ASH1925018M

by Iftekhar Efat
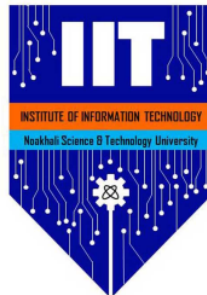
Phishing and scam in the Internet

Md Rokonuzzaman
ASH1925018M

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

This article is about phishing and scam on the internet. Phishing attacks target unsafe feature that exists in systems due to the human constituent. Nowadays many cyber-attacks spread for the weaknesses found in the mechanism of the end-user. Another keyword scam is relative to internet phishing. With help of phishing, an attacker can steal very personal and important data of the organization that will contribute to a big scam on the internet. Phishing is a huge threat and growing more widespread every year. 2021 Tessian research found that employees receive an average of 14 malicious emails per year.

[2]

1 Introduction

Present time refers to our world is called digital world and it's increasingly growing depending on the internet. With the internet, many people lead their life. The digital world is making our lives much easier by increasing the speed of communication, decreasing our travels, etc. Some digital dependency:

1. People do business on the Internet.

2. In education people like to share their knowledge and study online.

3. To make life easy people like to use digital electronic bank and payments transfers.

4. people like to share their personal life to the social media in the internet.

But at the same time it has many harmful side too.When an unethical snooping person or attacker try to exploiting vulnerabilities inherent in the design of applications and/or network security then its a big threat for the internet.They try to gain unauthorized access to the victims sensitive and critical information.They also use phychological tricks to fool people with phishing.The crime of stealing sensitive information often begins with a fraudulent email designed to lure a victim.As shown in Figure 1, the attacker sends a criminal email to steal sensitive information from the user. Email may contain a criminal link to steal sensitive information or email attachments (or both).

[2]

2 Background

To a large extent, the internet is the same with hip, tech-savvy, and young demographics. Highly influenced with pop culture and mainstream media, the modern Internet often seen in young entrepreneurs, juvenile delinquents, bloggers, social

Figure 1: Phishing attack
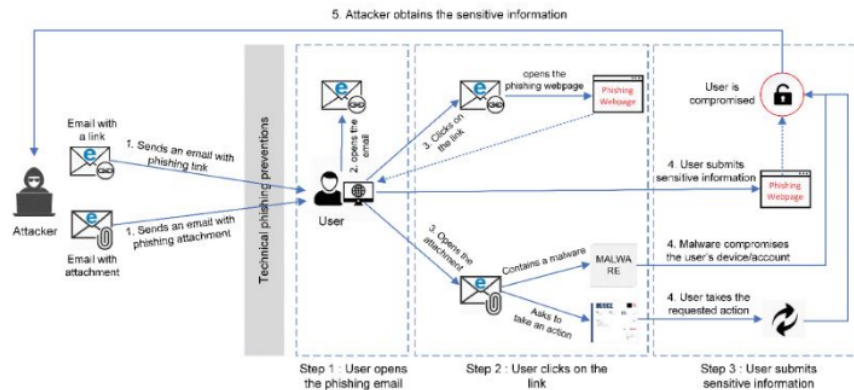
networking sites, online games, and file sharing. All things related to the older generation of internet users it seems to have been left out of the mix.There is many cause of falling in the threat of phishing scam. In might include:

- Growing Elderly Population.
- users lack security awareness.
- Criminals are (unsurprisingly) following the money.

The number of elderly people in the United States is growing at an alarming rate. According to the latest U.S. data. In the census, there are 35 million people Sixty-five or more live in the United States.It is easy to make the elderly foolish. The biggest door to cybercrime is, without a doubt, one that is labeled "security to know ". In particular, the lack of staff training is focused on issues such as ownership theft and ransomware are the main reasons for this successful attack. The main reason is this intent to steal money through the crime of stealing sensitive information of other people. [3]

3 Methods

Until recently, phishing scams relied heavily on fraudulent e-mails in order to launch a phishing scam. victims respond with information you want. The social networking sites these days are used to spread questionable links to lure victims to visit

criminal websites to steal sensitive information. Scammers use a variety of strategies and techniques to design criminal websites to steal sensitive information. These strategies can are divided into three basic groups:

1. Mimicking attack: In these attacks scammers often send an email to victims asking them to send it verify, update or verify their credentials by clicking the URL link within the email which will redirect them to a fake webpage. The Fishermen pay attention to you designing emails to be sent to victims using the same original logos website, or sometimes using fake HTTPS protocol. This type of attack is demeaning consumer confidence in electronics trading.

2. Forward attack: This attack starts when the victim clicks on a link displayed inside the email. He then redirected to the website asking her to submit his personal details. This information sent to a hostile server, and then the victim is transferred to the actual website using MITM technology.

3. Pop-up attack: Another method used by MITM is to encourage victims to bring their own information through a well-designed pop-up window. Fraudsters plead i victims who send their information through a pop-up window are highly regarded secure.

Figure 2: Email phishing
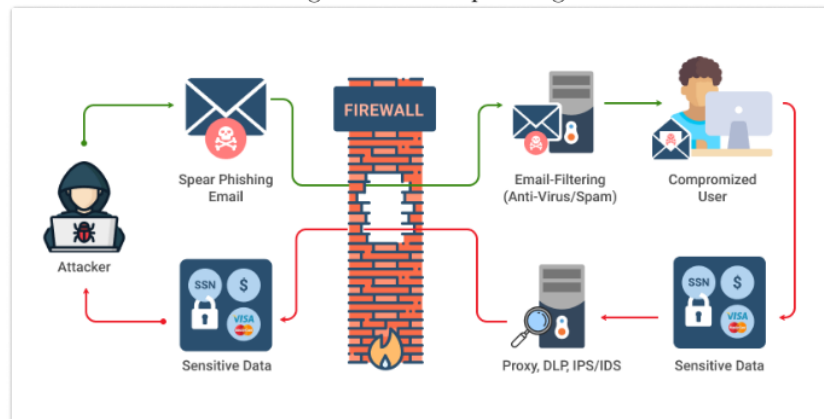
[5]

4   Results

The growth of internet and web services has it made life easier for most people. Some people enjoy selling stock online, some people like to buy music from their favorite artist on Amazon, and some people like to try to do fraud. In our work we

have highlighted the need for a strong online security model to address the emerging global issue of a criminal attack on the theft of sensitive information. Attacks on the crime of identity theft are also a very serious matter serious impacts worldwide. Anti-awareness measures attack strategies and tactics that can help reduce chances of becoming a victim. [4] [1]

5   Conclusion

In this study, we analyzed the effects of risk taking, decision-making, age, gender, and level of education about the effectiveness of the crime attack on identity theft. Theft of sensitive information is usually a process which scammers try to gain the trust of the victim and encourage them to open a phishing email for sensitive information, click the link (or open it infected attachments) and finally share sensitive information on the website of a phishing scam, such as bank account details or confidential information about their organization. If we understand the main reasons why people follow an attacker In each step of the crime of identity theft, this will help us to be more effective a system to prevent the attack of criminal theft of sensitive information every step of the way. These systems can work with existing technologies solutions to increase the level of prevention of identity theft both sensitive in our private and public life. [2] isn't usually needed.

References

[1] Neda Abdelhamid. Multi-label rules for phishing classification. *Applied Computing and Informatics*, 11(1):29–46, 2015.

[2] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9:44928–44949, 2021.

[3] Eric L Carlson. Phishing for elderly victims: as the elderly migrate to the internet fraudulent schemes targeting them follow. *Elder LJ*, 14:423, 2006.

[4] G Larcom and AJ Elbirt. Gone phishing. *IEEE Technology and Society Magazine*, 25(3):52–55, 2006.

[5] Rami M Mohammad, Fadi Thabtah, and Lee McCluskey. Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17:1–24, 2015.

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.

ASH1925018M

8 Submitted to University of Southern California
Student Paper

1 %

9 www.coursehero.com
Internet Source

1 %

10 Mohammad, Rami M., Fadi Thabtah, and Lee McCluskey. "Tutorial and critical analysis of phishing websites methods", Computer Science Review, 2015.
Publication

1 %

Exclude quotes   On
Exclude bibliography   On

Exclude matches   Off

ASH1925018M

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

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.

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.

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.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Confused You have used **its** in this sentence. You may need to use **it's** instead.

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

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.

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

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

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

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

(ETS) **Missing ","** You may need to place a comma after this word.

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

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

(ETS) **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.

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

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

(ETS) **Missing ","** You may need to place a comma after this word.