INTRODUCTION

Did you know more than 90% of data breaches and cyber attacks start with a phishing attack? Ever wondered why phishing is so widely used?

That's because it's easy to infiltrate into an organisation's network through this technique.

Malicious agents use Phishing methods to send legitimate-looking emails to users. These emails are designed to resemble legitimate businesses, and the goal is to trick the recipient into clicking malicious links and download malicious attachments. This will lead to revealing personal and sensitive information such as bank passwords & OTPs, social security numbers, birthdays, and other private data. It is the easiest way to gain entry into an organization. There is no foolproof way to block them as they leverage your end-users and highlight the problems of modern and remote work scenarios.

All phishing emails have the same goal - to compromise. Some target users' personal accounts knowing well that password reuse is common.

TYPES OF PHISHING ATTACK

1. Clone phishing
2. Spear phishing
3. Phone phishing
4. Malware based
5. Deceptive phishing
6. Session hijacking
7. Web trojans
8. DNS based attacks

> Phishing is the start to compromising your organization that allows bad actors to then traverse across systems and databases through the use of vulnerability exposure points. Attack surface management is a way to counter this inevitable situation - keeping ahead of knowing what is vulnerable and patching or putting in mitigating controls in place.

>> Here is a special glossary of Phishing terms to share, tweet, and spread awareness. Remember that April Fool's day comes once a year but threat actors would love to fool you every other day!

TYPES OF PHISHING ATTACK

CLONE PHISHING

In this type of attack, email addresses are replicated from a legitimate user or organization and sent to the target along with malicious links or viruses as attachments. This email is ultimately used to spoof an authentic user's email content and claim it is a simple resend. When you click on the attached link, it leads to the installation of malware or ransomware onto the systems. A Phisher can use clone phishing to gain a foothold to systems of the organization and infect other systems.

SPEAR PHISHING

Spear phishing is an attempt to obtain sensitive information such as financial documents or credentials to access a specifically targeted individual's computer system. Through spear phishing, threat actors acquire personal details of the victim and then disguise themselves as trustworthy entities through email or other online messaging.

PHONE PHISHING

Phone phishing is one of the widely used phishing attacks nowadays. In this type of attack, the attacker tricks the user with messages that gain their attention. Typically these messages are designed to encourage the user to share their personal details with them. The messages trick the user into believing that they have won a certain amount of money and by paying registration or by sharing personal information they get to claim the money. These days, threat actors have resorted to voice messages as well to steal private information.

MALWARE BASED

Malware-based phishing is where an attacker utilizes the duplicated email or a website to click downloadable links or software that installs malware on the system. The installed malware can use keylogger and screen loggers to record the keyboard strokes and track the user's actions. Then, the recorded actions are transmitted to the attacker's location.

DECEPTIVE PHISHING

Deceptive phishing attacks are scam emails sent in order to compromise information by requesting you to verify your account or request to change password. These attackers send scam emails on an extensive campaign and get lucky whenever someone gets fooled.

SESSION HIJACKING

A session hijacking attack is a type of mechanism where the session of the user is controlled, (which is usually managed by a session token). In this type of attack, the attacker uses the web session controller to trick the user and leverage the web server. For example, an attacker can record a user's banking application's web session and gain privileged access.

WEB TROJANS

Web trojans phishing are attacks executed through pop-ups while the user surfs a website which makes the session available to the attacker. When a user clicks on the pop-ups while performing bank transactions, it records all private information and transmits it back to the attacker.

DNS BASED ATTACKS

A DNS-based phishing attack is known as pharming, where the hackers use a duplicate of legitimate websites to acquire the users' IP addresses. The DNS in the system network is usually used to translate domain names into IP addresses for computer communications. In this type of attack, the user does not even know that they are entering their personal information in a redirected fraudulent website, giving long-term access to the attacker.

HERE ARE FEW THINGS YOU COULD DO TO STAY SAFE -

UNDERSTAND THE RISK

Organizations are at real risk here. Decision-makers need to fully understand what these attacks are ultimately trying to achieve and take action. A malware downloaded through a phishing link is enough to infect an entire network and an employee who is unaware of phishing could lead to a devastating cyberattack compromising your data, privacy, and reputation.

DEVELOP POLICIES

Consciously develop IT policies that adequately address email, website, working collaboration, social media, etc. at the workplace so that your employees do not fall prey to phishing. Make it easy to have suspicious emails quickly assessed by security teams.

BACKUPS

Having backups is never a bad idea, especially with escalating ransomware attacks. You can minimize the scope of loss or disruption when data can be restored quickly and securely.

EMPLOY ROBUST THREAT INTELLIGENCE

A real-time threat intelligence solution can defend and shrink your attack surface and keep your organization patched and updated against emerging threats.

THINK BEFORE YOU CLICK

Do not click on random links from unknown sources even if it proclaims you have won the jackpot! Threat actors have become more sophisticated and they may not fool you with the Nigerian Prince story, but they will try with another masterly deceptive email. They will target you through sites you use, people you know, and products you buy. Stay sharp.

Don't let the attackers fool you! Check your exposure today.
Write to us @ info@cybersecurityworks.com