International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 11 Issue 10 October. 2022 || PP. 118-120

Cybersecurity for Social Networking Sites Issues, Challenges, and Solutions

Dr. Kavita Purohit
Assistant professor in EAFM ,
Vishwa Bharti P.G. College , Sikar

The main purpose of social networking sites is to connect people and organizations. It has also developed many business opportunities for companies and firms. Social media has introduced significant changes in the way people communicate. Social networking sites bring out a specific concern related to the privacy and security of the user. The security and privacy of these sites mainly focuses on malware detection as it appears to come from a trusted contact, users are more likely to click on the link. The social networking sites have formed applications in many areas like-

If you want to Gain In-depth Knowledge on Cyber Security, please go through this link Cyber Security Online Training

Social e-commerce: social networking sites can be used for promotions and advertisements for e-commerce portal owners.

Branding: The social media provides a better platform for companies to attract customers for more business opportunities.

A. Issues

As the growth of social networking sites has brought various benefits it also has brought various security concerns. It also provides a

vulnerable platform to be exploited by the attackers. Some issues associated are as follows.

1) Misusing Identity: The attacker impersonates the identity of any user results in misusing identity. The attackers attack through the applications in which they ask for granting permission for accessing the information provided in Social Networking Sites.

When a user allows doing so, they will gain access to all the information and that information can be misused without the knowledge of the user.

2) Threats from using 3rd Party Applications: These applications seek permission from the user to access personal information for all the various games and apps. The user grants the app a certain level of permission concerning the user's information. And some of these applications which are playing at the foreground may download a malware on the user's computer or phone without their consent.

3) Trusting Social Networking Sites Operators: The contents that user uploads or posts on social networking sites, the information is available with the networking operators. The operators can save account data even after deletion.

Top 10 Operating Systems for Ethical Hackers and Penetration Testers (2020 List)

A hacker is a highly skilled computer operator who uses bugs and exploits to break into computer systems and networks…

medium.com

4) Viruses, Phishing Attacks and Malwares: Viruses and malware often find their way onto your computer through those annoying ads. After gaining access to the network, the attacker can access or steal confidential data by spreading spam mails.

5) Legal Issues: Posting contents that are offensive to any individual or community or country. There are legal risks associated with the use of social networking sites like leaking confidential information on sites or invading someone's privacy.

6) Tracking Users: It can cause physical security concerns for the user, as the third parties may access the roaming information of the user by collecting the real-time update on the user's location.

7) Privacy of Data: Users share their information on social networking sites and can cause privacy braches unless proper security measures are applied. For example, everyone can see the information of a user if the user's default setting is 'public'. More Info At Ethical Hacking Online Training

Accepting requests from unknown people can also create a security threat.

B. Risks and Challenges

With the increase in the number of users accessing social networking sites, has opened new routes for the attackers to gain access to the accounts of the individuals. The more Information that is posted creates a new threat on the privacy and security of the user.

Social Sites are growing rapidly posing new risks for individuals and organizations in this modern world of technology. And some of the challenges are as follows-

1) Phishing Attacks: It is a technique for accessing sensitive information. The attackers make fake web pages that look like the legitimate ones and ask users to enter their credentials and the user gets in trouble when the user enters the credentials.

Kaspersky Lab's statistics exposed that the fake social sites imitating Facebook user's accounts for nearly 22% of phishing attacks in 2014. According to Kaspersky Lab, phishing is a major threat in Russia and the Europe as the number of attacks has increased in this region, up 18% to 36.3 million attacks in Q3 2015 as compared with the same time period last year. For example, A Moldovan man ran a phishing scheme that ended in a loss of $3.5 million for a western Pennsylvania drilling firm.

A school district was almost tricked by the same scam into sending almost a million dollars. The email contains malware in a zip file attachment

2) Identity federation challenges: This is a technique used to share user credentials across multiple domains. For example, many sites offer users to log in with their Facebook account to make it more convenient for the user and not to create multiple accounts on different sites. It may seem convenient, but the user has no knowledge of how and to what extent their personal data may be shared between third-party applications.

3) Malware: Malware are programs that are installed on a user's device without the user's knowledge and consent.

It spreads quickly and infects the device. The AV-Test Institute (AV-TEST, 2016) registers 390,000 malicious programs every day. It causes security flaws in software, viruses, worms and trojans are examples of malicious software. Attackers can gain access to a user's personal information by monitoring the computer's activity, and the computer can also be controlled or engage in mass attacks without the user's knowledge, as malware can steal the user's identity, and malware can also crash computers. Hackers can also install forms of adware that can cause endless pop-up ads on the user's computer, e.g.

a) "LOL" virus: This virus is spread through the chat function of Facebook. This virus is sent by a user stating "lol" with an attachment. And when the user clicks on the link, the malware is downloaded to the user's system. The virus infects the system and spreads through the network, gaining access to the user's information.

b) Zeus: This is a Trojan that spreads by clicking on a link. And when the user clicks on the link, it scans all the files on the user's system and steals important information. The specialty of this Trojan is to steal the user's bank credentials.

4) Click Jacking Attacks: also called UI redress attacks. Where a Trojan horse on a website asks the user to click on a malicious link and malware is planted on the system. This is common on Facebook called as jacking, which means that when a user likes a page, picture or video, the user is caught by attackers. This type of attack is done to perform a malicious attack or to increase the popularity of a site.

Take your career to new heights of success with ethical hacking training

RECOMMENDATION

This section provides some recommendations for securing user information

Answer: There should be some email policies for the company so that the emails are not confused with other spam emails or phishing

B. A quality antivirus program should be used by both the individual user and the company to filter and block malicious website

C. Authentication should be performed at every level of the website to prevent attackers from gaining access to the user's personal information

D. Cryptography-based techniques should be used to ensure the security of user information provided on social networking websites. Group key exchange, data mining, encryption are some of the examples that can be used to increase security on social media

E. The government should conduct training and education programs to spread cyber security awareness. The government should conduct promotional campaigns and programs that include seminars, competitions, exhibitions on cyber security

F. Social networking sites that have privacy settings discuss the tools available to increase account security. Just like Facebook's privacy settings, where the basics of privacy are broken down as

1) Who-can-see-my-stuff: This is a priority setting for Facebook users where the user can limit the audience that can see the user's posts. Public posts should be avoided for security reasons

2) Login Notification: This setting allows the user to get a notification when anyone logs into their account from an unknown device or browser.
3) Third Party Verification: This is a new setting added to Facebook which allows you to generate a Facebook security code to verify any third party app.
4) How others interact with the user: This helps the user manage how other people's activity affects the user's profile. And the user can manage labels, "unfriend" or "block" someone.
G. Web Browser Security Settings
1) User should keep browsers up to date and automatic updates should be enabled for the browser.
2) Block plug-ins, pop-ups and phishing sites.
3) Set your browser not to save passwords.
4) Disable third-party cookies.
5) Browser-specific settings:
a) Firefox: install the NoScript add-on
b) Safari: Disable Java
c) IE: Setting of security zones.

CONCLUSION

With the growing popularity of social networks, these sites have become a major target for cybercrimes and attacks. Cybercrime is becoming widespread and poses a major threat to national and economic security. Both public and private institutions in the public health, information and telecommunications, defense, banking and finance sectors are at risk. Thus, organizations should take appropriate security measures to be safe from cybercrime and users should protect their personal information to avoid identity theft or misuse. Cyberspace is becoming a significant area for cybercriminals and terrorists to attack critical information. Thus, there is a need for universal cooperation among nations to work together to reduce the ever-increasing cyber threat.

REFRENCES

[1]. http://www.ic3.gov/ Internet Crime Report 2015"
[2]. Most number of cyber crime reports. Available https://factly in/cyber-crimes-in-india-which-state-tops-the-chart/
[3]. National Cyber Security Policy 2013. Available: https://en.wikipedia.org/wiki/National Cyber Security Policy 2013
[4]. Security. Privacy and Trust in Social Networking Sites, Richa Garg, Ravi Shankar Veerubhotla. Ashutosh Saxena. CSI Communications ISSN 0970-647X Volume No. 39 Issue No. 2) May 2015
[5]. Exploiting Vulnerability to secure user Privacy on a social networking site. Pritam Gunecha, Geoffrey Barbier, Huan Lui, ACM SIGKDD International conference on knowledge Discovery and Data Mining, August 2011.
[6]. Latest in phishing 2016. Available https://info.wombatsecurity.com blog/the-latest-in-phishing-first-of-2016
[7]. Malware statistics Available: https://www.av test.org/en/ statistics/malware/
[8]. Dolvara Gunatilaka "A Survey of Privacy and Security Issues in Social Networks www.cse.wustl.edu/-jain/cse571-11/ftp/social/index.
[9]. Facebook Privacy Basics [Online]. Available: https://www.facebook.com/about/basis
[10]. Browser Security Settings Available: http://its.ucsc.edu/ software/release/ browser-secure.html