

## PROTECT YOURSELF FROM FRAUD!

Email, text messages, mobile phones, firewalls and more...

### EMAIL

Fake email messages or phishing

'Phishing' is when fraudsters send thousands of emails in the hope that they will catch a victim. It just takes one to make it worthwhile. The email may look real, but there are always small clues to warn you.

- What is the full email address used – does it look odd?
- How are you greeted? Dear Customer / Your name / Nothing?
- Does it ask you to log in from a link on the email?
- Does it say there are security issues?
- Does it advise you that it is urgent and immediate?

Always take time to read an unexpected email. Fraudsters are counting on you being far too busy or worried so you don't think clearly and will do what they request.

Spoofing and hacking emails

Spoofing

A 'spoof' email is where a fraudster will send you a Phishing email, but it is from a name you may know. Well-known global corporates email formats are copied and fraudsters trick you into believing your package or order needs your attention by clicking on a link, to obtain your security details.

Recently this has developed into sending specific emails (also called 'spear phishing'). This might relate to a real estate sale or purchase or hospital expense, claiming to be from a lawyer and requiring your payment, to the attached bank details.

Fraudsters obtain details through various means and can create a spoof mail that looks legitimate and you are expecting it, making it even easier for them to persuade you to make the payment.

Hacking

Fraudsters have obtained access to your email account and are able to read and create emails in your name. This means they can mail your friends and contacts, as well as knowing what financial deals you may have underway, and create that 'spoof' email to encourage you to make a payment. Please change your password if you see or receive any unusual activity.

Don't unsubscribe on emails from random advertisers

To check if your email is valid, fraudsters send a spoof/spam email with shopping, sports, or holiday offers. If you click to unsubscribe, they will then have a valid email address and can target you as they try to obtain more information about you.

Review your Sent and Deleted items folder

Take time to check your Sent and Deleted items folder on your computer. Are there messages you have not sent? Your computer may have a virus or your email account may have been hacked or compromised.

Don't store confidential information in your email folders. Store personal documents and emails on your computer in a secure folder on your computer.

## Attachments or links

Avoid clicking on any links or opening attachments included in unexpected emails, texts, or social media messages. These may be disguised as a tax refund, parcel delivery or invoices to get you to click on them.

## TEXT MESSAGES

In the same way that email addresses can be spoofed, so can phone numbers. That way, it can look as though you're receiving a call from a trusted number – even your bank's genuine one. Text messages from spoofed numbers can appear in an existing thread of messages.

Recently, many consumers have been receiving fraudulent texts asking them to confirm a transaction they did not authorise, or verify a new beneficiary that has been added. However, the message will contain a link to click through to, if you don't recognise the transaction. This leads to a phishing page, where victims are asked to input their details. Alternatively, the compromised site can download malware to your device.

- If you get a message about account activity you were not expecting, call your bank immediately on a trusted number.
- Don't click on links contained in this type of SMS.
- If you want to access online banking, do so through your banking app or known website, which you can find on Google.
- You can also report suspicious texts by forwarding the original message to 7726, which spells SPAM on your keypad.

## MALWARE

Malware is a term for various forms of malicious software. It is transmitted via email attachments and infected websites. Here are the most common:

### Key loggers

Programs that record all keystrokes performed on an infected computer. This gives the attackers access to anything that may have been typed in such as account numbers, passwords, and PINs. This is transmitted when you are online and the fraudsters can begin to take over people's accounts.

### Spyware

Software that tracks and stores a person's movements on the internet, then provides pop-ups based on a person's spending habits, to lure them to a fake website in an attempt to trick them into entering their account details.

### Ransomware

A nasty form of malware that encrypts all information on the infected computer and demands a ransom fee to be paid in order to unlock the data. This type of infection can result in significant data loss.

### Trojans

Running in the background and hiding from view, these programmes frequently open a 'back door' into a computer, allowing a fraudster to access information or take full control over the machine. This allows them to intercept banking details and passwords as they are keyed in.

### Counterfeit or 'cracked' software

Acquiring 'cheap' computer operating or business software may not prove to be cheap in the long run, as fraudsters like to offer this online, but secretly add their own 'added value' – such as trojans/malware which can read your security details and passwords. Purchase genuine software. Keep your internet browser and other software on your computer up to date with the latest security patches, to protect yourself and your money.

## MOBILE PHONE

### Apps

Use only those 'Apps' that are downloaded from official sites. Free Apps from unofficial sources may have malware, the same as counterfeit or 'cracked' computer software.

## Antivirus

Ensure you have an antivirus installed if your operating software allows it. Just like your laptop or main computer, keep the antivirus and software up to date.

## Jailbroken devices

Jailbreaking a mobile device is the process of removing the software restrictions embedded by the device manufacturer, which may include the security protection mechanisms. In order to keep your account information secure, you are not able to use the Investec mobile apps on a jailbroken device.

## Passwords protection

Make sure you secure your mobile device by setting a passcode greater than a four-digit PIN or fingerprint scanning if your device supports this functionality.

## FIREWALLS AND ANTIVIRUS

Always install a personal firewall product and antivirus protection product for your devices. The firewall sits between your computer and the internet and acts as a security guard, restricting what can enter and leave your computer. Hackers try to access or infect home computers by connecting to your computer while you're surfing the internet. The best way to protect your computer from unauthorised connections from the internet is to install a personal firewall. There are several options on the market, some of which are free.

At first, the firewall may ask you what you want to allow in or out of your computer. However, it soon learns to make these decisions independently, based on the decisions you make early on. The most important point is never to allow anyone else to connect to your computer.

## PROTECT YOUR DEVICES

### Your computer

- Ensure no one has unauthorised access to your computer.
- Use a password to access your own computer, restrict access to prevent programme installations.
- Destroy or delete anything containing login details or security information, even if Investec has sent it to you.

### Free Wi-Fi

Please do not use free public Wi-Fi when trying to access your banking and online transactions.

In fact, do not try to access any account that requires a user name and password – even social media, when using free Wi-Fi, because of 'sniffing'. 'Sniffing' is the phrase used by fraudsters to capture data from your laptop or mobile phone. When you launch an App (especially those that have stored your user ID and password), your security details are re-sent every time you launch the app, sometimes in an unencrypted form. Then, when you view your email accounts or social media posts, your security details are captured and used by fraudsters, who begin creating a profile of you.

## PROTECT YOUR IDENTITY

- Your personal details are valuable. Don't respond to unexpected requests for validation of your security or personal details, by phone, text, or emails.
- Limit the number of personal details you share online (ie date/place of birth on social media sites etc)
- Review what social media sites or Google and other search engines know about you – erase what you don't wish to be known.
- Create and use different passwords for each service provided by financial service providers.
- Protect your printed or physical information and destroy or shred unwanted personal documents, old paper statements, and credit and debit cards.
- Never use complimentary computers in airport lounges and hotels to do your banking.

### Are you travelling?

Before travelling, let your banker know that you're away. They will be able to monitor your profile for any suspicious or fraudulent activity.