BOOK CHAPTER | Overcoming Phishing

Phishing Attack, Types, Mitigations and a Typical Case Study

Odirichukwu, Jacinta Chioma
Department of Computer Science
School of information and Communication Technology
Federal University of Technology, Owerri, Imo State, Nigeria
E-mail: chiomajaco6@gmail.com, jacinta.odirichukwu@futo.edu.com
Phone: +2348037394691

Abstract

The author reviewed phishing threat, types, solutions and real life typical experience. Phishing simply means pretending to be real but fake. Phishing attack is the act by which a social engineer (cybercriminal) attempt to obtain confidential information from individual(s) by sending message through social media/mails. This threat is one of the most popular cyber threats that many individuals have fallen victim of, hence, resulted to loss of money or assets. This paper elucidated different types of phishing attack namely; email phishing, https phishing, spear phishing, whaling/CEO phishing, vishing, smishing, angler phishing, pharming phishing, pop-up phishing, clone phishing, evil twin, and watering holes phishing. Possible guidelines on how to identify and avoid being attacked were given. Adhering to the discussed phishing Mitigations in this paper will help ICT user(s) from being victim(s) of phishing attack.

Keywords: Phishing, social engineer, fraud, cybercriminal, malicious actor.

Introduction

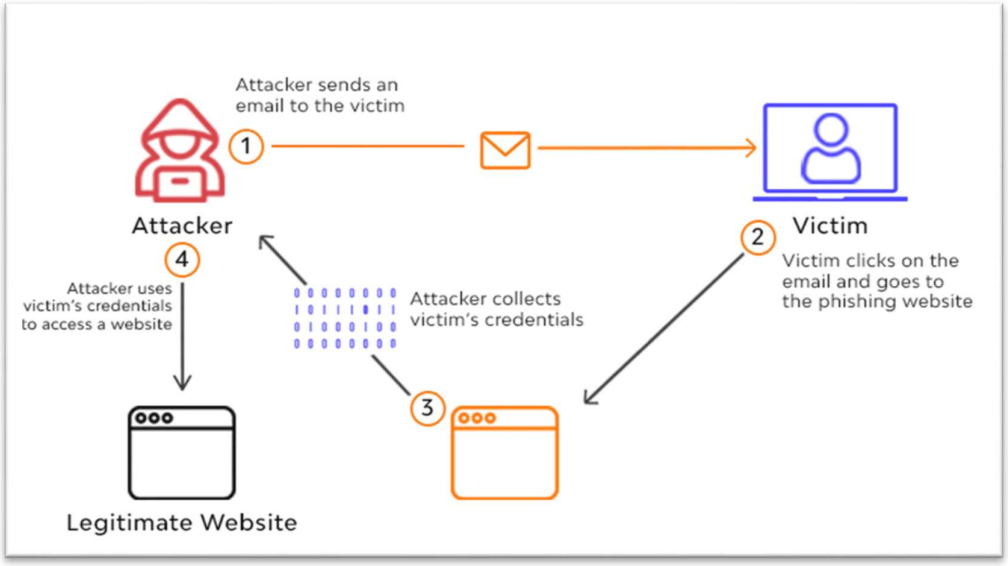
Phishing attack is the act by which a social engineer (cybercriminal) attempt to obtain confidential information from an individual by sending message through social media/mails. The message is meant to trick the recipient into installing malware on his or her computer or device or sharing personal or financial information (Ramzan, 2010). That is, convincing the victim to give some personal security information (e.g. password) by answering an email message or by going to a funny website and filling out a login form.

This is because;

i. Generally, the need for giving away the information, stems from fear of losing access to an important account (e.g. of on-line banking)
ii. The success of the scam lies not only on plausibleness of the initial approach, but also on the similarity of the phony website to the real one. It is one of the most worrisome threats to computer security nowadays (Odirichukwu, 2017).

Citation Odirichukwu, J.C. (2022). Phishing Attack, Types, Mitigations and a Typical Case Study. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 185 -190. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P31

Types of Phishing Attacks and How to Identify Them



Phishing Attack Scenario
Source: https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact

The following are the various type of phishing:

Email phishing
In email phishing attack, the social Engineer sends emails to individual(s) pretending to be from real organisation with the intent to lure the user(s) to open up a link or download app or video thereby allowing malicious software to be installed on the user(s) device. The aim is simply to hack confidential information from the victim.

How to identify email phishing:

To identity email phishing, look out for the following:

Legitimate information: Firstly, find out the contact information about the said establishment/company, identify wrong spellings, and fake email address domain.

Malicious and benign code: Avoid downloading or clicking any link at all for it contains malicious codes.

Shortened links: Run away from shortened links within an email content.

Fake brand logo: Avoid messages with faint logo.

Little text: Run away or delete any email containing little text and images.

HTTPS phishing

To increase security, hypertext transfer protocol secure (HTTPS) makes use of encryption technology which enables it to be considered a safe link to click. Due to the establishment of legitimacy, most organizations now use HTTPS instead of HTTP. Hence, cybercriminals are now making use of HTTPS in the links they put into phishing emails.

How to identify HTTPS phishing

The following will help identify https phishing:

Shortened link: Ignore the link if it does not contain all parts of the urls
Hypertext: Avoid clicking any part of the message that has hypertext.

Spear Phishing

This attack also uses email, howbeit the social actor here uses available intelligent gathering online tools to get different organisations websites and job positions of internal staff such as journal publishers websites assuming real positions like editor-in-chief to make the user(s) believe it is from original source. Most time, user(s) take action and become victim(s).

How to identify spear Phishing:

Abnormal request: Find out if that request is genuine by sourcing out the original site and reach to other internal position.

Shared drive links: Avoid link from shared drives from unknown person/organisation.

Password-protected documents: Avoid passworded document(s) from message not requested.

Whaling/CEO fraud

CEO fraud popularly known as whaling phishing uses open source intelligence to find out names of CEO of establishment(s) in order to lure the recipient(s) of message sent into assuming that the message is sent from the real CEO.

How to identify CEO fraud:

Abnormal request: In reality, one who has not had an initial contact with a CEO should not respond to such message.

Recipient email: Look out for work email with original domain name not personal email

Vishing

Visit is a call based attack whereby the social actor makes urgent request mostly at odd time where the recipient brain is too weak to think smarter. The attacker usually request for bank confidential details like card pin, date of birth and so on, for an urgent bank update. Sometimes, the attack threaten the recipient of loosing the account if the details is not provided urgently.

How to identify Vishing:

Caller number: The contact number is usually private or from an unknown location, but nowadays, the social actor uses real number, so do not respond to such request at all.

Timing: Such call is usually in line with a current event that is in line with such request. For instance, the case of BVN update in Nigeria, social actor took advantage of such update.

Requested action: The type of request is usually confidential information that should be always personal to the user. Personal information should always be personal.

Smishing

This is one of the most current form of attack employ by cybercriminals nowadays. The attacker usually send texts or chat requesting the recipient to open a link or download app/ video with the intent to steal information from the recipient if action is being taken by the recipient.

How to identify Smishing:

Delivery status change: Avoid text or chat requesting to click for a delivering status change. Always look for the original email with the company's domain name or go straight to your portal for a delivery status request.

Abnormal area code: Always check for the original area code by researching and comparing with your list.

Angler Phishing

This is a type of phishing attack where the social engineer trick the user to act using notification or chatting the user directly.

How to identify angler phishing:

Notifications: Avoid clicking on notifications that informed you of being included in an unsolicited group conversation of social media. It might contains hypertext that will move the user to web application that has malware.

Abnormal direct messages: Ignore direct message from someone that sound strange, and possibly requesting for download.
Link to websites: Ignore a direct message requesting to click on a link to a website if the user does not properly explain its purpose even when the websites appear legal.

Pharming

Pharming is a type of phishing attack where the cybercriminal employ a certain hacking technique to hijack a DNS (Domain Name Server is a server that translate IP address to website URL) such that when a user types a website URL, it redirects it to an illegal website IP address that appears genuine but contains malware.

How to identify pharming:

Insecure website: Ignore website that does not have https:// as url part.

Website inconsistencies: Avoid fake website with fake logo, images and spelling inconsistencies.

Pop-up phishing

This type of phishing attack used pop-up to lure the user into clicking thereby introducing malware into the devices.

How to identify pop-up phishing:

Irregularities: Review for spelling errors or abnormal colour schemes.

Shift to full-screen mode: Malicious pop-ups can turn a browser to full-screen mode so any automatic change in screen size might be an indicator.

Clone phishing
Here, cyber attackers research to gather information about the past services the users have used before, use such information to send email that seems legitimate to users.

How to identify clone phishing:

Abnormal timing: Beware of any unexpected email from a service provider, even one that is part of normal daily job function.

Personal information: Look out for emails requesting personal information that the service provider never asks for.

Evil twin phishing
Bam! Social actors know that some users need free Wi-Fi, here the come with unsecured free hotspot with the intent to steal confidential information of the user(s) as usual.

How to identify an evil twin phishing attack:

Unsecure: Do not connect to any hotspot (even familiar ones) that triggers an unsecure warning on a device.

Requires login: Ignore free hotspot that suddenly prompt for login.

Watering hole phishing
Here, the social engineer searches for recipient regular websites and infect such websites with code such that when click or download installs malware to steal confidential information.

How to identify watering hole phishing:
This brief Mitigations will guide against being victim to this attack:

Pay attention to browser alerts: Do not continue with a website when a browser indicate that it has malicious code.
Monitor firewall rules: Keep your firewall upto date (SecurityScorecard, 2021).

Case Study of Phishing Attack:
A typical case study of phishing attack could be seen from the chat below between the author and a suspected social Engineer on January 6, 2022:

[06/01 12:07] +234 705 366 3537: Gee e get watin i won give you if only you fit keep secret and hope say you get Android phone
[06/01 13:09] Dr. JACO: ?
[06/01 14:33] +234 705 366 3537: Watin just de be say if you promise me say u no go share this update with anyone except you don become boss on your own
[06/01 14:36] Dr. JACO: All ears
[06/01 14:36] +234 705 366 3537: I will send you a video that you watch so that you go understand the update wet I want teach you
[06/01 14:37] Dr. JACO: May I know you?
[06/01 14:37] +234 705 366 3537: Am Felix by name you might not know me I saw your contact on a group chat so I decided to message you about the update
[06/01 14:38] Dr. JACO: Very illegal
[06/01 14:39] Dr. JACO: You sound like a social Engineer
[06/01 14:47] Dr. JACO: What is your mission?
[06/01 14:48] Dr. JACO: Why the Intrusion attempt?
[06/01 14:49] +234 705 366 3537: Watch the video

[06/01 14:54] Dr. JACO: What are you intruding in someone's privacy?
[06/01 14:56] Dr. JACO: Only a village fool could watch a video sent by a social Engineer (cyber criminal).

You can see from the chat that as soon as he discovered I have caught him, he stopped chatting me.

Conclusion

This chapter reviewed phishing attack, different type of phishing attacks and how to identify them. A real life scenario of typical phishing attempt has been presented in this paper as a sample example of a typical approach social engineers use nowadays to attack social media users. The author also described Mitigations for each attack discussed.

Recommendation

Schools and Organisations heads should constantly involve their pupils, students and employees in training on how to identify cyber threats especially phishing attack and the possible Mitigations to avoid being victim(s).

References

1. Odirichukwu, J.C , Odii J. N, Adibe F. O, Okpalla C.L, Onwuama T.U. (2017). Combating Social Engineering Threats in Information Technology as a National Security Strategy. Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech 5(1), 59-66.
2. Ramzan, Z. (2010). Phishing attacks and countermeasures. In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.
3. SecurityScorecard, (2021). Retrieved from https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them (Accessed January 8, 2021).