CodeAlpha

Phishing Awareness Training

Recognizing and Preventing Phishing Attacks

Kakarla Vaishnavi

What is Phishing?

Phishing is a cyberattack where attackers trick users into revealing sensitive information

Attackers pretend to be trusted organizations

Information stolen includes passwords, bank details, and personal data

Phishing attacks are common and dangerous

Types of Phishing Attacks

- **Email Phishing**: Fake emails asking for urgent action
- **Smishing**: Phishing through SMS messages
- **Vishing**: Voice calls pretending to be officials
- **Spear Phishing**: Targeted attacks on specific people
- **Clone Phishing**: Copy of legitimate emails with malicious links

How to Recognize Phishing Emails

- Urgent or threatening messages
- Unknown or suspicious sender email address
- Poor grammar or spelling mistakes
- Requests for personal or login information
- Suspicious links or attachments

Identifying Fake Websites

- URLs look similar but contain small changes
- Website asks for login details immediately
- Missing HTTPS or security warning shown
- Poor design or broken links
- Fake logos or copied content

What is Social Engineering?

1. Social engineering manipulates human emotions
2. Attackers exploit trust, fear, and curiosity
3. Users are tricked into making security mistakes
4. Most phishing attacks rely on social engineering

Common Social Engineering Tactics

- Fear: “Your account has been compromised”
- Urgency: “Immediate action required”
- Authority: Pretending to be bank or IT staff
- Reward: “You have won a prize”
- Trust: Impersonating coworkers or friends

Best Practices to Avoid Phishing

Verify sender and email addresses

Hover over links before clicking

Do not share passwords or OTPs

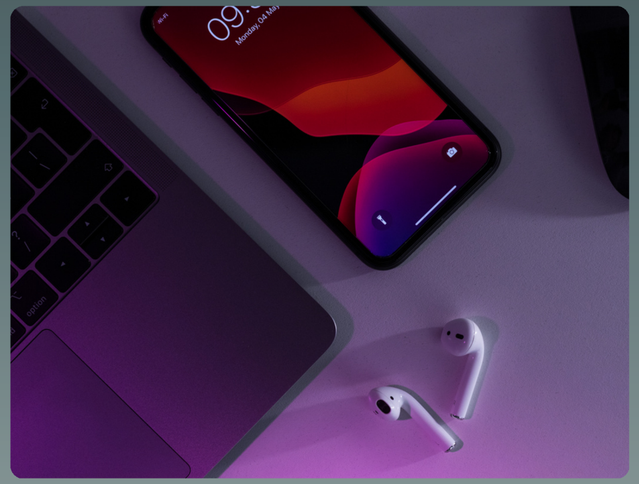
Enable two-factor authentication (2FA) and keep software, antivirus updated

Best Practices to Avoid Phishing

- Verify sender and email addresses
- Hover over links before clicking
- Do not share passwords or OTPs
- Enable two-factor authentication (2FA)
- Keep software and antivirus updated

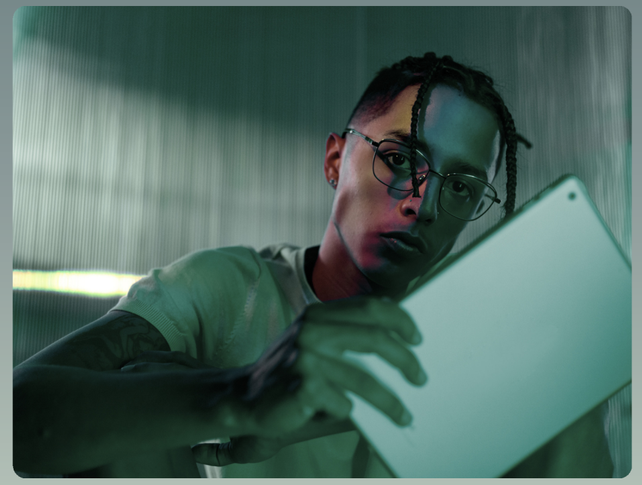
What to Do If You Receive a Phishing Message

Change passwords if information was shared



Do not reply to the message and delete it immediately

Report the email to your organization



Interactive Quiz - Question 1

About cybersecurity

Involves protecting data, devices, and networks from digital threats.

Types of cyberattacks

Phishing, ransomware, and social engineering are tactics used to steal or damage data.

Cyberattack lifecycle

Cyberattacks follow key stages, from gathering information to execution and achieving the goal.

Staying safe online

Using strong passwords, enabling 2FA, and avoiding suspicious links can go a long way.

Interactive Quiz - Question 1

Which is a sign of phishing?

A) Secure website
B) Urgent request for login
C) Known sender
D) Correct grammar
Answer: **B**

Your paragraph text

Interactive Quiz - Question 2

What should you do if you get a suspicious email?

A) Click the link
B) Share personal details
C) Report and delete it
D) Ignore security warnings
Answer: **C**

Key Takeaways

- Phishing attacks target human behavior
- Awareness is the best defense
- Always verify before clicking
- When in doubt, do not interact

Conclusion

Phishing awareness helps users:

- Protect sensitive information
- Prevent financial loss
- Improve cybersecurity practices
- Stay safe online