FSCA
Financial Sector
Conduct Authority

P.O. Box 35655
Menlo Park
0102

Tel. +27 12 428 8000
Toll free. 0800 20 3722
Fax. +27 12 346 6941
Email. info@fsca.co.za
Website. www.fsca.co.za

Recognising and avoiding digital banking scams.

Mamudupi Mampuru.
Given the speed at which criminals are shifting to digital platforms to lure victims out of their hard-earned money, ordinary South Africans must learn how to protect themselves against scams.

According to the South African Banking Risk Information Centre (SABRIC) 2024 crime statistics report, digital banking fraud accounted for 65,3% of all reported incidents. Cases almost doubled in volume, rising from 31,612 in 2023 to 64,000 in 2024, while losses increased from R1 billion to over R1.4 billion.

SABRIC highlights that these incidents were the result of scammers tricking people into sharing personal details, rather than technical compromises of banking platforms.

Similarly, the Financial Sector Conduct Authority (FSCA) has warned of a rise in scams via SMS, WhatsApp, Telegram, fake social media pages, and fraudulent banking apps. In its 2024 Regulatory Actions Report, the FSCA noted that it had issued over 100 public warnings during that year, highlighting impersonations, deepfake ads, and finfluencer scams as growing threats.

The FSCA also continues cautioning the public against criminals posing as FSCA staff to extort money, phishing (emails or links posing as banks or the South African Revenue Service), and finfluencers promising guaranteed returns. Regardless of the chosen method, the aim of scammers is the same, namely, to steal as much money as possible, and as quickly as possible.

Why consumers fall for scams. Scammers exploit urgency, fear, and trust to trick people. It is therefore important to understand how anyone can easily become a scam victim, no matter their earnings, circumstances, or level of education. Scammers rely on:

- **Urgency:** Creating panic to prevent clear thinking.
- **Trust:** Messages appear legitimate, from banks, the South African Revenue Service (SARS), or friends.
- **Financial pressure:** Tempting promises of “quick money.”
- **Technology tricks:** Fake websites, cloned apps, and realistic emails.
- **AI misuse:** Scammers use AI to create fake voices, flawless emails, and cloned sites, making scams harder to spot. Awareness of these tactics helps you to pause and think before reacting.

Common types of banking scams

Scams take many forms, with some of the most common being phishing and OTP fraud, identity theft, investment schemes, and impersonation scams. Scammers send links via SMS, email, or WhatsApp that mimic your bank's login page. Once clicked, you're redirected to a fake site where entering your details allows scammers to capture your username, password, or One-Time PIN (OTP). For example, an SMS may warn that your account will be blocked unless you log in, but the link is designed to steal your information.

How to protect yourself

Never click on SMS links to access your bank and remember your bank will never ask for your OTP or password by phone, SMS, or email.

Shred old documents and never share your ID unless certain of the recipient. With a copy of your ID or a leaked password, scammers can open credit in your name, often discovered only when debt collectors call or your credit applications are declined. For example, you email your ID for a fake job and later get a bill for an account you never opened.

It is a good idea to check your credit report regularly for unauthorised accounts. You can access your free report via the Credit Bureau Association or directly through Experian, TransUnion, ClearScore, Compuscan, RCS, or DirectAxis Pulse to spot fraud early.

Crypto scams

South Africa has been home to some of the world's largest crypto scams, including Mirror Trading International (MTI), which defrauded investors of about R8.6 billion. Smaller schemes like Obelisk also cost thousands of people over R112 million. These scams often spread through WhatsApp and Telegram groups, fake trading platforms, and social media finfluencers who promise to double your money in days. Instead, the group disappears along with your money!

Know this: If someone promises to easily double your money in days, it's a scam. Legitimate investments have compulsory paperwork, clear terms, and regulated providers. Scams may look official but often promise unrealistic returns, use vague or no paperwork, and apply pressure. Always verify registration and review documents before investing. Check on www.fsca.co.za that the company or advisor is registered and authorised for the specific type of investment.

Impersonation scams

Fraudsters often pose as trusted people, bank staff, officials, or even relatives to steal information or money. For example, you may get a WhatsApp or SMS from a relative urgently asking for money, but it could be a hacked or cloned account. If someone claims to be from your bank, hang up and go to the bank in person. If a "relative" asks for urgent money, confirm by calling them directly.

Protect yourself and others

The scams mentioned are only a glimpse of what exists, so constant vigilance is key. Stay informed, question anything suspicious, and take proactive steps to protect yourself, your family, and your community by reporting scams and spreading awareness. Remember that fraud is a threat to the entire financial system of our country.

Did you like this article? Share this with your friends and family and help build a financially prosperous South Africa.

For more articles and FREE financial literacy information visit www.fscamymoney.co.za or to request a free financial literacy workshop, kindly email CED.Consumer@fsca.co.za

Alternatively contact the Financial Sector Conduct Authority (FSCA) on 012 428 8000 or 0800 20 3722 and ask to speak to one of our call centre agents.

You can also follow the FSCA on the following social media platforms:

- Facebook: FSCA South Africa
- Twitter: @FSCA_ZA
- YouTube: FSCA Connect
- LinkedIn: Financial Sector Conduct Authority
- Website: www.fsca.co.za