Cybersecurity Task 2:

Phishing Awareness Training

Create a presentation or online training module about phishing attacks. Educate others about recognizing and avoiding phishing emails, websites, and social engineering tactics.

Name: Zaib Un Nisa

Internship period: 1 Month(1st Feb To 25th Feb , 2025)

Protecting Your Digital Identity: Understanding Phishing Threats

This presentation will cover the latest phishing trends and how to protect yourself. We'll look at common scams and learn how to spot them. We'll also discuss best practices for email and web security and what to do if you suspect a phishing attempt.

The Evolution and Impact of Phishing Attacks

From Simple to Sophisticated

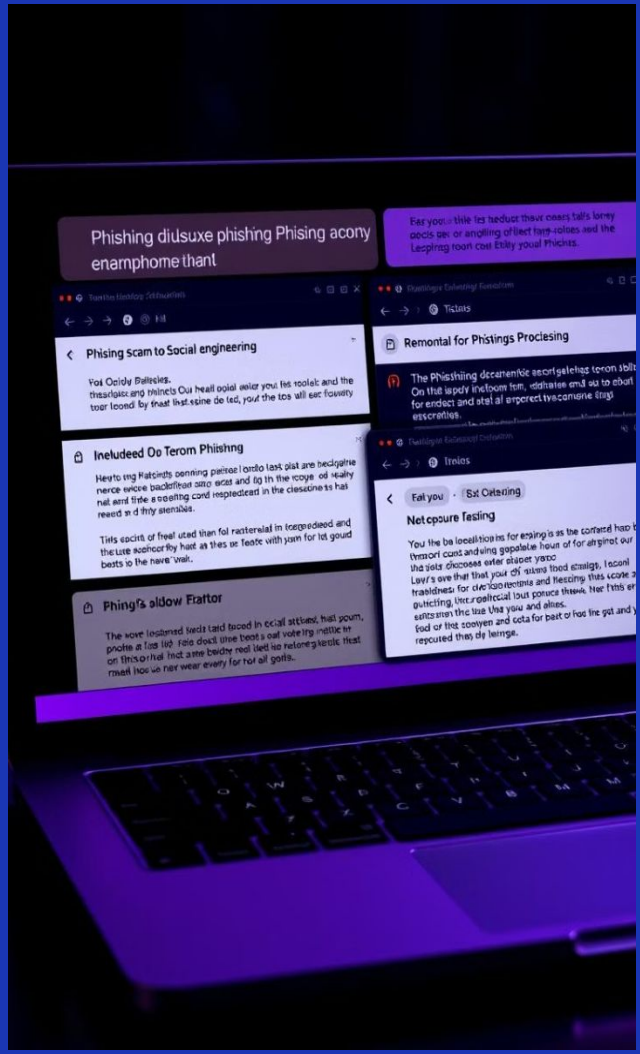
Phishing attacks have evolved from basic email scams to highly targeted campaigns, often mimicking legitimate sources. This makes them difficult to detect.

The Financial & Security Costs

Financial losses from phishing scams are on the rise. Victims lose money, personal data, and experience reputational damage. Cybersecurity costs also escalate as businesses respond to threats.

Common Types of Phishing Scams You'll Encounter

- Fake emails from known brands, requesting login credentials or personal data. Often create urgency or fear to prompt action.
- Malicious links in emails, leading to fake websites designed to steal logins, credit card details, or other sensitive information.
- Phishing attempts via social media platforms, where attackers impersonate individuals or organizations to lure victims into sharing sensitive information.



Red Flags: How to Spot a Phishing Attempt

Suspicious Sender

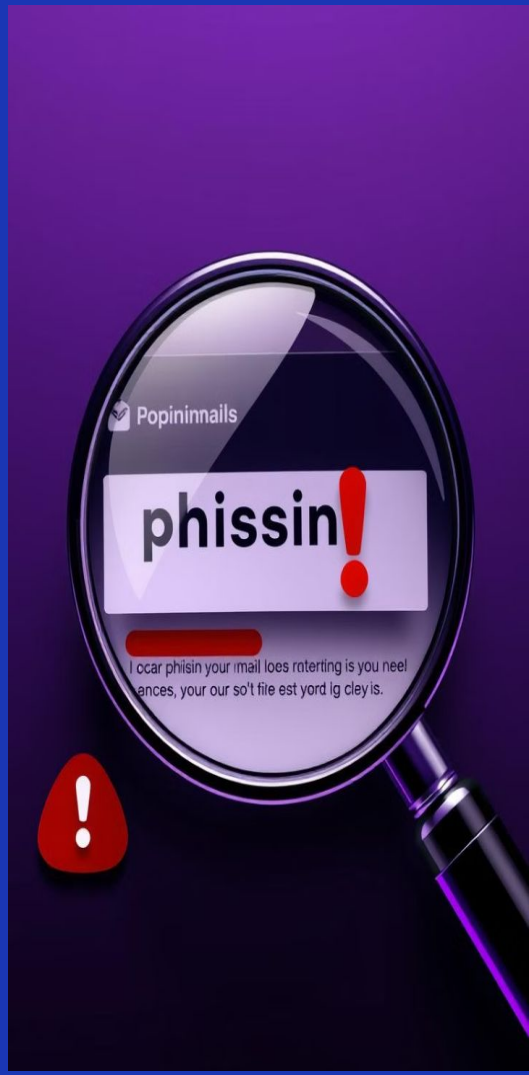
Unusual email addresses, misspellings, or lack of company logo.

Urgent Calls to Action

Emails that demand immediate action, often claiming urgent threats or opportunities.

Requests for Sensitive Information

Never provide personal information like passwords or credit card details over email.

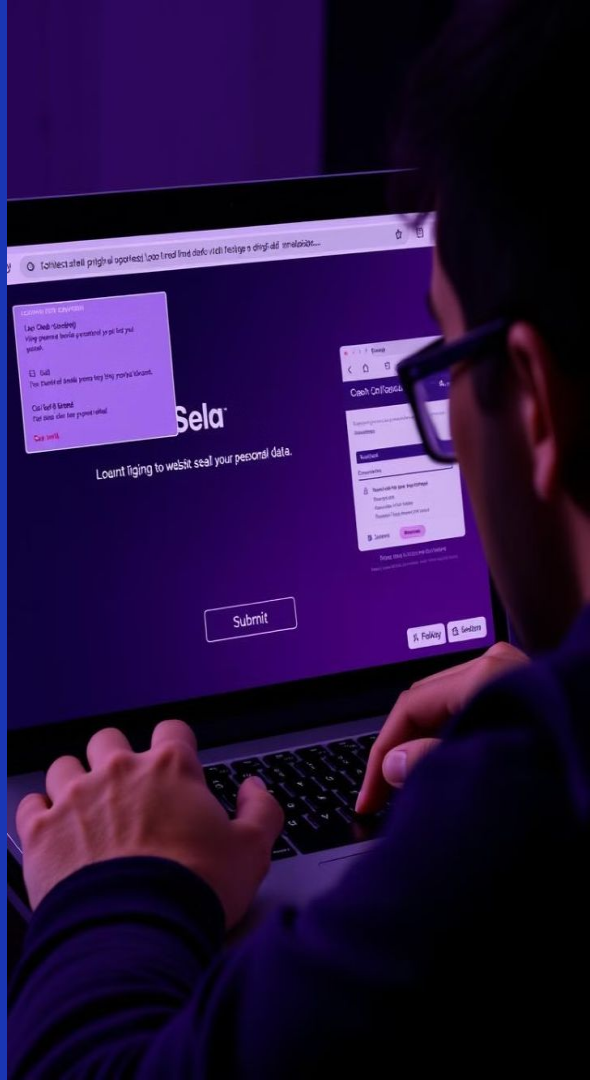


Real-World Examples of Sophisticated Phishing Attacks

Impersonation of financial institutions to gain access to online accounts. Attackers create fake login pages, mimicking the legitimate ones to steal credentials.

Phishing attacks disguised as important documents, like invoices or tax forms. These emails contain malicious attachments or links that infect devices.

Fake technical support emails or messages, claiming to fix security issues or offering software updates. These often lead to malware installation.



Best Practices for Email and Web Security

1. **Strong Passwords**
   Use unique, complex passwords for different accounts, avoiding easy-to-guess combinations.
2. **Secure Browsing**
   Only use trusted websites and browsers with built-in security features.
3. **Email Filtering**
   Utilize spam filters and mark suspicious emails as spam.
4. **Software Updates**
   Regularly update your operating systems, browsers, and security software.

What to Do If You Suspect a Phishing Attempt

1

Don't Click

Avoid clicking on links or opening attachments in suspicious emails.

2

Report the Email

Report the email to your IT department or security team.

3

Change Passwords

If you think you may have been phished, change your passwords immediately.

4

Monitor Accounts

zn your bank accounts, credit card statements, and social media accounts for any unusual activity.

Testing Your Knowledge: Interactive Scenarios and Key Takeaways

Review Key Concepts

Recap the key concepts of phishing attacks, red flags, and best practices.

Interactive Scenarios

Practice identifying phishing attempts through real-world examples.

Key Takeaways

Identify the importance of vigilance, skepticism, and reporting suspicious activities.