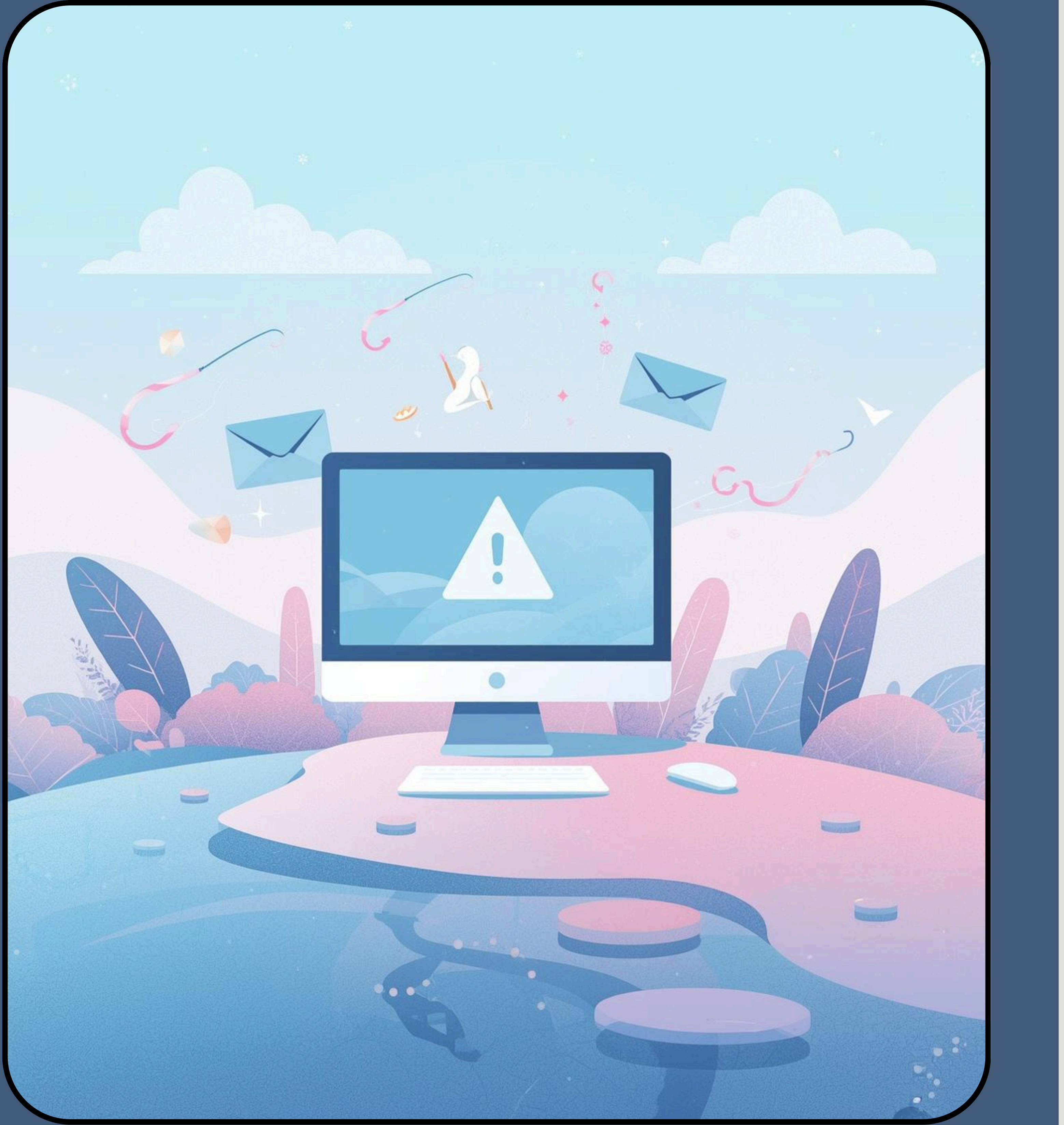
STAY SAFE ONLINE

Phishing Awareness Training

Prepared by: Sowmya S
Cyber Security Internship – CodeAlpha



Introduction to Phishing

What is Phishing?

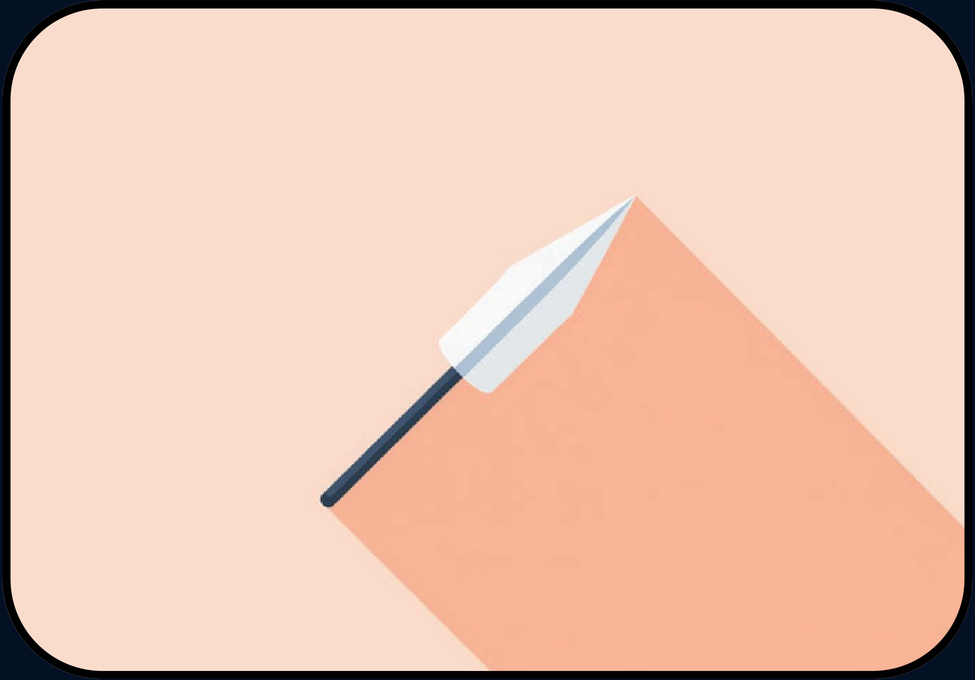
- Phishing is a cyber attack where attackers impersonate trusted entities.
- The goal is to steal:
- Login credentials
- Bank details
- Personal information

Phishing is a **cybersecurity threat** characterized by deceitful attempts to obtain sensitive information from individuals or organizations. These attacks exploit human psychology, often masquerading as trustworthy entities, making them particularly effective. The significance of phishing lies in its potential to cause severe financial losses and data breaches. In this presentation, we aim to raise awareness about phishing techniques, their impact, and effective strategies for prevention, ensuring everyone stays safe online.

Types of Phishing Attacks

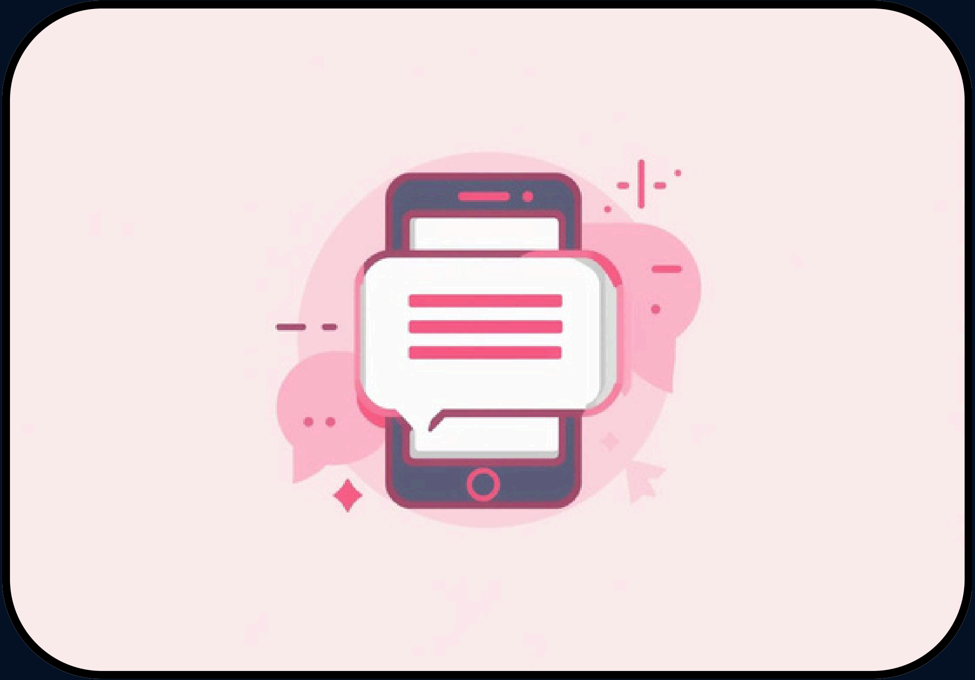
Email Phishing

Fake emails pretending to be legitimate sources.



Spear Phishing

Targeted attacks on specific individuals or groups.



Smishing

Phishing attempts via SMS messages to trick users.

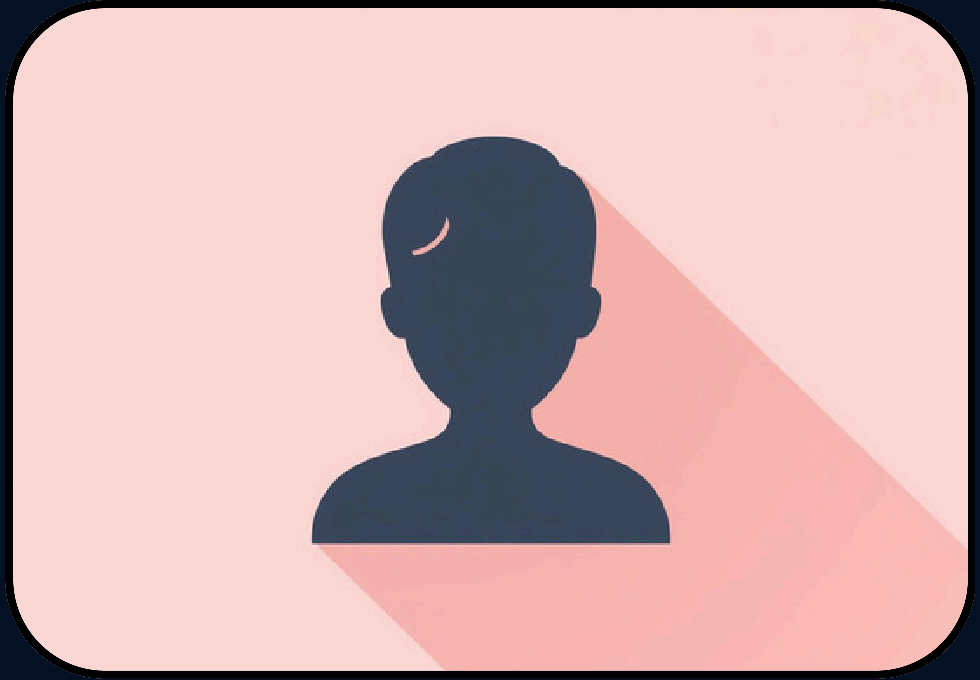
Recognizing Phishing Attempts

Suspicious Sender

Check sender addresses for legitimacy.

Urgent Language

Look for phrases that create panic.



Generic Greetings

Beware of impersonal salutations in emails.

Checking Email Headers and Verifying Websites

To avoid phishing attacks, always check email headers and verify website URLs for authenticity before sharing personal information.

Social Engineering Explained

Social Engineering Tactics Used by Attackers

Attackers manipulate human behavior by exploiting:

- Urgency & Fear – “Your account will be blocked immediately”
- Trust & Authority – Pretending to be HR, IT support, or a manager
- Rewards & Curiosity – Fake prizes, refunds, or offers
- Familiarity – Using personal or company-related information
- Helpfulness & Sympathy – Acting like they need assistance
- Routine Requests – Making malicious actions look normal

Key Message:

Phishing attacks succeed by manipulating people, not by hacking systems.

Real-World Example

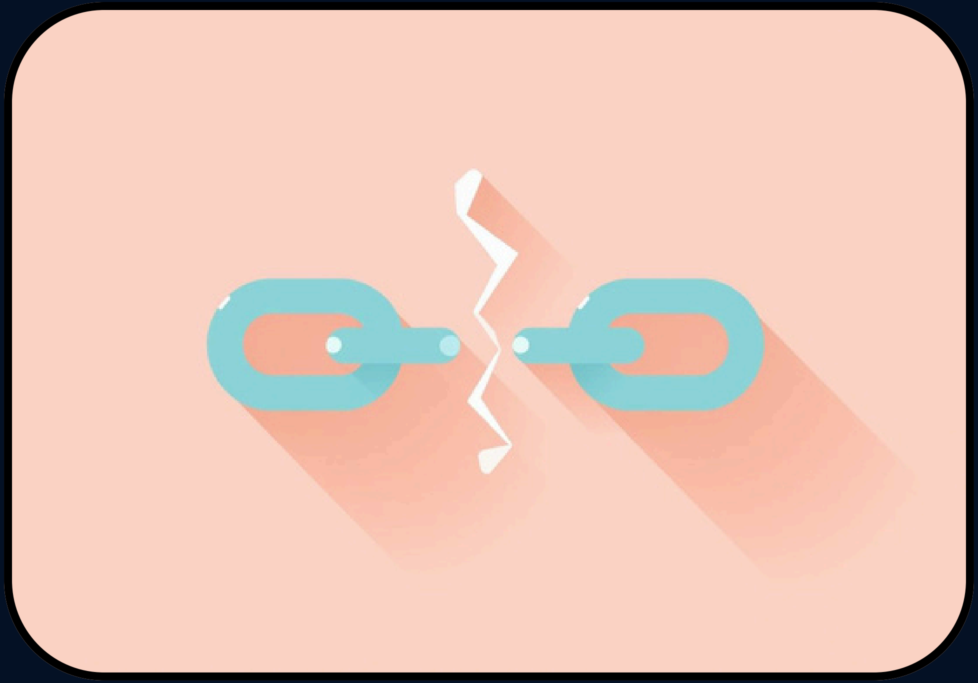
Example Scenario:

- User receives an email claiming to be from a bank or trusted company
- Email contains urgent language asking to verify the account
- A link redirects to a fake login page that looks real
- User enters username and password
- Attacker captures credentials and gains account access
- Stolen data may be used for financial fraud or identity theft

Lesson Learned:

Legitimate organizations never ask for passwords or sensitive information via email or links.

Best Practices to Stay Safe

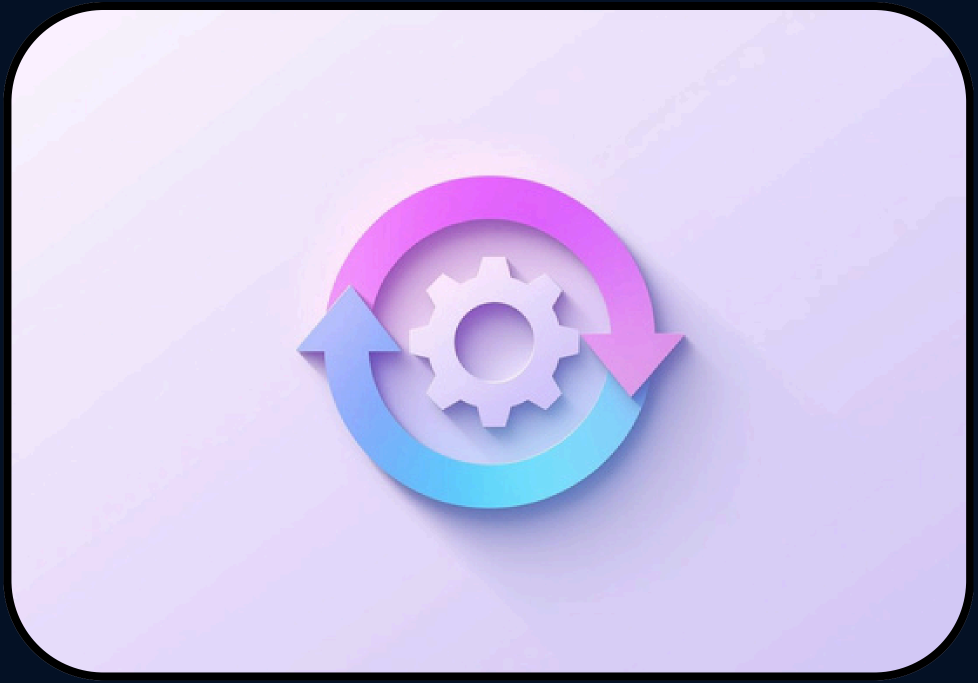


Don't Click

Avoid clicking on unknown links or attachments.

Verify Sender

Always confirm the sender through another channel.



Keep Updated

Regularly update your software and antivirus programs.

Responding to Phishing

Immediate Actions:

- Do NOT click on links or download attachments
- Do NOT reply to the email or message
- Report the phishing attempt to IT support or the service provider
- Delete the message after reporting

If credentials were shared by mistake:

- Change passwords immediately
- Enable Two-Factor Authentication (2FA)
- Monitor accounts for suspicious activity

Key Reminder:

Quick action can prevent data loss and account compromise.

Immediate action steps if phishing is suspected

Always report phishing emails, delete suspicious messages, and change passwords if you've shared any sensitive information.

Interactive Quiz

Q1: You receive an email asking for your password urgently. What should you do?
A) Reply immediately
B) Click the link
C) Ignore and report it ✅

Q2: Which URL looks suspicious?
A) https://www.amazon.com
B) https://www.amaz0n.com ✅

Q3: An email claims to be from IT support asking you to verify your account. What is the safest action?
A) Provide details
B) Click the link
C) Contact IT through official channels ✅

Q4: Which email subject is most likely a phishing attempt?
A) "Meeting Agenda"
B) "Your account will be suspended today" ✅

Quiz – True or False

Q1: HTTPS guarantees a website is always safe
❌ False

Q2: Phishing attacks only target technical users
❌ False

Q3: Attackers often use urgency to pressure victims
✅ True

Q4: Legitimate companies may ask for passwords via email
❌ False

Q5: Two-Factor Authentication helps reduce phishing impact
✅ True

Conclusion

- Phishing attacks are increasing every year and targeting all users
- Awareness is the strongest defense against phishing
- Attackers rely on human error, not technical weaknesses
- Thinking before clicking can prevent most attacks
- Verifying emails, links, and requests is essential
- Even one careless click can compromise sensitive data
- Security starts with informed and cautious users

Thank You

Stay alert, stay secure in cyberspace

Presented by : Sowmya S