Phishing Awareness Training

By Rohith A

Phishing Awareness Training

Phishing attacks are increasingly sophisticated and can cause significant harm to individuals and organizations. This presentation aims to educate participants on recognizing phishing attempts, understanding their tactics, and adopting preventive measures.

What is Phishing?

Definition of Phishing

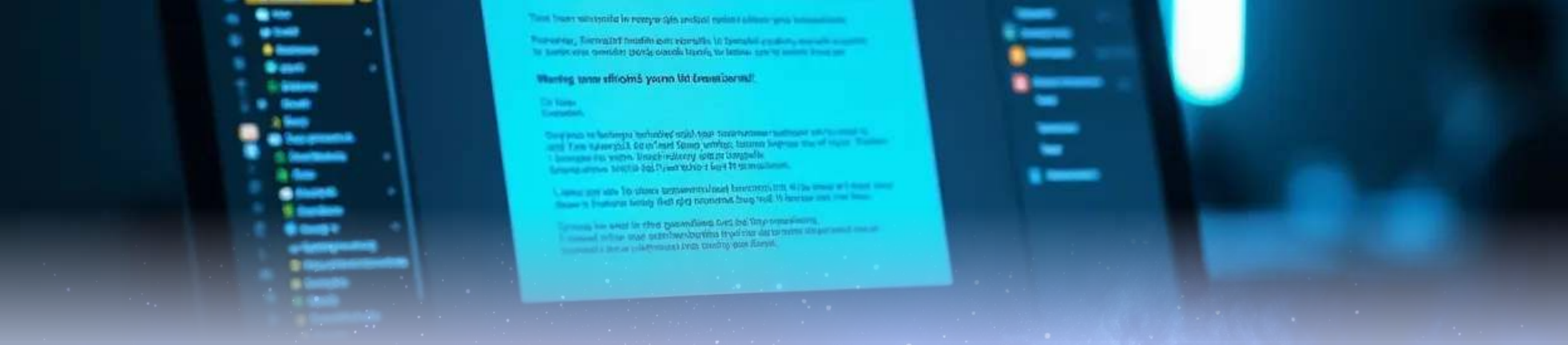
A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.

Types of Phishing

Includes spear phishing, whale phishing, and vishing targeting specific individuals, high-profile targets, or phone calls.

Impact of Phishing Attacks

Consequences include data breaches, financial loss, and reputational damage.



Recognizing Phishing Emails

1 Common Indicators

Phishing emails often contain suspicious sender addresses, generic greetings, and unusual requests for personal information. Look for typographical errors, poor grammar, and alarming subject lines that invoke urgency.

2 Hovering Links

Hovering over links without clicking can reveal the actual URL destination. If the link looks suspicious, it is likely a phishing attempt.

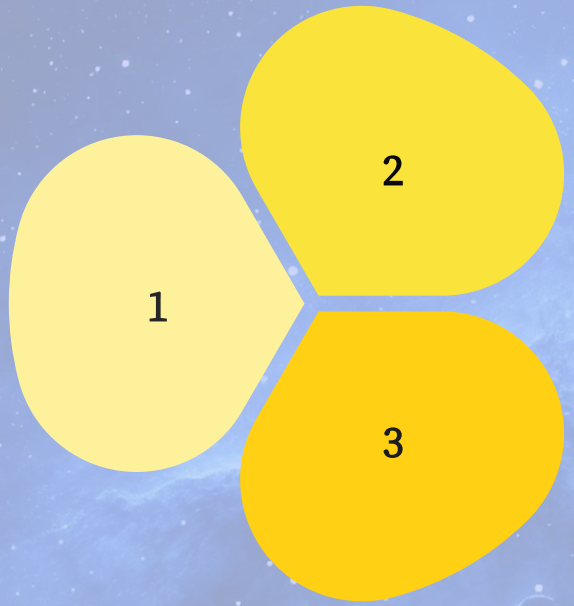
3 Attachments and Downloads

Be cautious of unsolicited emails with attachments or prompts to download files, as these may carry malware. Verify the sender's credibility.

Identifying Phishing Websites

URL Structure

Always verify the URL structure and ensure it matches the official website you intend to visit.



SSL Certificates

Ensure the website is secure and take note of any warnings displayed by your web browser.

Visual Design Cues

If the website feels off in any way, refrain from entering personal data until you can confirm its legitimacy.

Social Engineering Tactics

Manipulative Techniques

Phishing exploits emotions like fear, greed, or urgency.

Pretexting and Impersonation

Attackers impersonate trusted entities to gain credibility.

Building Trust and Rapport

Cybercriminals appear friendly to extract information over time.

Preventive Measures

Education and Training

Regular education helps identify phishing tactics and raises awareness.

Multi-Factor Authentication (MFA)

MFA adds security by requiring multiple verification factors to access accounts.

Reporting Mechanisms

Clear protocols for reporting phishing attempts ensure efficient responses.

Responding to Phishing Attempts

Step-by-Step Response

If you suspect a phishing email, report it to IT and delete immediately.

Account Recovery

Change passwords and enable multi-factor authentication if info is compromised.

Continuous Monitoring

Monitor accounts for unusual activity and heed alerts from financial institutions.

Conclusion and Key Takeaways

Importance of Awareness

Phishing is a formidable threat that exploits human vulnerabilities.

Adopting Best Practices

Encourage verifying sources and maintaining strong security measures.

Community Efforts

Staying informed about phishing tactics enhances overall security.