how can we help you?

protect yourself from fraud.

www.fnbnamibia.com.na

FNB
First National Bank

ATM Fraud

Do's

- If you think the ATM is faulty, cancel the transaction immediately; report the fault to your Bank and transact at another ATM.
- 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 in order to get your card or PIN.
- Follow the instructions on the ATM screen carefully.
- 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 of 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 and immediately 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 are able to identify any foreign objects attached to it.

Don'ts

- Do not ask anyone to assist you at the ATM not even the security guard 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, key pad or screen has been tampered with. It could be an attempt to get hold of your card.

Tips for **protecting your PIN**

- 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 members or a Bank official.
- Choose a PIN that will not be easily guessed. Do not use your date of birth as a PIN. Key your PIN in personally in such a way that no one else can see it e.g. 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 in order to keep both your card and PIN safe.

Tips for **protecting your cash**

- 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 N$2000.00), to protect yourself in the 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 or services as your Debit Card can be used for these transactions. You are able to 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.

Telephone numbers for **reporting ATM related incidents:**

Bank Windhoek	**061 299 1200** or **081 251 2425**
First National Bank of Namibia	**061 299 2999**
Nedbank	**081 127 3051** or **08 0000 2008**
SME Bank	**08 0001 1583**
STD Bank	**061 294 2363**
City Police	**061 302 302**
Nampol	**061 10111**

Card Fraud and Skimming

Important tips to **avoid card fraud**

- Review your account statements on a regular basis; query disputed transactions with your Bank immediately.
- When shopping online, only place orders with your card on a secure website.
- Do not send e-mails that quote your card number and expiry date.
- Ensure that you get your own card back after every purchase.
- Never write down your PIN or disclose it to anyone.
- Report lost and stolen cards immediately.
- Shred your credit card receipts before discarding them.
- Never let the card out of your sight when making payments.
- Sign your card on the signature panel as soon as you have received it to stop anyone else form taking ownership or trying to use it.
- Your credit card is not transferable. Only the person whose name appears on the front of the card is authorised to use it. This is the same with your debit cards, even though they don't contain your name on the front of the card.
- If you have debit, cheque and credit cards, don't choose the same PIN for them all, so that if you lose one, the others will still be safe.
- Always check transaction slips, check them against your statement to spot any suspicious transactions and query them immediately.
- Make a list of all your cards and their numbers and store them in a safe place. This does not include PINs and passwords.
- Should your card be retained by an ATM, contact your Bank and block your card before you leave the ATM.
- Store your bank's Call Centre number on your Cellphone so that you have it handy should you need to stop your card.
- Subscribe to your Bank's SMS notification services; this will inform you of any transactional activity on your account.

eWallet Fraud

- Be aware that NO bank will ask you to do an eWallet payment to release funds, not even for an insurance or life assurance policy.
- If you are called via the telephone and instructed to do an eWallet payment for any competition or to release funds:
    - Take the person's details, name, tel no and title of the person they claim to be

- Hang up the phone and call the company back via their switchboard number in the telephone directory, check if you have been contacted and did indeed win any money
- Report this to the Banking Institution at Tel: (061) 299 22 22/2101 Fraud Division

Cheque Fraud

Look out for:

- Alterations to the payee, amount in words and figures.
- Stamps that are placed over areas that could conceal alterations.
- Spelling mistakes on the printed areas of the cheque such as the drawer's details and the Bank Branch name.
- Tampering on the MICR Code line – black shaded areas.
- Cheques that appear faded, as chemicals could have been used to remove information.
- Shaky signatures, it could indicate that the signature was traced.

How to **protect yourself against cheque fraud:**

- Write clearly and neatly using a non-erasable ballpoint pen.
- Write the full names of the payee and spell them correctly. Avoid the use of abbreviations.
- Do not make any corrections to the cheque as alterations in any form will not be allowed on the cheque except for when the words 'bearer/order' has been ruled through. It is best to cancel it and write out another one.
- Don't leave large spaces between words and draw a line through any unused space to ensure that nothing can be added to the cheque.
- Write the amount of the cheque in the space immediately after 'The sum of'. According to the Bill of Exchange Act the amount in words will be considered the correct amount if there is a difference between the amount in words and figures.
- Write the amount in figures as close to the 'N$' as possible.
- Fill in the correct date.
- Remember to sign your cheque.
- Keep your cheque book and used cheques locked away and check that you have control over all the cheques by taking note of the number sequence.
- Reconcile your cheque book regularly to identify any irregularities.
- Report suspected cheque fraud to your bank and the police, immediately.

Identity Theft

What is **ID theft?**

Identity theft is when someone steals your personal information to use for illegal purposes.

What is **Personal Information?**

- ID
- Passport
- Driver's license
- Salary advice
- Municipal bill and merchant account statements
- Bank statements

There are people who gather personal information about you to enable them to impersonate you in order to access your funds. Make sure that you protect your personal information.

Don'ts

- 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 e-mail.
- Don't write down PINs and passwords and avoid obvious choices like birth dates and first names.
- Don't use Internet Cafe's or unsecure terminals (hotels, conference centres etc.) to do your banking.

Do's

- Protect your personal information at all times.
- Manager your personal information wisely.
- When destroying personal information, either shred or burn it (do not tear or put it in garbage or recycling bag).
- Store personal and financial documentation safely. Always lock it away.
- Keep PINs and passwords confidential.
- Pay attention to account cycles so that you can identify when communications intended for you have not reached you.

In the instance that your ID gets used to commit fraud or if it ever gets lost or stolen, you should alert the Namibian Police Services (NAMPOL) immediately. It is always advisable to keep an affidavit to that effect and also inform your banker to take note and update records.

- Follow-up on account statements not received, they may have been stolen with the aim of victimising you. Rather have your statements e-mailed to you. Request that sensitive documents be sent via registered mail or door-to-door mail, as items can easily be stolen while in the post.
- Verify all requests for personal information and only give it out when there is a legitimate reason to do so. Install firewall and antivirus software protection to prevent a computer virus sending out personal information from your computer.
- Should your ID or driving license be stolen, report it to the NAMPOL immediately.

Phishing

Fraudsters send unsolicited e-mails to recipients purporting to come from a reliable source like the bank, the Receiver of Revenue or your e-mail service provider. In the mail they ask you to click on a hyperlink or icon to either view additional information or to submit information. Once clicked, the link will divert the victim to a fraudulent website under control of the fraudsters and any information entered onto this page will be sent to the fraudsters. The information requested is usually personal information and could include usernames and passwords for banking platforms or e-mail accounts as well as Cellphone numbers and bank card details. Clicking on the link or icon could also result in the victim's computer being infected with malware.

Don'ts

- 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.

Do's

- Type in the URL for your bank in the internet browser if you need to access your bank's webpage.
- If you think that you might have compromised yourself, contact your bank immediately.
- Check that you are on the real site before using any personal information.

Internet Banking

Are you using your PIN and password correctly to keep your money safe and secure?

- Memorise your PIN and password, never write them down or share them, not even with a bank official.
- Make sure your PIN and password 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 services.
- Register for your Bank's Cellphone notification service and receive electronic messages relating to activities or transactions on your accounts as and when they occur.
- Inform your Bank should your Cellphone number change so that your cellphone contact number is updated on its systems.
- Regularly verify whether the details received from Cellphone notifications are correct and according to the recent activity on your account. Should any detail appear suspicious immediately make contact with your Bank and report all log-on notifications that are unknown to you.
- If reception on your Cellphone is lost, check what the problem could be immediately as you could have been the victim of an illegal SIM swop on your number. If confirmed, notify your bank immediately.

Are you sure you've logged on to **your bank's authentic Internet Banking website?**

- Ensure that you are on your Bank's secure website and not on a 'spoof' site that looks like the real website.
- Log on into your Bank's website by typing in the web address yourself instead of accessing 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 e-mail or sms.
- Make sure that you are not on a spoof site by clicking on the security icon on your browser tool bar to see that the URL begins with https rather than http.
- Remember to log off immediately when you have finished banking.

Is your own **PC secure?**

- Never do Internet Banking in public areas such as Internet Cafés, as you never know what software is loaded that may compromise your transactions.
- Make sure that no one has unauthorised access to your PC.
- Be especially aware that there are no security cameras concentrated on your PC and keyboard.
- Make sure that the software loaded onto your PC is correctly licensed.
- Update your operating system and browser with the latest patches.
- Never open suspicious or unfamiliar e-mails or attachments as these often contain harmful programs.
- Never click on links or attachments within suspicious e-mails.
- Prevent harmful software such as viruses, spyware & Trojans form infecting your PC by:
    - Having the latest anti-virus application loaded on your PC. Most banks provide this free of charge to their customers.
    - Installing a personal firewall on your PC.
    - Being aware of using infected storage devices (such as memory sticks and portable hard drives).
    - Browsing and downloading only from trusted websites.

Tips for **using your card safely on the Internet**

- Only make purchases with your credit card on reputable websites that are verified as secure sites (look for the lock image on the toolbar).
- When receiving promotions or special deals via e-mail or telephone or from online websites, always verify the validity of the source before providing your personal and banking details to be debited.
- Do not send e-mails 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 e-mails.
- Never allow any website of a merchant to save your personal and banking details. When the option presents itself, always remember to click 'No'.
- Never save passwords or PINs on your desktop as it may allow others to access your personal information without your permission.
- To ensure that you are using a secure shopping site, check for a picture of a closed lock at the bottom of your screen. On the Web page where you enter your credit card or other personal information, look for an 's' after 'http://' in the Web address of that page – it should read: 'https://'. The encryption is a security measure that scrambles your data as it is entered.

E-mail hacking

Possible **compromised e-mail addresses include:**

- Complaints about spam being sent from your e-mail address.
- You are not receiving any e-mail.
- You appear to be missing e-mail.
- You are receiving large numbers of undeliverable or bounce messages you did not send.
- You are not able to log in to your e-mail account.
- Unknown e-mail appearing in Sent Items folder.

If you suspect that your mailbox might have been hacked:

- Make sure your PC is current with OS updates and anti-virus/ malware software.
- Depending on how your account has been abused, you might have to contact everyone spammed by your hacked e-mail to advise them that the communications were not legitimate.
- Set up several e-mail addresses. Use your original e-mail address for personal or business communication as you'd normally do. Then another email address to communicate with your service provider, since many now ask for an alternative address as added protection. Then, use a totally separate e-mail address only for registered sites, newsletters, online shopping and other services. In this way, the risk of a possible compromise is lowered.
- Use different and strong passwords for each account – one that is at least six characters long, and is a combination of letters, numbers and capitals/lowercase.
- On a secure PC, log into your e-mail and then check whether or not any of the settings have been changed by a hacker. If any of the settings have been altered, delete the new settings.
- Once you have changed the settings, create a new password, and add your secondary e-mail account as your alternative address.

How to **prevent email hacking:**

- Never list your main e-mail address publicly anywhere online – in forums, in online advertisements, on blogs or any place where it can be harvested by spammers. Use a separate e-mail address for the internet which is not linked to your personal or business e-mail account.
- Don't use public computers to check e-mail; there's virtually no way to know if they are infected with malware accidentally, or have key logging spyware installed intentionally.

Cellphone Banking

The mobility of your cellphone allows you to bank at any time from practically anywhere. It is a safe way of doing your banking as it relies on encrypted SMS messages or secure WAP connections. WAP uses similar security as that used by Internet Banking.

Important tips:

- Memorise your PIN, never write it down or share it with anyone.
- Make sure no one can see you entering your PIN.
- Choose an unusual PIN that is hard to guess and change it often.
- Remember, for your own security you are required to re-enter your PIN before each transaction.
- If you think your PIN has been compromised visit your nearest branch and change it immediately.
- Protect your phone content and personal information you saved by using a PIN or Password to access your phone. Do not leave your phone unlocked.
- Do not respond to competition SMSs or MMSs.
- If you receive a phone call requesting personal information do not respond and end the call.
- If you use a Smartphone, install an up-to-date anti-virus application to your Cellphone. Most banks provide this free of charge to its customers.

Money Laundering

Allowing proceeds of crime to be laundered through your bank account, knowingly or unknowingly, is a criminal offence. Safeguard yourself from being involved in a serious criminal offence by following these tips:

Don'ts

- Do not open a bank account in your name on behalf of another person, irrespective of the circumstances.
- Do not allow your account to be used by another person to deposit or transact on.

Do's

- If you suspect that the money you are being paid with is the proceeds of crime, immediately report this matter to the police.

Scams

Fraudulent change of bank account details

How does this scam happen?

The scam operates by an innocent recipient receiving an e-mail or letter informing them that a particular supplier of theirs has changed their bank account details.
The correspondence will include the details of the new account. You will be asked to make future payments into the new account. The details are, of course, fraudulent with the consequence that moneys are paid to the fraudster and not the supplier.
Sometimes these fraudsters also phone the victims informing them of the change of details and that a letter will follow. The fraudster will use the telephone call so that they can extract more information to make their communications more believable.

How can you **prevent becoming a victim of this type of fraud?**

There are a number of basic steps that can make it extremely difficult for your company to become a victim of this type of fraud:

- Maintain a good relationship with existing suppliers and know your contacts so that you are able to liaise with them when required.
- If called by a 'supplier', ask to speak to your known contacts and do not take instructions from staff at the supplier who are not known to you.
- Beware of supposedly confirmatory e-mails from almost identical e-mail addresses, such as .com instead of .com.na, or addressed differently from the genuine one by perhaps one letter that can be easily missed.
- Instruct staff with the responsibility for paying invoices to scrutinise invoices for irregularities and escalating suspicions to a known contact.
- Ensure that your company's private information is not disclosed to third parties who are not entitled to receive it, or third parties whose identities cannot be rightfully verified.
- Rather shred your business and suppliers invoices or any communication material that may contain letterheads, than to discard in rubbish bins.

What can you do as a victim of this type of fraud?

- Should you be a victim of this type of fraud, it is important to contact your bank immediately so that they can assist you to stop any payments if possible, as a matter of urgency. It is always prudent to also lay a complaint with the Police.
- In the event that the fraudster has benefited from the fraud, you can consider civil recovery and also check with your insurer to see if it is an insurable loss.

Please remember that electronic payments are made based on the account number only. Any account given is not routinely checked as part of the automated payment process. This is the same for all Namibian, as well as South African Banks. It is your responsibility to ensure the account details being used are correct, by conducting an independent verification.

Deposit and Refund Scams

How does a **deposit and refund scam happen?**

A criminal orders goods or services from a business and makes a payment into the victim's account, mostly by means of a fraudulent cheque. Proof of payment is then sent to the business and goods are delivered to the criminal. When the bank processes the cheque, it is uncovered that the cheque is fraudulent and as a result no funds are transferred to the victim's account. The victim is thus out of pocket as they do not have the goods nor the money. In other instances the order is cancelled and an urgent refund is requested. Alternately a payment is made in 'error' and an urgent refund is requested.

How do you **protect yourself?**

- No 'refund' should be made without first verifying with the bank that the deposit that has been made into your account is indeed valid.
- In addition, a bank customer should wait for all cheque deposits to first be cleared before making the goods on sale to a depositor.

419 Scams

What is a **419 Scam?**

A communication by way of either letter, fax or e-mail is sent to a multitude of recipients making an offer that would result in a large pay off for the recipient ("victim"). The details vary and large amounts of money are usually involved. Whilst a vast majority of recipients do not respond to these request, a very small percentage do which makes it worthwhile for the fraudster. Invariably, the victims' banking details as well as sums of money are said to be required in advance in order to facilitate the payment of the funds. Essentially, the promised money transfer never happens and in addition the fraudsters may use the victims' banking details to withdraw money for themselves.

Some indications that this could be a 419 Scam:

- The communication sounds too good to be true.
- The promise of large sums of money for little or no effort on your part.
- The victim is requested to provide money upfront as a processing/administration fee.
- The request usually contains a sense of urgency.
- The victim does not know the person who has sent the communication.
- The sender at times requests confidentiality.
- Lottery, inheritance or prize themes are popular in the communications.
- Payments are often requested to be made by moneygram.
- In some instances genuine companies' letterheads are utilised to convince the victim of the authenticity of their request.

What should you do **when you receive a 419 Scam?**

If you receive a scam e-mail, do not reply. You can however forward a copy of the e-mail to the Internet Service Provides from where the e-mail originated. For example:

abuse@hotmail.com
abuse@yahoo.com
abuse@compuserve.com etc.

If you have fallen victim, immediately contact the Namibian Police Force (NAMPOL).

Sim-Swap

What is a **Sim-Swap?**

- SIM card swopping (also known as SIM card swapping) is a form of fraud where criminals request your cell phone service provider (SP) to transfer your existing cell phone number onto a new SIM card by pretending to be you, or pretending to act on your behalf. They usually have a copy of your ID (authentic or falsified) and other details that may convince the SP that the request is legitimate.
- Once they have illegally assigned your cell phone number to their SIM card, they will receive all your calls and SMS notifications, which include your in-Contact and One Time Pin (OTP) messages. Your phone will stop receiving any incoming calls or messages, but SIM swop victims usually only notice this when it is too late.

- The fraudsters usually use SIM card swopping as part of an extensive process which includes phishing. By the time they have swopped SIM cards, they usually already have enough of your personal banking details (login and password etc.) to transact on your online banking account - with the SMS OTP as the last link in the chain. Fraudsters are then able to add beneficiaries to your account and transfer money to accounts of their choice, and can authorize such processes with the OTP messages sent to the fraudulent SIM card.
- The second leg to a SIM swop scam, the fraudster at some or other point, might have gained access to your chequebook and stole a few pages out of the cheque book , if not the entire cheque book. They also obtain through illegal means, a sample of your signature. The stolen cheque is then presented to the bank for encashment.
- As per bank procedures, the clerk/teller will contact the customer on the system given mobile number and since a SIM swop was already done, when the bank confirms the legitimacy of the cheque, this confirmation is actually done with a member of the fraud syndicate and not the legitimate client.

Our golden rules

- If your phone suddenly loses signal for no apparent reason, don't simply ignore it. Contact your service provider immediately and find out whether a SIM swop has taken place. It's better to be safe than sorry!
- If your SP confirms that a SIM swop has taken place, instruct them to de-activate your SIM card immediately and to follow the steps required when a SIM card has been stolen.
- Promptly contact your Bank and inform them accordingly.
- Also read the rules regarding phishing.

Protect yourself

- Anyone is at risk of becoming a victim of a SIM swop, and you should never disclose any sensitive information such as login details, passwords, etc.

Tips to **staying safe**

- Always be aware of your cell phone's status. If you realize that you are not receiving any calls or sms notifications, something may be wrong.
- Have your SP's numbers written down somewhere close by. This way you can phone to check whether anything suspicious has taken place.
- Make a habit of checking your bank statements and online banking transaction history regularly. This way you will notice when any unauthorized activity has taken place.
- Familiarize yourself with the tips on phishing.