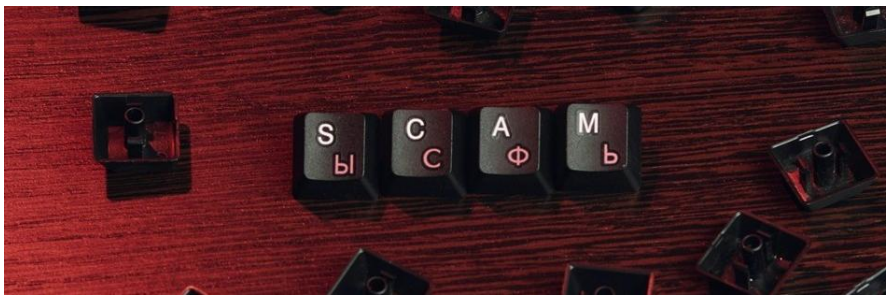
24/7 SECURITY SERVICES
Personal • Integrated • Effective

PERSONAL SAFETY BULLETIN

Bulletin 3, 2026

Digital Deception

Staying One Step Ahead of Fraudsters



In an increasingly digital and connected world, scammers are working just as hard as the rest of us — often harder. Their aim is simple: drain bank accounts, harvest personal data, or exploit urgency and confusion for financial gain. While many scams follow familiar patterns, fraudsters have become far more polished, frequently mimicking legitimate organisations convincingly enough to fool even cautious consumers.

One of the most common threats remains social engineering: **phishing** (email), **smishing** (SMS), and **vishing** (voice calls). These attacks typically involve criminals posing as banks, service providers or government departments. You might receive an SMS warning of 'suspicious activity' on your account, or a call from someone claiming to need to 'verify' your details. The message is almost always the same: act now. The safest response? Slow down. Contact the institution directly using official contact details from its verified website or app – never through the link or number provided in the message.

Another scam doing the rounds involves fake **traffic fine notifications**. Motorists receive alarming messages via SMS, WhatsApp, or email claiming outstanding fines must be paid immediately to avoid penalties or licence suspension. Fraudsters exploit that uncertainty by directing victims to cloned payment websites designed to capture banking details. Red flags include threatening language, unfamiliar web addresses and unsolicited messages from unknown numbers. Always verify fines through official government platforms rather than clicking embedded links.

Investment scams are also thriving. Slick, professional-looking trading platforms promise impressive returns with minimal risk. Once funds are deposited, communication dries up, and the money vanishes. If returns sound too good to be true, they almost certainly are.

Similarly, **job and work-from-home scams** prey on economic pressure. Adverts promise generous pay for little effort, but require upfront 'training' or 'verification' fees. After payment, the opportunity evaporates — sometimes along with your identity details.

Personal Scam Prevention Checklist

- Pause before clicking links or responding to messages from unknown sources.
- Verify any unexpected fines, investment opportunities or job offers through official websites or apps.
- Never share personal or banking information with unverified contacts.
- Keep devices and apps updated and use strong, unique passwords.
- Enable multi-factor authentication on financial and social accounts.
- Educate family and community members about common scams and red flags.
- Report suspicious contact to your bank, South African Revenue Service (SARS), or relevant consumer protection authorities.

Scams evolve as quickly as technology, but awareness remains your strongest defence.
A brief moment of caution today can prevent significant financial and emotional stress tomorrow.

#SafetyFirst