Cybersecurity: Phishing Prevention Training

Spruce Point GROUP

What is Phishing?

Phishing is a cybercrime where attackers pose as a trustworthy entity to trick you into revealing sensitive information, such as passwords, credit card details, or personal data. Phishing can occur through emails, phone calls, or text messages.

Types of Phishing Attacks

1. **Email Phishing:** Attackers send fake emails pretending to be from a reputable organization, like your bank or an online retailer, to steal your login credentials or personal information.
2. **Spear Phishing:** This is a targeted attack on a specific individual or organization, often using personalized information to make the message more believable.
3. **Smishing:** Short for SMS phishing, smishing involves sending fraudulent text messages to trick you into revealing sensitive information or installing malware on your device.
4. **Vishing:** This type of phishing occurs through phone calls. Attackers may impersonate a representative from your bank or a government agency to gain your trust and steal your information.

LEARN

IDENTIFY

PREVENT

REPORT

Identifying Phishing Attacks

1. **Generic greetings:** If the message starts with "Dear Customer" or "Dear User," it may be a phishing attempt.
2. **Urgency:** Phishing messages often create a sense of urgency, like "Your account will be closed if you don't respond immediately."
3. **Suspicious links:** Hover over links to check if the URL matches the sender's organization. If the URL looks strange, don't click it.
4. **Poor grammar and spelling:** Phishing messages often contain errors or awkward phrasing.
5. **Unusual sender:** Check the sender's email address. If it's not from the organization it claims to represent, it may be a phishing attempt.

Preventing Phishing Attacks

1. **Enable two-factor authentication** (2FA) on all your accounts.
2. **Use a unique, strong password** for each account. Consider using a password manager to help you manage your passwords securely.
3. **Update your software and devices** regularly to patch any security vulnerabilities.
4. **Never share your personal information or login credentials** over email, text message, or phone call.
5. **Verify the legitimacy** of a message or call by contacting the organization directly through their official channels.

Report

Forward phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org.