Phishing Recognition Checklist

1. Check the Sender's Email Address

- Is the email from someone you know?
- If it's from a company, does the email address match the company's official website?

2. Review the Email Subject and Content

- Does the email ask for personal information or login details?
- Is there a sense of urgency, like a threat to close your account?

3. Look for Grammar and Spelling Errors

- Are there obvious spelling mistakes?
- Is the grammar poor or does the email use unusual language?

4. Be Wary of Suspicious Links

- Hover over the link with your mouse (without clicking). Does the link address match what it claims to be?
- Is the link shortened? Be cautious as this can be used to hide the real destination.

5. Inspect Email Attachments

- Were you expecting an attachment from the sender?
- Be careful with .exe, .zip, and .pdf files from unknown senders.

6. Sense of Unprofessionalism

- Does the email look poorly formatted or unprofessional?
- Legitimate companies usually have high standards for their communications.

Remember: When in doubt, don't click! It's always better to be safe than sorry. If you think an email might be from a real company, it's best to go directly to their official website and contact them there.