Cybersecurity Internship

PHISHING AWARENESS TRAINING

Stay sharp and stay safe from phishing attacks online.

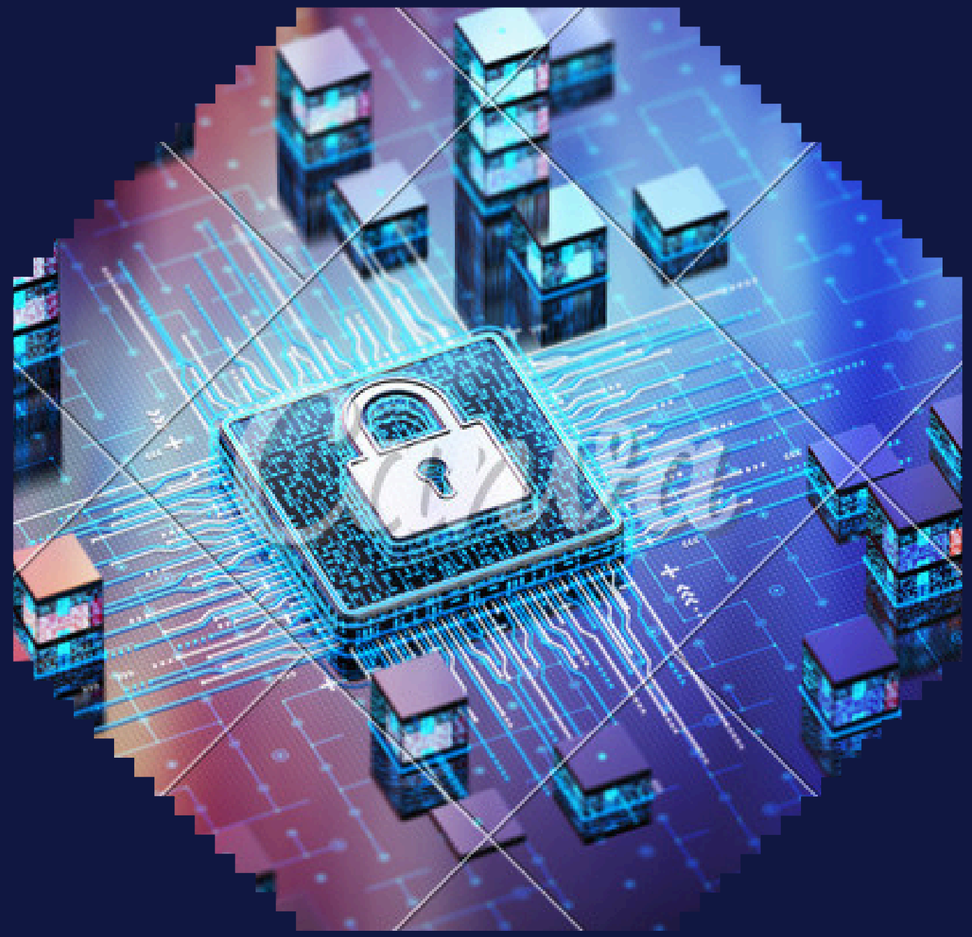
RAJ JAGESH SHARMA

Cybersecurity Internship, CodeAlpha

PHISHING AWARENESS TRAINING OVERVIEW

This presentation covers essential phishing awareness topics.

- Why phishing matters



UNDERSTANDING PHISHING TACTICS

Common Phishing Techniques Used by Attackers

Phishing schemes typically involve **deceptive emails** and fake websites designed to steal your personal information and financial data.

Recognizing Signs of Phishing Attempts

Being aware of **unusual requests** and poor grammar can help you identify potential phishing attempts and protect your sensitive information.

HOW TO SPOT PHISHING EMAILS

Recognizing urgent language and sender addresses

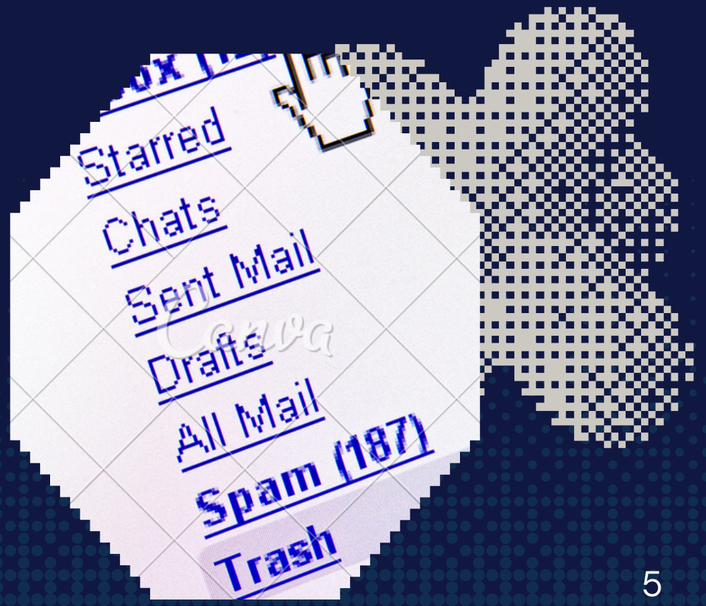
Phishing emails often use **urgent language** to create panic, urging you to act quickly without thinking. Always check the sender's address for authenticity.

Hovering links and unexpected attachments

Before clicking any links, **hover over them** to reveal the actual URL. Be cautious of unexpected attachments that could contain harmful malware.

PHISHING VS. LEGITIMATE EMAILS

Understanding the differences can help you identify potential phishing attempts in your inbox.



Phishing emails often mimic legitimate communications but contain subtle discrepancies that betray their true nature. By recognizing these differences, you can safeguard your personal and professional information from attackers seeking to exploit your trust.

SOCIAL ENGINEERING TRICKS

Understanding how emotions influence decisions

Attackers use **emotional manipulation** to exploit your instincts and create urgency, making you more likely to fall for scams.

Recognizing tactics to protect yourself

Being aware of common **social engineering tricks** can help you maintain your caution and make informed decisions before responding to suspicious requests.

BEST PRACTICES FOR SAFETY

Essential tips to avoid phishing scams and stay protected

Always verify the **source of emails** before opening links or attachments. Don’t rush; take time to assess the authenticity of requests you receive.

Use strong passwords and enable two-factor authentication

Implementing strong, unique passwords for different accounts helps **secure your information**. Using two-factor authentication adds an extra layer of protection against unauthorized access.

REPORTING PHISHING ATTEMPTS

Steps to report phishing emails effectively

If you suspect a phishing email, **immediately report it** to your IT department to help protect others from potential threats.

What to do if you click a link

If you've clicked on a phishing link, **act quickly** by changing your passwords and monitoring your accounts for unusual activity.

PHISHING AWARENESS TRAINING AGENDA

Explore phishing strategies, detection, and prevention techniques

- Why Phishing Matters
- What is Phishing?
- How to Spot Phishing Emails
- Social Engineering Tricks
- Reporting and Responding

WRAP-UP: STAY ALERT, STAY SAFE!

This section emphasizes the importance of recognizing phishing signs and protecting yourself against cyber threats.