PHISHING

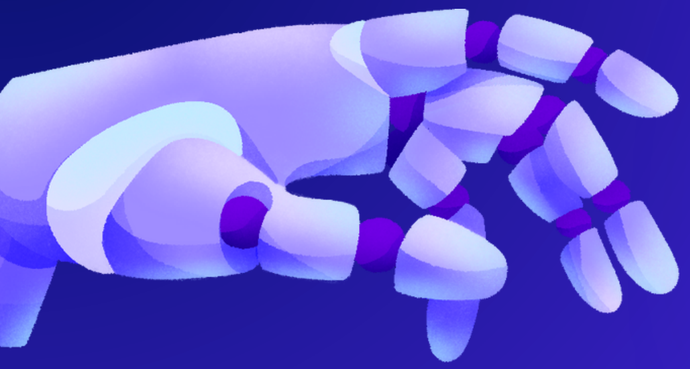
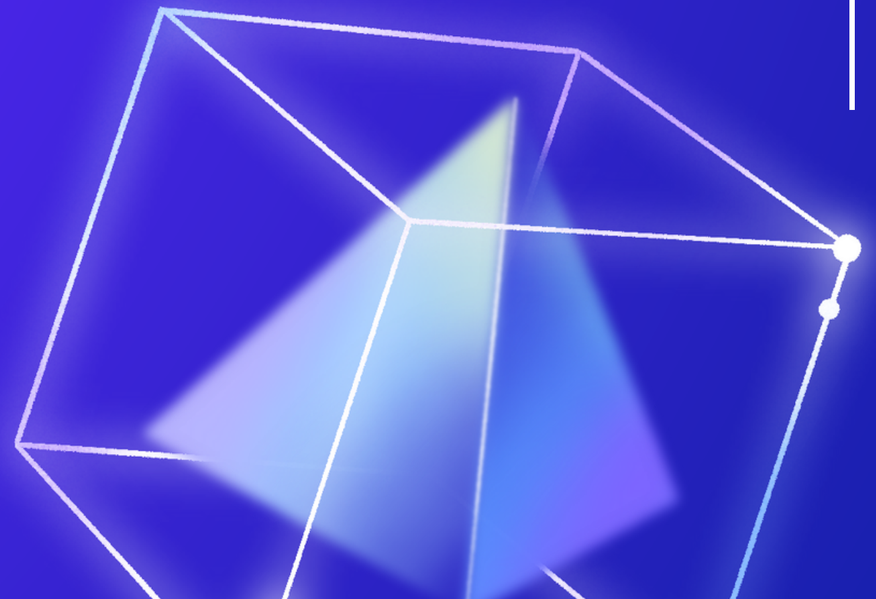


TABLE OF CONTENTS



INTRODUCTION

Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

WHY PHISHING AWARENESS IS IMPORTANT???

The reality is simple. Phishing attacks are more prevalent than ever before.

An estimated 3.4 billion fraudulent emails are sent out daily as part of phishing schemes, resulting in the FBI's Internet Crime Complaint Center (IC3) receiving over 651,800 phishing-related complaints annually.

Adjusted losses for affected organizations topped $2.4 billion, costing them losses of up to $17,700 per minute.

Although it's cause for concern, these numbers aren't here to scare you. These numbers are merely to raise awareness and help you make informed decisions.

PHISHING PROCESS

01

Savvy cyber criminals seek to contextualize their phishing attack by using large datasets from the dark web, to learn one or two facts about their targets

02

An attacker that seeks to pretend to be an authorized representative of one of your trusted service providers (for example, your bank), will then set the stage for interacting with you in a way that they believe will persuade you

03

Cyber criminals then launch the most essential portion of their attack: they communicate with you via email, SMS, or other means, to try to engage you in further interaction.

04

When they succeed in their attack, they may either use the information against you directly (for example, attempting to perform banking transactions with credentials you have revealed), or they may sell the information on the dark web.

TYPES OF PHISHING

SPEAR PHISHING

Spear phishing involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often first gathers information about the person before starting the attack, such as their name, position,

VISHING

Vishing, which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.

EMAIL PHISHING

In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

TYPES OF PHISHING

HTTPS PHISHING

An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.,

PHARMING

In a pharming attack, the victim gets malicious code installed on their computer. This code then sends the victim to a fake website designed to gather their login credentials.

CLONE PHISHING

A clone phishing attack involves a hacker making an identical copy of a message the recipient already received. They may include something like “resending this” and put a malicious link in the email.


HOW TO BE CAREFUL?

THINK BEFORE U CLICK!

Most phishing emails will start with “Dear Customer” so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.

USE FIREWALLS

High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they reduce the odds of phishers infiltrating your computer or network.

VERIFY SITE SECURITY

make sure the site’s URL begins with “https” and there should be a closed lock icon near the address bar. Check for the site’s security certificate as well.

KEEP UR BROWSER UP TO DATE

Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop.

CONCLUSION

- In conclusion, phishing poses a significant threat in our digital landscape, as highlighted in this presentation. We have delved into its definition, understanding why perpetrators engage in such malicious acts and explored the various types of phishing attacks. However, armed with knowledge, we can better protect ourselves and our organisations. By implementing robust safety measures such as multi-factor authentication, staying vigilant against suspicious emails, and educating ourselves continuously, we can fortify our defences against phishing attempts. Let us remember that awareness and proactive measures are our strongest allies in the fight against cyber threats.

THANK YOU!