FINANCIAL INTELLIGENCE CENTRE

DIGITAL FRAUD FOREWARNING REPORT

ISSUED: JANUARY 2026

Background

Digital fraud has emerged as a serious and growing threat in Namibia, driven by increased use of mobile phones, mobile money services, internet banking, and social media platforms.

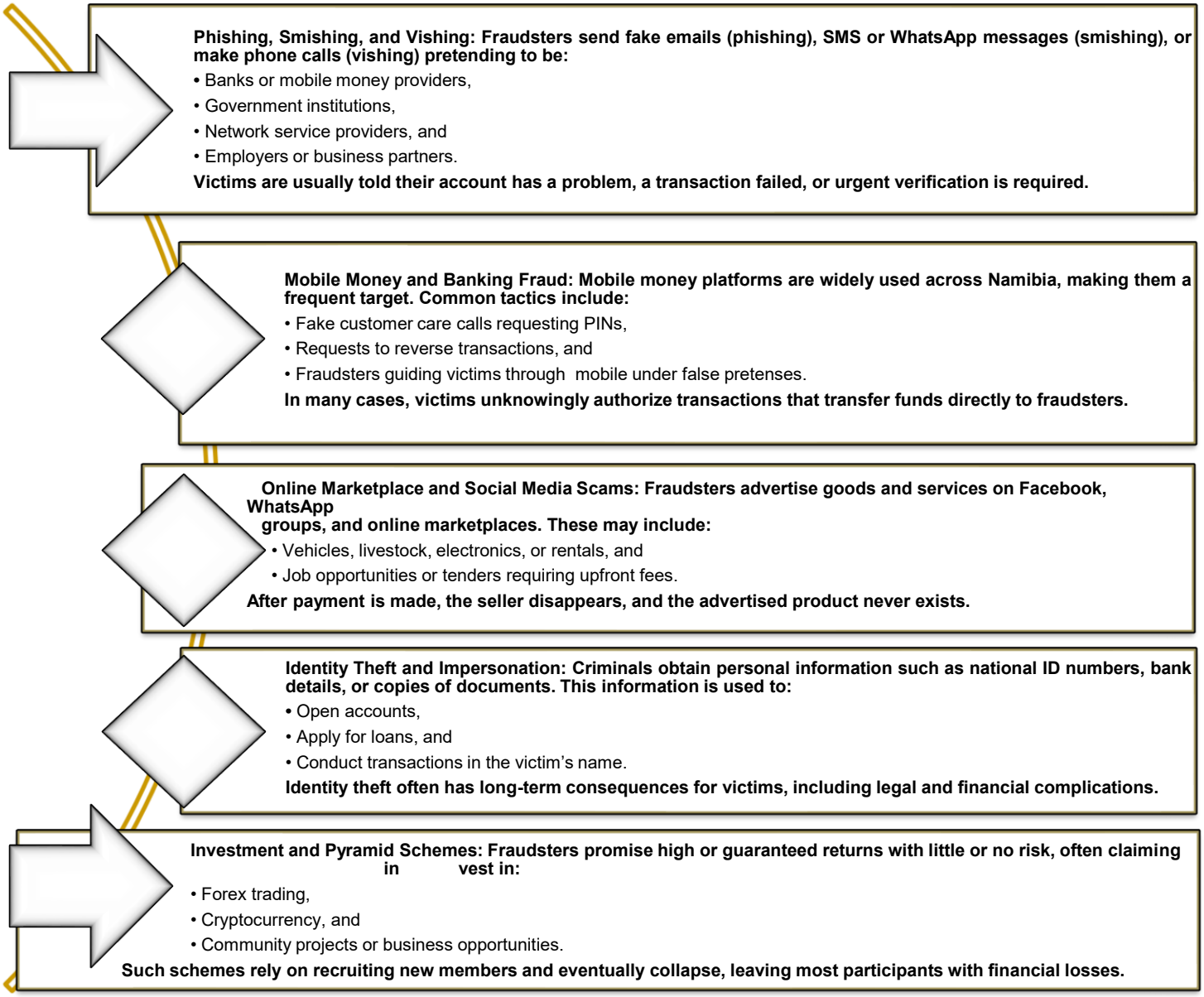
While digital financial services have improved access to banking and economic participation, they have also created opportunities for criminals to exploit individuals through deception and manipulation.

Digital fraud refers to any fraudulent activity conducted using electronic communication or digital platforms, including mobile phones, the internet, and online applications.

This report aims to forewarn the public on how digital fraud commonly occurs in Namibia, identify key risk areas, and provide practical guidance on how individuals can protect themselves from becoming victims. Other than financial losses, the proceeds from such activities are often laundered, undermining the integrity of our financial system.

How do these fraudulent scams operate?

Digital fraud in Namibia often targets ordinary citizens, small businesses, and vulnerable groups such as the elderly and first-time digital users. The most prevalent forms include the following:



Digital Fraud prevention measures/ How to protect yourself

Prevention Area	Key Actions to Take	Visual / Sign (for Design Use)
Protect personal information	* Never share PINs, passwords, or OTPs. * Secure your phone and SIM card. * Do not share ID or bank details unnecessarily.	 Lock / Shield Icon
Verify communications	* Legitimate institutions do not ask for confidential details. * Use official contact details to verify messages. * Be cautious of unusual or urgent messages.	 Check / Verify Icon
Practice safe digital habits	* Use strong, unique passwords. * Enable two-factor authentication (2FA). * Keep devices and apps updated.	 Mobile Security Icon
Be careful with payments and investments	* Do not send money to unknown persons. * Avoid “guaranteed returns” schemes. * Take time to seek advice before investing.	 Warning / Money Icon
Report Suspicious Activities	* Report immediately to your bank or mobile money provider. * Notify relevant authorities or the FIC. * Early reporting helps prevent further losses.	 Report / Alert Icon

THINK BEFORE YOU CLICK OR SEND

Digital fraud can happen to ANYONE.

One call, message, or link is all a scammer needs to steal your money.

Fraudsters pretend to be banks, mobile money agents, online sellers, or even friends you trust.

Never share your PIN, password, or one-time code.

Never rush — VERIFY FIRST.

If it sounds too good to be true, IT'S A SCAM.

STAY ALERT. PROTECT YOUR MONEY. PROTECT YOUR FUTURE.