The What, How and Why of Phishing ?

By Amos AKOGBE

What is Phishing?

Phishing is a common type of cyberthreats that is widely used by attackers to steal our data or to harm our system. Phishing is a fraud technique where a malicious actor sends messages impersonating a legitimate individual or organization, usually via email or other messaging system.

The main channel that is used for phishing attack is Email, and it uses human weaknesses to exploit possible vulnerabilities in the system like: obsolete OS or software, non-up-to-date antivirus or any possible vulnerabilities using malware file attachments likely.

But, the fact is that the threat is bigger than just what you just read below. There are numerous types of phishing attacks, but we will discuss here only about the eight common ones.

Why Phishing is so commonly used by attackers?

According to a trend, “in 2023, almost half (43%) of all successful attacks on organizations used social engineering, with 79% of these attacks carried out through email, SMS messages, social networks, and messaging apps.” from the article (Trends in phishing attacks on organizations in 2022–2023) by ptsecurity.com

Phishing attacks are thus very used by attackers because it is easy to implement and ways to learn how to craft a social engineering attacks are very opened. People are also very easy to trick since they are the target. Moreover, with the development of AI and technology, attackers are more and more equipped to craft the perfect social engineering attacks through phishing.

The main objective of phishing attacks are stealing personal data or credentials from users in order to perform more wide attacks on the organization’s systems through backdoors, spyware or virus installation on the network.

Type of Phishing attacks

Email phishing: Email phishing are fraudulent email that usually contains malicious malware or link and are sent to targeted user and impersonate real organizations. Its main goal is to ask the targeted user (user) to performs some actions that help the attackers to gain unauthorized access to the system or to steal, the user's personal data using trojans or other type of malware. The main channel used by the attackers to perform email phishing is, as it is said: Email.

Spear Phishing: Spear phishing attack specially target specific individual from an organization using fraudulent mail or message that are designed to specially plot them into a whole to steal their data or permissions to get access to more important data. The attacker often first gathers information about the person before starting the attack, such as their name, position, and contact details.

Vishing & Smishing : These two techniques are similar because they use a mean of telecommunication that is very popular, a phone. The trick that is used here is that the attacker impersonates someone you know and try convincing you to send your personal data or money. They can directly call you through phone or send you a message.

Type of Phishing attacks

Whaling attack : Whaling attack are phishing attacks that target higher-ups or any individual that hols a very important positions in an organization. It is therefore more elaborated and prepared, and is sometimes preceded by an intrusion among the close relations circle of the target to collect and study his habits. After that, the malicious mail or sms is then crafted to look very real and legal and is sent to the target.

Pharming : Pharming is direct across a group of users to trick them to click on an email link that is currently a malicious code installed on their computer and redirect them to a fake website that is used to steal their login credentials.

Pop-up phishing : This type of phishing exploits fake pop-ups to trigger an action from the user. Generally, when we start getting disturbed by a bunch of pop-ups, humans will do anything to, make them disappear. And that is this habit of users that is exploited by the attacker who place a malicious link or button in the pop-ups. Once it is clicked, it can install any malicious code on your computer.

HTPPS phishing : Most organizations today use HTTPS over standard HTTP to help establish the legitimacy of links. However, attackers can leverage HTTPS trust to make their links appear legitimate and increase the success of their phishing campaigns.

Type of Phishing attacks

Evil-twin phishing : Are performed specially on Wi-fi access point that seemed legitimate and are public. Once any client connect to this access point, the attacker is able to steal his credentials or have a certain level of access to his system data.

Watering hole phishing : This attack used any trend or very consulted website to find a way to infect the user's computer.

Deceptive phishing: The attackers present himself as a representative of a cybersecurity solution enterprise that wants to inform you that you are currently facing a cyberattack or attempt to break through your system and asked you to download or to use a link to get a solution that will help them support you to fight the attack In many cases the program to be installed is a malware.

Social engineering

When we talk about phishing, social engineering is the pick of phishing trick, because when you are victim of social engineering the method that is used is always the same: impersonating a relative, or a friend, that you trust to get you to send sensitive data about yourself and even steal your credentials.

A good example, is Facebook account hijacking. I have been the target so many times now, since I have my Facebook account, and all the times the source was the account of a friend of mine that have already fell for a social engineering attack (it’s replicable: same trick, different person). You are asked by the so-called friend to send you mail or your phone number that will be entered to get a reset password code to get back a stolen account.

How do I find out, it’s not my friend or my relative then?

Look and read well, re-read if it is necessary. The way of writing of your friend cannot be already known by the attacker, or maybe a detailed will betray him. But more importantly, call or join your friend or relative by another mean to ask,if really the message you received is from him.

How are IT systems doing vs Phishing attacks ?

Phishing attacks aimed at stealing info and data, also known as credential phishing, saw a 17% growth in 2023, with nearly 7 million detections. The trend saw minimal growth for known credential phishing detections at 5%, while unknown credential phishing detections leaped a significant 29%.

From https://www.trendmicro.com/vinfo/tmr/?/us/security/news/threat-landscape/email-threat-landscape-report-2023

However, the development of AI and computer vision as well as machine learning has really helped reduced the amount of successful attacks due to phishing. Users are also becoming more trained and conscious of the danger and of the existing threats.

Phishing is one of the main tools attackers use to obtain unauthorized access into organizations. In 2023, almost half (43%) of all successful attacks on organizations used social engineering, with 79% of these attacks carried out through email, SMS messages, social networks, and messaging apps.

From https://www.ptsecurity.com/ww-en/analytics/trends-in-phishing-attacks-on-organizations-in-2022-2023/

Best practices to adopt against phishing

As for most of the cyber threats that can damage any IT systems, the weakest point of failure remains humans, This is why it is crucial to train IT users about these cyberthreats in order to raise their security awareness against these types of attacks.

Here are four good habits that users should adopt, to reduce exposition to phishing attacks:

- Always look carefully at your mails
- Never click recklessly any link or document you receive from a certain source, always reach out by another channel to the supposed sender of the mail.
- Never use company or professional email for personal purpose
- Avoid connecting to a Public access point without using a VPN.

In addition, we need to implement the following methods and procedures to enhance the overall security posture of your organization: zero trust model, use network segmentation and defense in depth, use strong encryption and also multifactor authentication.

These methods and procedures are not the exhaustive list of what we can do to mitigate the risk of phishing attack. And it is the duty of all the users to ensure that they all shield against the potential threat that is phishing attack.