



How to spot skimming

At retail outlets:

A corrupt employee skims a customer's debit/credit card with a small, handheld electronic device that scans and stores the card data from the magnetic strip. The employee usually sells the information through a contact or on the Internet, at which point counterfeit cards are made. The criminals go on a shopping spree with a copy of the debit/credit card, and cardholders are unaware of the fraud until a statement arrives with purchases they did not make.

At ATMs:

One way of stealing your card information at ATMs is by pretending to "help" you, but actually using the opportunity to quickly swipe your card through a skimming device carried in their pockets or under clothing. These fraudsters often work in teams and then look over your shoulder to get the PIN.

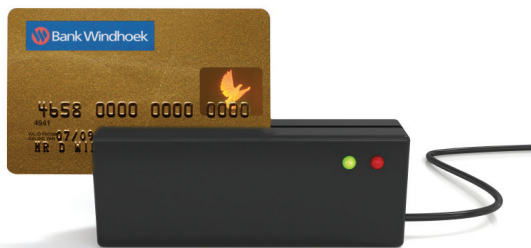
Another way is to place a skimming device over the card slot of an ATM and then place a small camera or cover on the keypad to record the PIN. So always examine the ATM for suspicious looking signs or features before using it, and always make sure you have your card before and after transacting. Resist "help" from "friendly" citizens

Avoid skimming

How to stay out of trouble.

- Make sure your card stays in sight, and never let anyone remove your card from your presence if you can help it. Skimming occurs most at restaurants since the waiter has to walk away with your card. If you are in a retail store and they say they have to go to another counter to run the card, follow them. If you are concerned about letting go of your card at restaurants, ask for a handheld device or take your card for payment to the counter yourself.

- Your credit/debit card is like cash. You need to be aware that your card is very valuable. Treat it like a diamond or cash. Would you just give someone cash and let them walk away with it?
- Monitor your card receipts and check them carefully against your statements. If you are married, sit down with your spouse to account for all charges. Some thieves take out small amounts in hopes cardholders won't notice.
- Shred unwanted financial solicitations and put your mail on hold when you leave town. This will not help with skimming, but it can help with other forms of identity theft.



How to deal with skimming

- Contact your bank immediately and tell them your card was stolen. If you don't make a report quickly, you may be liable for some or all of the unauthorized transactions.
- Call the police. When your identity or credit/debit card is stolen, it's just like having a car stolen. Make a police report and keep the police report number.

Contact Us

For lost or stolen cards: Bank Windhoek Helpdesk: 061 2991200



Protecting yourself against card fraud



Know your card

Whether you are a long-standing Bank Windhoek client or have just received your first debit card from us, we want to ensure that you are fully aware of the functionality of your card. We also want to help protect you against card fraud and fraudsters.

Signature panel

There is a white signature panel on the reverse side of the card. Sign your full signature on the panel with a ballpoint pen as soon as you receive your card. The signature will be used by merchants to verify that the card bearer's signature correlates with the signature of the card owner.

Daily withdrawal limit

The purpose of this limit is to minimize the losses of your ATM cash you might incur should a fraudster get hold of your Personal Identification Number (PIN) and card. The limit may be increased upon your request, but is at your own risk.

Daily POS purchase limit

The purpose of this limit is to minimize the losses you might incur when doing Point-Of-Sale (POS) purchases should a fraudster get hold of your debit card. The limit may be increased upon your request, but is at your own risk.

Liability for unauthorized transactions

You will be responsible for all transactions after receipt and activation of your card. That is why it is of utmost importance that you keep your card and PIN secure at all times and report your card as lost or stolen the moment you notice it is missing or you find unrecognized transactions on your account.

What to do when your card is lost or stolen

The loss or theft of your card should be reported as soon as possible to Bank Windhoek Helpdesk (061) 299 1200 or Visa's Global Customer Assistance Service. Alternatively contact your nearest Bank Windhoek branch.

Advice to cardholders

- Know where your card is at all times and keep it safe.
- Keep copies of all sales vouchers and Automated Teller Machine.
- Check your ATM withdrawal slips against your statements.

- When you are travelling, check your card's expiry date to ensure that it will not expire while you are away. Also check your card's ATM withdrawal and POS purchase transaction limits to ensure that you will be able to withdraw the required amount in foreign currency.
- Keep your PIN a secret – do not write it on your card and do not give it to anyone.
- If you suspect that your PIN has become known to another person, please notify your nearest branch immediately.
- Do not lend your card to anyone – not even family members.
- Never let your card out of your sight, even when making purchases.
- Do not give your debit card as security to anyone.



Taking care of your card

Visa cards are the safe way to take care of your spending. Lost cash is gone forever, but lost cards can be blocked with a simple telephone call — and replaced fast.

Lost your card?

To avoid even that inconvenience, you can take the following basic precautions:

When you get your card

- Sign the signature panel immediately.

- If you have been given a PIN to use at a cash machine or in shops, memorise it — never write it down.
- If you change the PIN you were given, avoid obvious choices such as your date of birth or telephone number.
- Do not tell anyone your PIN.

At home

Keep your sales and ATM receipts and check them against your card or bank statement.

If any amount is incorrect or you spot a transaction you did not make, call the Bank Windhoek Helpdesk immediately.

Keep a list of your card numbers, along with the telephone numbers you should call if they are lost or stolen. Keep this list safe as fraudsters can use card numbers as well.

In the shops

- Check the sales slip to ensure the amount is correct and the total has been filled in before you sign.
- Make sure the retailer gives the card back to you, along with your copy of the voucher.
- Keep your card close to you — beware of pickpockets.
- Do not leave your card in your car's glove compartment.

Telephone and mail order shopping

When you place an order over the telephone or by mail, give your card number only if you are confident about the company's reputation.

You might be asked for your Visa card security code — the three digits at the end of the card number printed on the signature panel. Give the seller that code but never give your PIN.

Know how they do it

Skimming

“Skimming” is a method by which thieves steal your credit/debit card information, and all it requires is a little illicit technology and a lot of criminal intent by those who handle your card. Skimming occurs most frequently at retail outlets that process credit card payments -- particularly bars, restaurants and some convenient stores as well.

Skimming at ATMs occurs frequently nowadays as well, and can be much more damaging because ATMs are self service devices and the identity of the client cannot be verified. Also, cash is the most attractive commodity for criminals.