Standard Bank

SafeGuard

A survival guide for when scams hit

Got scammed?
Here's what to do next.



Index

Introduction

- Think you've been scammed?

From panic to power

- 3-step emergency plan scam
- Quick tips to remember
- Ways to lock your money
- Take a breath. You are safe now

Your map to safety

- How to stop the loss and get back on track
- **Problem A:** I clicked a link in an SMS or email
- **Problem B:** I gave my PIN, password or OTP to a caller
- **Problem C:** I paid money for a job, a package or an investment, and now it's missing
- Getting your information together
- Reporting a scam to the police
- What happens after you've reported a scam?
- Beware of the 'second scam'
- Your checklist to move on from a scam

Dealing with the feelings after a scam

- Taking your power back
- Face-it to fix-it
- Handling money stress and panic
- Dealing with the feelings of pain and shame
- Worrying about what others might think

Glossary

If you think you've been scammed, you might feel scared, confused or overwhelmed. That's normal, and you're not alone.

Take a breath. You can still take control of what happens next.

This guide will give you simple tools and show you how to stay one step ahead to feel more confident in your daily life.

In this e-book, you'll learn:

- What to do right now to stop the scam
- How to report fraud and get help fast
- Simple ways to deal with the stress and feel in control again

If you suspect fraud on your Standard Bank account, call the Standard Bank Fraud Line on 0800 222 050 or report fraud on our Banking App.


From panic to power
3-step
emergency
plan

If you think you're being scammed, do these 3 things right now

1

STOP

Cut all contact and hang up straightaway.

Don't talk to scammers, don't even say goodbye. If it's on a message, delete and block the sender.

2

LOCK

Freeze or stop your card immediately on your banking app.

Change your passwords for your banking, email and social media. Turn on 2-step verification on your apps.

3

REPORT

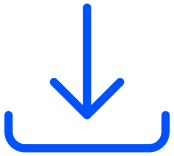
Call the bank and tell them what happened or report it on your Banking App.

If you don't report it, the bank can't help you, and the scammers will keep hurting others.

Quick tips to remember



Don’t send more money, even if they threaten you.



Don’t download anything they say will help you.

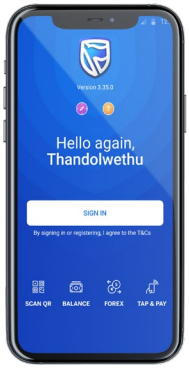


Don’t worry about being polite.

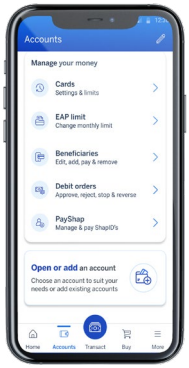
Ways to lock your money

If you've been tricked, you can switch your Standard Bank card on and off or cancel your card in the following ways:

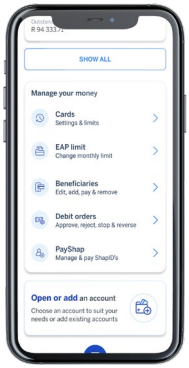
Banking App



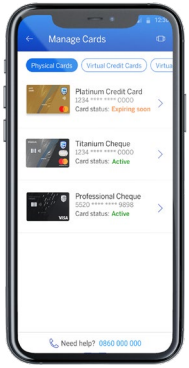
Sign in to our Banking App.



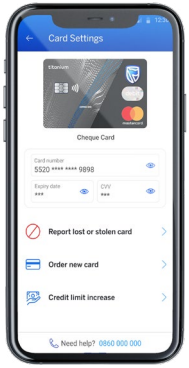
Tap on Accounts at the bottom of the screen.



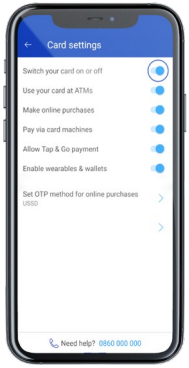
Scroll down and tap on Cards.



Select the specific card you want to manage.



Tap on Card settings.



Move the switches to turn your card On or Off.

Reach out instantly

- **Lost or stolen cards:** Report and block your card directly on the Standard Bank App, or call us on 0800 020 600.
- **Report fraud:** Use the secure in-app calling feature on your Banking App as your first option, or dial our Fraud Line on 0800 222 050.





Go to the bank

Visit your nearest Standard Bank branch and ask them to help you.

Take a breath. You are safe now.

You just pulled the emergency brake. By stopping contact and freezing your cards, you stopped the danger. The hardest part is over.

Right now, your heart may be beating fast. You might feel scared, confused or upset. This is normal. When something feels wrong, your body reacts this way — and that panic is exactly what scammers want you to feel.

You can break the panic for a few seconds so your mind can settle and you can handle the rest by trying this:



Feel your feet
Put both feet flat on the floor. Feel the ground under you.



Touch something
Put your hand on a table, your leg or a wall. Notice how it feels.



Look around
Name 3 things you can see out loud (like a chair, a lamp, a window).

This small body check-in brings you back to right now and helps the panic settle.

And remember that this wasn't your fault. Someone tricked you and committed a crime against you. So don't blame yourself.

There's a lot you can do to take charge. In the next part of this e-book, we'll walk you through what you can do to keep safe and start feeling like yourself again.



Key takeaway

Being scammed is not your fault. You can stop the danger right now with the 3 fast emergency steps: STOP. LOCK. REPORT.

What you can do today

- ✓ **Be kind to yourself today.** You did the hard part.
- ✓ **Use the body check-in** to go from alarm to calm.
- ✓ **Today you stopped the danger;** now you can get back on track.



Your map to safety

How to stop the loss and **get back on track**

3 Ways scammers find you (and how to stop them)

If you've been tricked by a scammer, what you do next is important to protect yourself from losing anything more. Because every scam is different, you need to take specific steps based on what happened to you.

Here are 3 different ways of how you could get scammed. Look for the one that sounds most like what happened to you and follow the next step to protect yourself.



Problem A: I clicked a link in an SMS or email

If you accidentally clicked a link, a hidden virus may have downloaded onto your phone. Scammers use these viruses to watch your screen and steal your passwords or information.

Follow these steps:

Go offline

Put your phone on 'Airplane Mode' or turn off your Wi-Fi immediately. This cuts the connection and stops the scammer from reaching your phone.

Change your passwords

Use a different device to change the passwords to your Banking App and email.

Clean your phone

Go to your phone's settings and look for 'Security' or 'Device Care' to run a built-in scan, or go to your app store and download well-known, free security apps to run a scan to clean your phone.

Did you know?

You can use our Banking App to **find and stop dangerous apps** from stealing your private banking details and keeping your account safe.

Problem B: I gave my PIN, password or OTP to a caller

If you gave scammers private information, you've given them entry into your bank account.

Did you know?

You can use our Banking App's quick safety features to lock scammers out before they can touch your money.

- Change your PIN so they can't sign in
- Freeze your cards so they can't spend your money
- Disconnect your account from any other devices, in case they are trying to sign in from their own device

Follow these steps:

End the call

If you are still on the phone, hang up. If the call has already ended and you realise you were tricked, block them.

Lock your account

Open your Banking App or Online Banking profile to freeze your card or account or sign in and quickly change your password/PIN.

Call the fraud line

Report the fraud on 0800 222 050 and tell them your bank details have been stolen and to block your profile right now.

Problem C: I paid money for a job, a package or an investment, and now it's missing

If you've been tricked into sending money, they are already trying to cash it out or move it before you can stop them.

Did you know?

Scammers rarely keep stolen money in one place. They quickly bounce it between different bank accounts to hide their tracks. That's why time is your biggest weapon. The faster you report a fraudulent payment, the better chance our fraud team has to freeze the scammer's account before your money is moved again.

Follow these steps:

Stop paying

If they've already gotten money from you, they'll try to contact you again to get more money out of you. Don't send any more.

Call us immediately

Report the scam and ask whether we can stop or reverse the transaction.

Reverse or stop payments

Sign in to your Banking App to cancel any debit orders, future-dated payments or cash vouchers (like Instant Money) that you set up for the scammer*.

*Terms and conditions apply.

To further take control of the bigger picture, here are 4 things you should do next:

Get a police CAS number



Go to your nearest police station and report the scam. This is very important. Your bank or insurance company will often ask for a police CAS number before they can help you get your money back.

Report the scammer



If the scam happened on a website (like Facebook Marketplace, a job portal or a dating app), report the scammer's profile to that website so they get blocked.

Check your credit report



Get a copy of your credit report (from a credit bureau or using the Credit Score feature on the Standard Bank App) to make sure the scammers haven't used your name to open store accounts or take out loans.

Protect your name



Register for free with the South African Fraud Prevention Service (SAFPS) to put a 'security guard' on your ID that will warn banks, stores etc. that your ID has been stolen to stop scammers from opening accounts in your name.

Getting your information together

To protect your name (and your money), you need to put together the right information for the bank and the police. To do that, you need to collect the facts of what happened.

Put these things together to show proof:

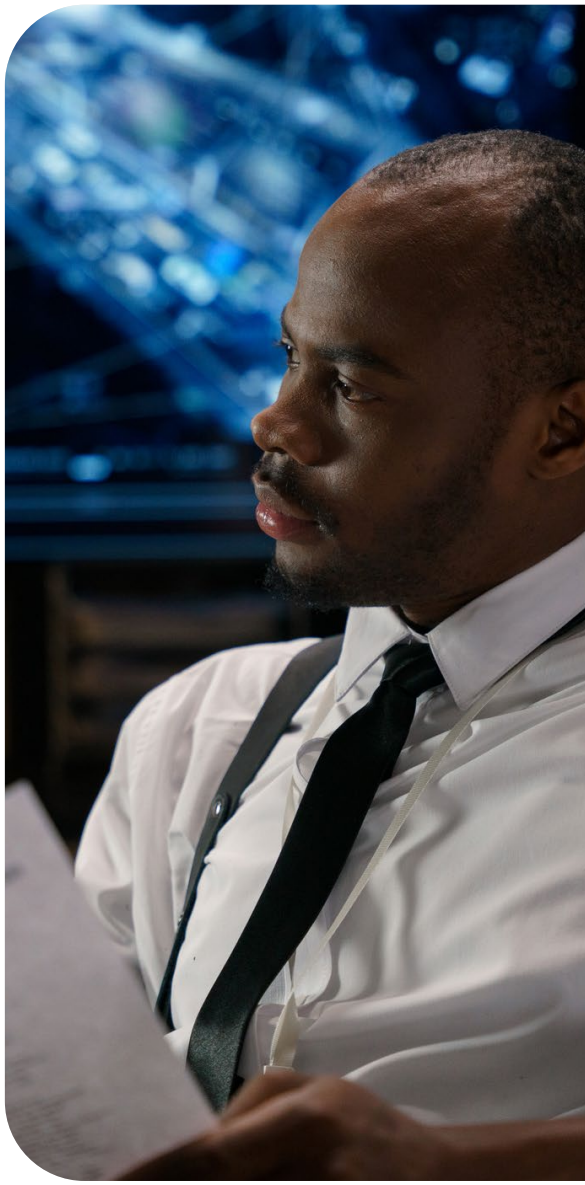
Screenshots: Take photos of your WhatsApp chats, SMSs or emails with the scammer. Also take screenshots of your call history showing the dates and times they called.

The scammer's details: Write down their phone number, bank account details and website links they sent you, or their names (even if they are fake names).

Bank statement: Print your statement and highlight the stolen money.

Sometimes you will need to report the scam to the police to get an official CAS number, here's why:

- Your bank may need proof before they look into your claim.
- Your bank could ask the scammers' bank to block their account and stop them from withdrawing more or moving your money.
- If the scammer stole your ID, they might try to take out loans or open store accounts in your name. Your police report will prove you are the victim, not the criminal.
- Reporting them can help the police track them down and protect others from falling into the same trap.



Reporting a scam to the police



Where do I go?
Go to your closest police station.



What do I bring?
Bring your ID/passport and the proof you've put together.



What do I say?
"I am a victim of a scam. I need to make a statement and open a case."



What do I get?
You get a CAS number. Keep it safe as the bank and the police need it to work on your case.

What happens after you've reported a scam?

Once you have reported the scam to the bank and the police, you might still have a lot of questions, especially this one: will I get my money back?

The answer is that how you lost the money matters:

- If your account was hacked without your help, meaning you didn't share your PIN, passwords or OTPs, the bank will look into it, and you could get your money back.
- If you made the transfer yourself (even if you were tricked) by clicking a link, making a payment or sending money to a fake investment or job, you won't.

However, the bank could still try to track the scammer's account. If they can catch it fast enough, they can freeze whatever money is left and try to get that back to you.

Waiting for updates can be stressful. If you want to check the progress of your investigation, you can easily follow up on your existing fraud case using the secure in-app calling feature on our Banking App.

Beware of the ‘second scam’

Unfortunately, right after a scam, you should be extra careful. Scammers are greedy, and because they know you are desperate to get your money back, they might target you a second time.

You might get a call or message from someone saying the following:

- They are a special police officer investigating your case
- They are a lawyer who can get the bank to pay you
- They are an expert hacker who can steal your money back from the scammer
- They have found your money, but you must pay a small fee to get it back

⊗ Don’t pay anyone to get your money back

⊗ No real police officer, lawyer or person from the bank will ever ask for more money to help you get your money back

Your checklist to move on from a scam



Block the scammer

☐



Change your logins

☐



Report the scam to the bank

☐



Report the scam to the police

☐

Get a police CAS number

☐



Register with SAFPS
(if you shared your ID)

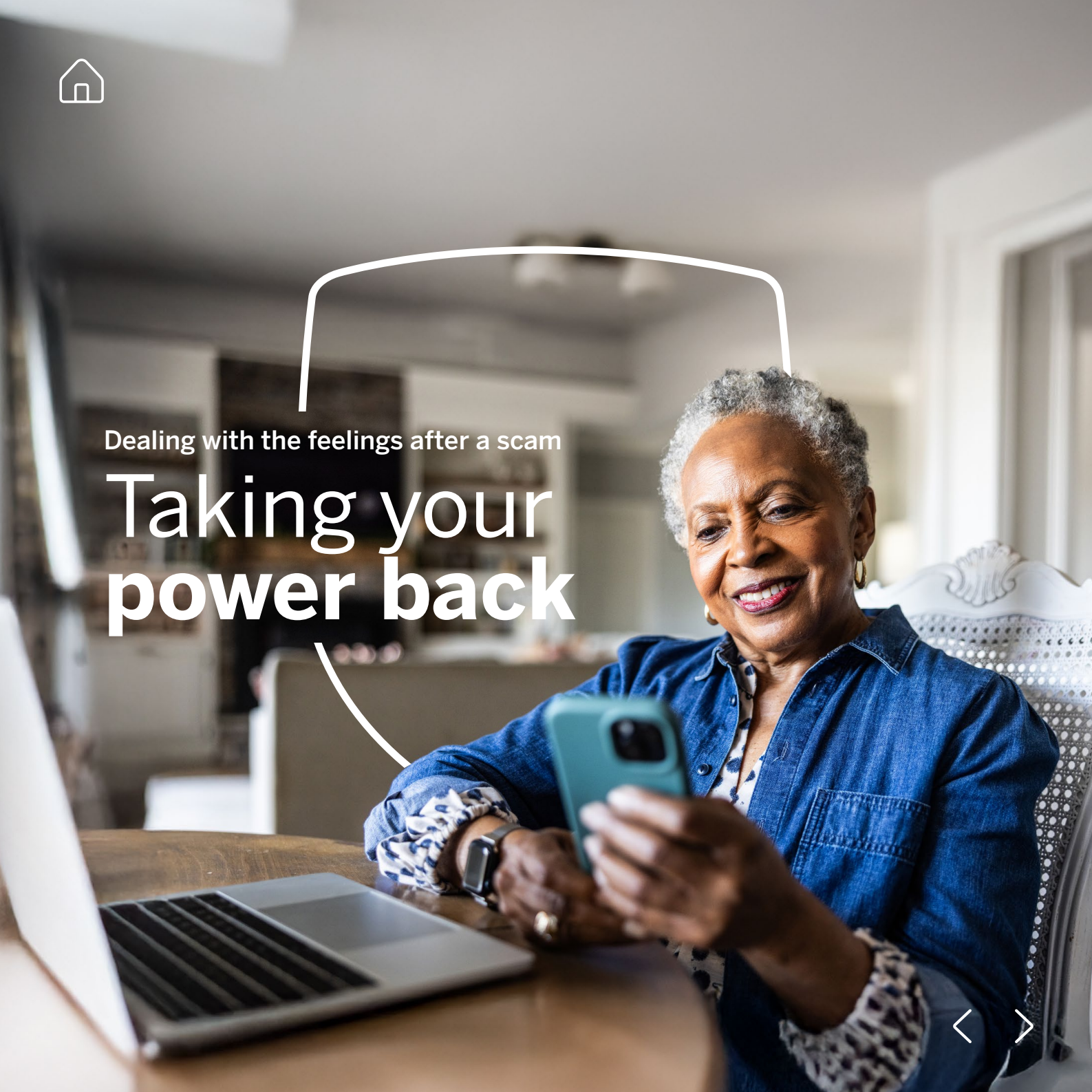
☐

Key takeaway

Getting your proof together and reporting the scam gives you the best chance to protect your money and your name. A police CAS number is the key to action on your case.

What you can do today

- ✓ **Take your screenshots** and bank statements to the police station to report the crime and get a CAS number.
- ✓ **Stay alert** and don't pay anyone who promises to get your money back — it's another trick.
- ✓ **Work through the checklist above,** ticking off each step as you go, so you know nothing has been missed.


Dealing with the feelings after a scam
Taking your
power back

A scam doesn't just take your money. It makes you lose trust in yourself and leaves you feeling ashamed, angry and unsafe. That's because when we are scammed, it hurts in more ways than one.

You feel worried about paying your bills; you might blame yourself and be scared about what other people will think.

These feelings are normal, but they don't have to last forever. To help you do this, we are going to tackle each of these 3 hurts—your money, your feelings and your name—using a simple 3-step tool to get through it and bounce back:



Handling money stress and panic

Losing money meant for food, rent or bills is scary. It can feel like a heavy weight in your chest, make it hard to sleep and leave you worrying about how you will survive the month.

Here's how to use the 3-step tool to help you move from feeling beaten to feeling in control:

Understand the feeling: Panic is what happens to your body when it feels it's in danger but panic also makes it hard to think clearly. While it is real and can be scary, panic doesn't last forever.

Before you do anything, give yourself a moment to settle. Things are hard right now, but there is always a way forward.

Take control: Having a plan, even a simple one, helps quiet the panic. Start by writing down how much money you have left, what you need to cover and which bills you need to pay first.

Talk to people early: Speak to the people you owe money to (like your landlord, bank or school) as soon as possible. Be honest. Tell them you have been scammed and are working to sort it out. Most places will understand and give you more time to pay.

Dealing with the feelings of pain and shame

When you've been scammed, you might feel a mix of sadness, embarrassment and anger, replaying it in your head or thinking, "How did I let this happen?"

Understand the feeling: Scammers are professional tricksters that use your kindness, fear and trust against you to trick you.

Take control: Be gentle with yourself and remind yourself that you didn't do anything wrong, and you didn't ask for it. You were a victim of a crime. Worrying about what you should have done just makes it harder to think straight.

Get support: Keeping a scam secret makes the pain worse. Tell a trusted friend or family member what happened. Keeping the worry and anger to yourself can make you feel sick or depressed. Talking to a trusted friend or calling free helplines like the South African Depression and Anxiety Group or LifeLine South Africa can help take away the shame and help you deal with the feelings.

Worrying about what others might think

It's normal to worry about what others will say when they find out you were scammed. You might worry that your family will lose respect for you or that friends will think you made a bad choice. These feelings can make you feel alone, like you have to keep everything to yourself.

Here is how you can face this fear and find your strength again:

Understand the feeling: We all want our loved ones to respect us, but keeping the secret to protect yourself usually just makes the worry grow and leaves you feeling worse.

Take control: Speaking up isn't a sign of weakness; it's a way of taking back your power. Scammers want you to keep quiet so they can keep tricking other people. Breaking the silence can help protect others and keep your community safe.

Take action: Use your story to protect others. When you feel ready, tell people around you what happened. By warning them about the scam, you can stop them from falling into the same trap.

Key takeaway

Losing money to a scam hurts. It isn't easy, but you don't have to stay hurt. You still have options, and by taking small steps forward, you can start to heal and get back on your feet.

What you can do today

- ✓ **Make a simple money plan** to help you handle what's happening and see your options clearly.
- ✓ **Be kind to yourself.** When you remind yourself that you did nothing wrong, it helps lift the shame and makes it easier to think about what you should do next.
- ✓ **Share your story with someone you trust.** This will help lift the weight of your feelings.

Next steps

As you recover from the scam, you're not just getting back to where you were; you're building a better future. Part of moving forward is finding your feet again and choosing what to do next.

Stay one step ahead

Knowledge is your best defence. Protect your future by exploring our other security resources:

Read Part 1 of this series: Download *Your guide to spotting and stopping scams* to learn the red flags and build your scam-proof shield.

Download Part 1

Disclaimer: This e-book has been prepared by Standard Bank for general educational and informational purposes only. The information contained in this e-book is intended to assist readers in understanding common fraud risks and preventative measures and does not constitute financial, legal, professional, or other advice. Readers should seek professional advice before acting on any information contained in it.

While every reasonable effort has been made to ensure the accuracy of the information at the date of publication, Standard Bank does not warrant that the information is complete, accurate, current, or suitable for any particular purpose.

To the fullest extent permitted by law, Standard Bank, its subsidiaries and affiliates accept no liability for any loss arising from reliance on the information contained in this e-book.

Glossary

#

2-step verification (extra security codes)

An extra lock for your account. When you try to log in, the app sends a secret code to your cellphone to make sure it is really you and not a scammer.

A

Airplane mode

A button on your phone that cuts off all internet, data and signal. It is like unplugging your phone from the world to stop scammers from controlling it.

C

CAS number (police case number)

The official receipt number the police give you when you report a crime. You must give this number to the bank so they can help you.

Credit bureau

A company that keeps a list of your debt, bills and loans. Banks and shops look at this list to decide whether they can trust you with a loan or a store card.

D

Debit order

An agreement that lets a company automatically take money from your bank account every month to pay for things like your phone, rent or insurance.

F

Fraud

A crime where someone tricks or lies to you to steal your money or your private details.

Freeze (locking a card or account)

To turn off your bank card or account for a short time. No money can go out, but you can easily turn it back on when you are safe.

Future-dated payments

Money you have scheduled to leave your bank account on a later day (like next week or next month).

I

Instant Money (cash vouchers)

A quick way to send money to someone's cellphone so they can take cash out of an ATM or at a till point without using a bank card.

O

One-time PIN (OTP)

A secret code sent to your phone to approve a single payment. It only works once. Never share this code with anyone, even if they say they work at the bank.

S

Scam

A trick used by criminals to get your trust so they can steal your money or information.

Scammer

A criminal who tells lies to trick people and steal from them.

South African Fraud Prevention Service (SAFPS)

A free service that acts like a security guard for your ID. If your ID is stolen, they warn banks and shops so scammers cannot use your name to get loans.

V

Virus (malware)

A hidden, dangerous program that sneaks onto your phone (usually when you click a bad link). It lets scammers watch your screen and steal your passwords.

For more information on scams and how fraudsters trick people, visit our Security Centre.

Learn more