

# INFORMASIE TECHNOLOGIE

## INFORMATION TECHNOLOGY

### WHATSAPP SCAMS

Several WhatsApp scams are popping up in South Africa at the moment and it might be a good idea to look out for these latest threats.

#### 1. WhatsApp Gold

This is a simple phishing attack where you receive a message that says you have been selected for WhatsApp Gold. Often this app is advertised as free and you are asked to complete a survey or make a purchase. The message contains a link to download WhatsApp Gold. Malware enables hackers to steal your information or even to spy on your messages. If you are falling for scams like this never click on unknown links or download apps from untrusted sources.

#### 2. Verification request

Scammers usually send verification requests from a number impersonating a fake business. They offer a voucher for a local supermarket in return for completing a survey. The survey leads to a fake website impersonating the supermarket's website. If you provide your details on the website, your information has been compromised and is fed back to the scammers. Several students have reported scams using their branding on a fake WhatsApp account.

#### 3. Spy apps

WhatsApp does not allow you to find a link to download a WhatsApp "spy app" claiming to be able to intercept your messages. However, there are many other apps available on the Google Play Store that claim to do this. Unfortunately, there is no way to intercept WhatsApp messages in this way as all WhatsApp conversations are encrypted. These fake "spy app" applications usually install malware on your phone or sign you up for expensive subscription services. Several students have reported that they have recently fallen victim to these scams. It is important to realise that the Google Play Store is not infallible and can also contain malware-infested spy apps.

#### 4. Verification request scams

The last two scams are by far the most popular in South Africa. Verification request scams are spread through compromised accounts. (some of people you might know) You will receive a message from a user on your WhatsApp contact list asking to send your WhatsApp verification code. If you do, scammers will have access to your WhatsApp account and can take over your number. Never divulge your WhatsApp verification code and be wary of strange requests from your contacts.

#### 5. SIM-swop takeover

Currently this is by far the biggest threat to South African WhatsApp users. The financial losses incurred by sim-swop victims in 2018 was a whopping R89 million. When SIM-swop fraud happens and the fraudsters take ownership of your number, they can easily and instantly install WhatsApp on their own smartphone and log in to your account. The two-factor authentication message will be sent to the number they now control and using WhatsApp, they can scam your contacts into divulging information or send them money by impersonating you.

This is also a serious threat to other platforms that use SMS two-factor authentication – including many banking apps. You should check immediately with your cell phone provider if you lose access to your cell phone network for no apparent reason, as this is the first sign that SIM-swop fraud might have been committed.



Posted in: [Communication](#), [Security](#) | | [With 0 comments](#)