STAY SAFE ONLINE

Phishing red flags checklist

Name _____ Business _____ Date _____

You will finish with
A safe way to open each business account without using links, and a red-flag check for any message.

Phishing is a fake email, SMS or WhatsApp message that tries to make you click a link, open a file or share a password or code. The safest habit: never log in from a link in a message.

1. Set up safe ways to log in

For each account, choose a safe way to open it: the official app, a saved bookmark, or typing the address yourself. Set it up, then tick.

Account	My safe way to open it	Set up (tick)
e.g. Business bank	Official bank app on my phone	Yes
e.g. SARS eFiling	Bookmark saved on my laptop	Yes
Email		

2. Check a message before you click

If you tick even one box, do not use the link. Open the account your safe way from section 1.

- **CHECKLIST**

Red flags

- [ ] I did not expect this message
- [ ] It says "urgent", "today" or "your account will be closed"
- [ ] It offers a refund, prize or tax money I did not ask for
- [ ] The sender's email address or number is not the one I have saved (look for small changes, e.g. one extra letter)
- [ ] The link address is not the real website (e.g. a strange name instead of your bank's normal address)
- [ ] The spelling or writing is different from real messages from them
- [ ] It has an attachment I did not ask for
- [ ] It asks for a password, OTP or card details
- [ ] It asks me to keep it secret

This resource is for educational purposes only. It is not tax, legal or financial advice. Rules and requirements can differ by business type and location. Check with the relevant authority or a qualified adviser for your situation.

Remember

1. Scammers copy logos. A logo proves nothing.
2. Real details (your name, a real order) do not prove the message is real.

3. If you already clicked

- **STEP BY STEP**

1. Stop. Do not type anything more.
2. If a file is downloading or installing, turn off Wi-Fi and mobile data.
3. On a phone or computer you trust, open that account your safe way from section 1 and change the password. If you typed it into the fake page, also change it on every account that uses the same password.
4. Work through the Fraud response checklist.

Share the habit

What I will do	Show sections 2 and 3 to everyone who reads business messages (e.g. the person who answers customer emails)
Who	
By when	

This resource is for educational purposes only. It is not tax, legal or financial advice. Rules and requirements can differ by business type and location. Check with the relevant authority or a qualified adviser for your situation.