🎯 TITLE : Phishing Awareness Training: Recognize, Avoid, Report

⍰ Module Structure:

- Introduction to Phishing
- Types of Phishing Attacks
- How to Recognize Phishing Emails
- Phishing Websites and Social Engineering
- Real-World Examples
- Best Practices & Prevention Tips
- Quiz & Interactive Scenarios
- Reporting Phishing
- Summary and Final Tips

🔍 1. INTRODUCTION TO PHISHING

Title: What is Phishing?

➡ **Content:**

- Phishing is a **cybercrime** where attackers trick individuals into providing sensitive information like usernames, passwords, and bank details.

- Done via **email**, **text**, **calls**, or **fake websites**.

➡ **Diagram Idea:**

Flowchart showing:

Phisher → Fake Email → User Clicks Link → Enters Credentials → Data Stolen

🎭 2. Types of Phishing Attacks

Title: Common Phishing Methods

➡ **Content:**

- Email Phishing: Fake emails pretending to be from trusted companies.
- **Spear Phishing:** Targeted attacks with personalized content.
- **Whaling:** Targeting executives or high-level employees.
- **Smishing:** Phishing via SMS.
- **Vishing:** Voice phishing over phone calls.
- **Pharming:** Redirecting users from real websites to fake ones.

📧 3. How to Recognize Phishing Emails

Title: Spot the Red Flags

Content:

- Suspicious sender address
- Urgent or threatening language ("Your account will be suspended!")
- Generic greeting ("Dear user")
- Attachments or links asking for personal data
- Spelling/grammar errors

🌐 4. FAKE WEBSITES & SOCIAL ENGINEERING

Title: Don’t Trust Every Link

➡ **Content:**

- Fake websites mimic real ones
- URL tricks: "www.faceboook.com"
- SSL padlock doesn’t always mean safety
- Social engineering manipulates human emotion (fear, trust, urgency)

🌐 5. Social Engineering Tactics

- - Impersonating authority figures
- - Creating panic
- - Offering fake rewards
- Example: Fake email from HR asking to log in to new system

⍰ 6. BEST PRACTICES TO PREVENT PHISHING

Title: Stay Protected with These Tips

Tips:

- Never click suspicious links
- Verify sender address manually
- Use two-factor authentication (2FA)
- Hover over links to preview URL
- Report suspicious messages
- Keep your software and antivirus updated

⍰ 7. INTERACTIVE QUIZ

Q1: Which is a red flag?

- a) Personal greeting b) Urgent tone c) Correct grammar
- Answer: b

Q2: Suspicious URL asks for password. What do you do?

- Answer: Close and report it

- Q3: True/False: HTTPS = Safe
- Answer: False

🔍 8. Real-World Examples

Title: Case Studies

Example 1:

- **Target Breach (2013)** via phishing email to HVAC vendor
- **Result:** 40 million credit card numbers stolen
- **Example 2:**
- **Google & Facebook** lost $100M to fake invoice phishing

✓ 9. Summary & Final Tips

Title: Key Takeaways

➡ **Content:**

- Phishing is one of the most common cyber threats
- Think before clicking
- Always verify the source
- Report and help protect others
- **Call to Action:**
  “Be smart. Be safe. Be cyber-aware!”

thank you