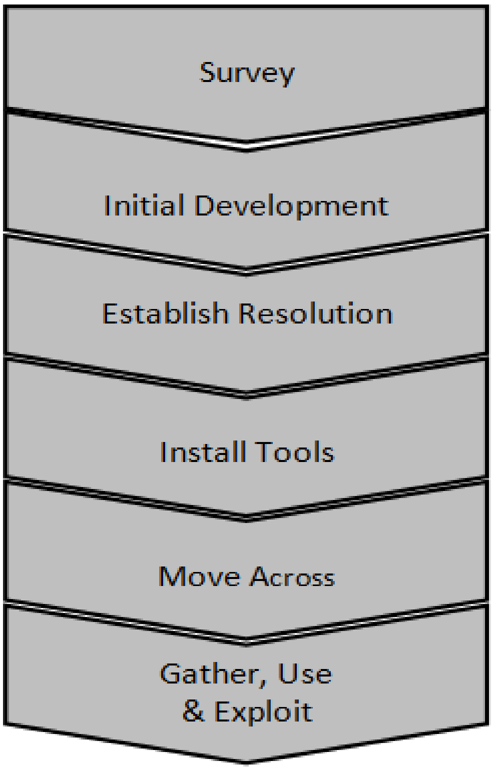

Figure 2: Phases of Cyber attacks

1. 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)
- Settings for privacy of your online accounts should be tightening.
- Block Search Engines from Tracking You.
- Using with secure VPN to Browse Online.

If social media users are still experiencing attacks despite following the suggested security measures, here are some additional steps they can take to enhance their online safety:

- **Strengthen Passwords:** Encourage users to create strong, unique passwords for their social media accounts. Passwords should be long, include a combination of letters, numbers, and special characters, and avoid easily guessable information such as birthdays or names.
- **Enable Two-Factor Authentication (2FA):** Advice users to enable 2FA whenever possible. This adds an extra layer of security by requiring users to provide a second verification factor, such as a temporary code sent to their mobile device, in addition to their password.
- **Be Cautious with Third-Party Apps:** Remind users to be cautious when granting access to third-party applications or services. Unauthorized or malicious apps may gain access to personal information or even hijack accounts. Users should review and revoke access for any apps they no longer use or trust.
- **Regularly Update Privacy Settings:** Encourage users to review and update their privacy settings on social media platforms. They should customize their privacy preferences to control who can see their posts, photos, and personal information. Regularly check for any changes or updates made by the platform that may affect privacy settings.
- **Avoid Suspicious Links and Attachments:** Remind users to exercise caution when clicking on links or opening attachments, even if they appear to come from trusted sources or friends. These may be phishing attempts or contain malware. They should verify the legitimacy of the source before interacting with such content.
- **Educate about Social Engineering:** Inform users about social engineering tactics commonly used by attackers, such as phishing emails, impersonation, or fake customer support calls. Encourage them to be skeptical of unsolicited messages or requests for personal information.
- **Monitor Account Activity:** Users should regularly monitor their social media account activity for any suspicious behavior. They should be aware of unfamiliar logins, unexpected posts, or changes in their account settings. If any suspicious activity is detected, they should report it to the social media platform and take appropriate actions to secure their account.
- **Stay Informed about Security Updates:** Encourage users to stay updated on the latest security news and advisories related to the social media platforms they use.

Following official blogs or social media accounts of the platforms can provide insights into security updates, vulnerabilities, and recommended actions.

- **Report and Block Abusive Users:** Instruct users to report and block any abusive or harassing individuals they encounter on social media. Platforms often have reporting mechanisms in place to address such issues. Encourage users to be proactive in protecting themselves and others by reporting inappropriate behavior.
- **Regularly Backup Important Data:** Emphasize the importance of regularly backing up important data such as photos, messages, or contacts from social media accounts. This ensures that even if an account is compromised or inaccessible, valuable information is not lost.

By implementing these additional steps, social media users can enhance their security posture and reduce the risk of encountering attacks. However, it's important to remember that no security measure is foolproof, and users should remain vigilant and adaptable to emerging threats.

V. CONCLUSION

Social media networks have been compromised by cybercrime as a result of rising usage and user numbers. Hackers track for ways to access users' accounts, personal information, or financial data, frequently through clicking on doubtful links or downloading dubious software. On a personal level, cyber security breaches can lead to identity theft and extortion attempts, which can gravely impact that person's life. Everyone is reliant on the privacy and security of their data. Many companies produce data protection software. This software protects the data. Cyber security is essential since it helps to secure data while also defending our systems from viral attacks.

Up until now, researchers from all around the world have proposed a range of methods to thwart cyber attacks or decrease the damage they cause. While some of the techniques are currently in use, others are still being researched. 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., Varga S., Brynielsson J., Franke U. (2021) “Cyber-threat perception and risk management in the Swedish financial sector” Comput. Secur. 105.