Phishing Attacks: Recognize, Resist, Respond

An interactive awareness module for employees and students

Learning Objectives

- By the end of this module, you will be able to:
- • Define phishing and identify common types.
- • Recognize phishing emails and fake websites.
- • Understand social engineering tactics.
- • Apply best practices to prevent phishing attacks.

What is Phishing?

- Phishing is a type of cyberattack that uses deceptive messages (often emails) to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal data.

- Common forms include:
- • Email phishing
- • Spear phishing
- • Whaling

How to Recognize Phishing Emails

- Look for these red flags:
- • Urgent or threatening language ('Your account will be locked!')
- • Suspicious links or attachments
- • Sender’s email address doesn’t match the organization
- • Grammar or spelling mistakes
- • Requests for personal or financial information

How to Identify Fake Websites

- Check for:
- • Insecure URL (missing https://)
- • Misspelled domain names (e.g., go0gle.com)
- • Unusual design or poor grammar
- • Fake login pages asking for credentials
- • No contact information or privacy policy

Social Engineering Tactics

- Attackers exploit human emotions and trust. Common tactics include:
- • Fear and urgency — 'Your account has been compromised!'
- • Authority — 'This is your bank manager calling.'
- • Curiosity — 'You’ve won a reward!'
- • Sympathy — 'Help a colleague in need.'

Best Practices to Avoid Phishing

- • Verify sender identity before clicking links.
- • Hover over links to preview URLs.
- • Use multi-factor authentication (MFA).
- • Report suspicious emails to IT/security team.
- • Keep software and antivirus updated.

Real-World Examples

- • 2016: Hillary Clinton campaign targeted by spear-phishing emails.
- • 2020: COVID-19 vaccine scams tricked users into sharing data.
- • 2022: Fake Microsoft 365 login pages used in business email compromise (BEC) attacks.

Interactive Quiz (Discussion)

- 1. You receive an email from 'support@micros0ft.com' asking to reset your password. What should you do?
- 2. The email includes a link to 'http://login-security-update.com'. Would you click it?
- 3. What are some signs this might be phishing?

- Discuss with your peers or choose the best answer.

Summary & Key Takeaways

- • Always think before you click.
- • Verify sources before sharing information.
- • Stay updated on phishing trends.
- • Report suspicious messages immediately.

Thank You!

- Stay cyber safe!
- For more information, contact your IT Security Team.