Quick Safety Checklist

1. Check the Sender

- Verify the full email address, not just the display name.
- Look for misspellings, extra characters, or unusual domains.
- Compare it with previous legitimate messages from this sender.
- Be cautious if the message is not addressed to you personally.

2. Inspect the Link Before Clicking

- Hover over the link to preview the real URL.
- Check the root domain — the part before ".com/.org".
- Be suspicious of long, complicated, or unfamiliar URLs.
- Avoid clicking links that create urgency or demand immediate action.

3. Evaluate the Message Content

- Look for urgent or threatening language.
- Check for unusual wording, typos, or formatting inconsistencies.
- Question unexpected attachments — especially .zip, .exe, .html.
- Ask yourself: "Was I expecting this email?"

4. Think Before Clicking

- Pause for a moment — phishing relies on rushed decisions.
- Consider whether the request makes sense in your work context.
- If something feels slightly "off," treat it as suspicious.
- When in doubt, verify through a separate, trusted channel.

5. Report Suspicious Emails

- Do NOT delete the email — report it first.
- Follow your company's reporting procedure (e.g., "Report phishing" button, IT ticket, forwarding to security).
- Even if you're not sure, reporting helps protect the entire team.
- It's always better to report a benign email than to miss a malicious one.