Standard Bank Offshore

PROTECT YOUR BANK ACCOUNT AGAINST SCAMS AND FRAUDSTERS

Frauds and scams are increasingly sophisticated but there are steps that you can take to keep your security and bank details safe. Being aware of different types of fraud and scams will help you be vigilant.

COMMON TYPES OF SCAM OR FRAUD

The Bank Transfer Scam

An unexpected telephone call from someone claiming to be from your bank, another service provider or even the police. The caller tries to persuade you to share bank security details or to provide access to your account. They may feed you snippets of personal information to persuade you that they are genuine and to gain your trust. You may even be told that your account has been hacked.

The Email or Text Scam

Scammers will use the email "phishing" technique, or "Smishing" if it's an SMS, to gain access to personal information by sending out spoof messages to fool you into sharing confidential information. For example they may send an online shopping offer or deal, which includes a link for you to click, or an email pretending to be your bank or credit card provider asking you to confirm your security details.

The "vishing" Scam

Telephone calls offering once-in-a-lifetime investment opportunities that really are too good to be true. The caller will pressure or try to persuade you to make a commitment immediately. Another common strategy is to pretend to be from a utility provider to which you have made an overpayment and where your bank details are needed so that a refund can be credited to your account.

Card Not Present (CNP) Fraud

CNP fraud can happen without the card or cardholder being present. Fraudsters can memorise or copy your card number, expiry date and 3-digit card validation code (on the back of your card) when you're using your card to pay. Your card information is used for fraudulent transactions online or over the phone, even though your card is still in your possession.

The Romance Scam

Romance scammers create fake profiles online and make up stories to convince you to send them money or gifts. They will shower you with compliments and often be fast to declare their "love". A request for money could be to help a sick relative, to pay for a flight to come and visit you or to pay for a computer to get that job they have always dreamed of.

The Card Skimming Scam

Fraudsters can duplicate your card by 'skimming' or copying your card details with a device they place in an ATM card slot. To get your PIN, they'll either set up a hidden camera, or watch you type it in. While you can't prevent your card being skimmed, you can prevent fraudsters from learning your PIN by shielding the ATM keypad from the view of other people when entering it.

The Authorised Payment Scam

Also known as an "email hack", "invoice scam" or "CEO fraud", you will receive what appears to be a genuine request to make a payment or a money transfer from a seemingly trusted and known source such as a tradesperson if you are having work done on your home, or from your boss at work.

The Card Swapping Scam

Fraudsters who see you having trouble at an ATM might offer to help you insert your card, only to pocket it as they watch you enter your PIN, and then swap it with a replica or even claim your card has been 'swallowed'.

The Remote Access Scam

By claiming to be from a technical service provider, this fraudster wants to take over control of your computer by convincing you that you have a fault on your system.

REPORT IT...

Whatever the scam, there is usually a sense of urgency and persistence about the action you are being asked to make because the fraudster does not want you to stop, think and verify the transaction.

If you are in doubt about a particular payment or suspect you may have been the victim of fraud, get in touch with us right away.

T +44 (0) 1624 643643 - If calling internationally
T 0860 033 269 - If calling from within South Africa
E personalbanking@standardbank.com

Use the Contact Us page on our website or send a secure message via your Internet Banking.

MOOT_V03