ASH1925011M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:10AM (UTC-0500)
Submission ID: 1782981269
File name: ASH1925011M.pdf (688.27K)
Word count: 2312
Character count: 11811

Social Hacking Dangers in 2022

Naimur Rahman
ASH1925011M

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

Typically, in today's digital world, social hacking is a process of identifying our weaknesses and exploiting them to gain access to valuable assets (such as personal identification information). Social hacking is a form of social engineering. Phishing emails are widely used as a link to gain personal pieces of information. Several studies have shown that social hacking attacks are happening on a large scale and impacting the population.

This paper will introduce some common social hacking methodologies as well as prevention methods.

1 Introduction

The intention of this paper is to introduce social hacking strategies and the prevention of these methods[3].
The proliferation of e-mails, social networking sites, and other forms of electronic communication has made social, hacking attacks on businesses increasing and more dangerous. Firewalls or other technological solutions do not help against this type of attack.
Keypoints of the paper are as follows:

1. Social hacking works to take advantage of our human weaknesses, with a variety of strategies including phishing, and pre-texting. LaTeX;
2. Technologies that integrate firewalls for web applications and advanced filters are effective in stopping multiple robberies before going to users' inboxes.
3. Of those spam emails, one of the most important tools for preventing successful attacks on social engineers is awareness training.

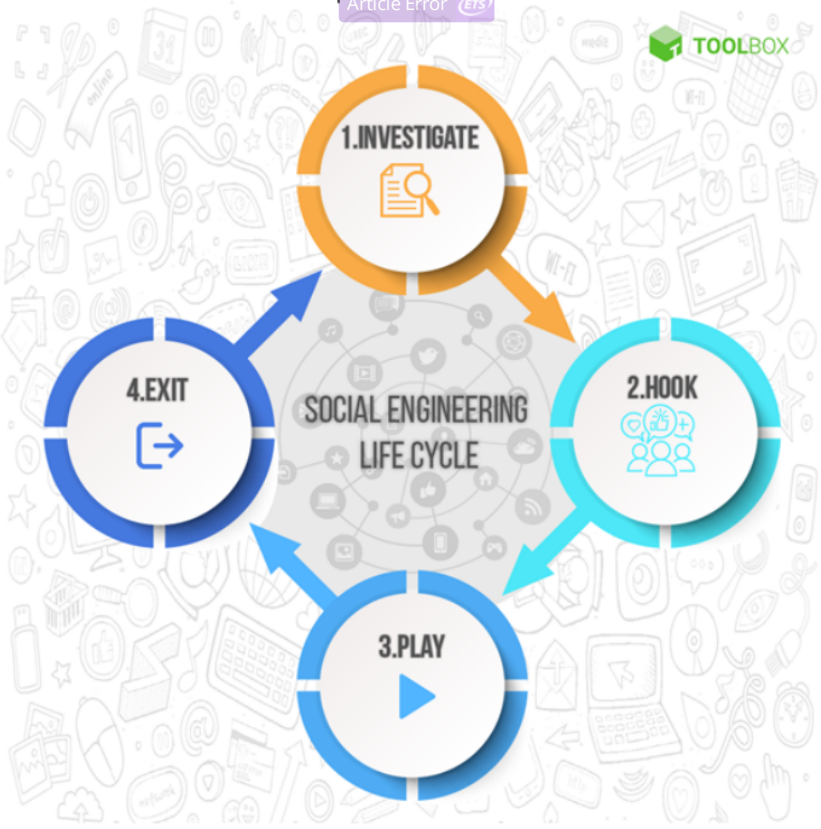
A cybercriminal calls one of your employees and pretends to be an administrator in the company's IT department. Previously, he had received information on social media, which should help him gain the trust of an employee. You open the conversation by talking about an existing project in the company. The employee, of course, assumes that the call is real.
The cybercriminal is now looking for pieces of the employee who are suspected of needing him. A few technical terms and abbreviations can help confuse the employee. And you have managed to access the system without much effort!
There are also many different ways of social hacking such as- phishing, baiting, scareware, pretexting, watering hole. We are going to review the methods of attacking and how to prevent them.

2 Background

A social engineer usually starts by researching the internet to [1] find open source intelligence (OSINT), digging into publicly available information to select specific

users who will deceive them.
Suppose a social engineer first searches the LinkedIn for everyone working in an organization. For example, we will call the company Tea Castle, an online retailer of loose leaf tea.
On LinkedIn, an engineer can see the job title of each employee, the person under whom he or she works, how long he or she has been an employee, the accounts he or she holds, etc. From there, the engineer may undo the door, choosing, for example, to point. marketing staff instead of a tech-savvy IT team.
The developer then searches the social media profiles of individuals of the marketing team, obtaining important information about their personal and personal information.

Figure 1: Life cycle of social engineering



You can see that VP Marketing posted a public photo on Instagram working remotely, claiming to enjoy working at his favorite store and enjoying local tea. The social engineer notices this, wondering what remote security threats he can use, knowing that he will probably have higher permits in the organization. He writes down that he uses the MacBook, which is the store where he works, the place where he probably lives based on his closeness to the store. He keeps scrolling and realizes

that he likes to work in restaurants on Fridays.
All information collected by a social engineer contains key pieces of the plot, which help to compile a fraudulent account. The developer uses this knowledge of the target to systematically plan the deceptive situations he will use against the VP.
With more OSINT hunting, the social engineer finds a district-wide tea shop called Steepers. You are creating a false email address, which mimics the email extension used on a tea owner's website. Pretending to be the owner of Steepers, the social engineer created a VP email for Tea Castle, introducing himself as the CEO of Steeper and asking if he would like to take a sample of their handmade tea. He even goes so far as to remove Steeper's earl gray ear which he says is his favorite (he knows from VP's writing that he likes this type of tea).
The VP responds that he would like to sample their best-selling tea and the social engineer has his own. You drag a sample of the Steeper tea list to their site and attach a non-computer program to PDF.
The evil character waits until Friday at 3 p.m. responding with his second email to identity theft, he knew the VP would probably enjoy the tea and would probably be very happy to try more. Then, send him a PDF, hoping you use public WiFi in the store and not on a secure VPN or home network.
When clicked, this attachment injects a VP computer into a non-computer program, giving the bad character a chance to get into his or her business plan. He may continue the conversation with the VP for a while, especially if he needs more information to pass additional restrictions on his system and needs to introduce another suspended cyberattack.

3 Methods

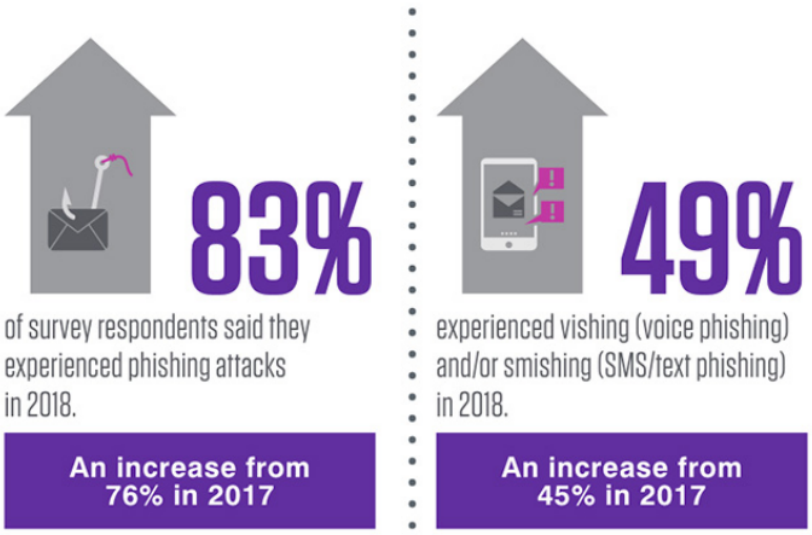
3.1 Phishing

[4] Phishing are social scams that often rely on emails to direct and convince the victim to disclose sensitive data or click a malicious link. There are several categories of identity theft crimes, including sensitive identity theft, where the attacker takes ownership of a trusted person, and whale fishing, where high-level targets, such as the CEO of a company, are targeted.

3.2 Pretexting

Closely related to the phishing, making a bad record is a robbery of social engineers where the attacker receives information about a series of lies and impersonations. For example, an attacker may pretend to be a company official or a legal officer to gain access to financial accounts and personal data.

Figure 2: Phishing attack survey



3.3 Watering Hole

In a public watering hole, the attackers directed the websites of certain groups of known users (or supposed) to visit them. Attackers put malicious code into the website, with the intent of infecting the computers of targeted users to gain access to their operating networks.

3.4 Baiting

Baiting attacks entice victims to disclose sensitive information or click malicious links with the promise of a refund for something, such as free music or a gift card.

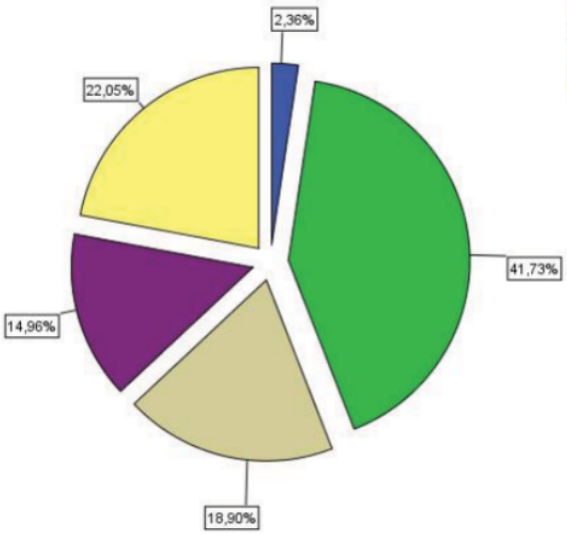
4 Preventing Social Hacking Methods

1. Manage unsolicited messages and phone calls with caution, especially those requesting identifying personal and business information.
2. Double check the authenticity of any suspicious emails and phone calls directly (and separately) by contacting the company from which the alleged communication originated.
3. Check the security of the webpage before entering any personal information.
4. Provide security awareness training to employees.
5. Use email filters to detect scams and fake messages - before they get into staff inbox.

5 Results

It was found that 25.4 percentage of respondents heard about it Social Engineering a few times, 49.3 percentage of respondents he showed that they had never experienced anything like it Social Engineering, 53.5 percentage of respondents indicated that heard permanently about cybersecurity, 57.7 percentage of respondents indicated that they had heard of the hijackers permanently. Regarding the fraudulent webpage launched, it was found that 66.2 percentage of respondents indicated that the image of the web page was dishonestly, 73.2 percentage of respondents indicated that they certainly did not put their details on the web page presented. In

Figure 3: Distribution by area o professional activity



the case of respondents' information on this topic, we found 52.4 percentage of respondents indicated that they could distinguish between trustworthy and trusted email, 87.3 percentage of respondents indicated that they were aware of the email of a phishing scam that, 73.2 percentage of respondents indicated that they knew Social Engineering attacks may be related to phishing emails, 57.7 percentage of respondents indicated that they were familiar with social engineering could be a crime of identity theft, 73.2 percentage of respondents were identified they would like to be trained instead to avoid that attacked by email for sensitive identity theft. It was found to be in the case by opening a criminal email for sensitive information theft, 94.4 percentage of respondents show that they did not upload links and / or open them Attachment, 97.2 percentage of respondents indicated that they did not reply to email with the requested information, 70.4 percentage of Respondents indicated that they would close the email immediately, 59.2 percentage of respondents

Figure 4: Distribution by age group

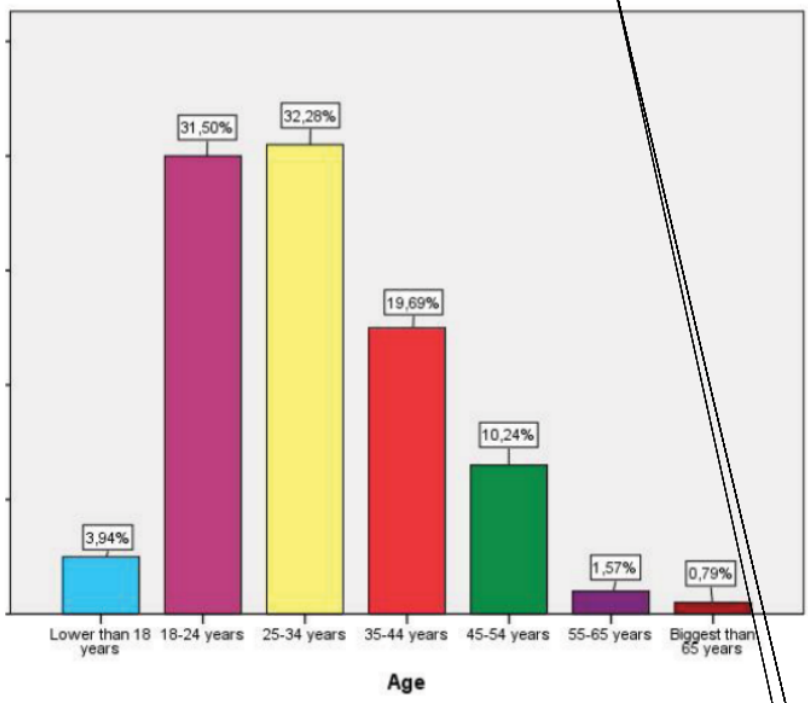


Figure 2 - Distribution by age group

indicated that they did not point their mouse at the link, not click on it.

6 Conclusion

With regard to criminal charges of identity theft it has been found that the context of Crime theft cases are the highest occupational by 66.2 percentage, respondents indicating that they have received a criminal attack on identity theft attempts with their professional email. It has been found that the tools are widely used Analyzing criminal emails to steal sensitive information are: "Mxtoolboox", "Browser", "Virustotal" and "Reverse IT"[2], are used in open source and free area. As per the limits of this investigation, it is emphasized that the answers to the questionnaire cannot happen to others of people, and the truth of the answers can not proven, as the respondents have completed their own questionnaire, unattended and it is noteworthy that conversations also IT professionals are driven by email. In this sense, it was it is impossible to detect their behavior, i.e. to react once movement that can answer certain questions and be able to allow a description of some questions based

on the topic of interview.
As a future activity, the same list of questions can be used by respondents from other countries with different cultures, values and ways of thinking. It would also be interesting to do a email a phishing scam and send it to a group of people who are checking their own response to such email.

Acknowledgements

This research is conducted in direct supervision of the Software Evaluation and Re-Engineering Research (SERER) Lab.

Notes: It is common that you will want to acknowledge the contribution of others to your work, even though these might not have been sufficient to warrant being a co-author.

Consider who might have provided valuable discussions, funding support, or moral support for the work.

BTW, you don't have to start each section on a new page. I have done that here for clarity, but it isn't usually needed.

A Appendices

This is a short appendix, just included as an example.

Notes: An appendix can be used to include material that is important, but not needed in the main body of the text, and which it might detract from the main point of the report.

A common example is code. You should not include code in the main body of a report unless it is particularly important or revealing.

However, for the convenience of your supervisors who may wish to examine the code, and for your own benefit (in having a self-contained document), you may wish to include the code in an appendix. If so, have a look at the `listings` package for LaTeX. For Matlab, there is also a `matlab-prettifier` package that may work more easily for you.

References

[1] Sudhanshu Chauhan and Nutan Kumar Panda. *Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques*. Syngress, 2015.

[2] Michal Dúbravčík and Štefan Kender. Application of reverse engineering techniques in mechanics system services. *Procedia Engineering*, 48:96–104, 2012.

[3] Vanessa Gomes, Joaquim Reis, and Bráulio Alturas. Social engineering and the dangers of phishing. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–7, 2020.

[4] Zulfikar Ramzan. Phishing attacks and countermeasures. *Handbook of information and communication security*, pages 433–448, 2010.

5

Notes: A critical component of the work is the list of references. We have discussed their use earlier – here I simply make some notes on their presentation.

This is one of the hardest parts to get just right. BibTeX can help a great deal, but you need to put a good deal of care in to make sure that

- the references are in a consistent format;
- all information is correct; and
- the information included is in the correct style for the intended audience.

Details *really* matter in this section. It's easy to lose marks in this section.

ASH1925011M

ORIGINALITY REPORT

51%	37%	14%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Vanessa Gomes, Joaquim Reis, Braulio Alturas. "Social Engineering and the Dangers of Phishing", 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020 Publication	14%
2	www.mitnicksecurity.com Internet Source	10%
3	v1.overleaf.com Internet Source	9%
4	www.mimecast.com Internet Source	8%
5	sv.overleaf.com Internet Source	4%
6	Submitted to University of Adelaide Student Paper	4%
7	global.oup.com Internet Source	1%
8	www.coursehero.com Internet Source	

1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925011M

PAGE 1

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

PAGE 2

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

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

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

PAGE 3

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

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.

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

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

PAGE 4

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

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.

PAGE 5

Confused You have used **of** in this sentence. You may need to use **have** instead.

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

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.

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

PAGE 6

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.

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.

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

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

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.

PAGE 7

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

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

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.

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.

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

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

Article Error You may need to remove this article.

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

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.

Confused You have used **a** in this sentence. You may need to use **an** instead.

Prep. You may be using the wrong preposition.

Confused You have used **A** in this sentence. You may need to use **an** instead.

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