Phishing Awareness Training

Introduction

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in electronic communications. It can have devastating results, leading to identity theft, financial loss, and more.

Common Phishing Tactics

1. Email Phishing: Fake emails that look legitimate.
2. Spear Phishing: Targeted attacks on specific individuals.
3. Whaling: Targeting senior executives.
4. Vishing: Voice phishing via phone calls.
5. Smishing: Phishing via SMS messages.

How to Recognize Phishing

1. Check the sender's email address.
2. Look for generic greetings.
3. Beware of urgent or threatening language.
4. Check for spelling and grammar mistakes.
5. Hover over links to see the actual URL.
6. Be cautious with attachments.

Prevention Tips

1. Use anti-phishing toolbars.
2. Verify a site's security before entering information.
3. Keep browsers up to date.
4. Use firewalls and antivirus software.
5. Educate yourself and your team.
6. Be cautious with emails asking for personal information.

What to Do if You Suspect a Phishing Attack

1. Do not click on any links or download attachments.
2. Report the email to your IT department.
3. Delete the email immediately.
4. Run a virus scan on your computer.
5. Monitor your accounts for any suspicious activity.

Conclusion

Phishing attacks can be highly damaging, but with awareness and caution, you can protect yourself and your organization. Stay vigilant, educate others, and always verify the authenticity of communications before responding.