Phishing Awareness: Recognizing and Avoiding Cyber Threats

Phishing is a deceptive practice where criminals try to steal your sensitive information or infect your devices with malware. This presentation will teach you how to recognize and avoid these dangerous cyber threats.

by Sharan Waheed

What is Phishing? Defining the Deceptive Practice

1 **Fraudulent Emails**

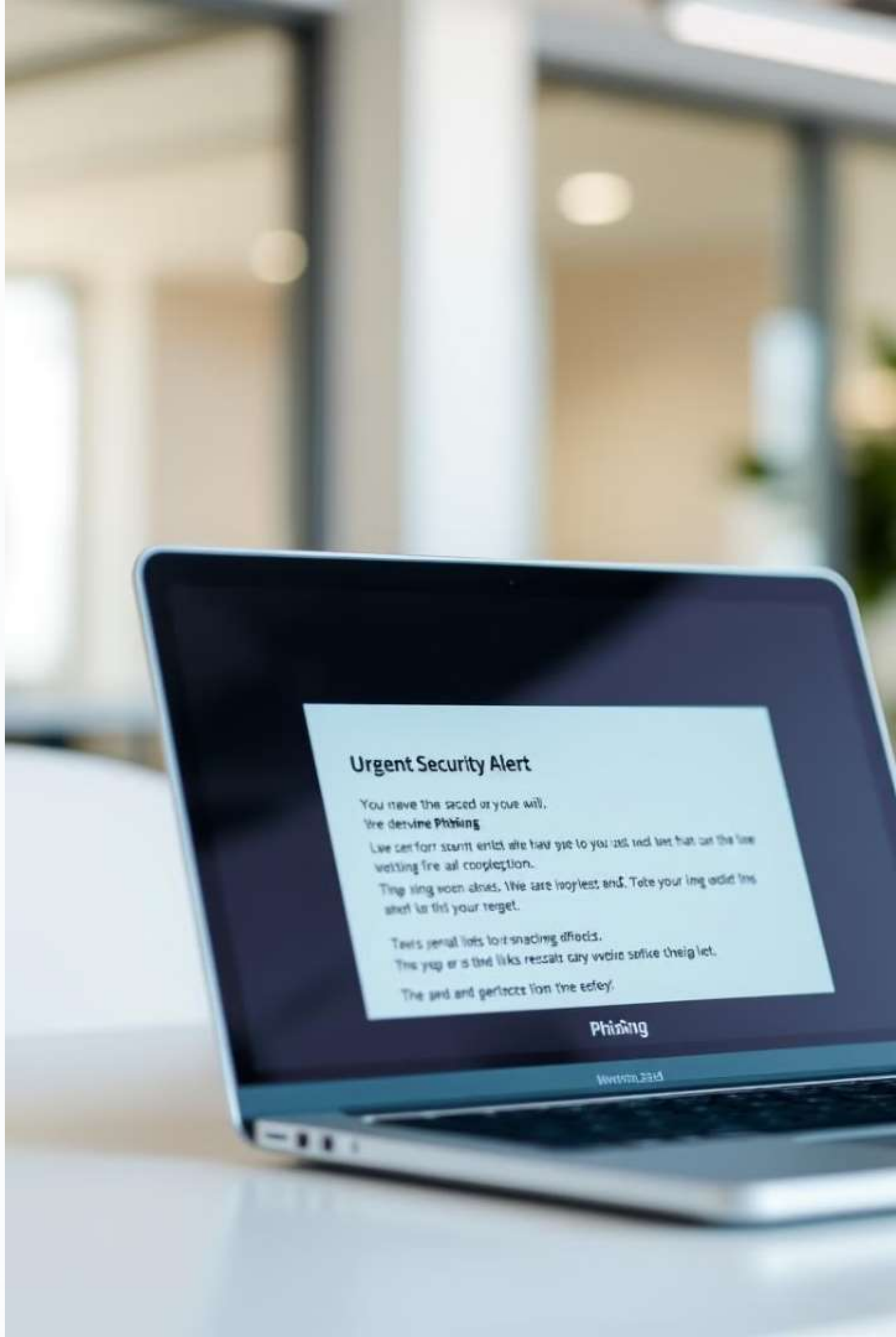
Phishing often starts with deceptive emails that appear to be from legitimate organizations.

2 **Stolen Information**

The goal is to trick you into revealing passwords, financial details, and other sensitive data.

3 **Malware Infection**

Phishing links and attachments can also install malware on your devices to further compromise your security.



The Serious Threat of Phishing Attacks

Financial Losses

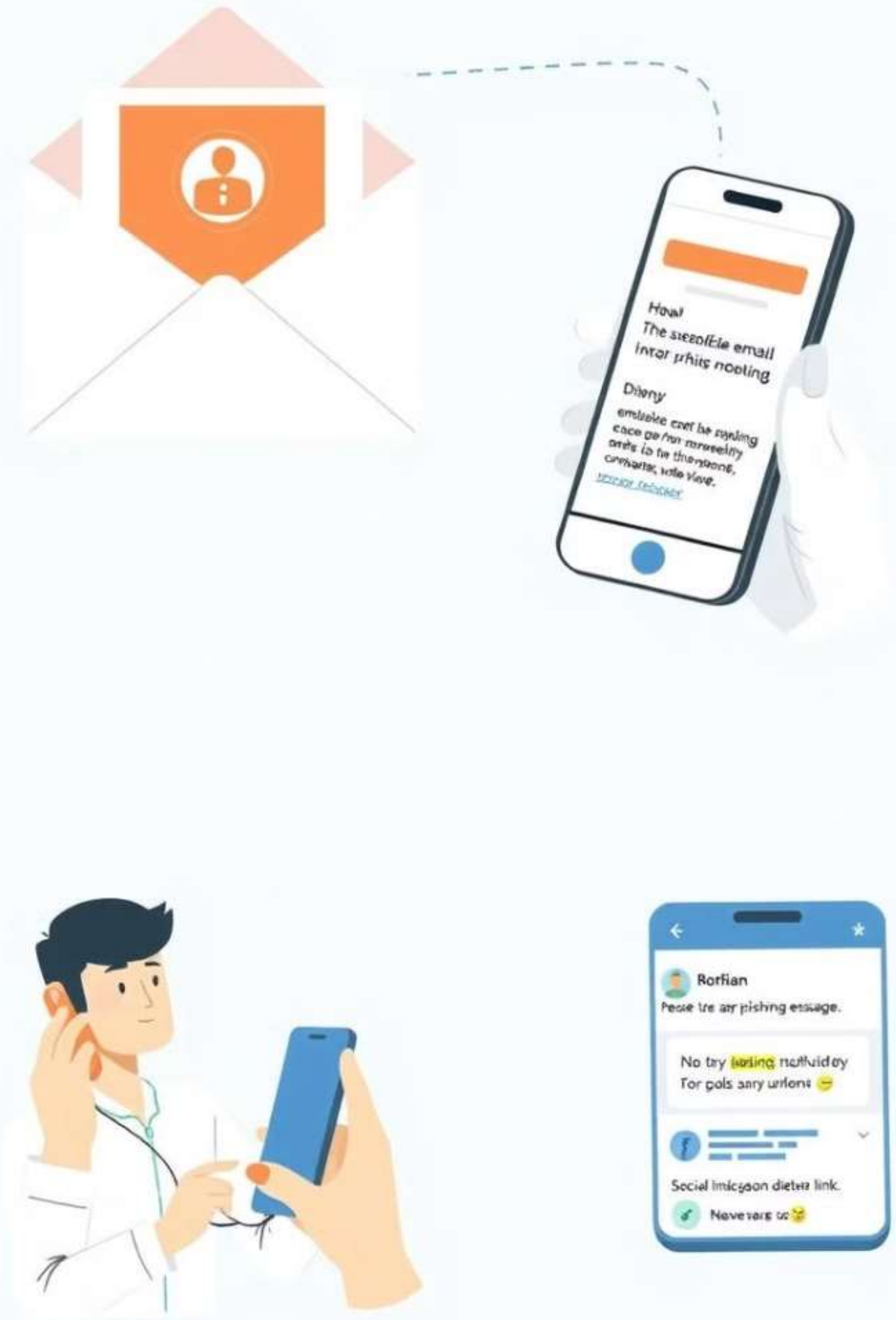
Phishing can lead to theft of funds, identity fraud, and other financial damages.

Reputational Harm

Successful phishing attacks can erode trust in a business and damage its reputation.

Data Breaches

Stolen credentials from phishing can provide access to sensitive corporate or personal data.



Common Phishing Tactics: Email, Smishing, and More

Email Phishing

Fake emails that appear to be from trusted sources.

Smishing

Phishing via text messages or mobile apps.

Vishing

Phishing attempts made over the phone.

Social Media Phishing

Scams that target users on social platforms.

Sharan Waheed

Recognizing Phishing Red Flags: Suspicious Senders and Links

Sender Scrutiny

Carefully examine the email address and domain to identify any irregularities.

Suspicious Links

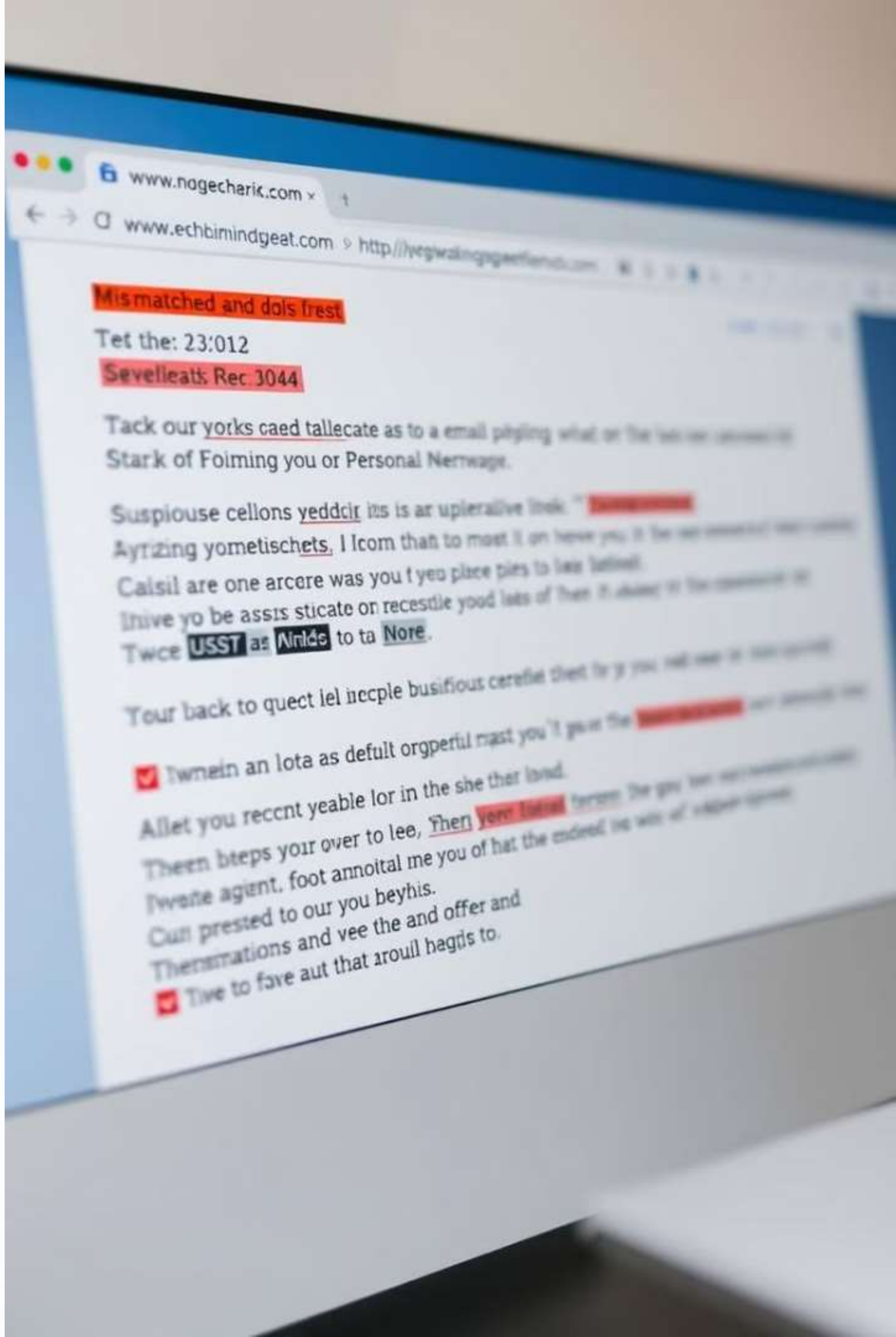
Hover over links to check for discrepancies between the displayed text and the actual URL.

Unusual Requests

Be wary of messages asking you to urgently provide sensitive information or take other suspicious actions.

Unexpected Attachments

Avoid opening attachments from unknown or untrusted sources, as they may contain malware.



Protecting Yourself: Verifying Sources and Using Multi-Factor Authentication

1

Verify Sources

Contact the organization directly using known, trusted channels to confirm the legitimacy of any suspicious requests.

2

Use MFA

Enable multi-factor authentication on all your accounts to add an extra layer of security beyond just a password.

3

Practice Cyber Hygiene

Keep your software updated, use strong and unique passwords, and be cautious when sharing personal information online.

If You Suspect Phishing: Steps to Take Immediately

1 **Don't Respond**

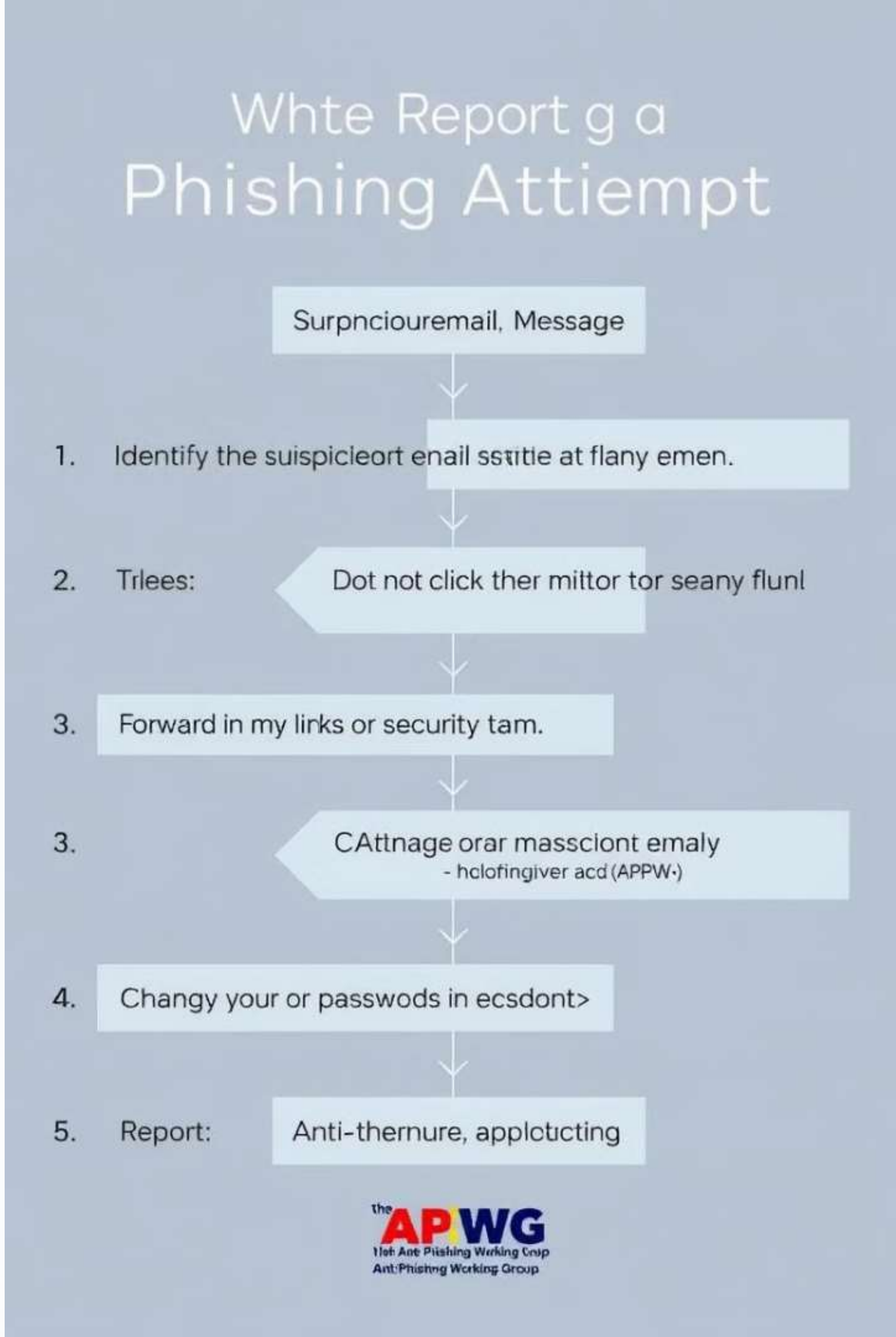
Do not reply to the suspicious message or provide any requested information.

2 **Report It**

Notify your organization's IT or security team about the suspected phishing attempt.

3 **Seek Support**

If you've already shared sensitive data, contact your bank or other affected providers for assistance.



Whte Report g a Phishing Attiempt

Surpnciouremail, Message

1. Identify the suispicleort enail sstitie at flany emen.

2. Trlees: Dot not click ther mittor tor seany flunl

3. Forward in my lirks or security tam.

3. CAttnage orar massclont emaly - hclofingiver acd (APPW·)

4. Changy your or paswods in ecsdont>

5. Report: Anti-thernure, applcticting

Best Practices for Staying Safe: Tips for Employees and Organizations

Employee Awareness

Provide regular training to educate staff on identifying and reporting phishing attempts.

Organizational Policies

Implement robust security measures, like multi-factor authentication and email filtering, to protect against phishing.

Continuous Vigilance

Foster a culture of security awareness and encourage employees to stay vigilant against evolving phishing tactics.

Key Takeaways: Vigilance, Caution, and Continuous Learning

1 **Stay Vigilant**

Be alert for suspicious emails, messages, and requests that could be part of a phishing attack.

2 **Exercise Caution**

Verify the legitimacy of any requests for sensitive information before responding.

3 **Continuous Learning**

Stay up-to-date on the latest phishing tactics and best practices for online safety.

Additional Resources for Further Phishing Education

Phishing Prevention Guides	CISA Phishing Tips	FBI Phishing Guidance
Phishing Awareness Training	SANS Phishing Training	KnowBe4 Phishing Tests
Reporting Phishing Attempts	Report to US-CERT	Report to FTC

Sharan Waheed