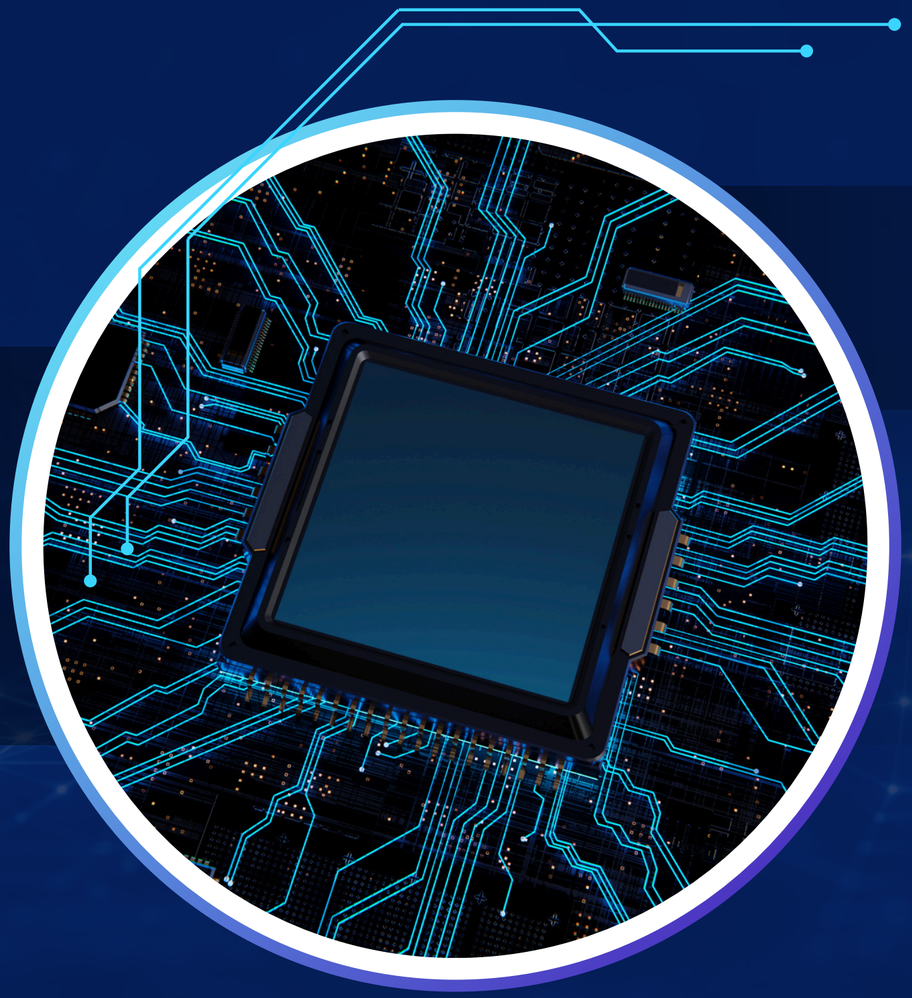
Cyber Security

Title: Phishing Awareness Training

Subtitle: Recognize and avoid phishing emails, websites, and social engineering attacks

CYBER SECURITY

Presented by: Rohit Kumar



Phishing Awareness Training

Phishing Awareness Training. You should explain that the session will help individuals understand what phishing is, how attackers use it to trick users, and most importantly, how to detect and prevent such attacks. Mention that phishing is one of the most common and dangerous threats in cybersecurity today, and awareness is the key to defending against it.

WHAT IS PHISHING?

phishing as a cyberattack where attackers impersonate legitimate organizations to deceive individuals into giving away sensitive data such as passwords, credit card numbers, or login credentials.

Explain that phishing is often delivered via email but can also occur through SMS (smishing), phone calls (vishing), or even social media messages. The main goal of phishing is to gain unauthorized access to personal or organizational data.

WHY IS PHISHING DANGEROUS?

Highlight that phishing attacks can lead to severe outcomes such as financial loss, identity theft, and data breaches. If successful, these attacks can compromise personal information or even the entire network of an organization. Also, emphasize that phishing is often a starting point for bigger attacks like ransomware or corporate espionage. Therefore, even a small mistake can have big repercussions.

TYPES OF PHISHING

Email Phishing

tart with email phishing, where bulk messages are sent to trick users. Then discuss spear phishing, which is more targeted and personalized.

Spear Phishing

Whaling targets high-level executives like CEOs and CFOs. Smishing and vishing involve SMS and voice calls, respectively, used to deceive the target.

Clone Phishing

Lastly, mention clone phishing, which uses a copied version of a real email with malicious content swapped in. Emphasize that attackers choose the type based on the victim’s role or vulnerability.

HOW TO RECOGNIZE A PHISHING EMAIL

Tell the audience to check for suspicious links by hovering the mouse over them to see the actual URL. Unknown senders, urgent language, or messages that demand quick action are red flags

Watch for generic greetings like “Dear Customer” instead of using your real name. Poor grammar or spelling errors are also common in phishing emails. Also, advise against downloading unexpected attachments.

PHISHING WEBSITE RED FLAGS

Explain that these sites often look like real ones but have slight URL differences, like spelling errors (e.g., gooogle.com instead of google.com). Mention that legitimate websites use HTTPS, so users should look for the lock icon in the browser.

ome phishing sites might have broken links, unusual designs, or ask for personal details right away. Encourage users to always double-check before entering any information.

SOCIAL ENGINEERING TACTICS

Attackers might pretend to be someone the victim trusts, like their boss or IT support. They create a sense of urgency or fear—saying accounts will be locked or warning of suspicious activity. Sometimes, they build trust over time by sending multiple emails or chatting on social media. This tactic, known as social engineering, manipulates human behavior rather than relying only on technical vulnerabilities.

HOW TO PROTECT YOURSELF

Start by saying that people should always be skeptical of unexpected or unusual messages. Advise not to click on links or open attachments from unknown sources.

Encourage the use of multi-factor authentication (MFA) to add an extra layer of security. Software and antivirus programs should be updated regularly.

Also, tell users to report phishing emails to IT departments or use reporting features in email services. Simply pausing and thinking before clicking can stop most phishing attacks.

WHAT TO DO IF YOU SUSPECT PHISHING

First, they should avoid clicking anything in the message and not respond. Instead, they should report it immediately. It’s a good practice to take a screenshot for documentation. The suspected sender should be blocked, and the device should be scanned for malware or viruses. If the person did click or enter details, changing passwords quickly is essential.

SUMMARY

Use this slide to wrap up the key points. Remind the audience that phishing is very common but can be prevented. Learning to recognize red flags, staying cautious online, and practicing safe behaviors are the best ways to avoid being a victim. Reinforce the idea that awareness and attention are the most powerful tools against phishing.

THANK YOU FOR YOUR ATTENTION

Presented by: Rohit Kumar