

INTERNET FRAUD

AVOID!!!! Doing banking on computers to which the general public has access.

It is the intention of the fraudster to gain access to your password and account details.

This is done by :

- a) placing keyloggers on the tower (keyboard in put) to record all your keystroke information.
- b) sending you an e-mail with keylogger software as an attachment
- c) Phishing : sending you an e-mail that appears to come from the bank (all logos and colours present)
- d) Sim-Swop: the victim's cellphone number is obtained by posing as the owner and reporting the cell stolen to the Cellphone Service Provider- this renders the victim's cell useless whilst the fraudster intercepts the password/pin sent by the bank for the online transaction.



- ▶ **NB!** Do not open e-mails if you are not familiar with the sender. Remember no Financial Institution would request for your login/logon details via e-mail.
- ▶ Remember to install up-to-date anti-virus and anti-spy software.
- ▶ Install adequate Phishing Filters. Do regular checks for foreign software.

<u>COMMERCIAL CRIME</u>	<u>TEL NUMBER</u>	<u>FAX NUMBER</u>
Middelburg	(013) 249 1413	(013) 249 1441
Nelspruit	(013) 752 1031	(013) 752 6462
Durban	(031) 332 2534	(031) 332 2544
Pietermaritzburg	(033) 845 8534	(033) 845 8529
Potchefstroom	(018) 299 7633	(018) 299 7628
Klerksdorp	(018) 464 5360	(018) 464 5365
Mafikeng	(018) 397 0323	(018) 397 5598
Germiston	(011) 871 5000	(011) 201 9758
Johannesburg	(011) 870 5312	(011) 870 5322
Pretoria	(012) 401 3349	(012) 401 3363
Limpopo	(015) 293 7265	(015) 290 7254
Oudtshoorn	(044) 803 4516	(044) 803 4680
Western Cape	(021) 918 3261	(021) 918 3306
Kimberley	(053) 839 2828	(053) 833 5210
Bloemfontein	(051) 503 2802	(051) 503 2909
Thabong	(057) 916 6510	(057) 352 1350
Bothlokong	(058) 307 5918	(058) 307 5904
Head Office	E mail: comm.banking@saps.org.za	



Making South African banking safe, secure and fraud free

www.sabric.co.za



DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

COMMERCIAL CRIME SAFETY TIPS



HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

CONTENTS

1. ATMS / CARD FRAUD
2. DEPOSIT SLIP/REFUND SCAM
3. CHEQUE FRAUD
4. INTERNET FRAUD

Always protect your PIN!! AT ATM'S...

Be **vigilant**. Carefully scan the area for suspicious characters. Do not be fooled by people who are well-dressed and eloquent. Fraudsters often pose as custodians of the bank.

Emphatically refuse ANY assistance offered by any person.

Do not allow people to look over your shoulder or press any of the keyboard keys of the ATM whilst you are busy.

If you are remotely suspicious, postpone using the ATM until it is safer to do so.

If you suspect your card has been compromised, cancel it immediately.

Check the machine for any attachments, often the crooks would position skimming devices or pin-size cameras at the ATM to obtain your details.

If your card is not returned, check the ATM slot for a strip of x-ray material which is glued inside with the intention of 'trapping' your card.

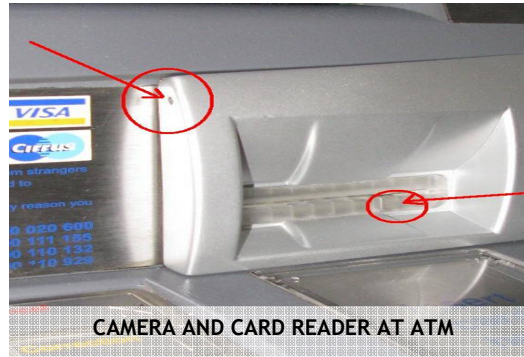
Do not allow your card to be swiped through any device.



THERE ARE VARIOUS LOOKING
SKIMMING DEVICES

FOLLOW YOUR CARD!!! This is one exercise which could save you thousands of rands. It takes a fraudster or a waiter two seconds to swipe your card through a skimming device in order to reproduce a cloned version of your card.

Ensure you are present to monitor the transaction at the point-of-sale device.



DEPOSIT SLIP/REFUND SCAM

In most cases the fraudster would deposit a fraudulent cheque into the victim's bank account. The victim would then be coerced into releasing goods or refunding monies without checking whether the funds are cleared. Another slant to this scam is to overpay the "quoted" amount and request a refund of the difference.

A favourite is to fax a letter to the victim which appears to come from one or other legitimate entity e.g. SARS; TELKOM; DEPT OF LABOUR etc. The fraudster would contact the victim and inform him that an erroneous payment or overpayment was made and that the difference should be repaid immediately.

Most people lose money because they are pressurized so by the fraudster and do not follow elementary business practices i.e. Wait for the mandatory clearing period for cheques; Speak to the bank to check the deposit made into your account; call the entity (SARS) as listed in the directory and not as on the fax; speak to your bank and request them to check whether the accountholder is indeed whom he says he is; if it is a cash deposit, then confirm with your bank that this is indeed so.

"ACCOUNT- TAKEOVER"

Be careful when being informed that one of the companies you are doing business with, has changed their account details.

The fraudsters would thoroughly research these details and request you pay the exact amount owing into a new account, one they are the beneficiary of. Confirm whom you are paying, it is in your best interest to do so.

CHEQUE FRAUD

Never sign blank cheques. File away cheques with your statements in a secure place as they provide a copy of your signature. Shred cheques if you wish to dispose of it.

Report losses immediately and always ensure the integrity of staff.

Do not use ink on cheques which can easily be erased, to complete cheques use a ballpoint pen or an inkjet printer.

DO NOT MAIL CHEQUES!! As the syndicates have placed people strategically to intercept them. Effect a direct payment or conduct an electronic transfer into the intended account. Check the authenticity of the ID which accompanies the cheque payment i.e. Compare the face; has the photo on the ID document been tampered with; you can even request the person's Driver's license to compare the two; Retain a copy of the ID and confirm the contact details.

BE ALERT WHEN LARGE CHEQUE TRANSACTIONS ARE DONE JUST BEFORE THE CLOSE OF BUSINESS.