

BANKING SAFETY AND FESTIVE SEASON TIPS

BEWARE OF CARD SKIMMING

Criminals are able to copy information on the black strip of your card (magnetic strip) and use that information to steal money from your account. The device used to copy information in this manner is called a skimming device. Skimming devices can either be hand held or be mounted to ATM's.

- Never let the card out of your sight when making payments. Always follow your card with your eyes
- Report any suspicious behaviour by the person to whom you have handed your card when making a payment to your Bank immediately
- Never accept help from anyone at the ATM
- Know what your ATM looks like, so that you are able to notice any foreign objects attached to it
- Never use an ATM that is tampered with or visibly damaged; this may also be a ploy to force you to use another ATM in close proximity on which a device may be mounted
- Report any foreign objects on ATMs, or suspicious people loitering around ATMs to your bank immediately

SAFE BANKING TIPS FOR FESTIVE SEASON

Criminals are able to use your card information to make Internet and mail order purchases without you knowing. Guard your card information as you would cash to avoid falling victim to card fraud.



Block 14, Thornhill Office Park, 94 Bekker Street, Midrand
P O Box 3682, Halfway House, 1685
Tel: 011 847 3000 • Fax: 011 847 3001



www.sabriz.co.za

What to do to prevent falling victim to Card Not Present fraud:

- Always check your bank statement for suspicious transactions. If there are any suspicious entries you should contact your bank immediately
- When disposing of bank statements – and any other financial information – you should shred or burn them
- Never leave your card or card details lying around
- Never let anyone else use your card or divulge your PIN to anyone
- Use the card security products offered by online merchants.
- When shopping online, only place orders with your card on a secure website
- Do not send e-mails that quote your card number, expiry date or any card details

FESTIVE SEASON SCHEMES AND SCAMS

Smishing

Never respond to an SMS stating that you have won a huge sum of cash and asking you to make contact with an unknown person. Chances are you are lured into a scam where you will be asked to part with money that you may never be able to recover.

Phishing

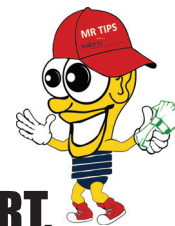
Your bank will never communicate with you via E-mail or SMS to request you to update your personal banking information for security or other reasons. Never click on the link purporting to be sent from a bank and supply your personal or banking details. Such requests are aimed at stealing your personal information.

Advertisement Scams

If the deal sounds too good, be cautious. Never pay a deposit without seeing the asset you intend purchasing. Know who you are doing business with and keep all records like E-mail communications, bank details and contact numbers. Negotiate to make full payment upon receipt of the asset.

HOTLINE CONTACT DETAILS FOR EACH BANK

AFRICAN BANK	0861 000 555
ABSA	0860 111 444
NEDBANK	0800 110 929
STANDARD BANK	0800 020 600
FNB	0800 110 132
BIDVEST BANK (Local)	0860 11 11 77
BIDVEST BANK (International)	+2711 407 3103
INVESTEC	011 286 9663
UBANK	0800 005 311
CAPITEC	0860 102 043
BANK OF ATHENS	011 833 2117



**“SWITCH ON, BE SMART,
FOLLOW THESE TIPS”**