

Pause before you click. Phishing creates urgency so you skip checks.

Red flags

• CHECKLIST

Treat as suspicious if...

- ☐ Unexpected urgency (“account closes today”)
- ☐ Sender name and address do not match
- ☐ Link text does not match the real website
- ☐ Attachment you were not expecting
- ☐ Request for passwords, OTPs or full card details

If you already clicked or entered information

• STEP BY STEP

- 1 Stop — do not enter more information
- 2 Disconnect if something is downloading
- 3 Change passwords for affected accounts
- 4 Contact the bank if banking was involved
- 5 Check account activity and beneficiaries
- 6 Warn staff or partners who could be next

Safer habit

Type banking, SARS and supplier portal addresses yourself, or use a saved bookmark — do not open them from an unexpected message.