Emergency Action Plan

What to do the moment you think you've been scammed (South Africa)

If you're in immediate emotional crisis:

SADAG Suicide Crisis Helpline:
0800 567 567 / 0800 21 22 23 (24/7)
LifeLine South Africa:
0861 322 322 (24/7)

1 0-10 minutes: stop further loss

- ☐ **End contact:** hang up/close chat; **do not** reply or explain.
- ☐ **Freeze money movement:** use your banking app to **lock cards** and **temporarily freeze accounts** if your bank allows.
- ☐ **Block the scammer** on phone/WhatsApp/SMS/social.

2 First hour: secure money + identity

- ☐ **Call your bank's fraud line** (use the number on your card/app):
  - Ask to **hotlist cards** and **block online purchases**.
  - If you paid by **card**: request a **chargeback** (fraud/misrepresentation).
  - If you paid by **EFT/instant payment**: request an **urgent recall/hold** on the transfer.
  - If you see **debit orders: reverse** unauthorised debits (typically fast if within ~40 days).
  - Ask the bank to **note your profile** for follow-on "refund/recovery" scams.
- ☐ **Open a SAPS case** (keep the **case number**).
  - **Emergencies**: 10111 - **Crime Stop**: 08600 10111.
- ☐ **Secure your main email account** (this protects all your logins):
  - Change the password to a **long, unique** one.
  - Turn on **2-factor authentication (2FA)** (authenticator app preferred).
  - Check **filters/forwarding rules;** remove anything you didn't set.
  - **Sign out of all sessions;** revoke suspicious third-party access.
- ☐ **SIM/phone safety:** ask your mobile network to add a **SIM-swap/port-out lock**; check there's no call-forwarding set.
- ☐ **Devices**: uninstall any remote-access tools you didn't install (e.g., **AnyDesk, TeamViewer, QuickSupport**); run a malware scan.

3 Same day: report + document

- ☐ **National Cybersecurity Hub (CSIRT)**: report the incident (email **cshubcsirt@cybersecurityhub.gov.za**).
- ☐ **Platform takedowns:** report the fake **ad/page/listing** (Facebook/Instagram/Marketplace/Google/WhatsApp Business, etc.)
- ☐ **Start a logbook** (this wins disputes): Timeline, amounts, merchant/beneficiary names, bank **reference numbers**, **SAPS case number**, phone numbers, email addresses, usernames, URLs, screenshots, and (if crypto) wallet addresses/TxIDs.

4 If you paid this way, do this too

- ☐ **Card:** chargeback under Visa/Mastercard rules; include screenshots and order/merchant details.
- ☐ **EFT / Instant:** ask for **recall/hold**; request that your bank files the necessary reports; ask about **FIC Section 34 intervention** (temporary hold up to 10 working days where warranted).
- ☐ **Debit order: reverse** immediately; ask your bank to **block** repeat debits from the same originator.
- ☐ **Cash-send/eWallet: cancel the voucher** if it hasn't been withdrawn.
- ☐ **Crypto:** move remaining funds to a **new wallet** you control; notify the exchange and provide addresses/TxIDs (recovery is rare, but flags can help).
- ☐ **Account takeover (email/social/bank):** use account recovery flows, rotate passwords, enable 2FA, and notify close contacts to ignore suspicious messages.

5 Identity protection (within 24-48 hours)

- ☐ **SAFPS Protective Registration** (free): flag your ID so lenders perform extra checks on new applications.
- ☐ **Credit checks:** pull your **TransUnion/Experian/XDS** reports; ***dispute*** unknown listings; set a monthly reminder for the next 3–6 months.

6 Privacy & takedowns

- ☐ **ISPA Takedown** (for SA-hosted scam pages/content).
- ☐ **Information Regulator** (POPIA/PAIA) if your personal data was abused or disclosed.

7 Escalation & recourse (as needed)

- ☐ **Ombudsman for Banking Services** (via the **National Financial Ombud Scheme**) for unresolved bank disputes.
- ☐ **FSCA / FAIS Ombud** if a "financial adviser" or investment pitch was involved.
- ☐ **OPFA (Pension Funds Adjudicator)** if retirement benefits/payouts were affected.
(These bodies can't promise refunds, but they compel responses and can order fair redress.)

8 Over the next week

- ☐ **Password manager** in place; **unique** passwords for email/bank/cloud/social.
- ☐ **2FA everywhere**; review bank **alerts; lower daily transfer limits** for a while.
- ☐ Warn family/colleagues: after a breach, victims often land on "**suckers lists**" — expect **refund/recovery** approaches; tell them not to engage on your behalf.
- ☐ Consider a short **counselling call** (SADAG/LifeLine) if sleep, anxiety, or rumination is heavy.

9 Red-flag reminders (stick this on the fridge)

- ☐ **No OTPs. Ever.**
- ☐ **No remote access** to your device for "refunds" or "verification".
- ☐ **Type the address yourself**; read the word **before** ".com/.co.za".
- ☐ **Urgent + secret = pause** and verify on a known, separate channel.

10 Keep this info handy (fill in):

Bank fraud reference #:

_____

_____

SAPS case #:

_____

_____

CSIRT report date:

_____

_____

Amounts/beneficiaries/refs:

_____

_____

☐ **Contacts warned**

www.offernet.net

offernet®
Informed by Data, Powered by Technology