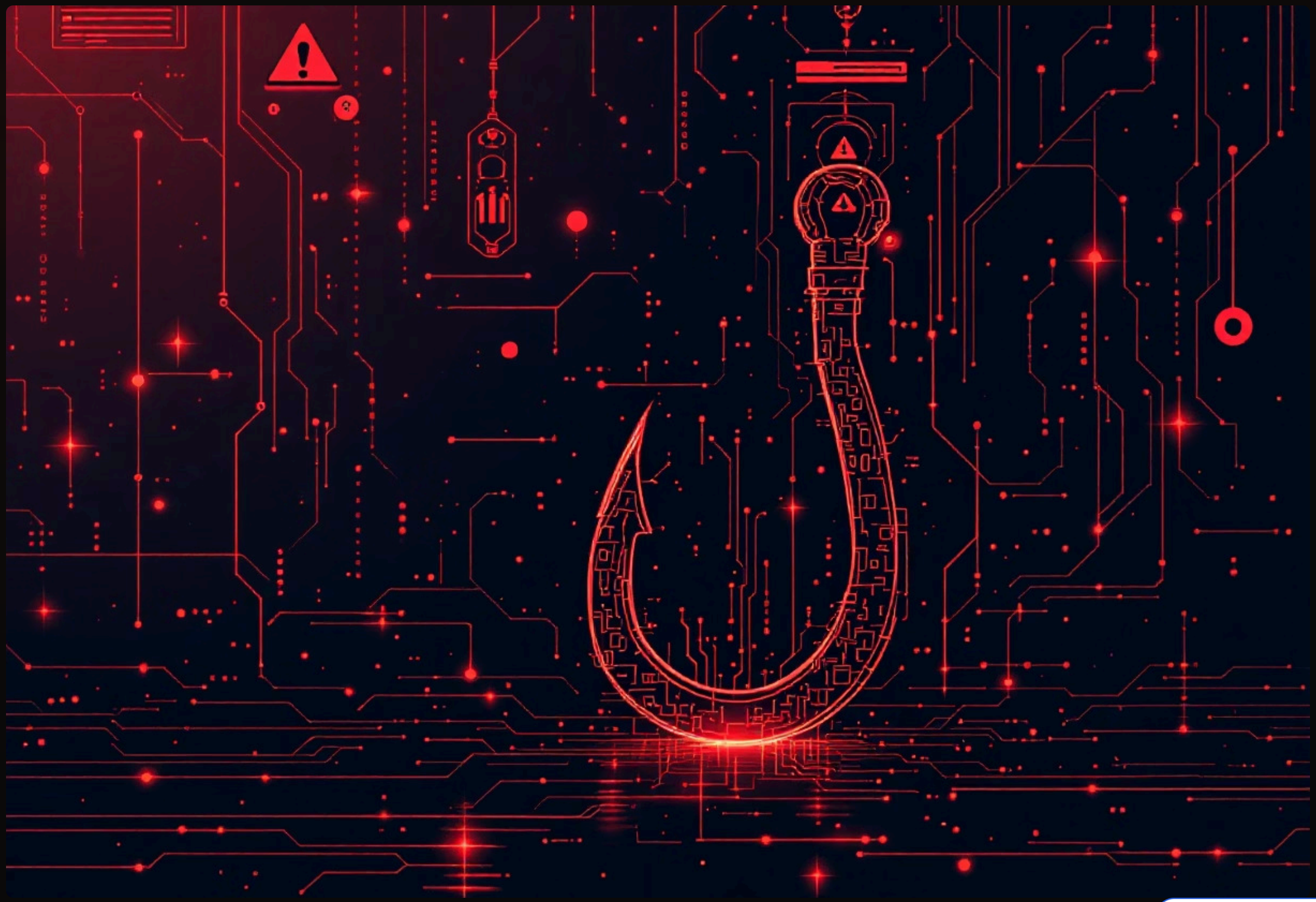
Phishing Awareness Training

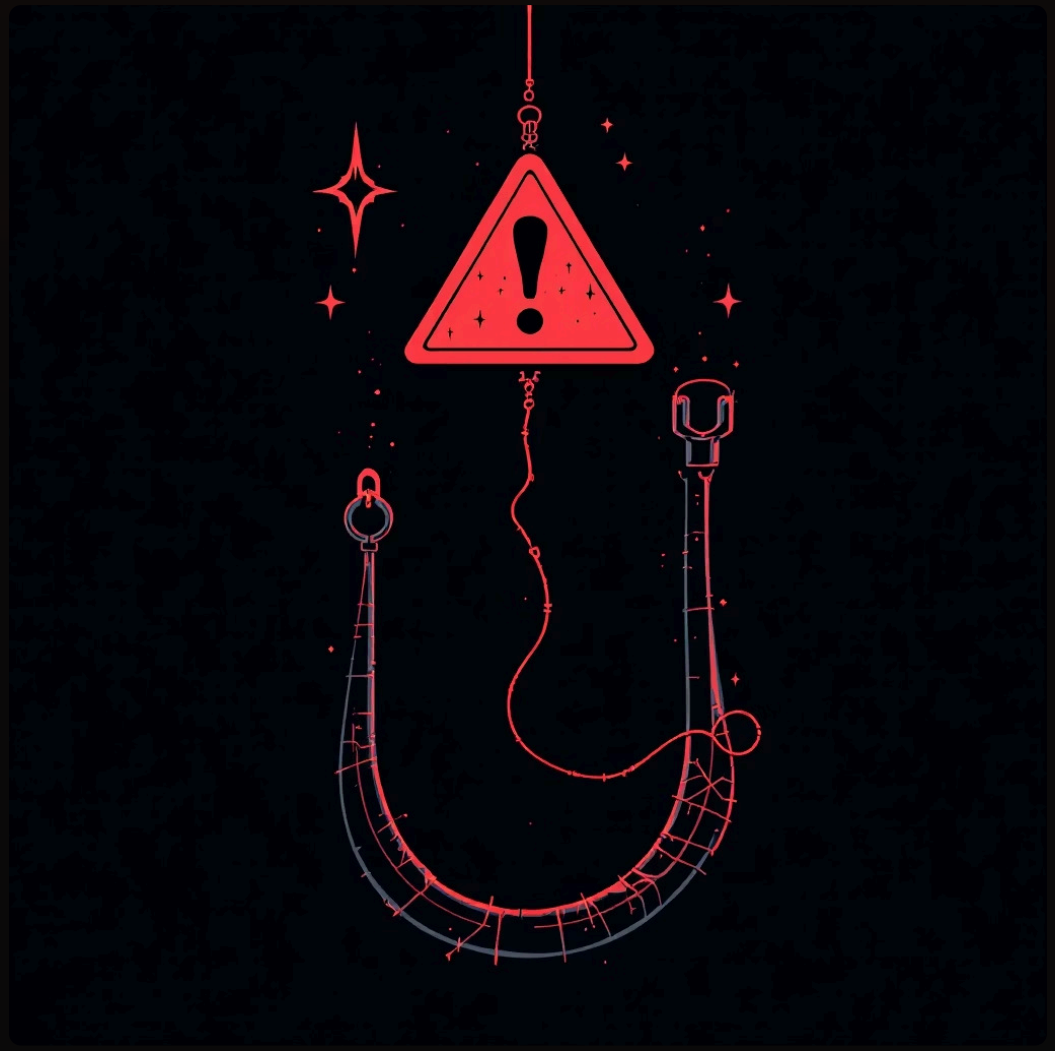
Protect Yourself from Online Scams and Attacks



Phishing Awareness Training Module

Title Slide

- **Title:** Phishing Awareness Training
- **Subtitle:** Protect Yourself from Online Scams and Attacks
- **Visual:** Image of a phishing hook or a warning sign.
- **Optional:** Company logo if for corporate training.



What is Phishing?

Definition

Phishing is a type of cyber attack where attackers trick individuals into revealing sensitive information like passwords, credit card numbers, or personal details.

Visual: Diagram showing attacker → fake email/website → victim → stolen info.

Key Point: Often delivered via email, messaging apps, or websites.

Common Types of Phishing

1

Email Phishing

Emails pretending to be from a trusted source (banks, companies).

2

Spear Phishing

Targeted attacks using personal information.

3

Smishing

Phishing via SMS/text messages.

4

Vishing

Phone call scams to extract sensitive info.

5

Clone Phishing

Copying legitimate emails with malicious links.

Visual: Table with type, example, and warning signs.

How to Recognize Phishing Emails

Check the Sender

Look for suspicious email addresses.

Look for Urgency

"Act Now!" or "Your account will be closed!"

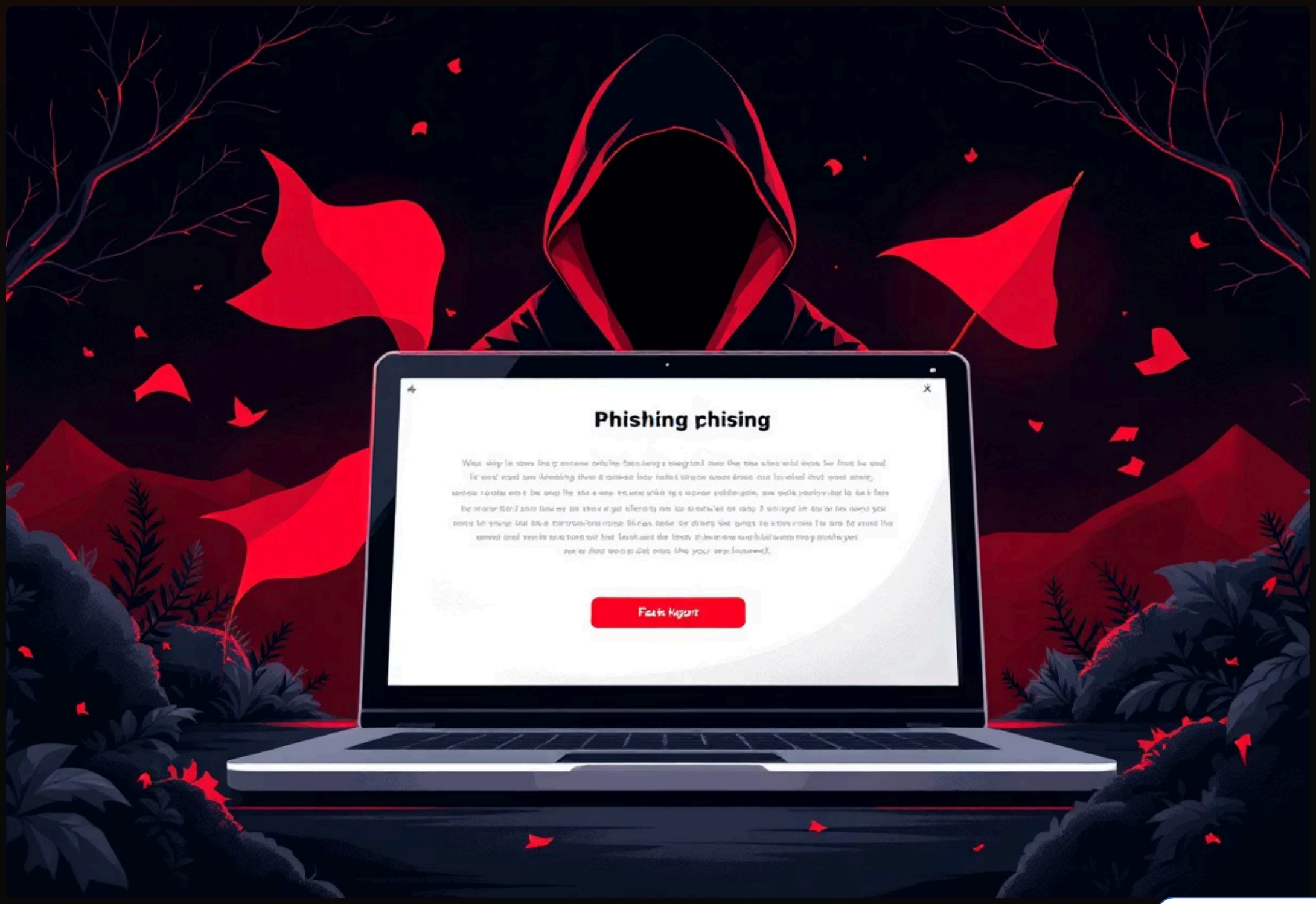
Check Links Before Clicking

Hover over URLs to see destination.

Beware of Attachments

Avoid downloading unknown files.

Visual: Screenshot of a phishing email with highlighted red flags.



How to Recognize Fake Websites

01

Check the URL

Look for typos, extra characters, or strange domains.

02

Check HTTPS & SSL Certificate

Ensure the padlock icon is present.

03

Verify Contact Info

Legitimate websites usually provide verifiable contacts.

Visual: Side-by-side comparison of real vs fake website.

Social Engineering Tactics

Impersonation

Pretending to be someone trustworthy.

Urgency & Fear

"Your account is compromised!"

Rewards & Incentives

"Claim your prize now!"

Emotional Manipulation

Gaining sympathy or trust.

Interactive: Ask participants: *"Which tactic is being used in this email?"* (Provide a fake email screenshot for them to identify.)

Best Practices to Avoid Phishing

- Never click unknown links.
- Verify the source of messages or emails.
- Use strong, unique passwords.
- Enable two-factor authentication (2FA).
- Regularly update software and antivirus programs.
- Report suspicious emails to IT/security team.

Real-World Examples

Example 1

2016 Dropbox phishing campaign.

1

2

Example 2

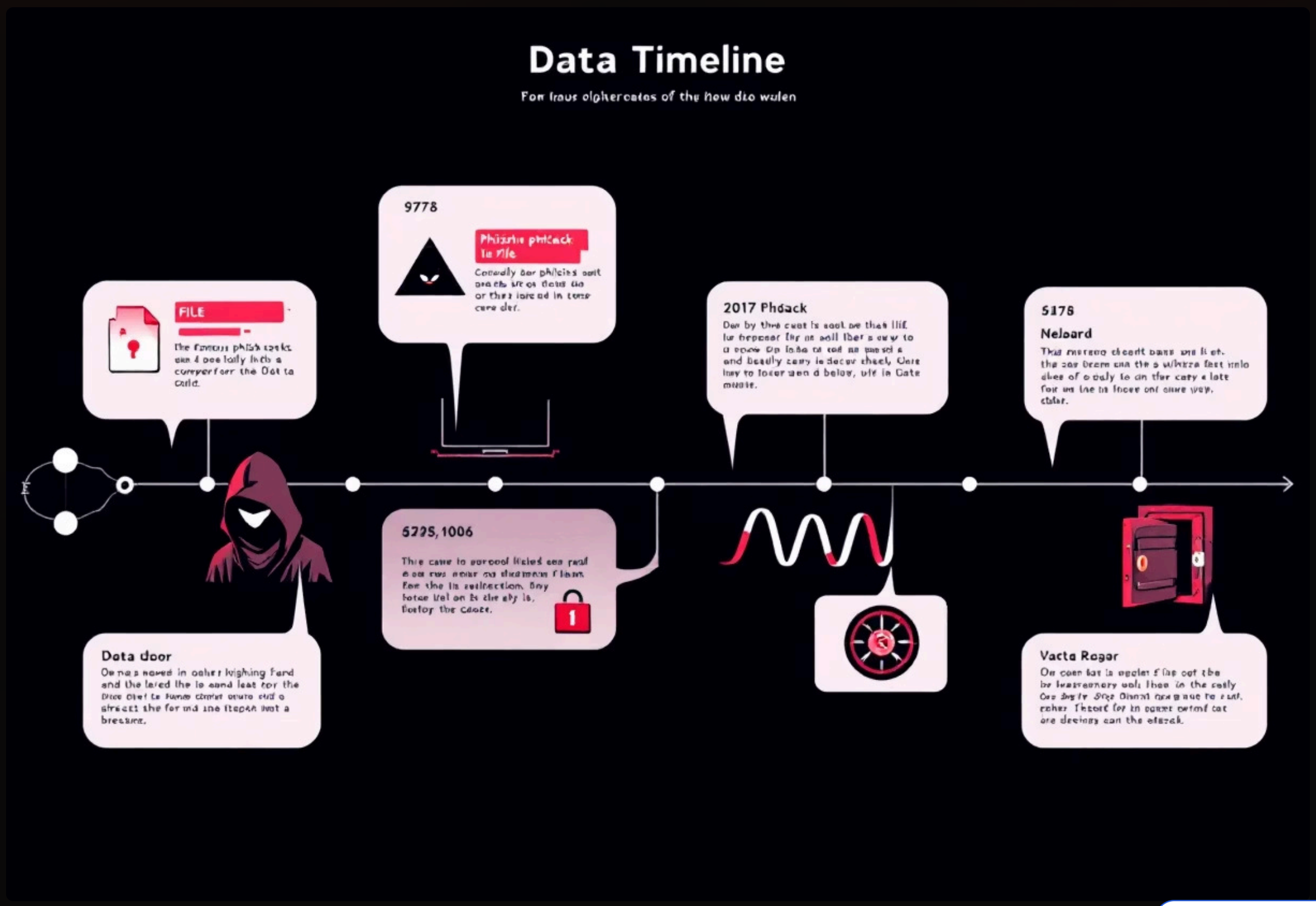
Fake bank emails stealing login credentials.

Example 3

CEO fraud – attackers requesting wire transfers.

3

Visual: Timeline or screenshots of real phishing attacks (censor sensitive info).



Interactive Quiz

Question 1: "Which of these is a sign of a phishing email?"

- A. Generic greeting
- B. Suspicious URL
- C. Urgent request
- D. All of the above

Answer: D

Question 2: "What should you do if you suspect a phishing attempt?"

- A. Click the link to check
- B. Report it to IT/security
- C. Forward to friends

Answer: B

Tip: Add multiple-choice questions, drag-and-drop activities, or scenarios for practice.