Phishing Awareness Training

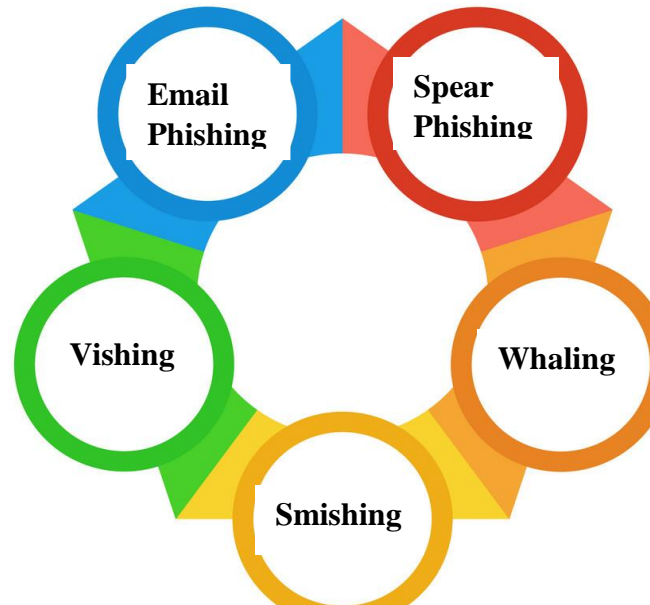By:

Dipali Hatwar

Introduction

Objective: To teach people about the risks of phishing and how to recognize and avoid phishing scams.

Phishing is a common type of cyber-attack that targets individuals through email, text messages, phone calls, and other forms of communication.

Types of Phishing
 Attacks

Email Phishing

Spear Phishing

Vishing

Whaling

Smishing

What is Phishing Email

A phishing email is a fake message sent by scammers to trick you into sharing personal information, like passwords or bank details. It often pretends to be from a trusted source and may include fake links or urgent requests.

Anatomy of phishing Email

Recognizing Phishing websites

• URL check: check unusual domains or misspellings.

• HTTP vs HTTPS: Legitimate sites typically use secure HTTPS connections. However, HTTPS alone does not guarantee safety.

• Example: Display visuals that highlight the differences between a genuine website and a fake (phishing) website for comparison.

Social Engineering Tactics

In-Person: Exploiting human interaction directly to manipulate individuals.

Phone: Using voice calls to trick targets into sharing sensitive information.

Digital: Leveraging emails, social media, or malicious websites to deceive victims.

How to Protect Yourself?

- Verify the sender: Always double-check the sender's email address for authenticity.
- Use strong passwords: Create unique, complex passwords for different account.
- Educate yourself: Stay informed about phishing tactics and train yourself to recognize them.
- Be cautious with emails: Avoid clicking on links or downloading attachments from unknown or suspicious emails.

Conclusion

Phishing is a common cyber threat where attackers steal personal information by posing as trusted entities. Stay safe by verifying senders, avoiding suspicious links, enabling multi-factor authentication, updating software, and reporting unusual activity to your IT team.