BKH1925025F

by Iftekhar Efat

Submission date: 13-Mar-2022 03:12AM (UTC-0400)
Submission ID: 1782992550
File name: BKH1925025F.pdf (177.98K)
Word count: 2287
Character count: 12414

How to recognize a social engineering attack

Ayesha Nasrin Ripa
BKH1925025F

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

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

Social engineering attacks have posed a serious security threat to cyberspace.It's a catch-all word for a wide range of malevolent operations carried out through human connections. It employs psychological tricks to persuade users to make security errors or divulge critical information. Communication systems are prone to social engineering assaults and can be readily exploited by hostile individuals.Because it takes advantage of the inherent human desire to trust, social engineering is one of the most difficult problems in network security. This paper provides a thorough review of social engineering attacks, including classifications, detection approaches, and prevention strategies.

1 Introduction

In the context of computer and cyber security, social engineering refers to a type of attack in which an attacker uses influence, persuasion, deception, manipulation, and inducing to obtain classified information, hack a computer system or network, gain unauthorized access to restricted areas, or breach the security goals (such as confidentiality, integrity, availability, controllability, and auditability) of cyberspace elements (such as infrastructure, data, resource, user and operation).Social engineering, the psychological manipulation of individuals in order to acquire access to a system for which the attacker is not permitted, is a serious danger to information security. Cybercriminals target the weakest link in a security system, which is generally humans rather than a robust computer system. If a user provides a password or other key information, all kinds of system security can be bypassed.[1] In this paper, we present about social engineering attacks, how to detect them. The rest of this paper is organized as follows. Section 3 Social Engineering Attacks and describes social engineering attacks. Section 4 provide an overview of detection techniques.Finally, a conclusion is given at the end.

2 Background

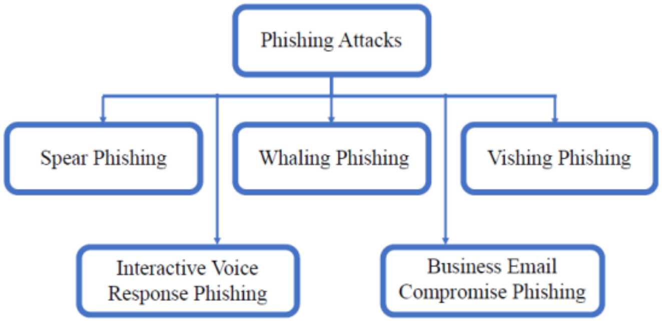
Previous work on automatic social engineering attack detection has been restricted to emails and websites, with no attempt to identify the more subtle class of social engineering assaults that are solely dialog-based. Previous research has focused on educating people about social engineering attempts so that they are more aware and resistant in the future. User training can give resistance to a larger spectrum of attack kinds, although its efficiency varies greatly based on the talents of individual users. An automated solution to detecting social engineering attacks that may be used to a wide range of attack types while requiring little work from the individual user is required.

3 Social Engineering Attacks

Attacks Description:

1. Phishing Attacks: Phishing scams, which are email and text message campaigns aiming at instilling a sense of urgency, curiosity, or terror in victims, are one of the most common social engineering attack types. It then pressures people into disclosing personal information, visiting fraudulent websites, or opening malware-infected attachments.

Figure 1: Phishing attacks[3]


Phishing Attacks
Spear Phishing
Whaling Phishing
Vishing Phishing
Interactive Voice Response Phishing
Business Email Compromise Phishing

2. Pretexting Attacks: Pretexting is a type of attack in which the attacker fabricates a situation in order to persuade the victim to divulge sensitive information, such as a password. Pretexting assaults include creating fictitious and convincing circumstances in order to acquire personal information from a target. They are predicated on pretexts that lead the victim to believe and trust the perpetrator. Phone calls, emails, and physical media are used to carry out the attack. To carry out their assault, attackers post information in phone books, public web sites, or conferences where collaborators in the same field gather. A pretext might be an offer to perform a service or obtain employment, a request for personal information, assisting a buddy in obtaining something, or winning a lottery.[2]

3. Baiting Attacks: Baiting assaults, as the term indicates, employ a false promise to spark a victim's avarice or interest. They trick consumers into falling into a trap in which their personal information is stolen or their computers are infected with malware.Physical media is used to disseminate malware in the most hated form of baiting. For example, attackers may place the bait—usually malware-infected flash drives—in settings where potential victims are likely to encounter it (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has a genuine appearance, with a label identifying it as the company's payroll list.Victims pick up the bait out of curiosity and place it in a work or home computer, causing malware to be installed automatically. Baiting schemes don't have to take place in real life. Baiting takes place online

in the form of appealing advertising that direct viewers to malicious websites or persuade them to download malware-infected software.[2]

4. Tailgating Attacks: Tailgating attacks, also called piggybacking or physical access, consist of accessing an area or building by following someone who has the security clearance to that place. They allow attackers access unauthorized buildings. For example, attackers ask a victim to hold the door open because they forgot their company' ID card or RFID (radio-frequency identification) card. They can also borrow a computer or cellphone to perform malicious activities such as installing malware software. For instance, RFID cards attacks are one of the most used attacks to access forbidden spaces for malicious purposes. Due to their wide utilization and low cost, RFID systems are considered as the most emerging technology used by companies to control the access to their facilities. Despite their advantages, they have vulnerabilities that can be exploited to cause serious security issues to companies. RFID attacks can be performed over several layers of the interconnection system model (ISO) [28]. For instance, at the physical layer, the RFID devices and the physical interface are targeted to manipulate an RFID communication. These attacks can cause temporary or permanent damage of the RFID cards. At the network layer level, the attacker manipulates the RFID network such as the communication between the RFID entities and data exchange between these entities.

5. Phone/Email Scams Attacks: For this type of attacks, the attacker contacts the victim via phone or email seeking specific information or promising a prize or free merchandise. They aim at influencing the victim to break the security rules or to provide personal information. Moreover, cellphone-based attacks can be performed via calls and via short messaging services (SMS) or text messages, which are known as SMSishing attacks. SMSishing attacks consist of sending fraudulent messages and texts via cell phones to victims to influence them. They are similar to phishing attacks but they are performed in different ways. The efficiency of the SMSishing attacks resides in the fact that victims can carry their cellphones anywhere and anytime. A received text message can include a malware even if it was sent from trusted and known transmitter. The malware works as a background process installing backdoors for attackers to have access to information such as contact list, messages, personal email, photos, notes, applications, and calendar. The scammer can install a root kit to control the cellphone completely.

6. Pop-UpWindows Pop-up window attacks refer to windows appearing on the victim's screen informing the connection is lost. The user reacts by re-entering the login information, which runs a malicious program already installed with the window appearance. This program remotely forwards back the login information to the attacker. For instance, pop-ups can be alert messages showing up randomly for online advertising to lure the victim in clicking on that window. Pop-ups also can be fake messages alerting about a virus detection in the victim's computer. The pop up will prompt the victim to download and install the suggested anti-virus software to protect the computer. They can also be

fake alerts stating that the computer storage is full and that it needs to be scanned and cleaned to save more space. The victim panics and reacts quickly in order to fix the problem, which activates the malware software carried in the pop-up window.

7. Other Attacks: There are many other types of attacks that can be summarized as follows:

   (a) Impersonation on Help Desk attacks: the attacker pretends to be someone with authority or a company's employee and calling the help desk requesting information or services.

   (b) Dumpster Diving attacks: consist of gathering sensitive documents from company's trash or discarded equipment such as old computer materials, drives, CDs, and DVDs

   (c) Quid Pro Quo attacks: baiting attacks offering free services to seduce the victim. They require an exchange of information in return for a service or product.

   (d) Diversion Theft attacks: consist of misdirecting a transport company to deliver a courier or package to the desired location.

   (e) Shoulder surfing attacks: consist of watching the victim while entering passwords or sensitive information.

   (f) Stealing important documents attacks: consist of stealing files from someone's desk for personal interests.

4 Detecting Social Engineering Attacks

1. Asking for immediate assistance: Social engineers will use language that instills a sense of urgency in their victims to try to pressure the victim to rush into action without thinking about it. If someone asks you to make an urgent wire transfer, this is a sure sign that you should slow down and ensure that the transaction you'll be conducting is legitimate.

2. Asking you to donate to a charitable cause: Social engineers will exploit our generosity with phony requests for donations to charitable causes which includes payment instructions on how to send money to the hacker. By researching you on social media, a social engineer can figure out what charitable causes, disaster relief efforts, or political campaigns that you are likely to support. They will use this information to craft messages aligned with your ideals.

3. Asking you to ”verify” your information: Another approach social engineers will take is presenting a problem that can only be resolved by you verifying your information. Included in their message will be a link that brings you to a form to provide your information.

   These messages and forms can look legitimate with the right logos and branding, which can lull you into believing the sender and the message are legitimate.

4. Responding to a question you didn't ask: Social engineers will pose as s customer service agent from a company you do business with and send you a message ”responding” to a request for help. Though you never sent a request for help, you might decide that since you already have a rep contacting you, this would be an opportune time to receive support for an issue you've been experiencing.Inevitably the attacker will request specific information from you to ”authenticate your identity.” In reality, they're just stealing your information.

5. Name of sender can trick you: Email addresses and domain names can be easily spoofed. It is, therefore, crucial that you check the domain name for spelling alterations on suspicious emails. Even if they appear to have come from a trusted sender, always double check.

6. Check for typos: Attackers are often less concerned about being grammatically correct. Which means that typos and spelling errors are often evident in messages. Such errors in an email could be a good indication that the message is not genuine.

7. Don't share sensitive information hastily: Any email that asks for sensitive information about you or your company is suspicious. For instance, no bank will ever ask for personal information over an email. Directly call your bank to ascertain if an email is genuine or not.

5 Conclusion

In this paper, we provided an overview of social engineering attacks, existing detection techniques, and current countermeasure methods. Unfortunately, these attacks cannot be stopped using only technology and a robust security system can be easily overcome by a social engineer with no security knowledge. Social engineering attacks have been increasing in intensity and number and are causing emotional and financial damage to people and companies. Therefore, there is a great need for novel detection techniques and countermeasure techniques as well as programs to train employees. Countries must also invest in cybersecurity education in order to build skilled and trained humans.

References

[1] Ram Bhakta and Ian G Harris. Semantic analysis of dialogs to detect social engineering attacks. In *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)*, pages 424–427. IEEE, 2015.

[2] Hiroki Nishikawa, Takumi Yamamoto, Bret Harsham, Ye Wang, Kota Uehara, Chiori Hori, Aiko Iwasaki, Kiyoto Kawauchi, and Masakatsu Nishigaki. Analysis of malicious email detection using cialdini's principles. In *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*, pages 137–142. IEEE, 2020.

[3] Fatima Salahdine and Naima Kaabouch. Social engineering attacks: A survey. *Future Internet*, 11(4):89, 2019.

BKH1925025F

ORIGINALITY REPORT

83%	75%	45%	71%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.mdpi.com Internet Source	36%
2	blog.twinstate.com Internet Source	13%
3	Submitted to CTI Education Group Student Paper	7%
4	futurelawyer.typepad.com Internet Source	6%
5	v1.overleaf.com Internet Source	4%
6	Ram Bhakta, Ian G. Harris. "Semantic analysis of dialogs to detect social engineering attacks", Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015), 2015 Publication	3%
7	www.coursehero.com Internet Source	3%

8	Zuoguang Wang, Hongsong Zhu, Limin Sun. "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods", IEEE Access, 2021 Publication	2%
9	Submitted to Sri Lanka Institute of Information Technology Student Paper	2%
10	global.oup.com Internet Source	1%
11	Submitted to University of Hong Kong Student Paper	1%
12	Submitted to Roehampton University Student Paper	1%
13	Submitted to Southampton Solent University Student Paper	1%
14	iosrjournals.org Internet Source	1%
15	www.researchgate.net Internet Source	1%
16	Submitted to Campbellsville University Student Paper	1%
17	Submitted to Santa Clara University Student Paper	1%
	www.journaltocs.ac.uk	

18	Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

BKH1925025F

PAGE 1

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

PAGE 2

PAGE 3

PAGE 4

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

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

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

PAGE 5

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

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to remove this article.

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 remove this article.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

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

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

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

Prep. You may be using the wrong preposition.

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

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 7

PAGE 8

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

PAGE 9