Title:
Phishing Awareness Training

Subtitle:
Learn To Recognize and Prevent Online Threats

What is Phishing?

- Phishing is a cyber attack where attackers trick users into revealing personal info.
- Usually done via emails, fake websites, texts, or phone calls.

Why Phishing Matters

- Over 90% of cyberattacks begin with phishing.
- Organizations lose millions due to phishing scams.
- Real-world cases: Facebook & Google lost \$100M to phishing scams

Phishing Tactics

Urgency: “Act now or lose access!”
Authority: Pretending to be your boss or IT team.
Fear: Your account has been compromised!”
Reward: “You’ve won a prize”

How to Spot Phishing Emails

- Check sender’s email address carefully.
- Look for generic greetings like “Dear user”.
- Beware of urgent or threatening language.
- Spelling/grammar errors are common.
- Avoid clicking suspicious links or attachments.

How to Spot Fake Websites

- Check for HTTPS and a padlock icon.
- Watch for misspelled URLs (e.g., goOgle.com).
- Poor layout or broken links.
- Sites that ask for personal info immediately.

Best Practices to Stay Safe

- Think before you click on links.
- Verify unexpected emails before acting.
- Use unique, strong passwords.
- Enable multi-factor authentication.
- Report suspicious messages to your IT team.

Real-World Examples

- Fake bank email asking to verify your account.
- CEO fraud: email asking finance to send urgent payment.
- Job offer email with malware-infected attachment.

Quiz Time!

- What should you do if you get a suspicious email?
- True or False: All HTTPS sites are safe.
- Identify the fake URL:
  www.goOgle.com vs
  www.google.com

Final Tips & Reporting

- Stay alert and cautious online.
- Always verify before clicking or replying.
- Report phishing attempts to the IT/security team.
- Security is everyone’s responsibility.