DOES IT LOOK FISHY? THEN, IT IS PHISHING!

P.O.P TRAINING PRESENTATION: DAY 1

WWW.HERINTERNET.ORG

PHISHING:

DEFINITION:

Phishing is a tactic or method through which sensitive personal information such as usernames, passwords and financial details can be attained using any form of electronic communication.

This can be through; illicit emails, text messages, social networks or fake websites for financial gain or identity.

LET'S GET TO KNOW SOME FACTS ABOUT PHISHING!

Latest statistics suggest that more than 90% of all cyber-attacks begin with phishing attempts online.

The above fact currently places phishing as #1 cyber threat to any organization or company's data and its budget.

Some tactics often used include; quizzes, freebies and salacious stories that get clicked on and give hackers access to your data

Google blocks around 100 million phishing emails daily.

COMMON TYPES OF PHISHING (1)

Email phishing: Is the commonest tactic where phishing attacks are sent by email.

A hacker, for instance, can register a fake domain that mimics a genuine individual or organization and send out generic requests.

COMMON TYPES OF PHISHING (2)

Smishing: Here, the method of communication in a phishing attack is by SMS or text messages.

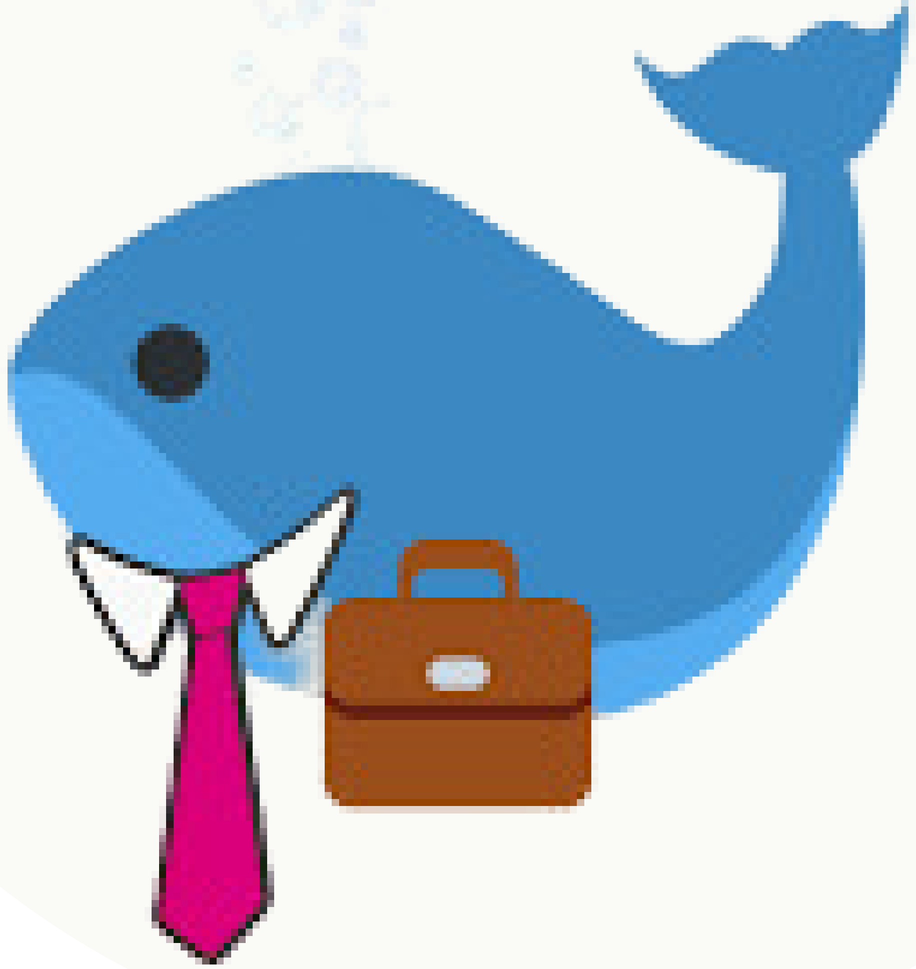
One of the most common smishing pretexts are messages supposedly from your service provider like your bank or telecom company alerting you of false suspicious activity for your immediate response.

COMMON TYPES OF PHISHING (3)

Vishing: Here, the method of communication used is phone or voice calls with a purpose to extract an individual's personal or corporate information.

COMMON TYPES OF PHISHING (4)

Spear phishing: This is a tactic that targets a specific individual or department within an entity for information of interest.



COMMON TYPES OF PHISHING (5)

Whaling: Aims for prominent individual(s) in positions of power because of their reputation.

EASY HINTS TO DETECT PHISHING SCAMS VIA EMAIL (1/2)

“Too Good To Be True” offers or statements that are eye-catching to attract your immediate attention like you won a lottery or lavish prize

Penalties or calls to action that beckon for your urgent response. For example; Airtel customers who are threatened by scammers to disconnect their network unless they update their personal details immediately.

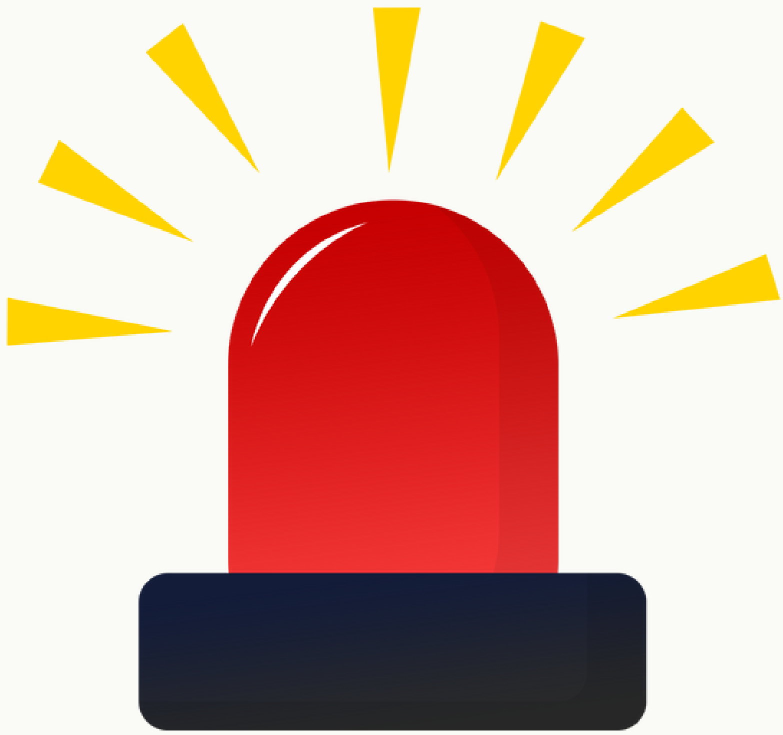
First time or infrequent emails that you don’t recognize or are not aware of.

EASY HINTS TO DETECT PHISHING SCAMS VIA EMAIL (2/2)

Misspellings and grammatical errors within the email addresses. These could be signs of deliberate attempts to evade filters.

Generic greetings as most organizations and companies today personalize their communication (They prefer to use an individual's first name rather than "sir" or "madam").

Shady links or unexpected attachments which can be detected by hovering over the link to show you the actual URL where you will be directed upon clicking on it.



SOME COUNTERMEASURES ON HOW TO AVOID OR MANAGE PHISHING ATTACKS ONLINE (1)

Utilize extra layers of digital safety on your socials and email accounts such as the 2FA, MFA.

Scan and update anti-virus and anti-spam software with the latest version. Include scanning of both incoming and outgoing emails and attachments.

Mention included attachments in the body of the email.

Always monitor the app permissions on your devices.

Stay up-to-date with information on new trends and solutions to cyber attacks.

SOME COUNTERMEASURES ON HOW TO AVOID OR MANAGE PHISHING ATTACKS ONLINE (2)

Avoid clicking hyperlinks or attached files in suspicious emails, socials or direct messages. (**#Tip:** Call the sender directly or visit your service provider physically to verify rather than clicking a link in an email).

Avoid over sharing personal information whether online or offline without caution

Check out website reliability often as you surf the internet.

Thank You