SIM SWOPS:

Through fraudulent SIM swops, criminals can take control of their victim's mobile number enabling them to receive SMS's sent by the bank to the client. These include Transaction Verification Codes (TVC), Random Verification Number (RVN), PINs or One Time Passwords (OTPs). Using these codes together with compromised login credentials, criminals can change, add beneficiaries and transfer money out of the victim's account.

Criminals are also known to port their victim's cell phone number fraudulently before doing a fraudulent SIM swop. Mobile Number Portability (MNP) gives mobile phone users the ability to move to another mobile network and still retain their mobile number (MSISDN). In this scenario, the victim's SIM card is deactivated and the criminal receives communication for the new SIM card issued by the second mobile network operator, enabling them to receive a victims Transaction Verification Codes (TVC), Random Verification Number (RVN,) PIN or One Time Passwords (OTPs).

TIPS

- Ensure that the device you use for internet or mobile device banking has the latest version of antivirus and antispyware software installed from a reputable vendor. Robust solutions should identify malware and prompt you to delete it.
- Do not do your banking on a public or unfamiliar computer found at libraries, internet cafes and hotels.
- Avoid using WiFi hotspots, and ensure your own wireless network is encrypted before performing any banking transactions on your private computer. Prevent illegal software from being downloaded on your computer by creating administrative rights.
- Be suspicious if you receive lots of spam email or SMS messages. It could indicate that your computer or cell phone has been infected.
- Beware of fake anti-virus software that is offered at no charge, as it could contain malware.
- Do not use unknown devices, such as USB flash drives on your system, as they may transfer malware unknowingly.
- Avoid downloading pirated software as it may contain malware.
- Memorise your PIN and passwords and never write them down or share them, not even with a bank official.

- Make sure your PIN and passwords cannot be seen when you enter them.
- If you think your PIN and/or password has been compromised, change it immediately either online or at your nearest branch.
- Choose an unusual PIN and password that are hard to guess and change them often.
- For your security you only have three attempts to enter your PIN and password correctly before you are denied access to your services.
- Register for your bank's cell phone notification service and receive electronic messages relating to activities or transactions on your accounts as and when they occur.
- If the reception on your cell phone is lost, immediately check what the problem could be, as you could have been a victim of an illegal SIM swop on your number. If confirmed, notify your bank immediately.
- Inform your Bank should your cell phone number changes so that your cell phone notification contact number is updated on the banking system.
- Regularly verify whether the details received from cell phone notifications are correct and correspond to recent activity on your account. Should any detail appear suspicious, contact your Bank immediately and report all log-on notification that are unknown to you.
- Log onto your Bank's website by typing in the web address yourself instead of accessing it via Google search as it might lead you to a spoofed site.
- Do not use web links that are saved under your favourites and never access your Bank's website from a link in an email or SMS.
- Remember to log off immediately when you have finished banking.
- Make sure that no one has unauthorised access to your PC.
- Be especially aware that there are no security cameras trained on your PC and keyboard.
- Make sure that the software loaded onto your PC is correctly licensed.

- Never click on links or attachments in unsolicited or suspicious emails as harmful viruses, spyware & trojans could infect your PC.
- Install a personal firewall on your PC.
- Be cautious when using storage devices such as memory sticks and portable hard drives, and if you do make use of them, ensure that they are password protected.
- Don’t send emails that contain personal information, such as your card number and expiry date.
- Install a spam blocker on your system. This will ensure that fraudsters find it difficult to send you phishing emails.
- Keep your operating system and browser patches, and antivirus software up to date on your personal computer/laptop or cell phone, as they include important security enhancements to help detect phishing sites and malware.
- Should you realise that you have responded to a phishing mail, change your internet banking credentials immediately and advise your bank.

https://www.sabric.co.za/stay-safe/internet-banking/