PROTECTING YOURSELF FROM PHISHING ATTACKS

PRESENTED BY

PRAGATI BHAGAT

WHAT IS PHISHING?

- Phishing is a type of cyberattack where attackers trick individuals into sharing sensitive information by pretending to be trustworthy entities.
- Examples:
- Fraudulent emails
- Fake websites
- Deceptive phone calls

COMMON PHISHING TACTICS

- Email Scams: Fake emails claiming to be from banks, companies, or government agencies.
- Fake Websites: Sites designed to mimic legitimate ones to steal login credentials.
- Social Engineering: Manipulating people into revealing confidential information.
- Smishing and Vishing: Phishing via SMS or voice calls.

RECOGNIZING PHISHING EMAILS

- Look for:
- Suspicious Sender Addresses: Unknown or slightly altered domains.
- Generic Greetings: 'Dear Customer' instead of your name.
- Urgent Language: Claims like 'Act Now' or 'Your Account Will Be Closed.'
- Spelling and Grammar Errors: Poorly written messages.
- Unusual Links or Attachments: Hover over links to check their destination.

AVOIDING PHISHING ATTACKS

- Think before you click: Avoid suspicious links.
- Verify the source: Contact the organization directly if unsure.
- Use strong passwords and multi-factor authentication (MFA).
- Keep software and antivirus updated.
- Report phishing attempts immediately to your IT or security team.

REAL-LIFE PHISHING EXAMPLES

Example 1: Suspicious Email

•**Red Flags Highlighted**:

- •Suspicious sender email -eg.admin@bank-secure-update.com)
- •Urgent tone: “Your account will be closed if you don’t act now.”
- •Hover-over link showing a fake domain.

Example 2: Fake Website

•**Signs of a Fake Site**:

- •URL slightly altered –eg: paypa1.com instead of paypal.com
- •Poor design or spelling errors.
- •Requests sensitive information like passwords or SSNs.

CONSEQUENCES OF FALLING FOR PHISHING

For Individuals:

- Financial loss.
- Identity theft.

For Organizations:

- Data breaches.
- Damage to reputation.
- Legal penalties.

REPORTING PHISHING ATTEMPTS

- How to Report:
- Forward suspicious emails to your IT or security team.
- Use built-in email reporting features, e.g.Report Phishing.

- Why Reporting Matters:
- Helps others stay safe.
- Prevents further attacks.

FINAL TIPS AND RESOURCES

- Key Takeaways:
- Keep learning about cybersecurity.
- Share knowledge with others.

- Resources:
- Official cybersecurity websites, eg. NIST, FTC.
- Company’s internal phishing awareness materials.

THANK YOU