NEDGROUP INVESTMENTS

Fraud awareness and prevention

Your guide to beating fraud

see money differently

Contents

Cybercrime:

Scams:

Banking safely:

Phishing, smishing and vishing

Phishing (email) and **smishing (SMS)** involve fraudsters asking you to click on a link or an attachment that takes you to a fake website where you must enter your personal information, for example your Nedbank ID and password or your card number and PIN.

Fraudsters convince you to follow these links by sending you communications that looks like it comes from Nedbank, saying that your account has been accessed, that you need to update your account or install new software to protect yourself.

Sometimes fraudsters also send you a fake proof of payment or a bank statement as an attachment to an email. Once you have clicked on this attachment, you're prompted to enter your Nedbank ID and password or card number and PIN to open the attachment, giving the fraudsters access to your credentials.

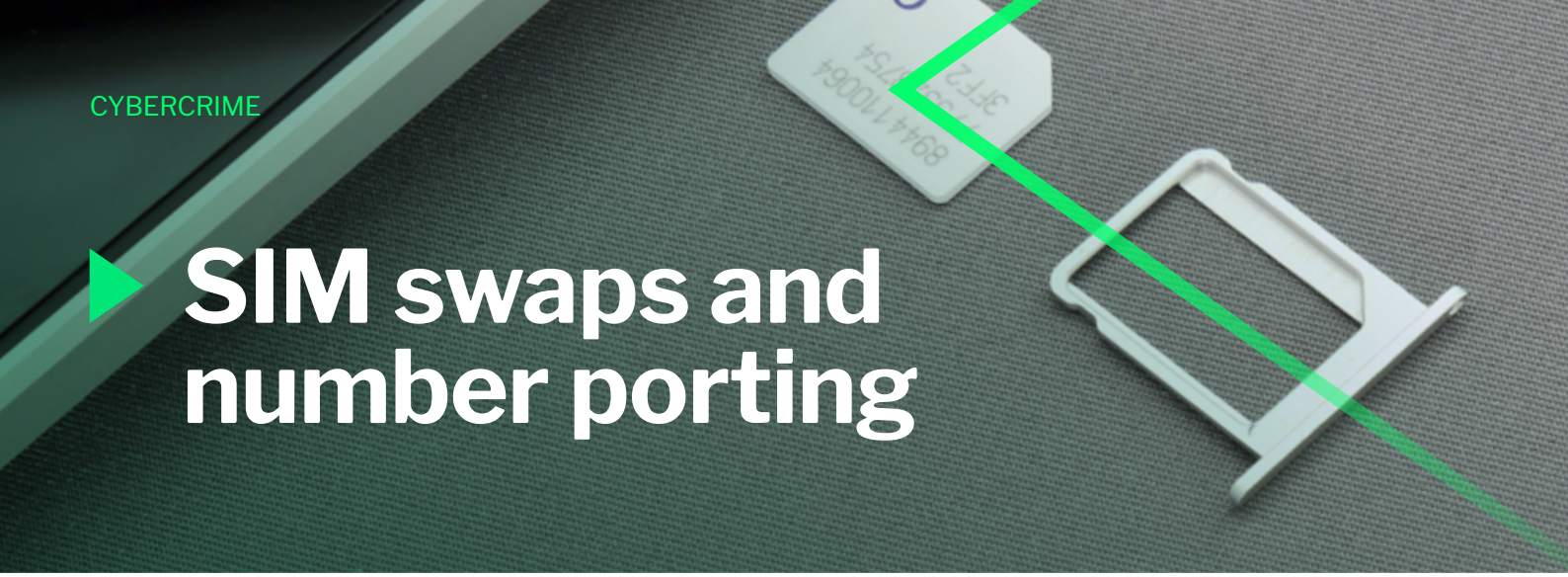
Vishing is social engineering over the phone. Fraudsters call you and pretend to be a bank employee, asking for your personal information. They may also try to trick you into calling them by sending a SMS saying that a transaction is being processed on your account, or that a new debit order has been registered on your account. When you then call the number in the SMS, the fraudsters ask you for your personal information to 'reverse' the debit order or transaction, hoping to get their hands on your banking details.

They also pose as representatives from Nedbank's fraud department and urge you to give them your card PIN or Nedbank ID and password to stop a 'fraudulent transaction' or 'reverse' a debit order. They even try to convince you to accept an Approve-it message or share a one-time password (OTP) with them, hoping that you won't read the message carefully and notice that they are indeed trying to transact on your account.

Fraudsters also use caller identity spoofing, when a call appears to be from a legitimate or known number to get their hands on your personal information. Once they have your Nedbank ID and password or card number and PIN, they can access your Online Banking profile and download the Money app.

Tips to keep safe

- Don't click on links in messages from unknown sources.
- Nedbank will never ask you to sign into Online Banking through an attachment or a link.
- Never give anyone your Nedbank ID and password or card PIN and CVV number (the three- or four-digit security number on the front or back of your card). Nedbank will never call you to ask for these details, not even a portion of it.
- Never share an OTP with anyone.
- Always read your Approve-it messages carefully before accepting them and decline the transaction if you didn't make it and report the incident to Nedbank immediately on **0800 110 929**.
- Keep your passwords safe. Don't store them on your device or in your browser and don't use the same username and password for all your logins. Your username and password should also be different.
- Always ensure that you have the latest version of your banking app loaded on your device.
- If you have the Money app on your mobile device and it's lost or stolen, contact Nedbank to deactivate the app immediately on **0800 110 929**.
- When calling back to confirm a call from Nedbank, don't just confirm if the person works at Nedbank. Talk to the individual to find out if they have indeed contacted you.
- Hover your mouse over any hyperlinks to see the actual URL. On mobile devices, you can long-press the hyperlink to see it.
- Don't respond to phishing emails. If you receive a suspicious email, forward it to phishing@nedbank.co.za immediately.
- Make sure you have the latest antivirus software installed on all your devices and install the latest updates or patches on your operating system as soon as they become available.
- Don't trust caller identity. Fraudsters use number-masking software to make it look like the call is from Nedbank when it's not.
- If you receive an SMS for a SIM swap or number port you did not request or seem to lose cellphone connectivity for a long time without reason, call your service provider and let us know immediately on **0800 110 929**.
- Do not do your banking on a public computer found at libraries, cyber- or internet cafes and hotels, and avoid using Wi-Fi hotspots.
- Check your statements frequently and let us know as soon as you see any unfamiliar transactions.
- Report fraud by calling us on **0800 110 929**.



SIM swaps and number porting

Fraudsters use SIM card swapping and number porting to commit fraud. They approach your service provider pretending to be you and ask for a transfer of your existing cell phone number to a new SIM card, or they ask that your number is ported to another service provider. They often present a stolen or fraudulent identity document and can answer the security questions posed by the service provider as if they were you.

How it works

- They call your service provider, pretending to be you, and ask for your cellphone number to be transferred to a new SIM card. Or they ask for your number to be ported to another service provider.
- They present a stolen or fraudulent ID and answer security questions that the service provider asks.
- They then call you repeatedly until you eventually turn off your phone to give them time to do a SIM swap or port your number without you knowing.

Tips to keep safe

- If you lose cell phone connectivity for some time for no apparent reason, receive an SMS for a SIM swap or a number port you did not request, contact your service provider urgently and let us know immediately by calling **0800 110 929**.
- Protect your personal information and be careful with whom you share it.
- Before fraudsters do a SIM swap or number porting, they will often call you numerous times, hoping to frustrate you so that you turn your phone off. This allows them to do the SIM swap or number porting, and you will not be aware that your phone has no signal.
- Ensure that you inform the bank immediately if you change your cell phone number, as notifications will go to your cell phone number loaded on the banking system.
- Make sure that you check your bank statement regularly and query any unauthorised transactions.
- Contact your service provider if you notice anything suspicious.
  - **MTN: 123 stop (123 7867)**
  - **Vodacom: 082 1946**
  - **Cell C: 084 140**
  - **Virgin Mobile: 0741 000 123**
  - **Telkom: 081180**

Whaling

This is a form of phishing that targets businesses by sending emails to finance departments impersonating a chief executive or chief financial officer to trick employees into making an 'urgent' payment. The employee makes the payment and the fraudsters get away with the money. Financial institutions and businesses are the primary targets of these scams.

How it works

- Fraudsters determine who in an organisation has the authority to make large payments. Then they source this person's contact details and any other information they can use to make the request for payment seem more legitimate.
- They make use of social engineering to gather information by trawling through social-media platforms and may even contact other employees to get more information about the person.
- They may even use a copy of the organisation's email template and the person's signature to make the request seem real.
- Fraudsters then send an email to the targeted employee, saying that a payment must be made into an external account, hoping that the payment will be made.
- They rely on employees never questioning or verifying an instruction from their superiors. And being busy, employees do not always take the time to look at the format, layout, grammar and punctuation in emails. Instead, they quickly scan through them, do what should be done and move on to the next email.

Tips to keep safe

- Make sure the email address on the email you have received is correct and matches the email address on your records. Fraudsters will make small changes, like adding a full stop or changing a letter, hoping that you won't notice.
- If you receive an email that seems strange or out of the ordinary, contact the sender and confirm that the email came from them.
- Do not click on links in a suspicious email, as you might unknowingly download malware onto your computer.
- Be careful what information you share on social media. Fraudsters use social media to gather information about their targets.

Email hacking

Email hacking happens when cybercriminals get hold of your email account username and password and access your email account. If you use your email account for banking or business purposes, cybercriminals pretend to be you to order goods or services, ask banks to make transactions on your behalf, or even notify business clients of a supposed change in banking details.

Apart from being able to send emails using your mailbox, cybercriminals also create a rule on your mailbox to move any emails from a specific sender to folders located on their computers. You will be totally unaware that your email credentials and confidentiality have been compromised.

How do fraudsters get your email details?

Phishing:

You could have given your email credentials to fraudsters by typing them into a fake website made to look exactly like your email provider's login page. These phishing emails look like they were sent by your email provider and often contain warnings to grab your attention, for instance that you are running out of storage space or that your account will be deleted if you don't log in immediately.

Malware:

Your computer may have been infected by malware that monitors your keyboard strokes or searches your computer for saved passwords.

Hacked website:

You may have registered on a website with the same credentials as your email account, and this website has been hacked.

Tips to keep safe

- Never enter your email credentials on a website that you have accessed via a hyperlink in an email.
- Also be careful of clicking on attachments from unknown senders, especially if these attachments are
- programs (eg files that have an .jar, .img, exe or .cab extension) or are contained in archives like zip files.
- Many websites require that you register with your email address and a password. Never use the same password that you use to access your email address to register these sites.

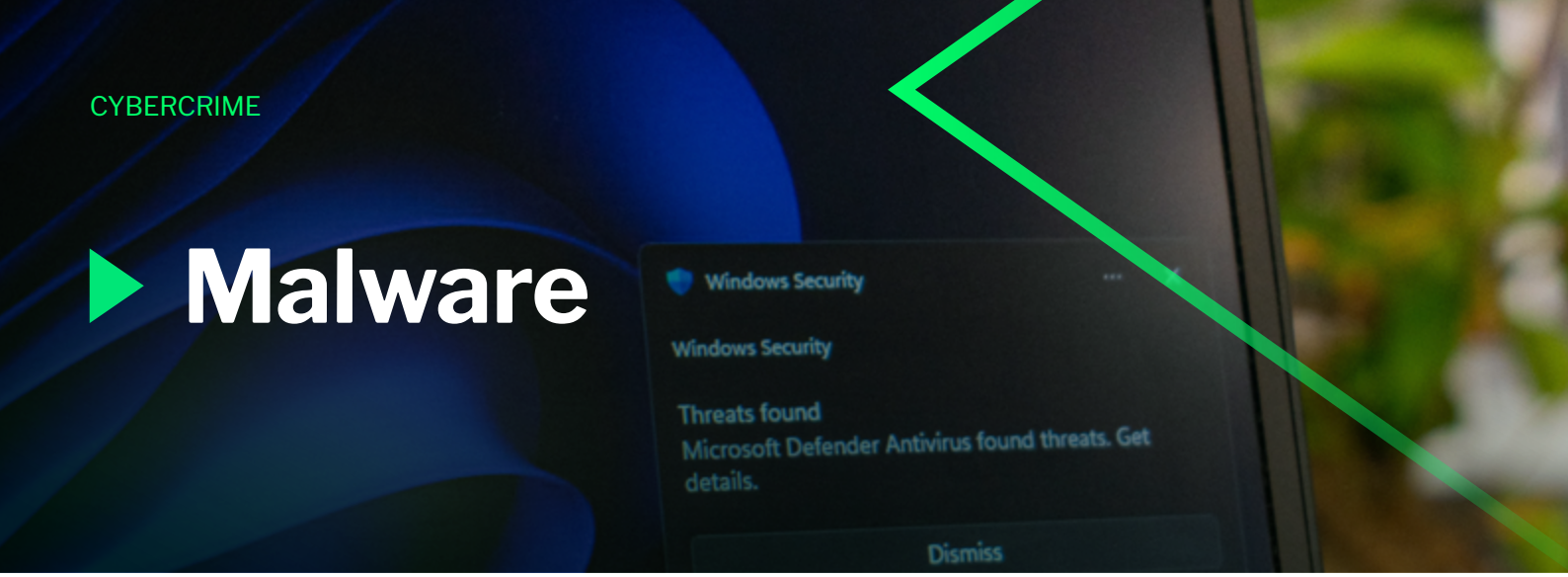
- Keep your passwords safe. Don't store them on your device or in your browser and don't use the same username and password for all your logins. Your username and password should also be different.
- Many email providers offer the option of out-of-band confirmation, like an SMS sent to your cellphone. If your email provider has this option, use it. If it doesn't, consider changing your email provider.
- You should have reliable, up-to-date antivirus software on your computer, regardless of whether it runs the Windows or MacOS operating system. You can get more information from test sites on the internet at www.av-comparatives.org or at www.av-test.org.
- It is important that you patch your computer regularly. Hackers are constantly discovering new weaknesses in operating systems and other common software like Adobe Acrobat. Make sure that you regularly update your PC or Mac with the latest patches.
- Keep in mind that you may also fall prey to email hacking if your clients' or suppliers' email accounts have been hacked. Never accept financial instructions, for example to make a payment into a supplier's new bank account, sent to you via email only. First call the supplier on a number that you have used in the past to confirm that their banking details have indeed changed. But don't use the contact number given in the email you have received. If it is a fraudulent email, you will be talking to the fraudster and not the supplier.

What to do if your email account has been compromised

- Immediately disconnect the computer on which you have accessed this email address from the internet until it has been thoroughly checked for malware and disinfected by a specialist.
- Change the password on a trusted, but completely unrelated computer that does not share the same network. If you can change the password from a device less prone to virus infection, like a smartphone or a tablet, so much the better.
- Once you've changed your password, immediately notify Nedbank on **0800 110 929**, as well as your banker, financial planner, suppliers, and any other people with whom you have a financial relationship. Ask them to confirm all emails with you before actioning them. It is also important to continue scrutinising your bank statements for any inexplicable entries.
- Examine the deleted items and sent items in your mailbox for any emails that could have been sent by hackers and take immediate action to remedy these activities.
- Sometimes, fraudsters cannot send emails from your email account and create a similar email address from which they send their fraudulent emails. If you are aware of such an email address, contact the email service provider immediately with evidence of the compromise and ask them to take urgent action to close this email address.
- Although this may not be the case, you should assume that any sensitive information on the computer has been compromised. This information could include your email correspondence, passwords for various facilities like your email account or online shopping accounts, as well as the contents of documents stored on your computer. You need to change all your passwords for online accounts, including your email account and online shopping accounts on an uninfected computer.

- If any fraud has occurred, open a criminal case with the South African Police Service.
- Contact the South African Fraud Prevention Service (SAFPS) at www.safps.org.za or **0860 101 248** and ask for their free protective registration service for identity theft.

Malware



Fraudsters send fake emails or messages that look like they come from your bank or other reputable organisations. These emails or messages have links or attachments containing malicious software, which is downloaded onto your device when you click on them.

Once your device has been infected with this malware, fraudsters gain access to everything stored on your device, monitor your keyboard strokes and record everything you type, including your Online Banking credentials.

How does malware work?

- You receive a fake email with a proof of payment or a bank statement as an attachment and click on the attachment.
- Someone calls you posing as an employee from an IT company, offering to help you download fake security software.
- You access a website that is infected by malware.
- You click on a link or an attachment, asking you to install or upgrade software.

Tips to keep safe

- Don't authorise an action to execute, install or upgrade software.
- Hover your mouse over hyperlinks to validate the website address (URL) before you click on it. If you long-press on a hyperlink on your mobile device, it should also reveal the underlying website address.
- Make sure that you have up-to-date antivirus software installed on all your devices.
- Ensure that you install the latest updates or patches to your operating system as soon as they are available to prevent criminals from exploiting security vulnerabilities on your device.
- Scrutinise your bank statements frequently and notify Nedbank on **0800 110 929** as soon as possible if you see any unfamiliar transactions.
- If you receive a suspicious email, please forward it to phishing@nedbank.co.za.
- Do not open attachments or click on links from unknown sources.
- Beware of any attachments that end in .exe, .cab, .img, .htm or .jar. These attachments often contain malicious software.

Security software scam

Security software scams is when someone posing as a representative from an IT company or as your network service provider calls you and asks you to allow them to access your computer to help solve a computer problem (e.g. increase your network speed, upgrade security software, remove viruses) or try to sell you a software licence.

How it works

- You receive a call from someone saying that they're from your network service provider or an IT company.
- They ask you to give them access to your device to solve a problem, like upgrading your security software, removing viruses, or increasing your network speed.
- They ask you to buy a software licence.
- They ask you for your credit card details to pay for repairs or software that you have ordered.
- You're directed to a fraudulent website to enter your credit card details and personal information.

Tips to keep safe

- Never give a third-party control of your computer, unless you can confirm from other sources that it is a legitimate representative of a computer support team from a company that you trust.
- IT companies will never cold call you to do repairs on your computer or to sell you software.
- Never give your credit card information to someone claiming to be from an IT company's (e.g. Microsoft) technical support team.
- Make sure that your computer antivirus software is always up to date.
- Ensure that you install the latest updates or patches to your operating system as soon as they are available to prevent criminals from exploiting security vulnerabilities on your device.

Change of banking details scams

Be careful when a supplier asks you to use updated banking details to make payments. It could be a scam. Always confirm new banking details with a person you know at the organisation before making any payments. And call them on the number that you normally use. Don't use the number on the communications that you have received, as this could be the fraudster's phone number.

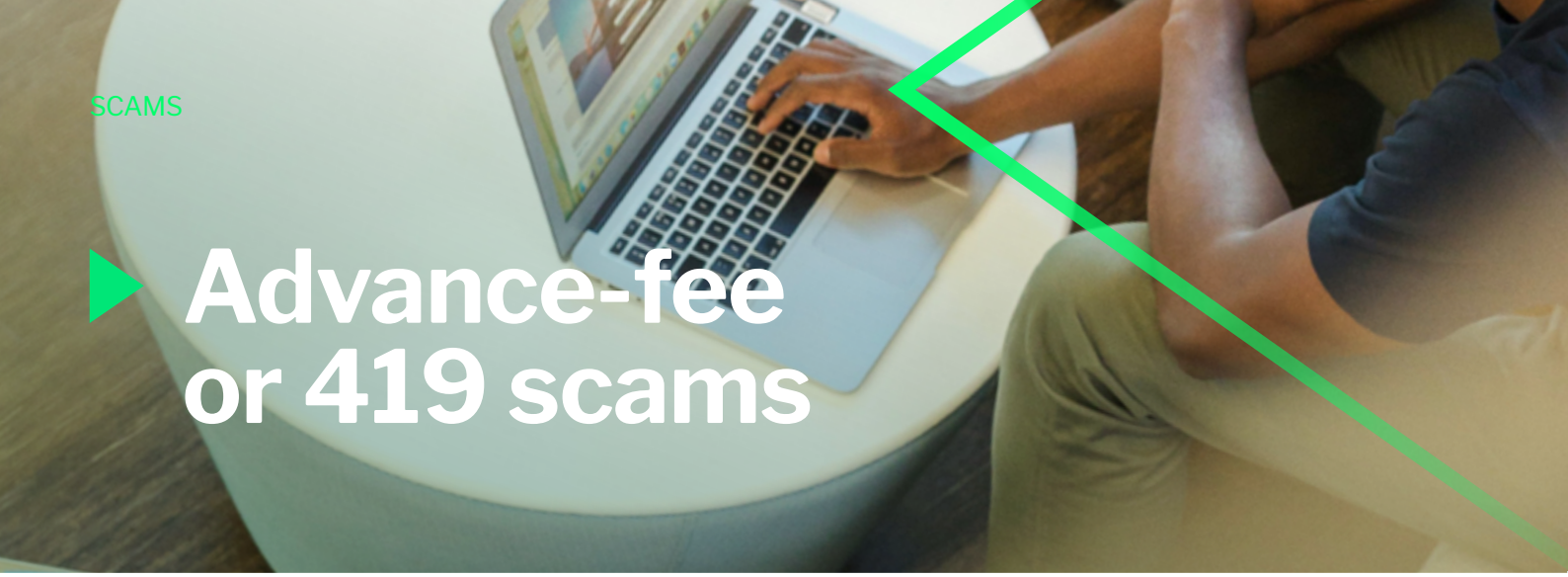
To make the request seem more legitimate, fraudsters may even attach an account confirmation letter as 'proof' that their banking details have changed. But always confirm new banking details that you receive via email with the supplier before making any payments.

How fraudsters trick you into using fraudulent banking?

- They hack the email account of a business, change the banking details on their invoices, and send these to all their debtors to make payments into their own (fraudster) account.
- They intercept an email you are meant to receive, change the banking details on the email or invoice, causing you to make the payment into a fraudster's account.
- They create fraudulent business letterheads or fax headers asking you to make future payments into their new account.

Tips to keep safe

- If you receive banking details by email for a once-off payment, always confirm the banking details telephonically before making a payment.
- Beware of near identical email addresses. They may add a full stop, replace one letter or the email may end with .com instead of .co.za.
- Hover over the email address to ensure that the response email address is the same as the email address of the sender.
- Use bank-defined beneficiaries on your Online Banking profile.
- Check all documents for spelling mistakes, errors, and suspicious changes.
- As a business owner, you could protect yourself by not placing your banking details on your invoices but rather providing them telephonically.



Advance-fee or 419 scams

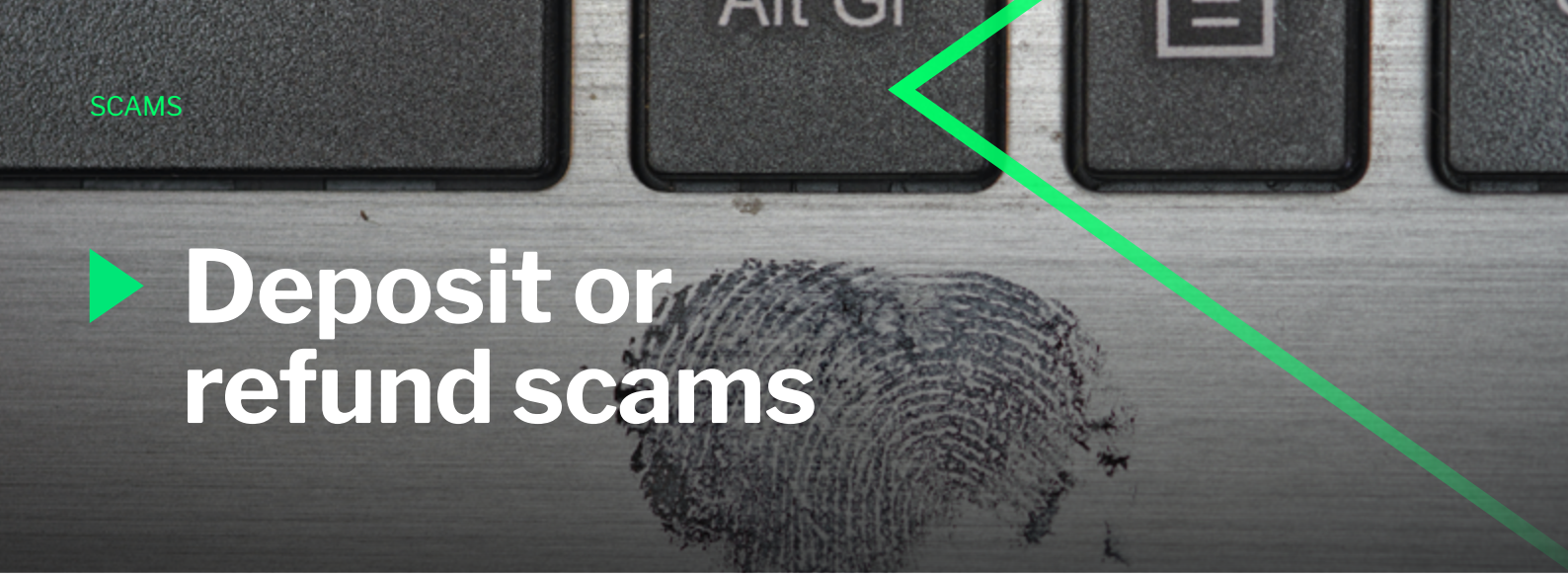
An **advance-fee or 419 scams** is a form of fraud where you are promised a lot of money, goods at discounted rates, or a job, but you first have to pay a fee upfront. Advanced-fee or 419 scams are very creative. Once you have made the payment, fraudsters either disappear with your money or try to get you to make more payments.

Some of the most common advanced-fee scams include the following:

- Fraudsters offer you a guaranteed loan at a low interest rate even if your credit record is bad but then ask you to make an upfront payment for 'administration fees' before you can get the loan.
- Fraudsters ask you to help with a business or financial transaction, for example importing goods. They promise you large sums of money in return for your help, but then ask you to cover some of the initial costs for the transaction, promising you a refund.
- You receive a tender request to supply very specific items. When you do a Google search, there is only one company that sells these specific items. You contact the company, and they agree to supply the goods but need an upfront payment. You make the payment, but the goods never arrive. Fraudsters created a fake tender request and a fake website of the company selling the goods to trick you into paying the money.
- You receive an email or an SMS saying that you've won a lottery or prize or inherited money, and that you need to contact someone to collect it. When you do contact the person, they ask you to pay taxes or administration fees to release the prize or the money.
- You apply for a job and go for an interview. You 'get the job', but then you're asked to pay for background checks or placement fees. When you arrive for your first day on the job, the company has no idea who you are.
- You see an advert for holiday or rental accommodation but need to pay an upfront fee to rent the property. Meanwhile, the property does not exist, has been rented out to someone else or to several people at the same time.

Tips to keep safe

- If it sounds too good to be true, it probably is.
- Never pay fees upfront unless you know it's a reputable supplier. If you're buying online from a private individual, opt for payment on delivery or collection.
- Do not be fooled by fake emails or SMSs. Always double-check with the company to confirm that they are running a tender or promotion or offering prizes. But do not use the number on the communication you have received, as you will be talking to the fraudsters.
- Look out for spelling and grammar errors in communications you receive.
- Forward suspicious emails to the South African Police Services at 419scam@saps.org.za.



Deposit or refund scams

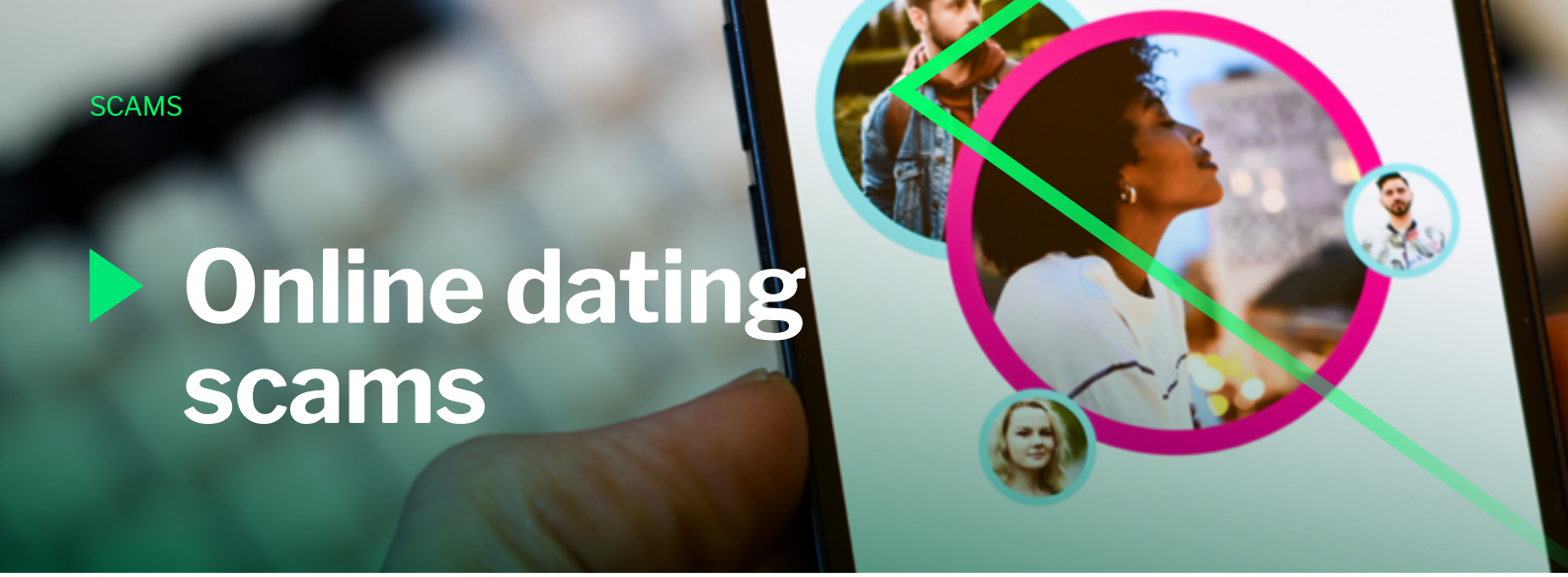
With these scams' fraudsters present a fake payment confirmation to trick you into believing that a cash or electronic payment has been made into your account.

With a **deposit scam** a fraudster will send you a fake payment confirmation to trick you into believing that a payment has been made into your account so that you release goods to them.

With a **refund scam**, fraudsters ask you to return an 'incorrect payment' or 'overpayment'. They also produce a fake proof of payment to trick you into believing that the payment was made.

Tips to keep safe

- Never rely on a proof of payment alone. Always double-check that the money shows in your account before you release goods or provide services.
- Look out for little errors on your proof of payment or possible changes, alterations, alignment and spelling or grammar errors. These are often signs of fraud.
- You can use Nedbank's Verify Payments service to confirm that an incoming payment notification from a Nedbank account is legitimate, and that the money is indeed on its way to you.
- Use bank-approved beneficiaries if possible.



Online dating scams

Many people seek love on the internet. While there have been success stories, there are many horror stories of fraudsters who steal unsuspecting victims' life savings.

The scammer will share a lot of personal information with you in the hope of getting you to trust them. The information and profile pictures provided are all false and are often used repeatedly with various other victims.

How it works

- They say they want to buy you an expensive gift but that you will need to pay import duties or taxes to receive it.
- They claim to have a business or family crisis and ask you to help them out by sending them some money, promising to pay you back.
- They ask you to help pay for the travel costs to visit you. They even send you copies of fake travel documents to prove they've booked the trip, but then never arrive.
- They propose to you online but then ask you to help set up your new home together by sending them money.

If you don't give them money, their messages will often become more desperate and persistent. If you give in and pay them the money, they may either disappear or ask you send them more money.

Tips to keep safe

- Be careful when you share personal information on social networking sites. Fraudsters use this to steal your identity.
- Watch out for people with extraordinary jobs who are always travelling to new places, for example people who claim to work for the army, navy, air force etc.
- Look out for emails with copied and pasted words or letters that differ in fonts and sizes. Or when people say, 'Hi, Beautiful' instead of using your name. Fraudsters target lots of people at the same time with the same messages.

- If you arrange to see someone you met online, meet in a public place and take a friend with you.
- Beware of people who keep promising to meet you but always cancel at the last minute.
- Never send money to anyone you've met online only.
- If you suspect that you are being targeted by fraudsters, stop all communication immediately and report it to the online dating service.

Pyramid and ponzi schemes

A multilayered marketing structure, like a pyramid scheme, isn't always illegal. There are businesses that use pyramid structures to promote and sell their products, for example cosmetic and health product suppliers. These schemes are not illegal, as a product is exchanged for money at fair value.

A pyramid scheme is illegal when you are required to make a deposit for no product or a product without a fair value of exchange. This is in contravention to the Banks Act, which has specific rules linked to the accepting deposits.

How to identify an illegal pyramid scheme

- Fraudsters offer you exceptional high returns and your returns increase with the number of people that you recruit to the scheme.
- They ask you to make an initial start-up deposit as an investment into the scheme.
- They ask you to recruit others in return for bonuses.
- The scheme has multiple levels of members, all collecting commission on a single transaction.
- The scheme isn't authorised by or registered as a financial services provider.
- If it sounds too good to be true, then it probably is. Stay away!

Ponzi scheme

Ponzi scheme is always illegal. This is a scheme that is operated by fraudsters who con people into investing their hard-earned money in a business venture or an investment that promises high returns in a short period of time. This scheme uses the money of new investors to pay returns to older investors. Once recruitment slows down, the scheme starts to collapse.

How to identify a Ponzi scheme

- They promise abnormally high investment returns, higher than those offered by financial institutions (30% and more).
- They often promise guaranteed returns. No return is ever guaranteed. All investments carry some risk.
- Make sure that you understand what you're investing in and be wary of too-good-to-be-true business models. If you don't understand the business model, don't invest.

- The scheme owners will try and pressurise you into reinvesting your profits as they need these profits to pay other people's returns.
- Only invest your money with credible FSB-registered institutions that you have researched properly.
- You will usually be introduced to the scheme by friends or family members who have made some money. They use this marketing ploy as you tend to trust family and friends, but remember, they need to recruit new members to pay interest to older members.

Like pyramid schemes, Ponzi schemes hide the true source of funds behind multiple transfers between different accounts. Members' bank accounts are used to channel money so that the scammers cannot be linked to the transactions. But although you are unaware of it, you're guilty of money laundering, because as a member, you allowed your bank account to be used to channel these funds.

Tips to keep safe

- Be careful of investments that guarantee you high profits, with little or no financial risk.
- Understand what you're investing in and beware of business models that are 'too good to be true'. If you don't understand the business model, don't invest.
- Know exactly where the money will be invested and do a background check on brokers or products before investing.
- These schemes operate on trust, so places like churches, social groups and community organisations are 'happy hunting grounds' for recruiting members. Rely on research over positive reviews and referrals from friends and relatives.
- Look out for short investment periods, sometimes as little as 10 days, with very high return rates and strong encouragement to reinvest automatically.
- Only invest your money with credible FSB-registered institutions that you have researched properly.

Online Banking

Fraudsters use many schemes to get your card number and PIN or Nedbank ID and password to access your Online Banking profile.

They coax you into clicking on a link or attachment in an email (phishing) or an SMS (smishing) or call you (vishing) to try trick you into disclosing your Nedbank ID and password or card number and PIN. They may even convince you to download malware onto you device or to download remote desktop software on your device so that they can access your Nedbank ID and password or card number and PIN.

Tips to keep safe

- Never share your Nedbank ID and password or card PIN with anyone, not even a portion of it.
- Don't be tricked into inserting your Nedbank ID and password or card number and PIN on any link you receive via an email or an SMS to access a proof of payment, a bank statement or to update or verify your bank account to avoid 'deactivation'.
- Do not click on links in an email or an SMS. Nedbank will never ask you to sign into Online Banking via an SMS or an email link.
- Never change your Nedbank ID username and password to one that someone else has given you over
- the phone. If they know your Nedbank ID username and password, they can access your bank account.
- Read every Approve-it message carefully before you accept it and decline the transaction if you didn't make it, then report the incident to Nedbank immediately on **0800 110 929**.
- Never share your OTP with anyone.
- If your mobile device has been lost or stolen, call **0800 110 929** immediately and have your Money app deactivated.
- If you get an SMS for a SIM swap or number port you didn't request or seem to lose cellphone connectivity for a long time without reason, call your service provider and let us know immediately on **0800 110 929**.
- Make sure you have the latest version of the Money app on your mobile device.
- Keep your passwords safe. Don't store them on your device or in your browser and don't use the same username and password for all your logins. Your username and password should also be different.
- Type in web addresses yourself rather than clicking on links in an email or an SMS.
- Hover your mouse over any hyperlinks to reveal the actual URL and double-check that it's the same address in the email.

- Look for the lock icon on a website's toolbar and 'https' in the web address before you enter your card details or personal information online.
- Be vigilant when visiting social-media sites like Twitter and Facebook, and never share your personal information on public pages.
- If you're making a first-time purchase, do some research and check online reviews before making a payment.
- Make sure you have the latest antivirus software installed on all your devices and install the latest updates or patches on your operating system as soon as they become available.
- Don't do your banking on public Wi-Fi or unsecure networks, as fraudsters can easily hack these networks.
- When you receive a suspicious email, forward it to phishing@nedbank.co.za and delete it immediately.

Money App Banking

The Money app is a secure and convenient way to manage your money. But fraudsters use many tricks to get your Nedbank ID and password or card number and PIN to access your accounts.

Tips to keep safe

- Nedbank will never ask you to disclose your Nedbank ID and passwords and card PIN, not even a portion of it.
- If you receive a call from someone asking for your card number and PIN or Nedbank ID and password, put the phone down immediately, because you're talking to a fraudster.
- Keep your passwords safe. Don't store them on your device or in your browser and don't use the same username and password for all your logins. Your username and password should also be different.
- Always read Approve-it messages carefully before you accept them and decline the transaction if you didn't make it, then report the incident to Nedbank immediately on **0800 110 929**.
- Never share your OTP with anyone.
- When your phone is lost or stolen, call us on **0800 110 929** to report it immediately.
- When you receive an SMS for a SIM swap or number port you did not request, call us on **0800 110 929** immediately.
- Make sure you have the latest version of the Money app on your mobile device.
- Granting Nedbank access to your GPS location helps with better service and fraud prevention.
- If you use biometric identity verification, remember that anyone else you allow access to your device with their fingerprint will also have access to the Money app.
- Make sure you have the latest antivirus software installed on all your devices and install the latest updates or patches on your operating system as soon as they become available.
- Make sure we always have your correct cellphone number. We use this number to send notifications and Approve-it messages to you. If you stop receiving your Approve-it messages, call **0800 110 929**.
- Report fraud by calling us on **0800 110 929**.

Identity theft

Fraudsters come up with creative scams to get their hands on your personal information. Once they have enough, they can easily pretend to be you. Through social engineering, fraudsters manipulate you into disclosing your ID, Online Banking password or card number and PIN or giving them access to your device.

They use scare tactics like saying your account will be blocked, that your account has been defrauded and that they need to 'reverse' the transaction, or that you need to update your security software.

They also entice you with promises of large prizes or rewards for converting your Greenbacks into cash.

How fraudsters get your personal information

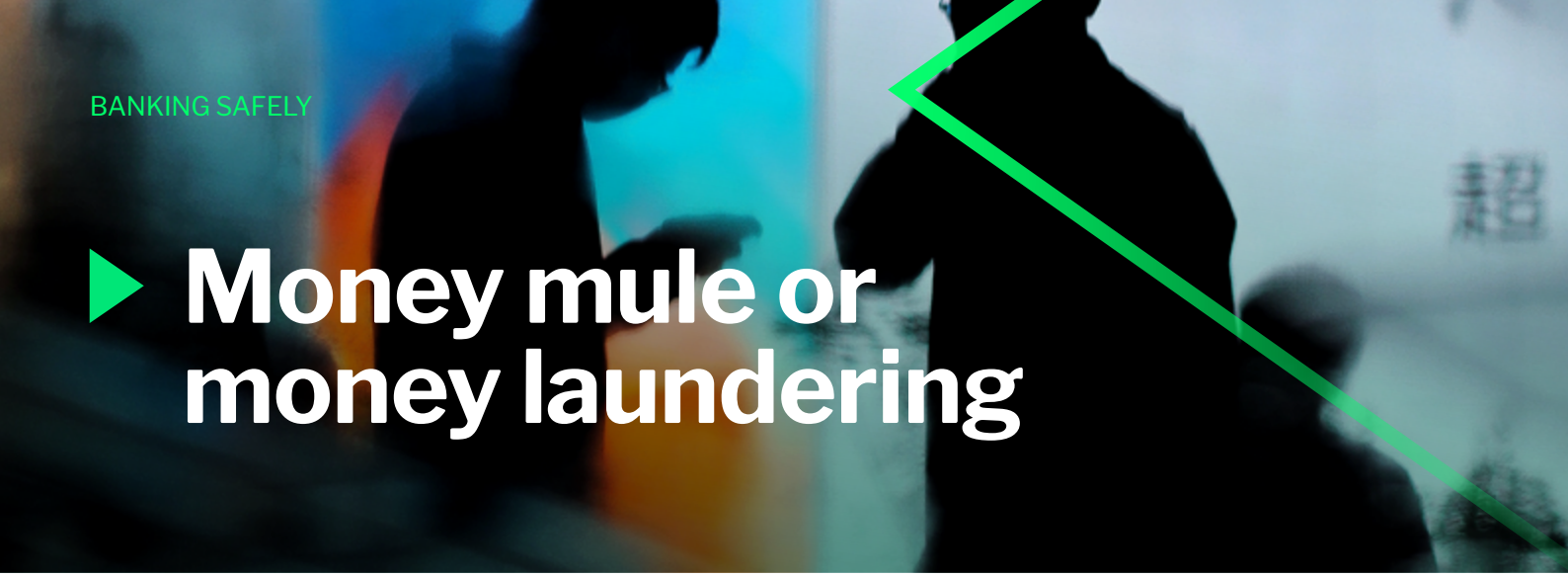
- Through social engineering, fraudsters manipulate you into disclosing your ID, Online Banking password or card number and PIN or giving them access to your device.
- Through social engineering, fraudsters manipulate you into disclosing your ID, Nedbank ID username and password or card number and PIN or giving them access to your device.
- They also entice you with promises of large prizes or rewards for converting your Greenbacks into cash.

Examples of personal information:

- ID number
- Driving licence
- Bank statements
- Municipal bills
- Payslips
- Email account login details
- Debit or credit card PIN
- CVV number (the three- or four-digit security number on the front or back of your card)
- Your Nedbank ID username and password, card number, PIN and CVV or OTPs

Tips to keep safe

- Slow down. Fraudsters always try to rush you. They want you to act now and think later.
- Never give anyone your Nedbank ID and password or card PIN and CVV number. Nedbank will never call you to ask for these details.
- Read every Approve-it message carefully before you accept it. If you receive an Approve-it for a transaction you did not perform decline the transaction and contact Nedbank immediately.
- Type addresses into your browser and do not click on links.
- Don't assume that the person calling you is who they say they are.
- Be suspicious of unsolicited emails. Do some research first. Emails can look legitimate when they're not.
- Make sure your mobile devices are all secured with passwords to prevent third parties from accessing them.
- Use different passwords for different online accounts.
- Make sure you have the latest antivirus software installed on all your devices.
- Install the latest updates or patches to your operating system as soon as they become available.
- Be vigilant when visiting social-media sites and never share your personal information on public pages.
- Use privacy settings on social media to make sure you share information only with friends and family.
- Do not carry confidential information in your wallet or leave it in your car.
- Shred documents containing personal information before throwing them away.
- Check your bank statements frequently and call us immediately on **0800 110 929** if you see any unfamiliar transactions.
- Forward suspicious emails to phishing@nedbank.co.za and then delete them immediately.
- If you think your information has been compromised, let us know immediately on **0800 110 929**.
- Report identity theft to the Southern African Fraud Prevention Services (SAFPS) on **0860 101 248** or at safps@safps.org.za.



Money mule or money laundering

Fraudsters trick you into allowing them to use your bank account to receive money made through illegal activities, like drug sales, human trafficking, smuggling, fraud or corruption. They do this so that they're not linked to the transaction and to make illegal transactions look legitimate. This is called money laundering.

If you hand your account over to someone to use and the transactions are linked to a crime, you could face criminal charges and prison time for being involved in money laundering.

Even if you didn't know a crime was being committed, you could be banned from having a bank account or credit facilities.

Fraudsters use several tactics to gain access to legitimate bank accounts.

Some of these include:

- Dating scams where you are requested to receive money and send it on to a third party.
- False offers of employment. You are lent money and asked to open a bank account and hand over your bank card and PIN so that they can withdraw the money owed from your first salary.
- You are offered money in return for allowing someone to 'borrow' your account for a large deposit and withdrawal.

Tips to keep safe

- Don't allow your account to be used by another person to deposit money into and then transfer or withdraw money from it.
- If you have any doubts about the origin of the money, or if a transaction appears unusual, (e.g., an unsuspected deposit into your account), report it to your bank and verify the details.
- Be cautious of requests to roll money through your account, regardless of how legitimate the request appears.
- Remember that handing over your credit or debit card and PIN will allow fraudsters to clone or use your card and withdraw your money or the proceeds of crime from your account without your knowledge.