Do not become a victim of fraud

The banking industry is experiencing an increase in digital fraud attempts, with fraudsters using a variety of techniques to obtain your login details and pass through two-factor authentication, usually a one-time password or Approve-it™ message, to access your banking accounts.

Access to login details

Some of the latest scams include fraudsters prompting you to click on a link or open an attachment in an email or SMS containing a fake bank statement, proof of payment or request to update your online banking profile to prevent your accounts from being blocked. The link typically takes you to a fake web page, where you are requested to insert your login details, while the attachment may contain malware that enables the fraudsters to record all your keystrokes.

Fraudsters may even call you and pose as a Nedbank employee with knowledge of your personal details, asking you for your profile number, your PIN and password, your Nedbank ID and password or your card details and PIN, because you have won a so-called ‘competition’ or because ‘fraud has been detected on your account’.

Passing two-factor authentication

Fraudsters may also trick you into accepting an Approve-it™ message or providing them with your OTP, hoping that you won’t read the message properly and therefore not notice that you are giving them access to your account or allowing them to move funds from your account. Alternatively, they do a SIM swap to gain access to your Approve-it™ messages and OTPs.

If you suspect fraudulent activities on your account or think you were approached by a fraudster, please report this immediately to 0800 110 929 or use the ‘Report Fraud’ function on the Nedbank Money app.

And lastly, please be assured that Nedbank’s digital channels remain highly secure – our security features match global standards and you can easily protect yourself against becoming a victim of fraud by always adhering to the safety guidelines provided below.

Digital banking - how to stay safe

- **Never disclose your login credentials** (i.e. your profile number, PIN and password, your Nedbank ID and password, or your credit or debit card number and PIN) **to anyone, not even a Nedbank employee.**Please note that your card or profile number **without the PIN and password** may be required to serve you through our contact centre.

- **Never enter your login credentials on any site that was accessed through a link received by SMS or email.** Always make sure you navigate to online banking from the nedbank.co.za home page. Please forward all suspicious emails to phishing@nedbank.co.za so we can have the phishing sites deactivated.

- **Validate the website address (URL) before you click on it** by hovering your mouse over the hyperlink. If you long-press on a hyperlink on your mobile device, it should also reveal the underlying website address.

- **Beware of any attachments that end in .exe, .zip, .cab, .htm or .jar.** These are executable files that allow malware to be loaded onto your computer without your knowledge when you click on them. Be careful of files that prompt you to execute, install or upgrade software.

- **Always have the latest antivirus software and a robust firewall on all your devices.** Nedbank recommends that you install the online fraud protection software 'Trusteer Rapport', which is available to all Nedbank clients for free.

- **Don't trust caller identification software.** Fraudsters use number-masking software to make it seem as if you are receiving a call from Nedbank when you are actually not.

- **Always read your Approve-it™ and OTP messages carefully.** These messages will indicate that you are about to authorise a payment or enrol for the Nedbank Money app. If you haven't requested this, make sure to reject the transaction or, in the case of an OTP, do not disclose it to anyone. Remember to report the incident to us.

- **If you lose cellphone connectivity** for no apparent reason or receive an SMS for a SIM swap you did not request, contact your cellphone service provider urgently and contact us to block your accounts.

More tips to reduce risk:

- **Reduce your instant and beneficiary payment limits** to the amount you need to run your day-to-day banking. The bigger the limit, the higher your risk exposure.

- **Activate eNotes** so that you receive real-time SMS notifications of payments made.

- **Do not access internet banking from third-party devices,** such as those provided in internet cafes, while you are travelling, as you have no control over any potential malware on those devices.