Standard Bank

SafeGuard

# Your guide to **spotting and stopping scams**

A practical guide to understanding scams and protecting yourself.



# Index


## Introduction

Protecting yourself and your money

## Understanding how scams work

Why anyone can get caught off guard

How scams play on your feelings

What to do when you think it's a red flag

Quick quiz: Real life or scam?

## The scammers playbook

Spotting the scammer's tricks

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

**Unmasking scams:** What to watch out for

**Phishing and smishing:** The digital hook

**Phone scams:** The voice that lies

**Online shopping and investment scams:** Too good to be true

**Romance scams:** Playing with your heart

**AI scams:** The latest trick

Sharpen your scam radar

The 3-step plan to shut down scams

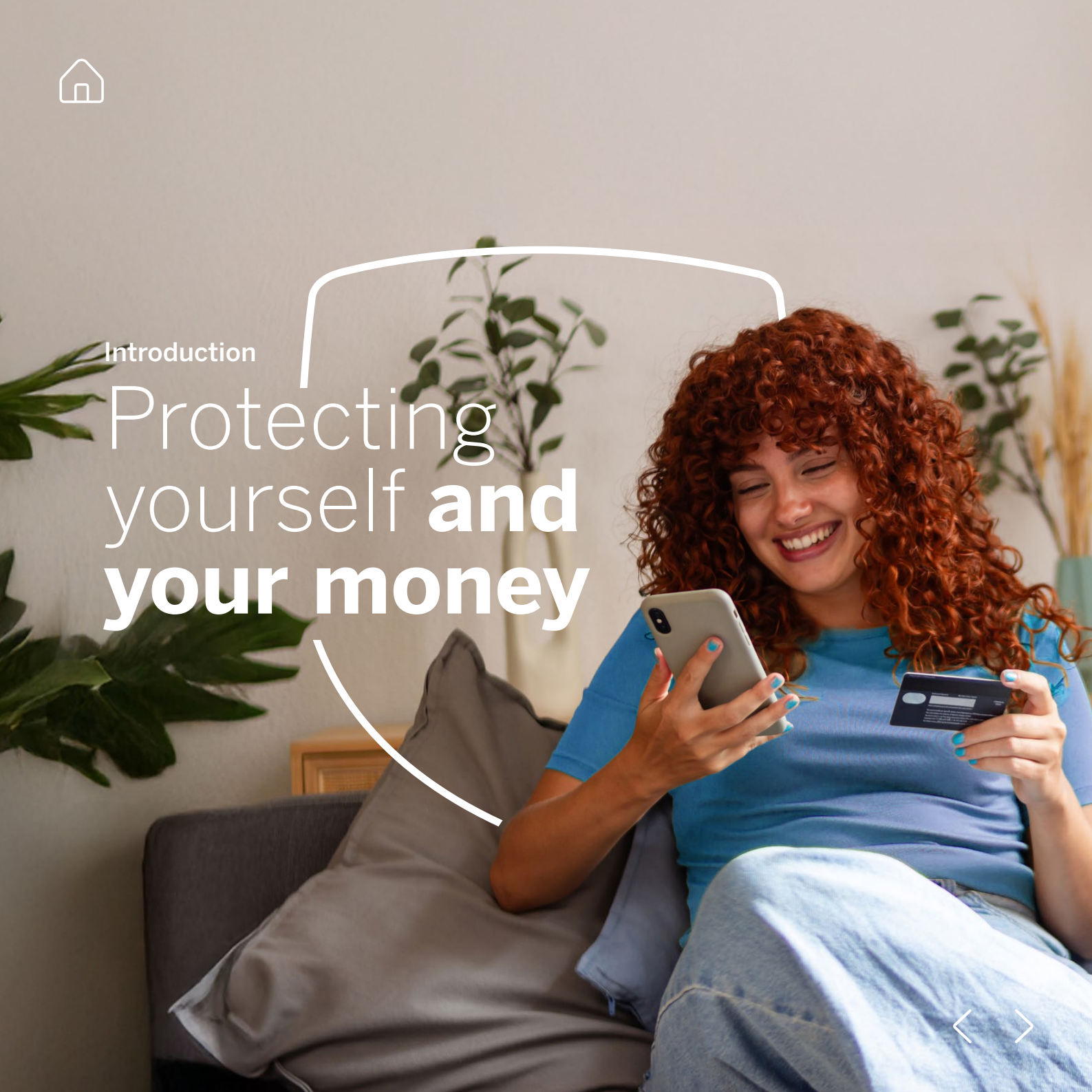
Scam checklist

## Build your scam-proof shield

Smart habits for safety

Your personal safety checklist

## Glossary



Introduction

# Protecting yourself **and your money**

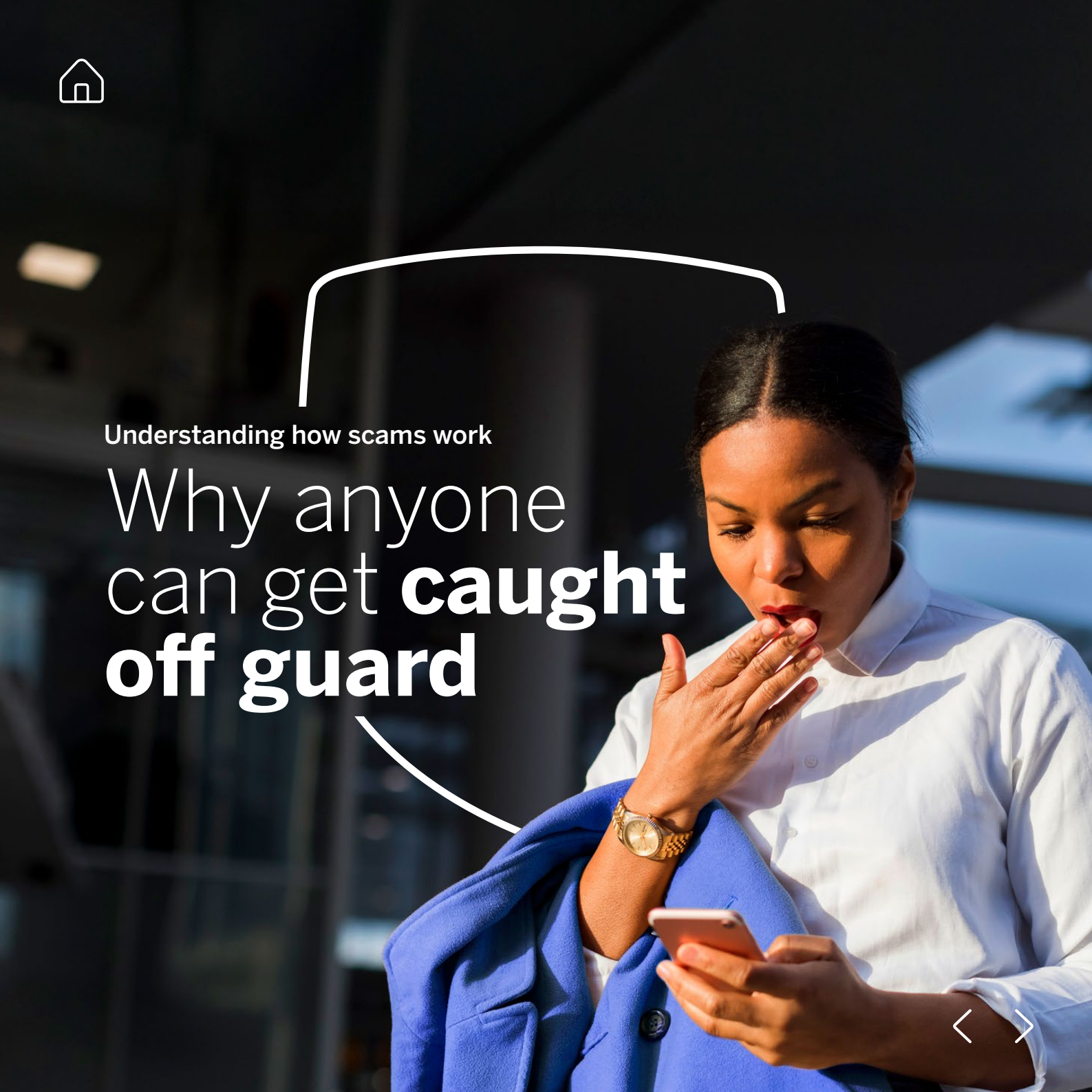
**Welcome!** By downloading this e-book, you've taken an important step to protect yourself and your money.

Today, scams and fraud are everywhere. They can happen to anyone, even if you're careful. It's easy to feel unsure or worried, but the good news is that there is lots you can do to protect yourself.

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:**

- Why anyone can fall for fraud (and why it's not about how smart you are)
- How scammers trick people and what warning signs to look for
- Simple habits you can use every day to keep your money and your personal information safe



Understanding how scams work

# Why anyone can get **caught off guard**

# **It’s easy to think** only certain people fall for scams

The truth is, anyone can be targeted and become a victim, no matter how smart or tech-savvy they are. Scammers are good at playing on human nature, so anyone can become a victim.

This isn’t because you’re easily fooled or because they are geniuses. It’s because the tricks that scammers use are designed to put you under pressure and make you react without thinking.

To build a strong defence, it helps to understand the 3 natural habits scammers try to use against you:

01

**We are wired to trust:** We naturally want to believe people are who they say they are. We are also taught to respect official voices, such as bank managers, police officers or the government. Scammers pretend to be these trusted figures because they know our first instinct is to believe them.

02

**We want to help:** When a family member, a friend or even a stranger is in trouble, our natural reaction is to help. Scammers make up fake emergencies and use our kindness and care against us.

03

**We live in a noisy world:** We get emails, messages, social media alerts and news all day, and it's difficult to be careful every second of the day.

# **How scams** play on your feelings

Scammers don't just hack computers; they hack your feelings, and they use those feelings to get into your head and your wallet. For example:



## Fear

Getting a scary text saying your account has been blocked, you click on the link to pay or get fined/arrested.

They want you to panic so you won't think things through and give away your PIN or personal information to fix it.

**Real banks or businesses don't threaten.**



## Rushing

Someone pretends to be from SARS, rushing you to update your FICA or your account will be frozen.

They want you to hurry, with no time to think, ask questions or get a second opinion.

**Real banks or businesses give you time to make decisions.**



## Greed

You get a message promising you that they can grow your money or that there is a big inheritance from a long-lost family member; you just have to pay a small fee.

They want you to focus on getting something, not the lie and the warning signs.

**If it looks too good to be true, it is.**

# **What to do when** you think it's a red flag

When a message or call triggers one of your red-flag feelings, here's how to handle it in the moment:



**If you feel fear or panic**

Hang up the phone or close the message immediately. Don't speak to the caller, reply to the text or click on a link.



**If you feel rushed or pressured**

Stop everything. Hang up or delete the message. If there's a small chance that it might be real, close it and check it out yourself.



**If you feel excited by a deal or prize**

Don't use the links provided in the message. Go directly to the website or app to check if the offer is real.

# **Quick quiz:** Real life or scam?

### The delivery SMS

**Post Office:** Your package cannot be delivered due to an incorrect address. *Click here to update: www.post-office-update-info.co.za*



**Is it a scam?**
**YES**

**How to tell:** Did you really order a package? If not, delete it. If you did, go to the official website yourself. Never use the link in the SMS.

### The safe account call

Hi, I am calling from your bank's fraud unit. We see a suspicious payment of R2 000 on your card. To stop it, read me the OTP code I just sent to your phone.



**Is it a scam?**
**YES**

**How to tell:** The bank will **never** ask for your OTP. An OTP is like your house key: **never** hand it over to anyone, even if they say they work at the bank.

### The social media bargain

Closing down sale! Brand-new leather couch for only R1 000. Cash transfers only. 5 left. Buy now!



**Is it a scam?**
**YES**

**How to tell:** A price that is far too low combined with the rush to 'buy now' using cash transfers is a major warning sign.

### The fraud alert message

Your account details were used to sign in to our website. If this was you, you can ignore this message. If not, go to our website or sign in to the app to let us know.



**Is it a scam?**
**NO**

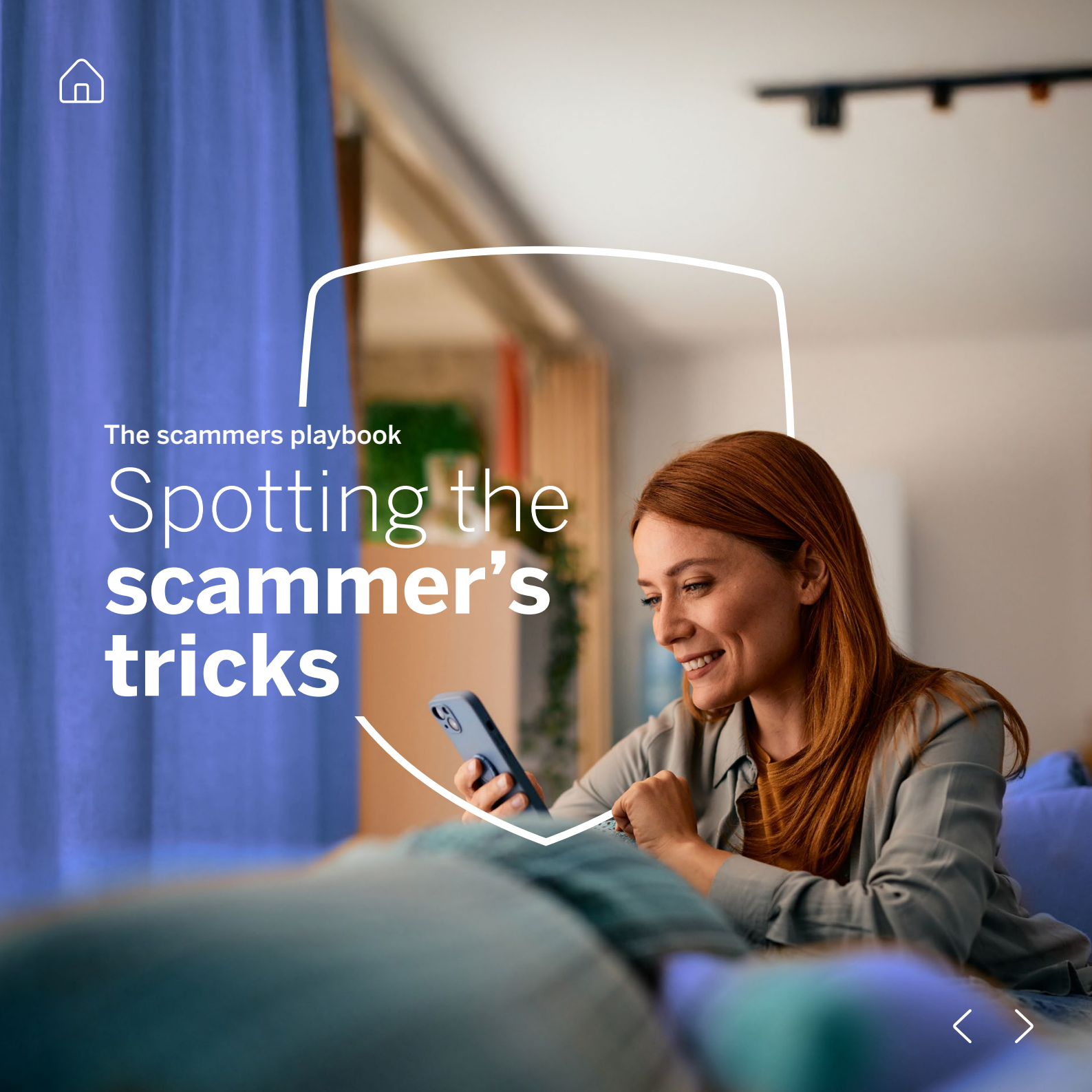
**How to tell:** This is how a real business alerts you. Look closely at what is missing: there are no links to click, and it does not ask you to type in your password, PIN or sign-in details. It simply tells you about it and suggests what you can do if it wasn't you.

# **Key** takeaway

Keeping yourself safe does not mean you have to fear technology or stop trusting people. It is simply about understanding how scammers try to trick you, so you don't have to fall for it.

## What you can do today

- ✓ **Tune into your feelings:** If a message or call makes you feel scared, excited or hurried. That feeling is your warning sign.
- ✓ **Share the quiz with someone:** Knowing what to look for can keep them safe.
- ✓ **Block out the noise:** Block spam numbers on your phone and turn on spam filters on your email so messages from scammers can't reach you.



The scammers playbook

# Spotting the **scammer's tricks**

Scammers want your money and your identity. But before they even send you a message, they look for clues you might have left behind online. They use these clues to contact you and make their lies sound real.

Here is how scammers find their way in, and the simple steps you can take to lock them out.



# **6 Ways scammers** find you (and how to stop them)

## Data leaks

When companies get hacked, your old passwords, emails and phone numbers can end up online. Scammers buy this information to contact you.

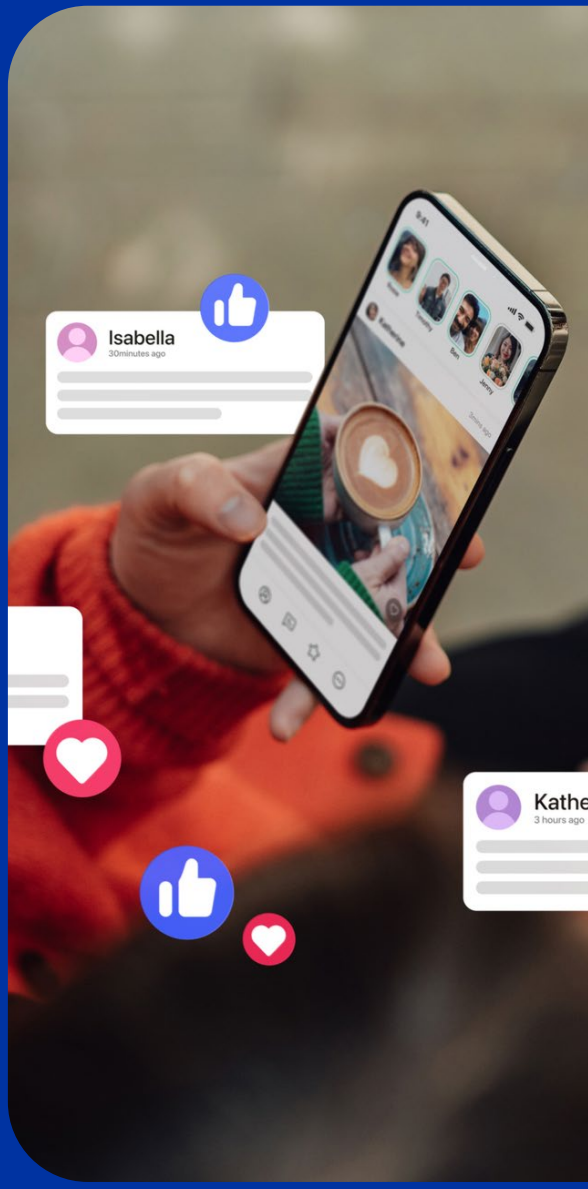
Turn on 2-step verification on your bank and email accounts. This sends a security code to your phone when signing in, meaning a scammer cannot access your account without having your physical phone.



## Over-sharing on social media

If your social media is public, scammers can see your pets' names, family members or when you are on holiday. They use these details to make their lies sound believable.

Set all your social media accounts to private. Before you post, ask yourself if someone would be able to use this against you.



## Weak passwords and public Wi-Fi

Using the same password for everything makes it easy for scammers to get into all your accounts at once. Free public Wi-Fi (at the mall) can also let strangers see what you are doing online.

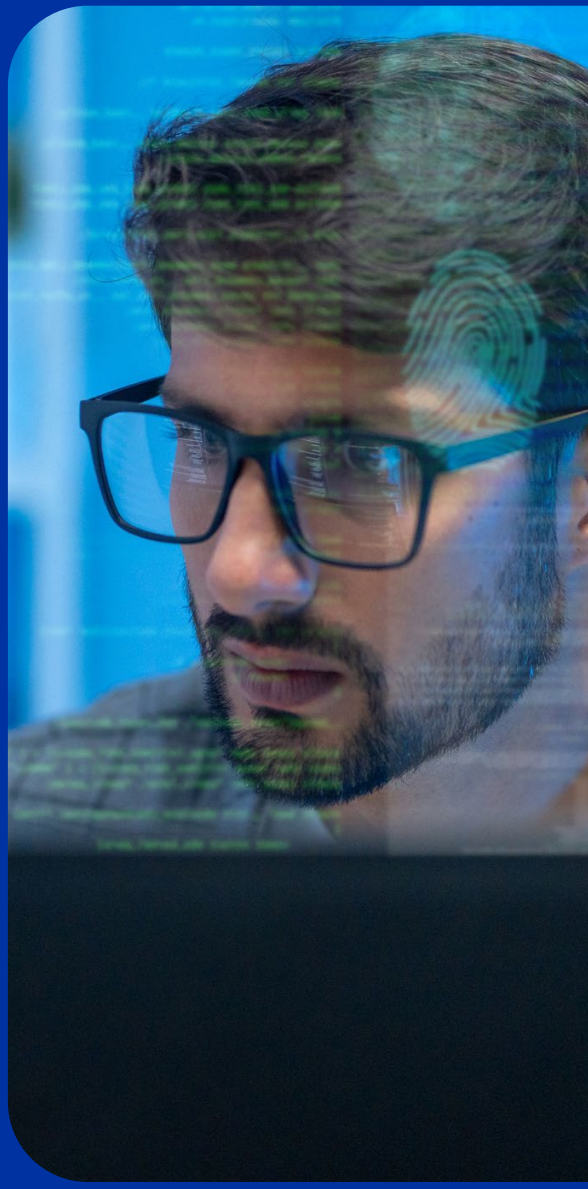
Use different, strong passwords for every account. Never do online banking or shopping while connected to public Wi-Fi.



## Publicly available information

A simple online search can often show your home address, phone number or where you work. Scammers use this to pretend they know you or live near you.

Search your own name online to see what is public. Remember: just because a caller knows your name and address does not mean they are official.



## Fake links and websites

Scammers send texts or emails with links that look exactly like your bank, tax office or streaming service. If you click and sign in, they steal your password.

Never click links in unexpected texts or emails. If you need to check your account, close the message and type the official website directly into your browser or use the official app.



## Bad apps and software

Scammers try to trick you into downloading help apps or security software. Once installed, these apps let them see your screen and control your device.

Only download apps from the official app stores. Keep your phone and computer updated: these updates act as a shield against hackers.



# **Protection** against apps and software that take over your devices

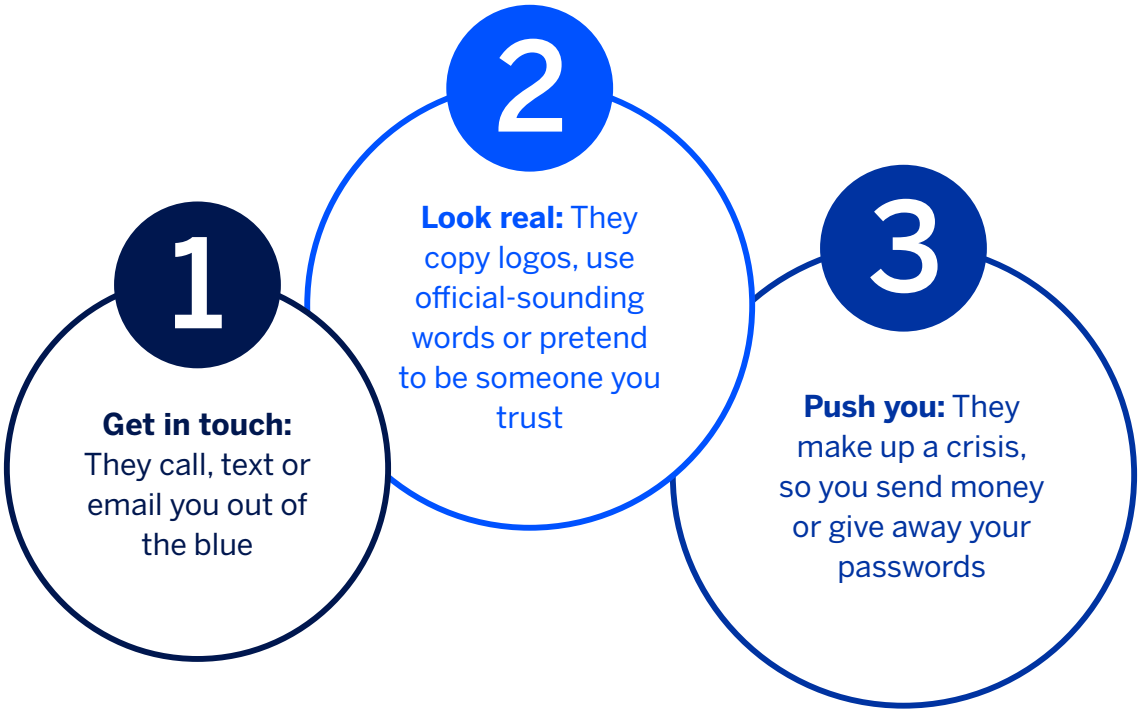
**Did you know?** Our Banking App can find malicious apps on your device when you sign in to it. If we find suspicious apps, we will guide you to remove those apps.

Download on the App Store | GET IT ON Google Play | EXPLORE IT ON AppGallery



# **Unmasking scams:** What to watch out for

Every scam has the same goal: to steal your information and your money. While their stories and technology are always changing, the way scammers operate stays the exact same. They always rely on a combination of pretending, pressuring and demanding using this 3-step plan:



# **Here is what this looks like** in real life and how to spot it:

## **Phishing and smishing:**
The digital hook

Email (phishing) and text scams (smishing) pretend to be trusted brands to steal your passwords or bank details.

This is how Sibongile almost fell victim to it and what you should look out for.

# Meet **Sibongile**



Sibongile is a paediatrician at a hospital in Cape Town. Driving home after a long day, her phone buzzed. An SMS from an unknown number said:

> "Urgent: You owe R350 for a traffic fine (Ref: TF567890). Pay now at: official-traffic-za.co.za/payfine or face bigger fines and arrest."

She knew about a speed camera on her way to work and sometimes drove fast for emergencies. R350 sounded real, but the 'arrest' shocked her.

Her first thought was to click the link and deal with it fast to avoid more trouble, but a small warning bell rang in her head, thanks to scam alerts from her bank, and she paused.

At home, Sibongile checked her banking app for fines. None! It was a smishing scam to steal her bank details. Relieved, she deleted the message and blocked the sender right away.

**DO:** Stop, take a breath and check whether the message is real by signing in to your banking app or the official website yourself.

**DON'T:** Click on any links in unexpected texts or emails, even if they threaten you.

**Did you know?**

You can easily check and securely pay for outstanding traffic fines on our Banking App.

## **Phone scams:**
## The voice that lies

With phone scams (vishing), criminals call pretending to be from your bank or a trusted business. They use pressure and panic to win your trust and trick you into sharing details or sending money.

Here's how it played out when Mr Jansen was targeted and what you can do if they call you.

# Meet **Mr Jansen**



Mr Jansen, a retired man from Pretoria, got a scary phone call one morning. The voice, formal and strict, said it was from SARS. He was told he owed a lot of tax. If he didn't pay right away, he'd be arrested and get a big fine.

The caller was scaring Mr Jansen, threatening him and telling him not to talk to anyone else because it was private and sensitive.

Worried and confused, Mr Jansen panicked. He didn't use online banking often, but the caller carefully told him how to make an instant transfer to a 'special SARS holding account'.

Later that night, he told his daughter what happened. She knew right away that it was a scam. She told him that SARS would never ask him to pay into an account over the phone or threaten arrest like that.

Mr Jansen knew something was wrong: his savings for retirement were gone.

**DO:** Hang up immediately, look up the business' official phone number and call them yourself to see if the ask is real.

**DON'T:** Send money or share personal details over the phone to a caller who demands instant payment or tells you to keep it a secret.

## Online shopping and investment scams:
Too good to be true

Buying and investing scams use fake online shops with cheap prices or get-rich-quick schemes. Scammers reach you through exciting ads and fake websites, rushing you to force a quick decision.

To see how this works in real life and how to avoid it, let's look at how scammers targeted and fooled Alex.

# Meet **Alex**



A new law graduate, Alex had already saved R10 000 for a trip to London, but it was taking too long, and he wanted his money to grow faster.

He saw an ad for ‘CryptoPeak Pro’ on social media. It promised to grow his savings quickly with amazing AI crypto trading. He’d heard friends talk about crypto success, so he thought he’d give it a try.

The CryptoPeak Pro website looked real: well-designed, with a fancy dashboard, live charts, big claims about how well it did and how its AI worked.
It also had great reviews from users and promised guaranteed growth.

Alex put in R2 000, and right away, his balance showed a 5% profit. He felt excited and happy to see his money grow.

Soon, a ‘personal investment advisor’ named Sarah called him. Her messages and market tips made him feel confident, but Sarah quickly pushed for more, “Alex, our AI found a limited-time chance to triple your money, but you must act now: the opportunity is ending soon.”

Alex was smart and thought he was good with money, but the exciting online profits and Sarah's pushing made him forget his common sense.

Sarah kept rushing him, "Put in another R2 000 within the next hour if you want to grow your money more." Caught up in the moment, Alex sent R2 000. When his balance shot up, he felt he had to act fast to make the most of it, so he put in his last R6 000.

A week later, the CryptoPeak Pro website was gone. He couldn't get a hold of Sarah, and Alex's R10 000 (and the fake profits) were all gone.

**DO:** Double-check the company's registration to see if it's legal and safe. Talk to someone you trust before thinking about investing.

**DON'T:** Let excitement or pressure rush you into sending more money to grow your money.

## **Romance scams:**
### Playing with your heart

In romance scams, criminals use fake profiles on dating apps to build loving relationships. When they have your trust and know you have feelings for them, they start asking you to send money for fake emergencies.

To understand how this can happen and how to guard against it, let's see how Zaynab experienced it firsthand.

# Meet **Zaynab**



Zaynab is a lively and successful interior designer in her late 50s. A friend told her to try a popular dating site.

There, she met David, a good-looking, caring and interesting architect who said he was working on some projects overseas.

They quickly moved their chats from the dating site to WhatsApp. He sent her sweet messages and called often, talking about their future together. Zaynab asked for video calls, but he always had an excuse, saying the internet was bad where he was. The relationship felt good, so Zaynab ignored the lack of video calls.

Months later, David sounded worried. He said his child needed money for an unexpected medical bill right away, and hospitals wouldn't treat them without instant payment. He said his own money was stuck because he was overseas.

He asked Zaynab to help him, and being deeply in love and trusting, she sent a large part of her savings to him.

A few weeks later, David said he needed more money for a plane ticket to finally come meet her. But Zaynab's daughter, Fatima, felt something wasn't right and told her mom to wait and let her check it out.

Together, they couldn't find any proof that David was real. They quickly found many stories online that used David's exact tricks and even found his profile picture was of an actor.

Zaynab's heart broke as she understood she'd lost both her money and her trust.

**DO:** Check them out online and talk to a friend or family member about your new relationship if they start asking for help.

**DON'T:** Send money to someone you have only met online, even if they have an emergency and promise to pay you back.

## AI scams:
The latest trick

AI scams use computer-generated voices and videos that sound real to copy people you know and use fake emergencies to panic you into sending money.

Here is how a scammer used this technology to target Mark.

# Meet **Mark**



Mark, the CEO of a clean energy company, was in the middle of a big business deal. He couldn't afford any surprises or bad news. His phone kept buzzing from an unknown number during a meeting.

He had just said hello when he heard a voice that sounded exactly like his daughter, Carla. Crying and scared, she said she was out for lunch with friends, had a few drinks and crashed into an expensive car. The owner was angry and said he was going to call the police and press charges if they didn't pay R50 000 right away.

He also said he'd post it all on social media. "Dad, if the police come, I'll be arrested and go to jail. I'm so scared," she cried.

"Wait, where are you? Are you OK? I'll come right now," Mark said. "Dad, please, there's no time. If you don't do this right now, I don't know what will happen."

Wanting to protect his daughter, he was about to sign into online banking on his laptop when he thought of something: a news story about AI voice scamming rich people.

Then he knew: the unknown number, the hurry for money, telling him not to ask questions. He quickly hung up and called Carla's real number.

Carla answered, she was perfectly fine.

The criminals had used AI, taking bits of her voice from social media videos or public recordings, to make a real fake voice. They had used his love and feelings against him, creating a fake emergency that almost cost him money and his good name.

**DO:** Hang up right away and call your loved one back on their normal, saved number to check if they are safe.

**DON'T:** Let the panic of a crying voice or a shocking story rush you into making a payment to an unknown account.

# **Sharpen** your scam radar

Seeing how easily people like Sibongile, Mr Jansen, Alex, Zaynab and Mark were targeted can be scary, but luckily there are ways to stop scammers in their tracks.

No matter what story a scammer tells, they all use the exact same 3-step playbook to try to trick you:



Pretending to be someone you trust



Creating a crisis or a prize



Rushing you into doing something right away

If you spot even one of these steps, you are dealing with a scam. Here is your 3-step action plan to shut it down.

# **The 3-step plan** to shut down scams

## **Step 1:** STOP the unexpected contact

Scammers contact you out of the blue, pretending to be your bank, the police, a delivery company or a loved one in trouble.

- **The trap:** Using logos, voices and words to make you believe they are real.
- **Ask yourself:** Am I 100% sure this is really them, or is it just because they know my name?
- **How to shut it down:** Cut the connection. Hang up or delete the text or email.
- **The golden rule:** Never trust a random call, text or message. It doesn't matter how real the caller ID looks or how polite the voice is.

## **Step 2:** CHECK your feelings

Scammers must get you to feel fear, panic or excitement.

**The trap:** They make up a problem to get you to panic or become excited, so you stop thinking clearly.

**Ask yourself:** Is this message making me feel scared, rushed, angry or excited?

**How to shut it down:** Make a small movement with your body.

- On a call: move your phone from your ear to a table and put it on speaker or mute.
- If you're reading a text, turn the phone face down.

This slows down the rush of information and gets their voice 'out of your head' and into the open, giving you the chance to step out of the fear for a second to think clearly.

**The golden rule:** If a message makes you feel even a little strange, treat it as a scam.

## **Step 3:** REJECT their rushing

Scammers can't afford to let you think, ask questions or talk to anyone else.

**The trap:** They might tell you to do it now or something might happen, you could lose out or that things can get worse if you don't do it right away.

**Ask yourself:** Why can't this wait?

**How to shut it down:** Take back control of the clock:

- Tell them, "I need to check this first. I will call you back." (A real bank will always agree to this. A scammer will get angry or panic.)
- If they try to argue or try to keep you on the line, simply hang up. You don't need to explain why.

  Once you hang up, block the number so they can't call or text you back to pressure you further. Call a friend or family member and tell them what just happened. Hearing yourself explain the story out loud to someone you trust is the fastest way to see the scam for what it is.

**The golden rule:** You don't have to be polite to a stranger who is rushing you. It is okay to hang up on them or ignore their messages.

# **Scam** checklist

Before you click, respond or share any information, run through these questions to check if there are scam warning signs.

## Email, SMS, messaging, social media

- ☐ Are they asking for passwords, bank details, your ID number or CVV?
- ☐ Does the message have strange links, QR codes or attachments?
- ☐ Did this message or call come out of nowhere, or were you expecting it?
- ☐ Is the message saying you need to do something now or something might happen?
- ☐ Are they using ‘Dear Sir/Madam’ or ‘Dear Valued Customer’ instead of using your name?
- ☐ Does something about it just feel off or too good to be true?

## Online shopping and investment opportunities

- ☐ How excited are you about this offer (from 1-10)?
- ☐ Have you ever heard of this shop or place before?
- ☐ How do they want you to pay? If they ask for strange ways to pay, look out.
- ☐ Are they pushing to buy/invest right now with limited-time offers or guaranteed growth?
- ☐ Is there real and easy-to-find contact information on their site?

## Romance and love

- [ ] How quickly is this person moving the relationship?
- [ ] How much do you really know about them, except for what they told you?
- [ ] Have they asked you for money, gifts or loans?
- [ ] Do they avoid meeting in person or making video calls?
- [ ] Do they look too good in their profile (e.g. like a movie star or athlete)?
- [ ] Do they claim to be in a difficult-to-reach place?
- [ ] Is their life story very exciting or does it keep on changing?

## AI scams (fake voices, videos and smart bots)

- [ ] Does their voice sound like it usually does, or does it seem a bit strange?
- [ ] Has the person calling you ever asked (and rushed you) for money?
- [ ] In chats, do they answer too quickly, and do their answers feel strange?

# **Key** takeaway

Scams are always changing, but if you can see (or feel) that something isn't right, you can stop them in their tracks.

## What you can do today

- ✓ **Manage your online trail:** Keep your personal information safe from online scammers.
- ✓ **STOP. CHECK. REJECT:** Use this simple rhyme to beat tricksters.
- ✓ **Use the scam checklist:** Know what to look for and if something feels off.


Build your scam-proof shield
Smart habits for safety

We've looked at the warning signs and the clever tricks scammers use, but you don't have to wait to be targeted. There's a lot you can do to stay one step ahead of scammers.

### Lock them out of your life

Using the same password for everything dangerous. If a scammer steals just one of your passwords, they can get into all your other accounts, including your online banking.

To protect yourself, you can do the following:

- **Use 'password sentences' instead of passwords:** Simple passwords (e.g. Password123) are easy to guess. Instead, use a short sentence with a mix of letters, numbers and symbols that only you know, such as 1LoveWarmCoffeeInM@y!.
- **Double-lock your accounts:** Turn on 2-step verification on your email, banking and WhatsApp. This works like a security gate. Even if a scammer steals your password, they still can't get into your account without a code sent directly to your phone.
- **Secure your identity with DigiME:** Take a few minutes today to set up a secure digital profile on our Banking App. This means hackers can't pretend to be you to change your banking details:

1. Select **More** on the bottom navigation on your home screen
2. Click the **DigiME** option
3. Allow permission to access your camera
4. Select **HOME OR WORK** and provide your ID number
5. Click **NEXT,** then scan your face and follow the prompts

## Take back control

Scammers want to rush you into making snap decisions. They don't want to give you time to think. But real businesses, banks and government offices will never force you to make a quick decision on the spot.

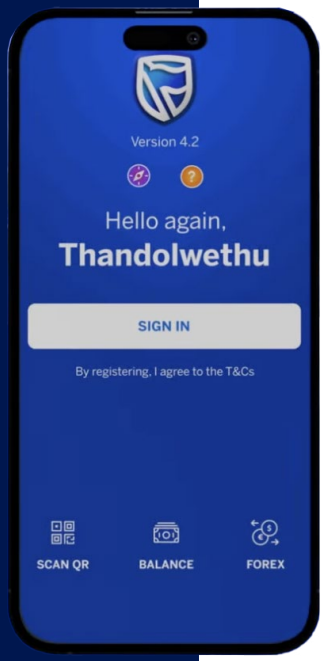
You are always allowed to slow down, ask questions or walk away. If you get a call that makes your feel scared or rushed, hang up (or delete the message). Don't worry about being polite.

## Easily protect yourself from phone scams with Trust Call

The **Trust Call feature on our Banking App** lets you be sure that a call is really from Standard Bank, not a scammer trying to steal your money or information.

A pop-up instantly confirms calls from our bank agents. If a call isn't confirmed, a warning message gives you scam-stopping tips and allows you to securely block the number or use in-app calling to contact us directly.

For your safety, if you initiate a payment on the app while on a phone call, we may temporarily pause the transaction to prevent coerced transfers. If the payment is genuine, simply end the call and try again.



## Put your safety first

- **Check before you click:** If you get an unexpected email with a link or attachment, don't click it. Hover your mouse over the link (or long-press it on a mobile phone) to see the real website address. If it looks strange or misspelled, delete it.
- **Be careful of using Wi-Fi:** Free public Wi-Fi networks in cafes, malls or airports are not safe, scammers can use it to see your screen. Only sign into your banking app using your own data or safe home Wi-Fi.
- **Update your devices:** When our phone or computer tells you to update, do it. These updates have security patches to block the latest hacking tools.

## Pause and push back

Scammers want you to keep secrets because keeping quiet makes their tricks work.

- Make a rule to never make a sudden, big money decision without talking to a trusted family member or friend first.
- Talk openly about scams so that those you care about know what to look out for.

### Add a trusted contact person to your banking profile

Add an extra layer of safety to your account with the **Trusted Person feature on our Banking App**. This feature lets you choose a trusted friend or family member to help protect your money. When you make an unusual transaction, they'll get a quick notification to review and confirm the transaction, but they'll never have access to your accounts, balances or banking details.

# **Your personal** safety checklist

This quick checklist helps you build easy safety habits that protect you every day.



**Protect your online self**

- ☐ Use strong, unique passwords.
- ☐ Turn on 2-step verification.
- ☐ Check your social media privacy settings.



**Stay sharp and trust your gut**

- ☐ Pause whenever you get an unexpected call, message or offer.
- ☐ Talk to a trusted friend before making big decisions.



**Always check things yourself**

- ☐ Never use contact details (phone numbers, links) provided within a message or call you're unsure about.
- ☐ Hover over the link to check where it truly goes.
- ☐ Never click on links or attachments in unexpected messages.

# **Key** takeaway

You have the power to stop scammers in their tracks. Keeping yourself safe isn't difficult, it starts with simple, daily habits.

## What you can do today

- ✓ **Lock your accounts:** Take 5 minutes to set up strong passwords and turn on 2-step verification.
- ✓ **Pause before you act:** Stop, think, and double-check any unexpected message or call.
- ✓ **Practice safety habits:** The more you practice these simple steps, the easier it becomes to keep yourself safe every day.

# **Next** steps

Now that you know how to spot scams, you're ready to take the next step in protecting your money and your identity.

**Download your next guide:** *How to recover when fraud hits.* This guide will show you exactly what to do if you are ever targeted by a scam, and how to get your money and accounts back on track.

**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

## A

**AI (artificial intelligence) scams:** When scammers use smart computer programs to copy a voice or face to make a fake emergency sound completely real.

## C

**CVV:** The three small numbers on the back of your bank card. It is a secret security code that you should never share with anyone.

## D

**Dangerous apps:** Fake or harmful programs that scammers trick you into downloading onto your phone or computer. Once installed, these apps allow scammers to secretly watch your screen, steal your passwords, and control your device to access your banking details.

**Data leak:** When a big company gets hacked and information like phone numbers, emails, and passwords are stolen and shared online.

## F

**FICA:** A legal check in South Africa to prove who you are and where you live.

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

## I

**Identity:** The private information that proves who you are. This includes your full name, ID number, home address, and bank details. Scammers want to steal this information so they can pretend to be you, open accounts in your name, or take your money.

## O

**OTP (one-time PIN):** A unique security code sent to your phone to confirm a payment. It acts like a key to your money—you must never give it to anyone else.

## P

**Phishing:** Fake emails sent by scammers pretending to be trusted companies (like SARS, banks, or courier services) to trick you into sharing your details.

**Public Wi-Fi:** Free internet access offered in public places like malls, airports, or coffee shops.

## R

**Red flag:** A warning sign or a gut feeling that tells you something is not right.

**Romance scams:** When a scammer pretends to be in love with you online to earn your trust and eventually ask you for money.

## S

**SARS:** The South African Revenue Service (the tax office). Scammers often pretend to be from SARS to threaten you with arrest if you do not pay them immediately.

**Scam:** A clever trick or lie used by criminals to gain your trust so they can steal your money or your personal information.

**Smishing:** Fake SMS text messages sent by scammers to trick you into clicking a bad link.

**Spam:** Unwanted junk messages.

**Spam filters:** A spam filter is a setting on your phone or email that automatically blocks these messages from reaching you.

## V

**Vishing (voice phishing):** Phone call scams where a criminal calls you and pretends to be from your bank, the police, or a business to trick you.

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

Learn more