Phishing Awareness Training

Learn to Recognize and Avoid Phishing Attacks

May 2025

What is Phishing?

Phishing is a cybercrime where attackers impersonate legitimate organizations to trick individuals into revealing personal information, such as passwords or credit card numbers.

Techniques:

- Email spoofing
- Deceptive links
- Fake websites mimicking trusted entities

Common methods: Emails, text messages, fake websites, phone calls

Types of Phishing Attacks

Email Phishing: Broad, unsolicited emails targeting many users

Spear Phishing: Targeted attacks on specific individuals with personalized information

Whaling: Attacks aimed at high-profile executives or decision-makers

Vishing: Voice phishing using phone calls to extract information

Key Point: Each type uses tailored approaches to maximize deception

Impacts of Phishing

Consequences:

Significant financial loss
Data breaches
Identity theft

Statistic: Over 90% of data breaches are caused by phishing

Takeaway: Vigilance and education are critical to prevent these outcomes

Recognizing Phishing Emails

Look for these red flags:

- Unexpected emails requesting urgent action
- Spelling or grammar mistakes
- Suspicious sender addresses (e.g., `support@amaz0n.com`)
- Generic greetings (e.g., “Dear Customer”)
- Links or attachments you didn’t expect

Spotting Fake Websites

Check for these signs:

- Incorrect URLs (e.g., `amaz0n.co` instead of `amazon.com`)
- Missing "https://" or a padlock icon
- Poor website design or broken links
- Requests for sensitive information (e.g., passwords, credit card details)
- No contact information or privacy policies

Social Engineering Tactics

Phishers manipulate emotions to bypass defenses:

Fear: “Your account will be locked!”

Greed: “You’ve won a prize!”

Trust: Impersonating a colleague or authority figure

Curiosity: “Click to see exclusive content!”

How to Stay Safe

Protect yourself with these steps:

Hover over links to check the URL before clicking

Avoid opening unexpected attachments

Enable two-factor authentication (2FA)

Verify requests directly (e.g., call the company)

Keep software and antivirus updated

Interactive Quiz

Is this email suspicious?

"Dear User, Your bank account is at risk. Click here to secure it now."

Yes: Urgent, vague emails are a red flag.

No: This email uses urgency and lacks personalization, which are phishing signs.

Conclusion

Phishing attacks rely on deception, but you can stay safe by:

- Being skeptical of unsolicited requests
- Verifying sources independently
- Staying informed about new tactics

Stay vigilant and keep learning!