Phishing Awareness Training

Phishing attacks are a major threat to individuals and organizations, costing billions in damages each year. This presentation will educate you on how to recognize and avoid phishing attempts, including common techniques, red flags, and best practices for staying safe.

-Himanshu Singh (CA/S1/9623)

What is Phishing?

1 Deceptive Tactics

Phishing is a type of social engineering attack that uses fraudulent emails, messages, or websites to trick victims into revealing sensitive information or performing harmful actions.

2 Malicious Objectives

The goal of phishing is often to steal login credentials, financial information, or other personal data that can be used for identity theft or financial gain by the attackers.

3 Widespread Threat

Phishing attacks are highly prevalent, with millions of people falling victim each year. Staying vigilant and knowing the warning signs is crucial for protection.

Common Phishing Techniques

Fake Emails

Phishers often send emails that appear to be from legitimate organizations, such as banks or government agencies, in an attempt to steal login credentials or other sensitive information.

Fraudulent Websites

Phishing websites are designed to mimic the appearance of real websites in order to trick users into entering their login credentials or other personal data.

Social Engineering

Phishers may also use various social engineering tactics, such as creating a sense of urgency or authority, to manipulate victims into taking the desired action.

Identifying Phishing Emails

Suspicious Sender

Check the email address to ensure it's from a legitimate source. Phishers often use domain names that are similar to the real one.

Generic Greetings

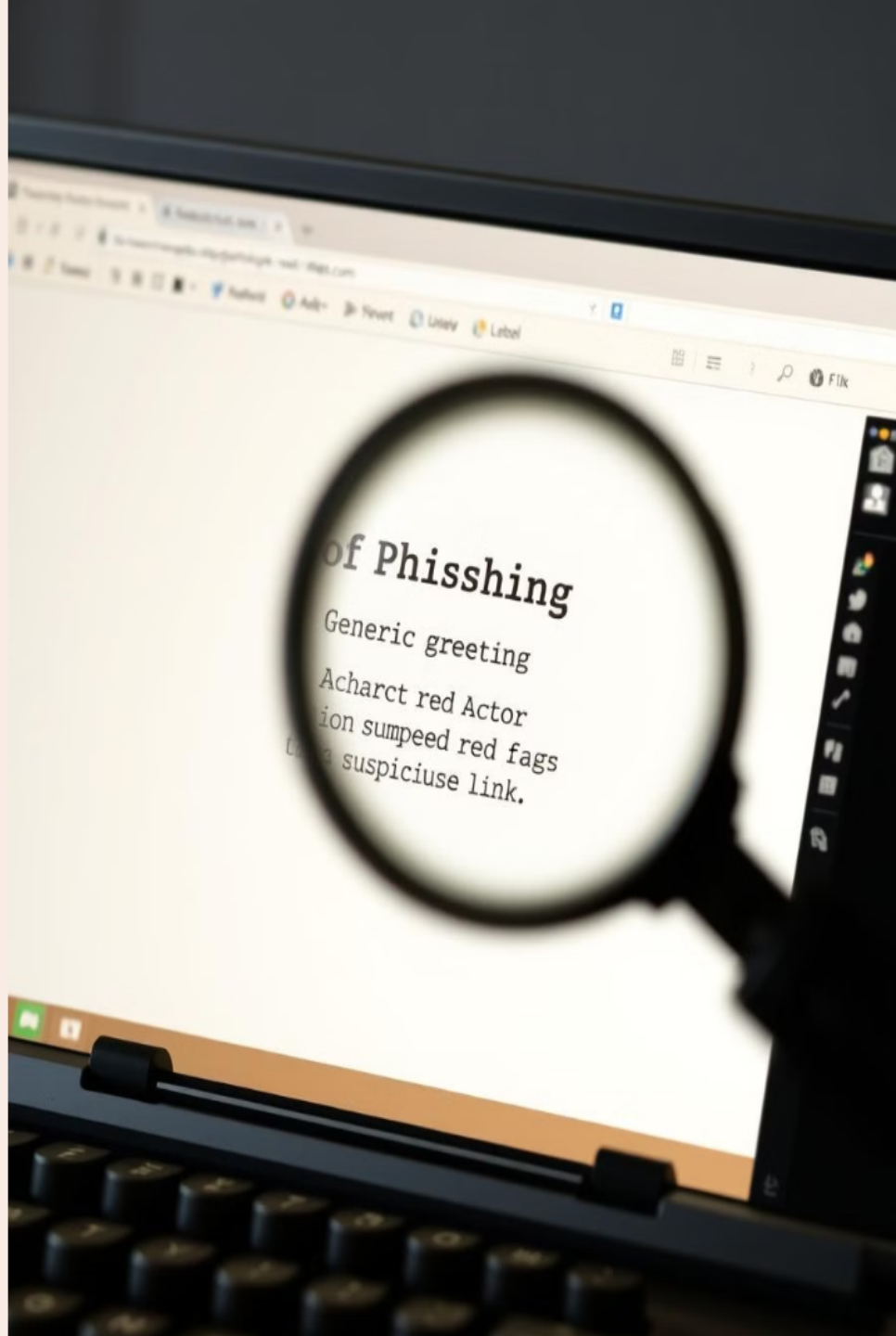
Phishing emails often use generic greetings like "Dear Customer" instead of your name, indicating it's a mass-sent message.

Urgent Calls to Action

Phishing emails may create a sense of urgency, pressuring you to take immediate action without properly verifying the request.

Suspicious Links/Attachments

Avoid clicking on links or opening attachments in emails unless you can verify they are from a trusted source.



Phishing Website Red Flags

URL Inspection

Check the URL for misspellings, unusual domains, or unfamiliar subdomains that may indicate a phishing site.

Security Indicators

Look for the presence of a valid SSL/TLS certificate and the "https://" prefix, which indicate a secure connection.

Visual Cues

Be wary of websites that have poor design, outdated branding, or other visual inconsistencies compared to the legitimate site.

Trust Your Instincts

If something about the website seems suspicious or doesn't feel right, it's best to err on the side of caution and avoid it.

Social Engineering Tactics

1 Authority Figures

Phishers may impersonate trusted authority figures, such as IT support or government officials, to pressure victims into revealing sensitive information.

2 Emotional Appeals

Phishers may use fear, curiosity, or a sense of urgency to manipulate victims into taking immediate action without proper verification.

3 Tailored Approaches

Phishers often research their targets and craft personalized messages to make the attack appear more legitimate and convincing.

Best Practices for Avoiding Phishing

1

Verify Sender

Always check the email address and sender information to ensure it's from a legitimate source before taking any action.

2

Scrutinize Links/Attachments

Hover over links to check the URL, and avoid opening attachments unless you can verify their safety.

3

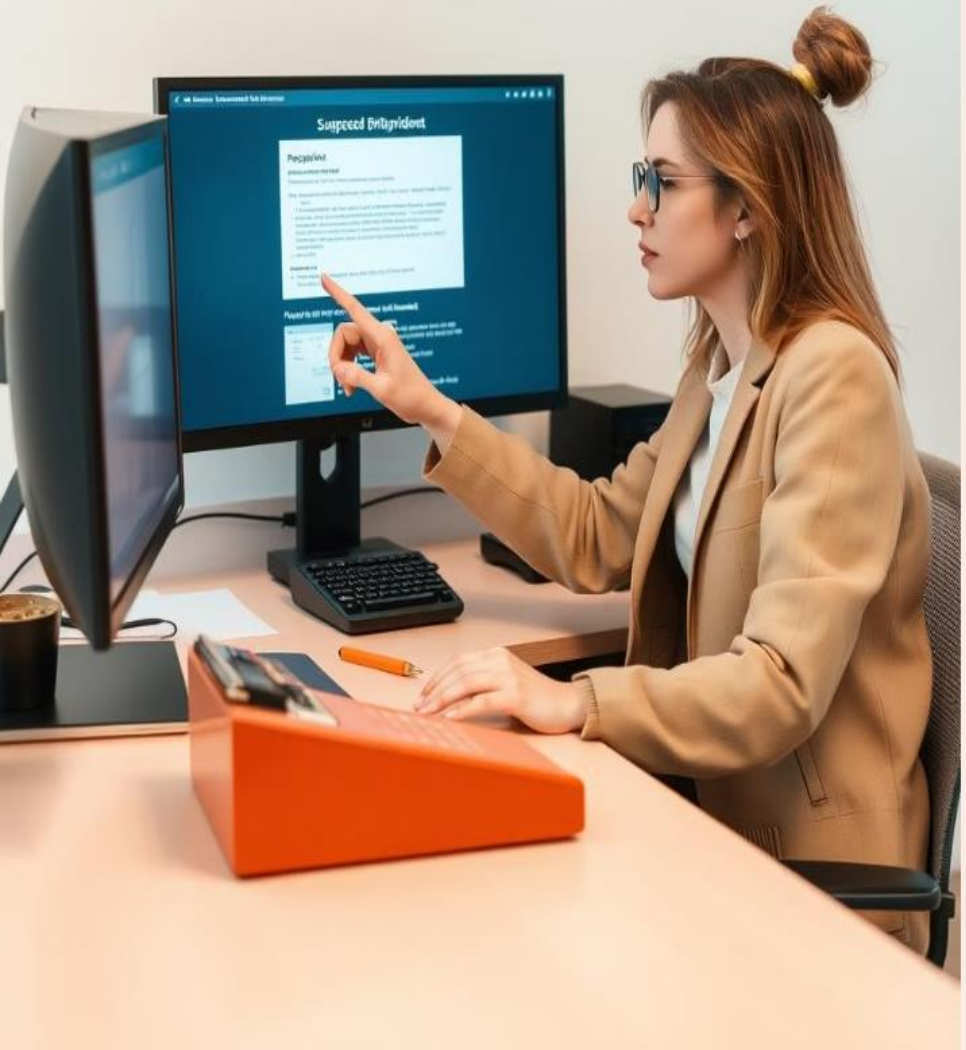
Stay Vigilant

Be wary of unsolicited requests for personal information, even if they appear to be from a trusted organization.

4

Report Suspicious Activity

If you suspect a phishing attempt, report it to your IT department or the appropriate authorities to help prevent others from falling victim.



Responding to a Suspected Phishing Attempt

Don't Respond	Do not reply to the suspicious email or interact with the phishing website.
Don't Click	Avoid clicking on any links or opening attachments, as they may contain malware.
Report It	Notify your IT department or the appropriate authorities to investigate the incident.
Change Passwords	If you've already provided any login credentials, change them immediately to secure your accounts.

Key Takeaways

1 Recognize Threats

Understand the common techniques used in phishing attacks and the red flags to watch out for.

2 Adopt Best Practices

Follow proven methods to avoid falling victim to phishing, such as verifying sender information and scrutinizing links/attachments.

3 Respond Promptly

Know how to properly respond to a suspected phishing attempt to minimize the potential damage.

4 Stay Vigilant

Phishing threats are constantly evolving, so maintaining a high level of cybersecurity awareness is crucial.