ASH1925004M

by Iftekhar Efat

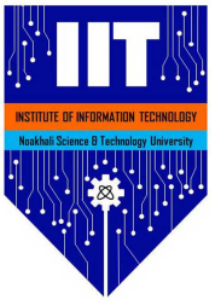
Submission date: 13-Mar-2022 12:50AM (UTC-0500)
Submission ID: 1782973222
File name: ASH1925004M.pdf (190.11K)
Word count: 2558
Character count: 14007

How does Facebook protect itself from cyber-attacks?

Sunaan Sultan
ASH1925004M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University



Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

Facebook is a social network made up of nodes, which are persons or organizations linked by one or more distinct types of interdependency, such as friendship, shared interests, financial transactions, beliefs, knowledge, or prestige. A cyber-threat can take several forms. It can be both unintended and purposeful, targeted or nontargeted, and come from a wide range of sources. criminals, hackers, and virus makers, as well as foreign states engaged in espionage and information warfare employees who are dissatisfied with their jobs and contractors who work for a company. Facebook is not a social media platform. not only to communicate or interact with other people on a worldwide scale, but also as a commercial tool promotion. The cyber risks on Facebook are investigated and studied in this research. We examine the amassing history as well as the cyber risks that are suggested, as well as the techniques and sloppy trends of such popular websites.

1 Introduction

1.1 Sub Intro

Facebook, with over 1 billion monthly active users, is a tempting target for cyber-criminals. When Facebook employees accessed a hacked mobile developer website in January 2013, they became the victims of a sophisticated cyber-attack. The Facebook Security team discovered malware on many company devices after noticing a suspicious domain in their corporate DNS logs. They discovered no evidence, however, that any Facebook user data had been hacked.[9]

Hackers have been hired by Facebook to identify security flaws in its products. In August 2011, Facebook's new "bug bounty" security effort handed out over 40,000 dollars in less than a month. The corporation is offering a 500 dollars bounty and publicly thanking "white-hat hackers" on its Facebook page.

Researchers from the University of California Berkeley and the University of Maryland developed ShadowCrypt, a prototype browser extension that makes it simple to send and receive encrypted text on Twitter, Facebook, and other websites, in February 2014. Nonetheless, we must address the most serious source of cyber-threats: human mistake. Regardless matter how secure a communication channel is or how unbreakable a cryptographic technique appears to be, everyone is responsible for the 10.11 Cybersecurity Awareness: Everyone's Responsibility. The endpoints - the sender (before encryption) and the recipient — are frequently the weakest links in cyber attacks, prevention, and countermeasures (after decryption)[9]

2 Threats

Many users have become unwittingly exposed to threats to their privacy and security as a result of the increased use of Online Social Networks. These dangers can be classified into four groups. Traditional dangers, such as privacy and security issues, are included in the first category.

The United States Computer Emergency Readiness Team (US-CERT) has been collecting phishing email messages and website addresses in order to help people avoid becoming victims of phishing scams. Phishing emails should be forwarded to phishing-report@us-cert.gov by the recipients. Furthermore, users of social media platforms should report any suspicious phishing communications to phish@fb.com for Facebook.[9]

Many different ways Facebook protects itself from cyber attacks. The figure below diagrams all the specific threats listed in the follow ing sections

1. Classic Threats

Traditional threats have been an issue since the Internet's inception.It achieved wide acceptance. Malware, also known as spam, is a type of computer virus.Cross-site scripting (XSS) attacks, also known as phishing, are on the rise. Be a continuing problem despite the fact that these dangers have been handled.They have previously gotten extremely viral as a result of the OSNs have a unique structure and nature,

and they can quickly propagate among people. users of the network Traditional threats can take advantage of a user's ignorance.Personal information uploaded on a social networking site was used to launch an assault simply by modifying the settings, not only the user but also their friends will benefit. threat of storing the user's private information An attacker may, for example, embed harmful code in a visually appealing spam message that uses a user's Facebook profile information. Because of the personal character of this designed communication, the odds of an innocent user opening it and becoming infected are high. These threats frequently target vital and common user resources including credit card details, account passwords, processing power, and even computer bandwidth (in order to send spam emails). Worse, these threats can use the infected user's stolen credentials to send messages on his or her behalf or even change the user's personal information. The several traditional risks are explained here, along with real-life examples of how these threats have affected the privacy and security of real users.

Malware

Malware is malicious software that is designed to disrupt a computer's operation in order to steal a user's credentials and access their personal information. Malware that spreads through social networks exploits the OSN framework to spread among users and their friends.

Phishing Attacks

Phishing attacks are a type of social engineering that entails impersonating a trusted third party in order to get user-sensitive and private information. According to a recent study[2] Due to their gregarious and trusting character, people who participate on social networking websites are more prone to fall for phishing schemes. Furthermore, phishing efforts within OSNs have expanded dramatically in recent years. According to the Microsoft Security Intelligence Report[4],

Spammers

Spammers are those who utilize electronic messaging systems to deliver unwanted messages to other people, such as ads. By creating bogus profiles on the social networking platform, spammers exploit it to distribute advertisements to other users.[7].

2. Modern Threats

The majority of modern attacks are specific to OSN settings. Typically, these attacks target users' personal information as well as their friends' personal information. For example, an attacker attempting to obtain a Facebook user's high school name — which is only visible to the person's Facebook friends — can build a false profile with relevant data and send a friend request to the targeted user. If the user accepts the friend request, the attacker will have access to his or her personal information. Alternatively, the attacker can utilize an inference attack to get data from the user's Facebook friends.

Clickjacking

Clickjacking is a harmful practice that entices consumers to click on something other than what they expected. The attacker can employ clickjacking to trick the victim into publishing spam messages on his or her Facebook timeline, accidentally "liking" links (also known as likejacking), and even recording the user using a microphone and webcam.[10]

Face Recognition

Many people use social networking sites to share photos of themselves and their acquaintances. Every day, tens of millions of images are uploaded to Facebook. Furthermore, many Facebook user profile images are viewable and downloadable by the general public. The Faces of Facebook webpage, for example,[1] allows visitors to browse the profile photographs of over 1.2 billion Facebook members on the internet. These photographs can be used to build a biometric database that can be used to identify OSN users without their permission.

Fake Profiles

Automatic or semi-automatic profiles that replicate human activities in OSNs are known as fake profiles (also known as sybils or socialbots). Fake accounts may be used to steal personal data from social media users in numerous circumstances. The socialbots can obtain a user's private data by starting friend requests to other users in the OSN, who frequently accept the requests. According to a recent story, the market for buying false followers and retweets is already a multimillion-dollar industry.[11].

3 Methods and Solutions

The best practices for protecting Facebook login credentials are:

1. On Facebook, and other websites, turn on two-factor authentication. Facebook began supporting Security Key, an open standard that allows you to log into an account using a physical device (such as a USB) and an online password, in October 2014.

2. Avoid dictionary terms, acronyms, and abbreviations while creating a password. A password should be tough to guess yet simple to remember, so it does not need to be written down. For example, if Jack and Jill are married and take their three children to Disneyland twice a year, a strong and easy-to-remember password would be "JJ3di2ya," which incorporates mixed case letters, digits, and punctuation. It's also simple to change your password on a frequent basis by gently rearranging the password phrase. For example, "JJ3di2ya" might be shortened to "JJ3di2ya."

3. Use different passwords for different websites. Instead, make each site's password unique. If you have accounts on several different websites, it may appear to be a big chore, but there is a simple two-step approach. The first step entails: Make a strong stem for your password. Step two: Add a sentence to the stem that is particular to the location. A strong password stem is "JJ3di2ya," as seen in the example password above. If Jack and Jill share a Gmail account that Jill set up on the day her mother-in-law arrived from England, a strong and easy-to-remember password for their Gmail account may be "JJ3di2yaMotherEng." Similarly, one of Jack and Jill's bank accounts may have the password "JJ3di2yaBettyBoop" since they dined at a nearby "Betty Boop" restaurant on the day they opened it. The primary concept is to combine a strong password stem with associative memory or good imagination words.

4. Don't give direct answers to the online security questions. Instead, utilize the answers as passwords, provide a lengthy response, or simply be inventive.[9]

Authentication Mechanisms

OSN operators use authentication mechanisms such as CAPTCHA, photos-of-friends identification, multi-factor authentication, and in some cases even requesting that the user send a copy of his or her government issued ID to ensure that the user registering or logging into the social network is a real person and not a socialbot or a compromised user account.[5].

Report Users

Operators of OSNs can try to safeguard young children and adolescent users from harassment by allowing them to report abuse or policy breaches by other network users. In certain countries, social media platforms such as Facebook and Bebo have incorporated a "Panic Button" to help protect minors.[3].

Phishing Detection

Many researchers have proposed antiphishing approaches for detecting and preventing phishing attempts; the majority of these solutions are based on techniques for detecting phishing websites and URLs. [8].

Fake Profile Detection

Researchers have created algorithms, strategies, and tools to detect phony profiles and avoid sybil attacks using OSNs in recent years. 3 Yu et al. proposed the SybilGuard decentralized protocol in 2006, which aids in the prevention of sybil attacks. Yu et al, also presented the SybilLimit protocol in 2008, which is a near-optimal protection against sybil assaults leveraging social networks. Danezis and Mittal introduced the SybilInfer defensive algorithm in 2009, which can tell the difference between "honest" and "dishonest" users. Tran et al. presented the SumUp sybil defensive system in the same year, with the goal of reducing the amount of fraudulent votes cast by sybils.[13]

FB Phishing Protector

When a suspicious action, such as a script-injection attempt, is identified, FB Phishing Protector[6] is a Firefox add-on that alerts Facebook users. This add-on protects you from a variety of phishing attempts.

Internal Protection Mechanisms

Several OSNs shield its users against spammers, phony accounts, frauds, and other risks by incorporating extra internal protection mechanisms. Facebook, for example, uses the Facebook Immune System to safeguard its users from hostile assaults and data collection (FIS). The FIS is an adversarial learning system that performs real-time inspections and classifications on Facebook's database read-and-write operations.[12].

4 Conclusion

Facebook has become an integral part of our daily lives, with most Internet users spending more time on social media than on any other online activity. We like interacting with other people on Facebook by sharing our experiences, photos, and videos. Nonetheless, social media sites have a dark side populated by hackers, scammers, and online predators, all of whom are capable of utilizing Facebook to find new victims. We have described situations in this research that risk facebook users' identities, privacy, and well-being in both the virtual and real worlds. Furthermore, we have supplied instances of many of the risks discussed in order to show that these threats are genuine and may put any user at risk. We've also highlighted several risks that put people's safety at jeopardy.

References

[1] Alessandro Acquisti, Ralph Gross, Fred Stutzman, et al. Faces of facebook. *Black Hat*, 2011.

[2] Tarek Amin, Oseghale Okhiria, James Lu, and James An. Facebook: A comprehensive analysis of phishing on a social system. *Dep. Electr. Comput. Eng.*, 2010.

[3] S Axon. Facebook will add a "panic button" for uk teens, jul. 2010.

[4] D Cavit, J Salido MM, JT Arroyo, J Faulhaber, D Pecelj, C Seifert, V Gullotto, A Penta, F Simorjay, S Wu, et al. Microsoft security intelligence report volume 10.

[5] Josh Constine. Facebook launches verified accounts and pseudonyms. *Retrieved February*, 2:2018, 2012.

[6] Michael Fire, Roy Goldschmidt, and Yuval Elovici. Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4):2019–2036, 2014.

[7] Michael Fire, Gilad Katz, and Yuval Elovici. Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. *Human journal*, 1(1):26–39, 2012.

[8] Sujata Garera, Niels Provos, Monica Chew, and Aviel D Rubin. A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode*, pages 1–8, 2007.

[9] Newton Lee. Cyber attacks, prevention, and countermeasures. In *Counterterrorism and Cybersecurity*, pages 249–286. Springer, 2015.

[10] Rich Lundeen, Jesse Ou, and Travis Rhodes. New ways im going to hack your web app. *Blackhat AD*, pages 1–11, 2011.

[11] Nicole Perlroth. Fake twitter followers become multimillion-dollar business. *The New York Times*, 5, 2013.

[12] Tao Stein, Erdong Chen, and Karan Mangla. Facebook immune system. In *Proceedings of the 4th workshop on social network systems*, pages 1–8, 2011.

[13] Dinh Nguyen Tran, Bonan Min, Jinyang Li, and Lakshminarayanan Subramanian. Sybil-resilient online content voting. In *NSDI*, volume 9, pages 15–28, 2009.

ASH1925004M

ORIGINALITY REPORT

44%	38%	35%	27%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	mafiadoc.com Internet Source	15%
2	link.springer.com Internet Source	10%
3	v1.overleaf.com Internet Source	3%
4	Submitted to University of Central Lancashire Student Paper	3%
5	Submitted to City University of Hong Kong Student Paper	2%
6	Counterterrorism and Cybersecurity, 2015. Publication	2%
7	Michael Fire, Roy Goldschmidt, Yuval Elovici. "Online Social Networks: Threats and Solutions", IEEE Communications Surveys & Tutorials, 2014 Publication	2%
8	global.oup.com Internet Source	2%

9	Submitted to University of Moratuwa Student Paper	1 %
10	ieeexplore.ieee.org Internet Source	1 %
11	Submitted to Gusto International College Student Paper	1 %
12	lancecorner.com Internet Source	1 %
13	Submitted to Curtin International College Student Paper	1 %
14	www.coursehero.com Internet Source	1 %
15	www.mdpi.com Internet Source	<1 %
16	www.rickytech.in Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925004M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

Sentence Cap. Remember to capitalize the first word of each sentence.

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to remove this article.

PAGE 3

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

PAGE 4

Missing "," You may need to place a comma after this word.

Possessive You may need to use an apostrophe to show possession.

Word Error Did you type "**the**" instead of "**they**," or have you left out a word?

PAGE 5

Sentence Cap. Remember to capitalize the first word of each sentence.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

Sentence Cap. Remember to capitalize the first word of each sentence.

Missing "," You may need to place a comma after this word.

Article Error You may need to remove this article.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 6

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 7

Article Error You may need to remove this article.

Article Error You may need to remove this article.

PAGE 8

Article Error You may need to remove this article.

Sentence Cap. Remember to capitalize the first word of each sentence.

PAGE 9

Prep. You may be using the wrong preposition.

PAGE 10