Checklist: How to Safely Verify Links (Phishing Defense Guide)

This professional checklist provides a step-by-step process for cybersecurity professionals and users to verify whether a link is legitimate or a phishing attempt before engaging with it.

- 1. Inspect the URL carefully: Check the domain for misspellings, extra characters, or suspicious top-level domains. Hover over links before clicking to confirm they match the displayed text.
- 2. Use WHOIS / DNS lookups: Review domain registration details (creation date, registrar, organisation). Freshly registered or anonymised domains are red flags.
- 3. Check SSL/TLS certificate: Click the browser padlock and verify that the certificate is valid, issued by a trusted CA, and matches the organisation.
- 4. Use link-scanning tools: Submit the URL to reputation services like VirusTotal, Google Safe Browsing, or Cisco Talos to check for phishing/malware reports.
- 5. Validate the organisation: Cross-check with the official company careers page, LinkedIn jobs, or press releases to confirm legitimacy.
- 6. Isolate before opening: If in doubt, open the link in a sandboxed VM or secure browser container to avoid exposing your main system.
- 7. Report suspicious links: Escalate to your Security Operations Center (SOC) or IT security team if a phishing attempt is suspected.

■ By following this checklist, you can identify phishing attempts early and protect your organisation’s systems, data, and users from compromise.