Be aware of **fraud.**

How can we help you?

Contents

1 ATM Fraud

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.

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 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 and immediately report the incident using your Bank's Card Cancellations Contact Centre number, which is displayed on all ATMs as well as on the back of your Bank card.
- FNB customers call: 0800 110 132, should you believe your card was "retained" by the machine
- Should you have been disturbed whilst transacting, immediately


8
9
5
6
2
1
0
.

ATM Fraud (continued)

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.

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 the keypad with your other hand, when punching the numbers even when alone at the ATM as some criminals may place secret cameras to observe your PIN. Stand close to the ATM, thus using your body as a shield to protect your card and PIN.
- In order to keep both your card and PIN safe, don't let anyone stand too close to you.

Tips for protecting your cash

- Ensure that once you withdraw cash, it's put away immediately and kept safely in your possession, as fraudsters often take advantage of customers failing to do so.
- Take your time to complete your transaction and secure your card and your cash in your wallet, handbag or pocket before leaving the ATM.
- To protect yourself in the event that your card and PIN are compromised, you can change your daily withdrawal limit on FNB Online or in a branch, to suit your withdrawal needs. You can control your exposure to these types of losses, by ensuring that you set a realistic daily withdrawal limit.
- 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. If for some reason, you do not feel comfortable withdrawing cash at the ATM, make use of the **"Cash @ till"** facility – these withdrawals are free of charge with purchases made at Checkers, Shoprite, Pick 'n Pay and Boxer stores.

- 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.

Telephone numbers for reporting ATM related incidents

FNB	**0800 110 132**
ABSA	0800 111 155
AFRICAN BANK	0861 000 555
ALBARAKA BANK	0860 225 786
BANK OF ATHENS	011 833 2117
BIDVEST BANK	0860 111 177
CAPITEC BANK	0860 102 043
CITI BANK	1800 950 5114
INVESTEC BANK	011 286 9663
MERCANTILE BANK	0860 119 925
NEDBANK	0800 110 929
STANDARD BANK	0800 020 600
SA POST OFFICE (POST BANK)	0800 535 455
UBANK	0860 008 322

2 Card Fraud and Skimming

Important tips to avoid card fraud

- Review your account statements on a regular basis and query disputed transactions with your Bank immediately.
- 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 card receipts before discarding them.
- Never let your card out of your sight when making payments.
- Sign your card on the signature panel as soon as you receive it to stop anyone else from taking ownership or trying to use it.
- Your card is not transferable. Only the person whose name appears on the front of the card is authorised to use it.
- 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 for correct purchase amounts before you sign them.
- Keep your transaction slips and 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.

3 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 where 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 'R' 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 your 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.

Branch No.

6:30 21:

4 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

Fraudsters 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 Cafes or unsecure terminals (hotels, conference centres etc.) to do your banking.

DO'S

- Protect your personal information at all times.
- Manage your personal information wisely.
- When destroying personal information, either shred or burn it (do not tear or put it in a 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.

To prevent your ID from being used to commit fraud if it is ever lost or stolen, you should alert the SA Fraud Prevention Service immediately on **0860 101 248** or at **https://www.safps.org.za.** To protect your interests, your information will be put on a database used by Banks and retailers.

- 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 drivers license be stolen, report it to the South African Police immediately.

5 Phishing

Phishing is the most prevalent social engineering attack used by fraudsters to steal personal information. Fraudsters send out e-mails to recipients purporting to come from a reliable source like a banking institution, the Receiver of Revenue or your e-mail service provider. The e-mail will typically prompt for your information to be updated or validated through a hyperlink or icon. Once clicked on, the link will launch a fake website that has the same look and feel as the legitimate website. The information requested is usually personal information and could include usernames and passwords for banking platforms or e-mail accounts as well as cell phone numbers and bank card details. Any information that is entered on the fake website is captured by the fraudsters and can be used to perpetrate fraud. Additionally to harvesting personal information, fake websites can be used to infect your machine with malicious software which can be used to gather sensitive information.

Golden rule: NEVER open attachments if you do NOT know the sender.

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.

DO'S

- Type in the URL 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 your computer might have been compromised, contact your Bank immediately.

6 E-mail Hacking

Possible compromised e-mails include:

- Complaints about spam being sent from your e-mail address.
- You are not receiving any e-mails.
- You appear to be missing e-mails.
- You are receiving large numbers of undeliverable or bounce messages you did not send.
- You are not able to log into 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 e-mail 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 registering for sites, newsletters, online shopping and other services. In this way, the risk of a possible compromise is spread.
- 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 e-mail 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.

4
8
1
End
5
2

7 Online 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 is 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 cell phone notification service and receive electronic messages relating to activities or transactions on your accounts as and when they occur.
- Inform your Bank should your cell phone number change so that your cell phone notification contact number is updated on its systems.
- Regularly verify whether the detail received from cell phone 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 cell phone 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.
- Make use of the "Account Owner Verification" tab on Online Banking.

Are you sure you've logged on to your Bank's authentic Online Banking website?

- Ensure that you are on your Bank's secure website and not on a 'spoof' site that looks like the real website.

Online Banking (continued)

- Log on to 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 Online Banking in public areas such as Internet Cafe's, 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 trained 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 programmes.
- Never click on links or attachments in suspicious e-mails.
- Prevent harmful software such as viruses, spyware and trojans from infecting your PC by:

    - Having the latest anti-virus application loaded on your PC. Most Banks provide this free of charge to their customers (Webroot).
    - 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 card on reputable websites that are verified as secure sites (look for the lock image on the toolbar and ensure that the address starts with https://).
- 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.

8 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 SMS's or MMS's.
- 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.

9 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 monies 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 telephone call will be used by the fraudster 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 .co.za, or addresses that differ from the genuine one by perhaps one letter that can be easily missed.
- Instruct staff with the responsibility of 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 discarding these in rubbish bins.

- Make use of the "Account Owner Verification" tab on Online Banking.

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 name given is not routinely checked as part of the automated payment process. This is the same for all South African Banks. It is your responsibility to ensure the account details being used are correct, by conducting an independent verification.

10 419 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 requests, 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 the 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 Provider from where the e-mail originated. For example:

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

- Contact the Points of Presence Support Centre on **087 577 4188** or Fraud Line on **087 575 9444** or e-mail **bchotline@fnb.co.za.**
- Forward the e-mail to the South African Police Services at **419scam@saps.org.za.**
- If you have fallen victim, immediately contact the South African Police Services.

11 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, you should wait for all cheque deposits to first be cleared before handing the goods over to a depositor.
- Take great care to protect personal information and that of your company; it is through access to this information that perpetrators gain access to you and your organisation.
- Staff dealing with finances in your organisation should be educated about such scams.

Lodge Scam

- Merchants would receive bookings from customers, and process the payment as per normal. The customers would then request the merchants to make payments to third party accounts on their behalf after they have built a "trust" relationship with our merchants. The funds would then be transferred to the Third Party (fraudster account). The customers never stays at the merchants facility. Once the transactions are disputed by the customers the merchant would lose the funds transferred to the third party account, as well as the actual transaction amounts.

Cheque No.

100 14


ON
SELL
STOP
4
2
1
M−
0
MRC
C/CE

12 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.

13 Dating and Romance Scams

Dating and romance scams try to lower your defences by appealing to your romantic or compassionate side. They play on emotional triggers to get you to provide money, gifts or personal details.

How to protect yourself from dating and romance scams:

- Try to remove the emotion from your decision making no matter how caring or persistent they seem.
- **Think twice** before sending money to someone you have only recently met online or haven't met in person.
- **Never** provide credit card or online account details to anyone by e-mail.
- If you agree to meet in person, tell family and friends where you are going.
- Avoid any arrangement with a stranger that asks for up-front payment of funds.

14 Holiday Scams

Criminals are exploiting potential holiday makers through falsely advertising holiday accommodation or timeshares on the Internet via classified adverts. Before you get trigger happy looking for the ideal holiday, it is important to know how to find legitimate accommodation packages and deals using your local classifieds.

Take these precautions to avoid being scammed:

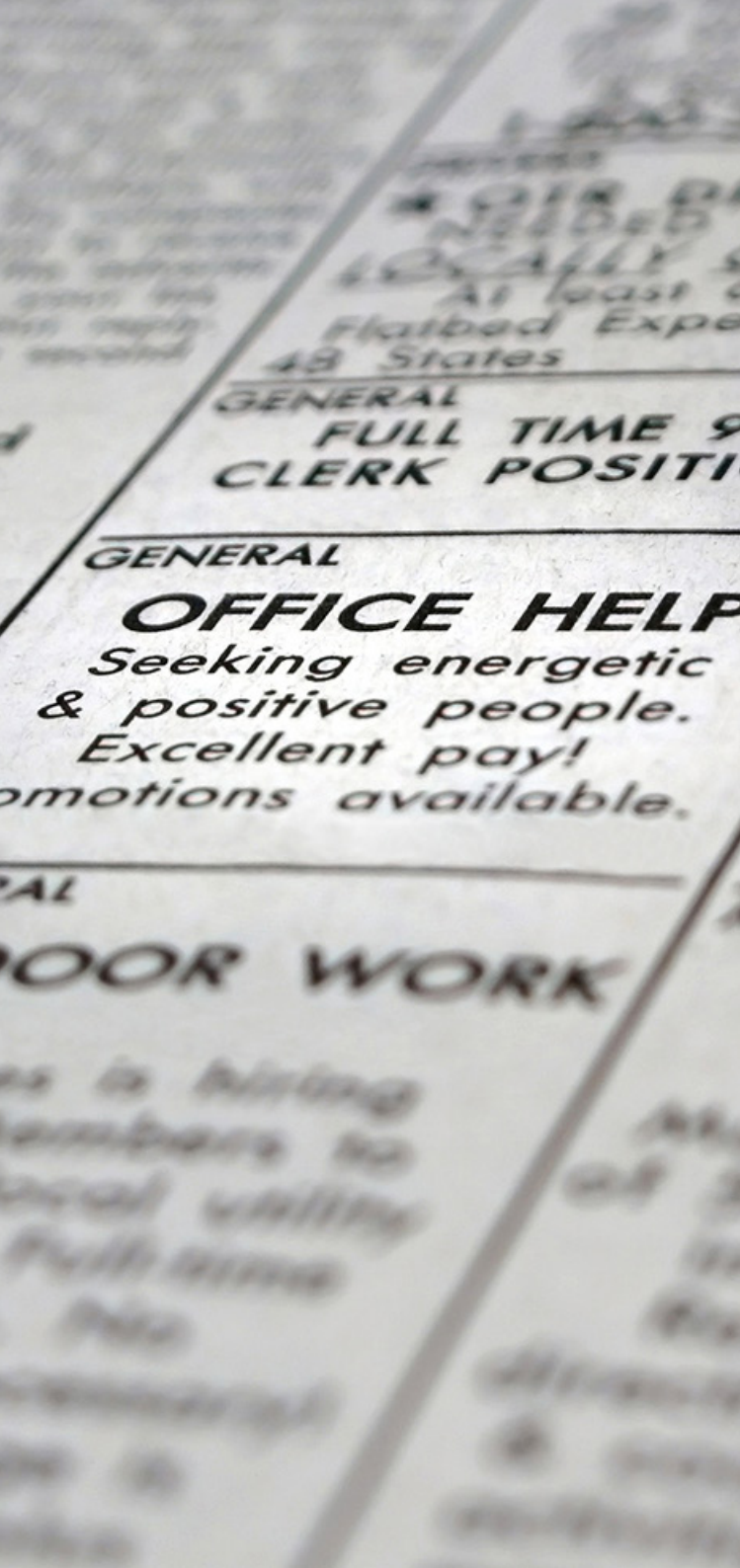
- Use search engines - If you're worried about a property, simply check it out yourself.
- Don't send money - Don't deposit or transfer money to an individual's bank account.
- Make some calls. Before you officially decide to book, give the owner or property manager a call and ask for references.
- Book direct. To completely avoid scams, it's best to shy away from adverts and check out properties from a reputable rental agency.
- Suspicious behaviour - take notice of bad grammar in emails, foreign phone numbers, or if the owner / property manager is not responding to emails. These can all be warning signs.

15 Classified Scams

While making classified transactions, be wary and vigilant to ensure that you are not a victim of crime. If situations make you feel uncomfortable, rather be safe and avoid the deal than lament being a victim later. Follow your gut feeling and let the other party know that you will never take any risk under any circumstances.

How you can prevent becoming a victim of this type of fraud:

- If something sounds too good to be true, it most probably is.
- Don't be afraid to ask a buyer or seller questions; if they have nothing to hide no amount of questions should be unwelcome to them.
- If you're interested in buying something and the seller can't show you the item; don't pay them before you've inspected it.
- Don't hand over an item to a potential buyer unless you are 100 percent sure that the funds they've deposited are available in your account and that you're able to use it.
- Take note that some potential buyers ask money for petrol or airtime. Don't give potential buyers/sellers money for anything else except for the item that interests you.
- Sell on your terms; don't let a potential buyer dictate terms to you.
- Don't meet a potential buyer or seller in a dodgy area. Insist on meeting at your local police station or at a public area like a shopping mall.
- When it comes to company names used in a web based e-mail address, alarm bells should be going off (such as junkmail@yahoo.com, @hotmail.com, @gmail.com, @ymail.com etc).
- Fraudsters also sometimes send victims a SMS which looks like an InContact message. Especially when they make arrangements to meet to exchange the merchandise.


Flatbed Expe
48 States
GENERAL
FULL TIME
CLERK POSITI
GENERAL
OFFICE HELP
Seeking energetic
& positive people.
Excellent pay!
omotions available.
AL
OOR WORK


D
C
B
A
K

16 MoneyGram

MoneyGram is a person-to-person money transfer service. It was designed to allow you to send money to your family and friends i.e. people you know personally and whom you trust.

Take note that the once a MoneyGram payment is made and has been collected by the receiving party, it is final. It cannot be reversed.
If you ask FNB to pay someone using the MoneyGram service and it turns out that person has defrauded you or not met their obligations to you FNB and MoneyGram cannot be held responsible and reverse the payment.

FNB and MoneyGram cannot be legally responsible (liable) to you or any other person for any loss or damage you suffer because you used the service.

- Do not send money to someone you do not know or for any of the following reasons:
- Donations
- Lottery winnings
- Purchasing of a vehicle
- Online purchases
- Banking facilities
- Online romance
- To secure accommodation bookings
- To secure employment

17 Money Mules

What is a Money Mule?

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/ illegal money via their bank account(s). Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

Don't's

- Do not respond to e-mails asking for your bank account details for any overseas job offer, first confirm the identity and contact details of the employing company.
- Do not get carried away by attractive offers/ commissions or consent to receive unauthorised money.
- Do not accept payments from anyone and then transfer part of the proceeds by money wire.
- Do not open a new bank account to receive money from people you don't know.

Do's

- Try to investigate the person or company before doing business with them
- When transferring money, use a method that protects the transaction. For example, many banks, credit cards and services such as PayPal may offer fraud protection
- Check the ad or email for poor language and grammar
- Monitor the transactions, including checking for withdrawals from your bank account and tracking an order
- If you notice any problems, immediately contact the appropriate authorities. Depending on the circumstances, these authorities may include your bank, the service you used to conduct the transaction and law enforcement.

Notes

FNB Contact Centre

087 575 9444

FNB Card Cancellations

0800 110 132
087 575 9406
+27 11 369 1189