Phishing Awareness Training Module

Name:Namrata Nitin Kamble

Domian:Cyber Security

Introduction to Phishing:

Definition: Phishing is a type of cyberattack where attackers impersonate legitimate entities to trick individuals into providing sensitive information such as passwords, credit card numbers, or other personal data.

Goal: To educate participants on how to identify and avoid phishing attempts.

Common Types of Phishing Attacks

- Email Phishing: Fake emails that appear to come from trusted sources.
- Spear Phishing: Targeted phishing aimed at specific individuals or organizations.
- Clone Phishing: Duplicate emails prviously sent by a legitimate source, with malicious content.
- Smishing: Phishing attempts sent via SMS or text messages.
- Vishing: Voice phishing using phone calls to gather sensitive data.

How to Identify Phishing Emails:

Suspicious Sender Addresses: Look for unusual or misspelled email addresses.

Urgent or Threatening Language: Phrases like “Your account will be closed” or “Immediate action required.”

Spelling and Grammar Errors: Legitimate organizations usually have well-written communications.

Unfamiliar Links: Hover over links to check the real URL.

Attachments: Be cautious with unexpected attachments.

Real-Life Examples of Phishing Attacks

Example 1: A fake bank email asking for account verification.
Example 2: An imitation of a popular online service requesting password resets.

Tips to Avoid Phishing Scams

Verify the Source: Double-check sender information.
Don’t Click on Unverified Links: Navigate to the website directly by typing the URL.
Keep Software Updated: Ensure your anti-virus and software are current.
Use Multi-Factor Authentication (MFA): Adds an additional security layer.
Be Skeptical: If it seems too good to be true, it probably is.

Social Engineering Tactics

Pretexting: Fabricating scenarios to gain information.
Baiting: Offering something enticing to induce a response.
Tailgating: Physically following someone to gain access to a restricted area.

Steps to Take if You Suspect Phishing

Do Not Respond: Avoid replying to suspicious messages.
Report the Incident: Notify your IT department or use built-in reporting tools.
Change Your Passwords: Secure your accounts if you clicked on a phishing link.
Run a Security Scan: Check your devices for malware.

Conclusion:

Phishing attacks remain one of the most prevalent and dangerous threats in cybersecurity. By understanding their tactics, recognizing warning signs, and adopting proactive measures, individuals and organizations can significantly reduce the risk of falling victim to these scams. Ongoing vigilance and education are key to staying safe in today’s digital landscape.