Warning for South Africans who use WhatsApp on their phones

Criminals are increasingly using impersonation tactics, posing as friends, family members, or colleagues to deceive people into handing over money or sensitive information.

This is the warning from cybersecurity expert Lucas Molefe, who warned South Africans about the growing wave of scams targeting WhatsApp users.

“First of all, they typically focus on SIM swaps, which steal the actual number, and this is usually done through phishing attempts,” Molefe explained.

“Another way is through your linked accounts, because WhatsApp is connected to Instagram and Facebook, scammers can gather information like your birthday or family connections to make their impersonation more convincing.”

According to Molefe, the most common and dangerous method remains SIM swaps, where criminals trick victims into sharing one-time passwords (OTPs).

Once they have access, scammers can hijack WhatsApp accounts, bank profiles, and even broader digital identities.

These scams often begin with fraudsters pretending to be someone you trust. They may claim to have a new number, clone or spoof an existing number to appear legitimate, or use stolen profile pictures to set up convincing duplicate accounts.

To increase the pressure, they create urgent stories that make the victim feel compelled to act immediately.

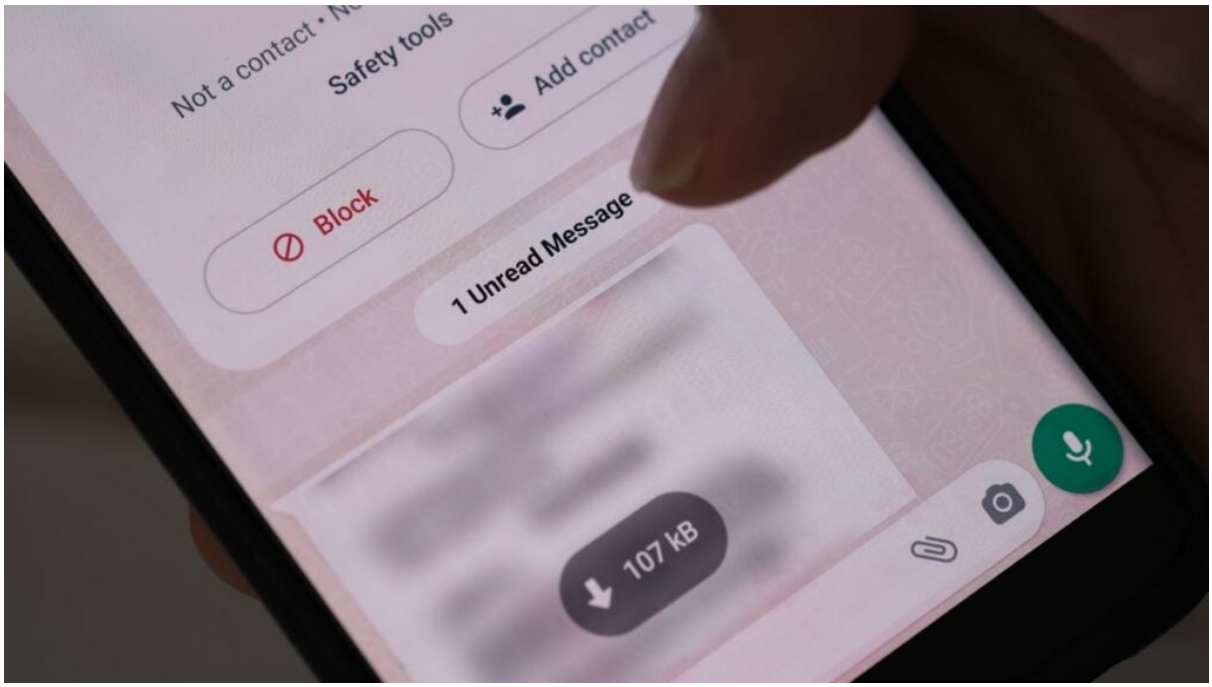
“Sometimes they impersonate someone you know or someone you trust. This happens a lot in NPOs and NGOs, and even in businesses,” Molefe warned.

“They impersonate a colleague and say, ‘Hey, I just want to check, do you see a WhatsApp OTP that just appeared? Can you give it to me quickly? I need it urgently.’ You’re going to give it because it comes with urgency.”

The psychology behind these scams makes them highly effective. “If I’m your friend or a family member and I send you a message with urgency, you’re going to first look at it and say, ‘Okay, I know Lucas,’” Molefe explained.

“Because you know me, it’s easier to communicate with me and provide assistance. And that’s what scammers exploit: urgency and trust.”

Verify the person’s identity



Criminals also use information gathered from Facebook and Instagram to make their impersonation even more convincing, piecing together birthdays, family connections, and other personal details to build credibility.

Common warning signs include receiving an unexpected message from someone claiming to have a new number, being asked for money or sensitive details with urgency, refusal to take voice or video calls, and requests to share OTPs or click on suspicious links.

“WhatsApp takeovers are often preceded by someone pretending to be from a bank or service provider who asks for the OTP sent to a user’s phone,” Molefe explained.

Recovering a hijacked account is not always straightforward, especially in cases involving SIM swaps.

“If it’s taken via SIM swap, they’ve actually taken control of your number, so that’s a bit difficult,” Molefe said.

“The best advice is to go straight to your network service provider and tell them what’s happening, so they can help. It’s also important to alert your bank.

“Once your number is taken, it’s not just your WhatsApp that’s at risk, but your whole digital identity.”

He added that criminals sometimes even clone numbers so both the victim and scammer receive the same messages, making it harder to detect the fraud. Molefe stressed that the best defence is prevention.

“Businesses are using WhatsApp, everyone is using WhatsApp, and the best way is to just protect yourself by enabling things like two-factor verification,” he said.

To stay safe, Molefe advised that people never share OTPs or personal details via WhatsApp, even with contacts they know.

If a request seems suspicious, users should verify the person’s identity through another method, such as a direct call or face-to-face conversation.

If an account is compromised through a SIM swap, victims should immediately contact their mobile provider and their bank to secure their number and accounts.

“Ultimately, scammers are exploiting trust and urgency. The more people are aware of these tactics, the harder it becomes for criminals to succeed,” said Molefe.