

With the ever-changing technology landscape, cyber-crime and fraud is on the rise. Not all fraud however relies on sophisticated technology systems and solutions. It could also be a simple and common deceptive request sent to you.

Itransact want to help you, as the investor to be aware of the more common and known fraudulent scams, tool and methods fraudster are currently using. By being proactive, taking care and understanding what security measures to use, you as the investor will be able to protect yourself, your data, identity and investment.




1. Brand impersonation



Someone contacting you claiming to be from Itransact by telephone, e-mail, SMS & texts, social media platforms, WhatsApp, letter or even directing you to a website appearing to be Itransact's.

Often this communication appears legitimate as the fraudster adds official looking company logos, details and information.

2. Protect yourself from fraud

- Only log in to the secure Itransact website or mobile site from your own devices. You can also validate the safety of a website by clicking the padlock icon next to the website address e.g.
 -  Secure
 -  Info or Not secure
 -  Not secure or Dangerous
- Do not log in from public computers, internet cafes and public devices.
- Do not save login credentials such as usernames and password in your devices browser.
Never log in to the Itransact website via a link sent to you via e-mail, SMS & texts or any hyperlinks.
- We strongly advise you to create complex passwords that are difficult to guess and crack. Always keep your login credentials safe and secure.
- We will never ask for login details (e.g. usernames and passwords) via e-mail, SMS & texts, WhatsApp, telephone or any other channels.



3. Protect your identity and devices



Protect your identity

- Your personal information is valued. We will only contact you to verify your information if you have sent us an instruction. Do not respond to unexpected requests to validate your personal details by phone, SMS & texts or e-mail.
- Be cautious of your personal details you share online or on social media. Sharing of the wrong information (e.g. Identity number) could be used against you.
- Never leave confidential information lying around for people to see.

Protect your devices

- Always ensure your devices have a secure password and pin.
- Always ensure no one has unauthorised access to your devices.
- Please do not use free and public Wi-Fi when trying to process a transaction online because of 'sniffing'.
- 'Sniffing' is used by fraudsters to capture the data you are entering from your device and is then used to commit fraudulent transactions.
- Always install personal anti-virus protection products on your devices. This is the best way to protect your personal information and device from hackers and fraudsters.
- Ensure your devices operating systems are up to date (Windows, macOS, Android, iOS etc.).

4. Be aware of and avoid malware



Fraudsters use malware to access your devices. Malware is malicious software. The purpose of malware is **to intrude on a machine for a variety of reasons**. From theft of financial details to sensitive corporate or personal information, malware is best avoided, for even if it has no malicious purpose at present, it could well have so at some point in the future. Malware is used to perform cyber-attacks on your devices by fraudsters using infected websites, hyperlinks or via e-mail. The types of common cyber-attacks are:

Phishing - Where fraudsters attempt to access your confidential information. This occurs either by sending an e-mail request for information or by directing you to a fake website or link. *Be alert to hyperlinks that contain misspellings of the actual website name or e-mail addresses that have been altered and have web-based e-mail addresses e.g. @gmail.com, @yahoo.com, @hotmail.com etc.*

Vishing - This is similar to 'phishing' but instead you receive a fake telephone call from the fraudster pretending to be from the company and they get you to reveal your personal information and possibly username and password. Never handout or provide usernames and passwords to anyone.

Remote Access - This is becoming a very popular way for fraudsters to gain access to your personal information. They use sophisticated software to take control of your devices over the internet and you may not be aware this is occurring.

Smishing - This is similar to 'phishing' but via SMS & texts where the fraudster requests you to disclose your personal information. The message will appear to be from the company and you will be prompted to select or click on a link. Do not click on such invalid links. Contact the company or go to the valid website.

Contact us or report any concerns:

If you receive any correspondence or have any uncertainty about any communication received from Itransact that concerns you, please contact us.

Contact number: 0861 432 383 | info@itransact.co.za or officer@aospartner.com