Be your money’s best protection by following these tips provide by SABRIC

1. Tips when using ATM’s

- If you think the ATM is faulty cancel the transaction IMMEDIATELY, report the fault to your Bank and transact at another ATM.
- Avoid ATMs that are dimly lit or surrounded by loiterers, and never allow your children to draw money using your card, since they're the most vulnerable to perpetrators.
- Have your card ready in your hand before you approach the ATM to avoid opening your purse, bag or wallet while in the queue.
- Be cautious of strangers offering to help as they could be trying to distract you to get your card or PIN.
- Follow the instructions on the ATM screen carefully.
- ONLY punch in your PIN once prompted by the ATM.
- Report suspicious items or people around ATMs to the Bank.
- Choose familiar and well-lit ATMs where you are visible and safe.
- Report any concerns regarding the ATM to the Bank. Toll free numbers are displayed on all ATMs.
- Be alert to your surroundings. Do not use the ATM if there are loiterers or suspicious people in the vicinity. Also take note that fraudsters are often well dressed, well-spoken and respectable looking individuals.
- If you are disturbed or interfered with, whilst transacting at the ATM, your card may be skimmed, by being removed and replaced back into the ATM without your knowledge. Cancel the transaction immediately and report the incident using your Bank's Stop Card Toll free number which is displayed on all ATMs, as well as on the back of your Bank card.
- Should you have been disturbed whilst transacting, immediately change your PIN or stop the card, to protect yourself from any illegal transactions occurring on your account.

- Know what your ATM looks like so that you can identify any foreign objects attached to it.
- Do not ask anyone to assist you at the ATM, not even the security guarding the ATM or a Bank official. Rather go inside the Bank for help.
- Never force your card into the slot as it might have been tampered with.
- Do not insert your card if the screen layout is not familiar to you and looks like the machine has been tampered with.
- Don’t use ATMs where the card slot, keypad or screen has been tampered with. It could be an attempt to get hold of your card.
- Your PIN is your personal key to secure banking and it is crucial to keep it confidential.
- Memorise your PIN, never write it down or share it with anyone, not even with your family member or a Bank official.
- Choose a PIN that will not be easily guessed. Do not use your date of birth as a PIN.
- Cover your PIN when punching the numbers even when alone at the ATM as some criminals may place secret cameras to observe your PIN.
- Don't let anyone stand too close to you to keep both your card and PIN safe.
- Some fraudsters wait until you’ve drawn your cash to take advantage. Be wary of people loitering around the ATM and ensure that you are not followed.
- Take your time to complete your transaction and secure your card and your cash in your wallet, handbag or pocket before leaving the ATM.
- Set a daily withdrawal limit that suits your needs (the default amount is set at R1000.00), to protect yourself in an event that your card and PIN are compromised.
- Check your balance regularly and report discrepancies to your Bank IMMEDIATELY.
- Avoid withdrawing cash to pay for goods/services as your Debit Card can be used for these transactions. You can use your Debit Card wherever the Maestro/Visa Electron logo is displayed.
- After you have completed your transaction successfully, leave the ATM area immediately. Be cautious of strangers requesting you to return to the ATM to

finalise/close the transaction because they are unable to transact. Skimming may occur during this request.

- Prioritise the setting of daily withdrawal and transaction limits.
- Set a daily ATM withdrawal limit that suits your needs.
- Transaction limits should also be in line with daily spending.
- Set limits on international transaction expenditure.
- Inter account transfer limits should also be managed wisely.

2. <u>Tips to prevent Phishing and Vishing</u>

Phishing:

- Do not click on links or icons in unsolicited e-mails.
- Do not reply to these e-mails. Delete them immediately.
- Do not believe the content of unsolicited e-mails blindly. If you are worried about what is alleged, use your own contact details to contact the sender to confirm.
- Type in the URL (uniform resource locator or domain names) for your bank in the internet browser if you need to access your bank's webpage.
- Check that you are on the real site before using any personal information.
- If you think that you might have been compromised, contact your bank immediately.
- Create complicated passwords that are not easy to decipher and change them often.

Vishing:

- Banks will never ask you to confirm your confidential information over the phone.
- If you receive a phone call requesting confidential or personal information, do not respond and end the call.
- If you receive an OTP on your phone without having transacted yourself, it was likely prompted by a fraudster using your personal information. Do not provide the OTP telephonically to anybody. Contact your bank immediately to alert them to the possibility that your information may have been compromised.

- If you lose mobile connectivity under circumstances where you are usually connected, check whether you may have been the victim of a SIM swop.

3. Tips for Carrying Cash Safely

Tips for Individuals

- Carry as little cash as possible.
- Consider the convenience of paying your accounts electronically (consult your bank to find out about other available options).
- Consider making use of cell phone banking or internet transfers or ATMs to do your banking.
- Never make your bank visits public, even to people close to you.

Tips for Businesses

- Vary the days and times on which you deposit cash.
- Never make your bank visits public, even to people close to you.
- Do not openly display the money you are depositing while you are standing in the bank queue.
- Avoid carrying moneybags, briefcases or openly displaying your deposit receipt book.
- It is advisable to identify another branch nearby you that you can visit to ensure that your banking pattern is not easily recognisable or detected.
- If the amount of cash you are regularly depositing is increasing as your business grows, consider using the services of a cash management company.
- Refrain from giving wages to your contract or casual labourers in full view of the public; rather make use of wage accounts that can be provided by your bank.
- Consider arranging for electronic transfers of wages to contract or casual labourers' personal bank accounts.

Tips for Stokvel Groupings

- Refrain from making cash deposits of club members' contributions on high-risk days (e.g. Monday after month end).
- Ensure persons depositing club cash contributions or making withdrawals are accompanied by another club member.
- A stokvel savings club or burial society can arrange for members to deposit cash directly into the club's account instead of collecting cash contributions.
- Arrange for the club's pay out to be electronically transferred into each club member's personal account or accounts of their choice.
- Take another person with when going to deposit club cash contributions

4. <u>Tips for protecting your Personal Information</u>

- Don't use the same username and password for access to banking and social media platforms.
- Avoid sharing or having joint social media accounts.
- Be cautious about what you share on social media.
- Activate your security settings which restrict access to your personal information.
- Don't carry unnecessary personal information in your wallet or purse.
- Don't disclose personal information such as passwords and PINs when asked to do so by anyone via telephone, fax or even email.
- Don't write down PINs and passwords and avoid obvious choices like birth dates and first names.
- Don't use any Personal Identifiable Information (PII) as a password, user ID or personal identification number (PIN).
- Don't use Internet Cafes or unsecure terminals (hotels, conference centers etc.) to do your banking.
- Use strong passwords for all your accounts.
- Change your password regularly and never share them with anyone else.
- Store personal and financial documentation safely. Always lock it away.
- Keep PIN numbers and passwords confidential.

- Verify all requests for personal information and only provide it when there is a legitimate reason to do so.
- To prevent your ID being used to commit fraud if it is ever lost or stolen, alert the SA Fraud Prevention Service immediately on 0860 101 248 or at safps.org.za.
- Ensure that you have a robust firewall and install antivirus software to prevent a computer virus sending out personal information from your computer.
- When destroying personal information, either shred or burn it (do not tear or put it in a garbage or recycling bag).
- Should your ID or driver's license be stolen report it to SAPS immediately.

5. <u>Tips for protecting yourself against SIM Swops</u>

- If 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 its systems.
- 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.
- Regularly verify whether the details received from cell phone notifications are correct and according to the recent activity on your account. Should any detail appear suspicious immediately contact your Bank and report all log-on notification that are unknown to you.
- Memorise your PIN and passwords, 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.