CYBER SAFETY GUIDE

Understanding the most common cybercrime threats – and how to avoid them

AfriForum

Content

Introduction

South Africa remains one of the most heavily targeted countries for cybercrime in Africa and globally. In 2025, telecoms fraud alone cost operators over R5,3 billion (per COMRiC), while digital banking fraud losses surged significantly, mostly through phishing. SABRIC reports highlight that phishing accounts for around 78% of digital banking fraud in recent years, and over 40% of South Africans were scammed in 2025 according to global surveys.

Most cybercrimes do not involve sophisticated hacking. Criminals rely on deception, manipulation, social engineering and increasingly AI tools to trick people into giving access to their banking details or money.

This guide sets out the most common threats that affect South Africans today (updated for 2026 trends) and provides practical, up-to-date steps to protect yourself.

Phishing attacks

Phishing is still the most common cybercrime threat in South Africa.

Criminals send fraudulent emails, SMSs (smishing), WhatsApps or calls, pretending to be legitimate organisations like banks, couriers, SARS, government departments or service providers.

The goal is to trick you into revealing your banking login details, passwords, one-time PINs (OTPs), credit card numbers or clicking malicious links/QR codes.

Common phishing scams in South Africa

- Fake bank security alerts or "suspicious login" warnings
- Fake courier delivery messages requesting a small "release fee" or customs payment
- Fake tax refund or SARS notices
- Fake subscription renewals (Netflix, Showmax, Amazon)
- Fake job offers, prizes or urgent family emergencies
- Quishing: fraudulent QR codes in emails, posters or messages leading to fake login pages

Warning signs

- Urgent language: “Act immediately or your account will be blocked/closed.”
- Requests to verify/update your personal information or scan a QR code
- Links/QR codes to unfamiliar or slightly misspelled websites
- Poor spelling/grammar (though AI now corrects the grammar of many of these)
- Unexpected calls or voice notes with cloned voices

How to protect yourself

- Never click links or scan QR codes in unsolicited messages about banking or security.
- Always access your bank by typing the official website or app directly into your browser line.
- Never share passwords, OTPs or personal details via links, calls or messages.
- If you are unsure, end the call and contact the organisation by using the official numbers from their website or app.
- Use caller ID apps like Truecaller to screen suspicious calls.

SIM swap fraud

SIM swap fraud remains a major banking threat in South Africa, with telecoms losses exceeding R5,3 billion in 2025.

Criminals trick your mobile provider into transferring your number to their SIM. They then intercept OTPs, reset passwords and access bank accounts.

How criminals carry out SIM swap attacks

- They gather your personal info from social media, data leaks or phishing.
- They impersonate you to request a SIM swap (often using fake IDs or documents).
- They use the new SIM to hijack banking OTPs and drain your accounts.

Warning signs

- Sudden loss of the network signal
- Unexpected SIM swap notifications from your provider
- Unsolicited password reset messages or OTP requests

How to protect yourself

- Immediately contact your service provider (Vodacom, MTN, etc.) if your signal drops unexpectedly.
- Add a SIM swap PIN, extra security password or SIM swap alert with your network.
- Limit personal info that you share publicly on social media.
- Enable banking app alerts and prefer app-based or biometric authentication over SMS OTPs wherever available.

Business email compromise (invoice fraud)

This affects businesses and individuals, especially in property deals, supplier payments or large transactions. Criminals monitor emails or impersonate legitimate parties to send fake "updated banking details".

How the scam works

1. The perpetrators spy on real email threads.
2. They then send a message as a supplier, lawyer or colleague.
3. They provide fraudulent payment instructions.
4. The victim transfers the money, and the funds are quickly moved onward.

How to protect yourself

- Always verify banking details by phone (using known or saved numbers) before paying any invoice.
- Never rely only on email for financial changes.
- Be suspicious of sudden "updated" details, even if they look legitimate.
- Confirm large or high-value payments through a secondary channel (a telephone call or WhatsApp voice note from a known contact).

Banking and mobile app fraud

Mobile banking apps are heavily targeted. Attacks include fake apps, malware, fake support calls and social engineering. Criminals often call and pretend to be "fraud departments," urging you to share information or grant them remote access.

Important rule

Banks **never** ask for passwords, OTPs, remote access or to install apps over the phone.

How to protect yourself

- Download banking apps only from the official Google Play or App Store.
- Never share OTPs with anyone, including callers who claim to be from your bank.
- Do not allow strangers remote access to your phone or computer.
- Use strong, unique passwords and enable biometrics (your fingerprint or face ID).

Malware and malicious downloads

Malware steals information via infected files, apps or sites. It then spreads through email attachments, fake software, pirated content or compromised websites. It can capture keystrokes and banking details, or lock your files. Cell phone theft (unlocked devices) is a major entry point.

How to protect yourself

- Avoid pirated software, movies or games.
- Do not open suspicious attachments or download files from unknown sources.
- Install reputable antivirus (e.g., from Play Store/App Store).
- Keep your phone or computer's operating system and apps updated.
- Lock your devices with a PIN or biometrics, and enable remote wiping, in case your phone gets stolen.

Ransomware attacks

Ransomware encrypts files and systems, and the perpetrators then demand cryptocurrency payment. They primarily target organisations, but individuals (especially with poor backups) can also fall victim to these attacks.

How to protect yourself

- Regularly back up important data to external servers or the cloud (offline where possible).
- Avoid suspicious attachments or links.
- Keep your device's software updated.
- Only use reputable cybersecurity tools.
- Never pay these ransoms; it funds crime and recovery is never guaranteed.

Investment and cryptocurrency scams

These scams promise high returns from low-risk investing, often via WhatsApp groups, social media ads or fake platforms. Many use fake celebrity endorsements or AI-generated content.

Warning signs

- Guaranteed profits or "secret" opportunities
- Pressure to invest/act immediately
- Requests for crypto payments
- Difficulty withdrawing funds

How to protect yourself

- Do thorough research on platforms like these (check FSCA registration).
- Be sceptical of guaranteed returns.
- Avoid unknown investment schemes or groups.
- Consult a licensed financial advisor.

AI-powered and advanced social engineering scams

AI supercharges scams in 2026, which allow for better phishing, deep faking and voice cloning.

Common in South Africa

- Deepfake videos or audio that impersonate family, bank staff or celebrities
- Voice-cloned calls ("emergency" calls from “relatives” who need money)
- AI-written perfect phishing messages
- Fake investment ads with cloned endorsements

Warning signs

- Unusual voice or odd phrasing in calls and/or voice notes
- Urgent requests for transfers (especially crypto)
- Too-good-to-be-true opportunities on social media and WhatsApp
- Your requests for live video proof get ignored

How to protect yourself

- Verify unexpected requests via known/saved contact methods.
- Ask for live proof (e.g., specific gestures or words) on video calls.
- Be sceptical of unsolicited voice calls or video; rather hang up and call back.
- Do not download apps from calls or messages.
- Report suspicious content to the applicable platform or the authorities.

Key cyber safety habits

These habits can prevent most incidents:

1. Protect passwords: Use strong, unique ones (consider a password manager).
2. Never share OTPs: legitimate entities never ask for these.
3. Think before you click or scan: Avoid suspicious links, QR codes and attachments.
4. Verify the details before you transfer money: Confirm the details via a direct call.
5. Protect your personal information: Do not share personal information online.
6. Enable multi-factor authentication: Prefer app or biometrics over SMS.
7. Check for data breaches: Use sites like https://haveibeenpwned.com/.
8. Lock your devices and report theft immediately.
9. Use scam-preventive tools such as Truecaller and bank alerts.
10. Stay updated: Follow SABRIC, your bank, or trusted sources.

What to do if you are a victim

1. Contact your bank immediately to freeze your accounts and block your cards.
2. Report the crime to the SAPS (cybercrime unit or your local station).
3. Notify your mobile provider for SIM issues.
4. Change all your passwords and enable extra alerts.
5. Report phishing to the organisation that is being impersonated.
6. Seek help from SABRIC resources or consumer protection if needed.

Final thoughts

Cybercriminals thrive on speed, confusion, urgency and trust. With AI making scams more convincing, the best defence is awareness, vigilance, caution and verification.

Cybersecurity is about habits and informed decisions, and not just technology.

Remain vigilant – threats evolve fast.