PHISHING AWARENESS TRAINING

Recognizing and Avoiding PhishingEmails, Websites, and Social Engineering Tactics

08-01-2025

CONTENTS

01

Identifying Phishing Emails

Common Characteristics of Phishing Emails

01 Suspicious Email Addresses

Phishing emails often come from addresses that mimic legitimate sources but have slight alterations, such as extra numbers or misspellings.

02 Generic Greetings and Salutations

Phishers typically use non- specific greetings like "Dear Customer" instead of personalized names, indicating a mass distribution technique.

03 Urgent Language and Threats

Phishing emails frequently use alarming language, urging immediate action to prevent supposed negative consequences, creating a sense of panic.

Techniques to Spot Phishing Emails

Hovering Over Links

Hover over links to preview the URL before clicking; phishing links often lead to unfamiliar or suspicious sites not matching the email's context.

Analyzing Email Headers

Review email headers to check the sender's true identity and ensure the message has not been spoofed or hijacked.

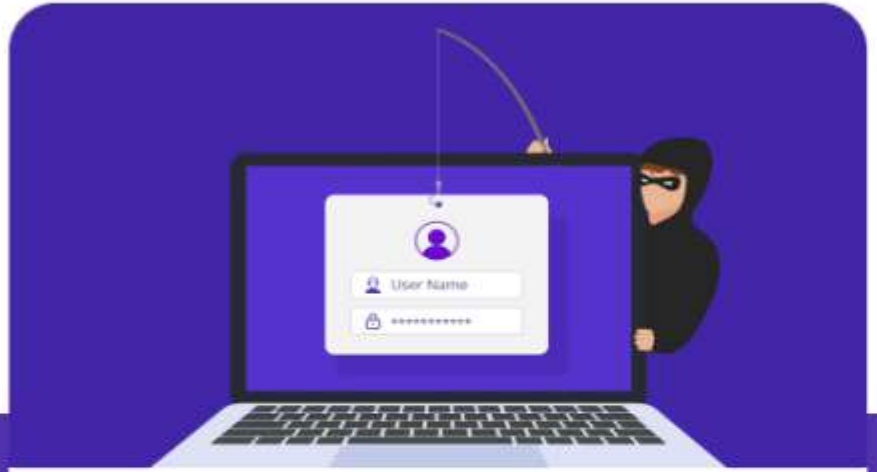
Awareness of Email Attachments and Embedded Links

Be cautious of unsolicited attachments or embedded links; they are common vectors for malware, often disguised as harmless files or familiar links.

02

Recognizing Phishing Websites

Indicators of a Fraudulent Website



URL and Domain Name

Examine the URL for misspellings or unusual characters. Look for slight variations in domain names that mimic legitimate sites.

Website Design and Content Quality

Assess the professionalism of the website's design and content. Poor- quality graphics, numerous typos, and inconsistent layout can indicate a phishing site.

Tools and Techniques for Verification

Using Safe Browsing Tools

Utilize modern browser features and plugins that alert users to potentially dangerous sites, helping to ensure safe browsing.

Checking Website Certificates

Verify the presence of a valid SSL certificate by looking for "https://" and a padlock icon in the browser's address bar.

Cross-referencing with Trusted Sources

Compare the website's information with data from authoritative sources. Trusted databases and directories can confirm the legitimacy of a site.

Understanding Social Engineering Tactics

Types of Social Engineering Attacks

Pretexting and Baiting

Pretexting involves creating a fabricated scenario to steal a victim's personal information. Baiting uses false promises to entice victims into harmful actions.

Quid Pro Quo Scams

Quid pro quo scams deceive victims by offering a service or benefit in exchange for information, exploiting their desire for help or an advantage.

Tailgating Techniques

Tailgating, or "piggybacking," occurs when an unauthorized person follows an authorized individual into a restricted area, bypassing security protocols.

Methods to Protect Against Social Engineering

01

Verifying Identities

Implementing strict identity verification processes helps ensure that only authorized individuals can access sensitive information or areas.

02

Educating on Common Scams

Training employees and stakeholders on the latest social engineering tactics increases awareness and reduces the likelihood of falling victim to scams.

03

Implementing Security Protocols

Enforcing comprehensive security protocols, such as restricted access and regular audits, mitigates the risk from social engineering attacks.

04

Prevention and Response Strategies

Best Practices for Individuals

01

Utilizing Two-Factor Authentication (2FA)

Two- Factor Authentication (2FA) adds an extra layer of security by requiring two forms of verification, thereby greatly reducing the risk of unauthorized access.

02

Regularly Updating Software and Patches

Keeping software up- to- date ensures that all known vulnerabilities are patched, preventing potential exploitation by hackers.

Organizational Measures

Conducting Regular Security Trainings

Regular security trainings educate employees on recognizing threats like phishing, securing sensitive data, and adhering to organizational security protocols.

Implementing Email Filtering Systems

Email filtering systems help in identifying and isolating suspicious emails, preventing phishing attacks and reducing the entry points for malware.

Establishing Incident Response Plans

An incident response plan outlines the steps necessary to quickly and effectively address a security breach, minimizing damage and facilitating recovery.

Thanks

BY ABHINANDAN BAIS

08-01-2035