Learn to identify cybercrime, fraud and scams

As businesses have shifted their workforce to flexible, hybrid models, the risk of cyberattacks has increased. Threat actors take advantage of current events and changing circumstances to exploit those who are most susceptible. While countermeasures exist to safeguard employees working from home – they're not infallible.

The only way to foster a truly secure environment is through continued diligence from users.

It is up to you to stay informed about scams and think twice before sharing your personal information, whether online or telephonically.

Types of Scams

Scammers and cybercriminals are always looking for ways to lure you in and trick you. It is important to be aware of the various types of scams.

This type of banking fraud is becoming more common in South Africa (businesstech.co.za)

Phishing

Phishing is when you receive an unsolicited email from fraudsters in which they claim to be from a reliable organisation such as your bank, SARS, or a similar institution.

The email looks as if it comes from your bank, with a link to your Internet Banking Profile. Once you click on the link, you are redirected to a fake webpage where you will be asked to fill in your account details, username, and/or password for internet banking, email account, cellphone number, or bank card details. This will give the fraudster access to all the information they need to steal from you.

For instance, the email will state:

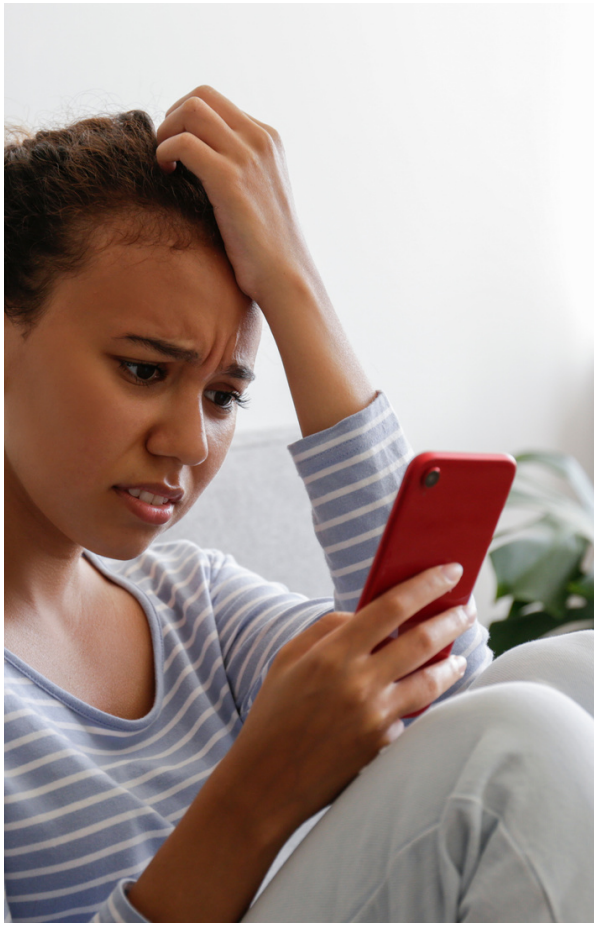
- You have been a victim of fraud, but to report the incident and cancel your bank card, you need to click on a link and sign in to your account, or
- A SARS refund is due to you, but to receive the funds, you need to click on a link and sign into your account.

Vishing

Vishing is a combination of the words “Voice” and “Phishing”. The fraudster will contact you telephonically, pretending to be somebody from a service provider or the bank asking for personal and bank account details.

The fraudster will pretend that they are phoning:

- To confirm personal or bank account details because of a payment or additional payment that is apparently due to you, or
- From the bank’s fraud department to notify the account holder that funds were fraudulently taken from the account holder’s bank account and confirmation of bank details are required to stop the transaction from going through.



SMShing

As the name suggests, SMShing is much like Phishing but occurs via text message on mobile devices. In these cases, you’ll get a scary message supposedly from your bank telling you that your credit card has been stolen or a large sum of money has been withdrawn from your bank account. It will include a link for you to follow to input your PIN and other sensitive and personal information in some kind of “reporting” environment. Don’t do it!

If you’re concerned about your bank accounts, phone your banking institution’s lost or stolen cards or fraud helpline.

In a very recent SMShing scam that was covered in the media, existing and previous Standard Bank clients were targeted. Click on the link below to read the article published by Business Tech on 20 November 2021.

Standard Bank warns of new scam targeting customer (busniesstech.co.za)

Deposit and Refund scams

If anybody ever contacts you to tell you that they’ve “accidentally” paid money into your bank account, you should be suspicious. Scammers provide fake “proof of payment” and ask you to refund their money. You will pay it, believing that the money will clear in your bank account soon. Of course, it never will. Always double-check these deposits with your bank. Click on the link below to read the article about Deposit and Refund Scams

Deposit and Refund Scams (d1a528lnc1alz9.cloudfront.net)

Key loggers

Did you know that it is possible to record every single key you press on your keyboard? With the right code, scammers can identify your usernames and passwords by tracking the keystrokes you have used on sites; hence this online scam is known as a key logger. It can be transferred to your device through an email attachment or memory stick.

Keep your security software up-to-date and never open unknown e-mail attachments.

Email hacking scams

Fraudsters gain unathorised access to your email address through malware viruses and start sending emails to your family and friends, pretending that you are in trouble and need financial assistance.

Stolen phones scams

A fraudster can access your personal and banking information on your stolen mobile phone, which is why it is crucial that you de-link a stolen device from your digital profile immediately or report the device as stolen.

SIM swap scams

Fraudsters usually perform a SIM swap without your knowledge, allowing for your phone calls and SMS’s to be intercepted. A SIM swap usually takes place after the fraudsters have received your internet banking login details following your response to a phishing email, vishing call, or SMShing message. Once the fraudster has access to your personal information, they can pose as you to request a SIM swap. This will give them access to your phone calls, SMSes, and OTP’s.

Number porting scams

A number porting scam is where fraudsters transfer your cellphone number from your current network service provider to another without you knowing. Number porting usually takes place after the fraudsters have received your internet banking login details following your response to a phishing email, vishing call, or SMShing message.

Never ignore an SMS from your mobile network provider confirming that your number has been transferred to another service provider. If you ignore such an SMS, the fraudster can complete the porting and it will give them access to your phone calls, SMSes, and OTP’s.

Identity Theft

Identity theft occurs when someone steals your personal information to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many ways and its victims are typically left with damage to their credit, finances, and reputation.

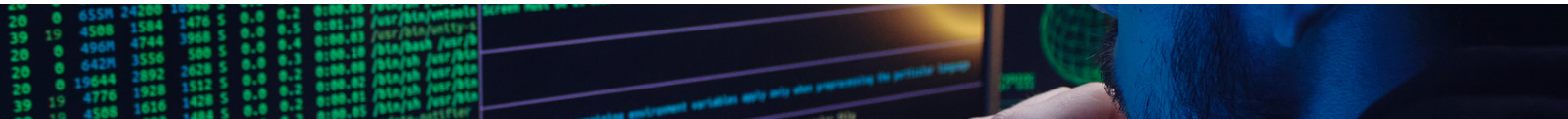
Identity thieves increasingly use technology to obtain other people's personal information for identity fraud. To find such information, they may search the hard drives of stolen or discarded computers; hack into computers or computer networks; access computer-based public records; use information-gathering malware to infect computers; browse social media sites; or use deceptive emails or text messages.

To find out more about the ten most common ways identity thieves get hold of your data, click on the link below.

How to spot a scam?

Common scam techniques include:

- You are told either telephonically or via email that they're from the fraud department of your bank, and that you have been a victim of fraud such as, for example, that funds have been fraudulently taken from your bank account and you need to confirm your personal and bank account details so the funds can be returned to your account. There is always a sense of urgency in the phone call or a threat to freeze or suspend your bank account if you do not provide personal information.
- You are asked to update or confirm your bank account number, PIN, or password over the phone or by clicking on a link.
- The offer, for example, a tax refund, sounds too good to be true.
- You're asked for an urgent refund before you can verify with the bank that the payment was made into your bank account and is valid.
- You are no longer receiving calls or messages on your cellphone or your cellphone suddenly has no signal.



Tips to protect yourself against fraudsters

Think Twice!

Don’t open or respond to emails from unknown sources. Do not open e-mail attachments or click on links in SMS messages if you don’t trust the source or don’t know what it is.

Strength in your password

Create strong online passwords with a combination of letters, numbers, and characters. Find a pattern that will be easy to remember, but impossible to guess.

Keep your passwords and pins secret

Your bank will never call and ask you to confirm your PIN or an OTP telephonically or be expected to send it via e-mail or through any other messenger applications. If somebody is asking you to do this, they do not represent the bank.

Question every link

Criminals can make websites that look just like your online banking environment and fool you into inputting your username and PIN. Rather open a fresh browser and type the address in yourself.

Don’t hide things in plain sight

It can be hard to remember all your passwords and PINs but don’t write it on post-it notes and hide it under your keyboard, or in your diary that you leave in a drawer or save them on your laptop. Always make sure that your devices auto-lock and are password protected.

Secure websites

When you are on a secure site, a padlock (see screenshot on next card) will be visible on the left-hand side of the website address in your browser. This means that you are in a secure environment to bank or make online payments. It is recommended that you do not use public computers, such as an Internet Café, to do your internet banking.

Anti-virus Software

Always ensure your anti-virus software on all your devices is up to date.

Destroy

Securely destroy or shred old bank statements and similarly printed documents with your personal information, account numbers including expired bank cards. Click on the link below to read the article published by the South African Police service.

Be Alert | SAPS (South African Police Service)

Ransomware affecting Companies

It is not only individuals being affected by fraudsters and scammers. According to Interpol's African Cyberthreat Assessment Report released in October, during the first quarter of 2021, South Africa was the worst affected on the continent in terms of targeted ransomware attacks. These ransomware attacks can pose a threat to people, critical infrastructure, and the economy.

Some of the South African ransomware attacks that come to mind:

the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

TRANSNET

The Department of Justice and Constitutional Development suffered a debilitating ransomware attack in September, affecting all its electronic systems.

Transnet and its division operating South Africa's biggest ports was also recently a target. The cyberattack affected all their crucial systems.

Click on the links below to read more Cyber attack and cyber security:

Basil Read SA's latest target of cyberattack | Fin24 (news24.com)
https://www.moneyweb.co.za/news/tech/bureau-veritas-hit-by-cybersecurity-attack/

With the drastic increase in scamming and cybercrime, and the constant development of new, smarter cons - It is up to each of us to stay informed and think twice before sharing our personal information, whether online or telephonically.

If ever in doubt, please contact the IT Department to verify if an email or IP address is legitimate or a link is safe to click on.