

SCAMS AND SCHEMES WATCH LIST

ADVANCE FEE FRAUD SCAMS (419 SCAMS)

Background

- This is one of the oldest scams that have been doing the rounds for some years already. The scammers use surface mail, faxes as well as e-mails or sms's to communicate with their victims. There are many versions of these scams many of which allegedly originate out of West Africa. The reality is that the criminals who perpetrate these scams come from all over the world. In spite of the longevity of this type of scam and the large amounts of publicity that it has received, many people around the world are still being conned out of substantial sums of money.
- Unsolicited messages that masquerades as some manner of business proposition, request for assistance, notice of a potential inheritance, opportunity to help a charity or that your email was selected in a Lotto draw, are circulated. The message will claim that your help is needed to access a large sum of money, usually many millions of dollars. The scammers use a variety of stories to explain why they need your help to access the funds. The stories are generally aligned to regional or international developments like the upcoming FIFA 2010 event to be hosted in South Africa. As the victim's communication progresses with the scammer, requests for money to cover certain "necessary" fees to have money released will be made. The more the victim responds positively, the more money will be asked. At the end of the day, the victim will pay away large sums of money but the prize money or share of the inheritance, will never arrive. From there the term "advances fee fraud".

Prevalent advance fee fraud scams

- **Lottery scam:** The victim receives an e-mail stating that they have won a lottery with a huge price usually in another country. The lottery is usually in the UK or Canada but the communicating agent responsible for paying out the money could be in another country. The victim then has to claim the prize and communication then starts between the scammer and the victim. Bank details are requested and later demands for payment are made and when the victim refuses, violent threats could follow.
- **Request for assistance:** These e-mail communications are received randomly and the writer purports to have access to millions of dollars but

cannot move the money because of a political situation is because the next of kin of a deceased have to be traced. An offer to share in the benefits is put to the victim and when contact is made, the process to extract advance payments for alleged costs, are made to the victim.

- **FIFA 2010/ SOCCER WORLD CUP:** E-mails purporting to be official competitions marketing the FIFA 2010 Soccer World Cup are sent to victims who are informed that they have actually won prizes that they need to claim. Again the victims are tricked into paying for costs upfront but the prize money never arrives.

What to do

- If you receive one of these scam emails, it is important that **you do not respond** to it in any way. The scammers are likely to act upon any response from those they see as potential victims. The people who run these scams are criminals and could even resort to violence and intimidation to meet their aims. Before you delete the message, you might like to report the scam by forwarding the email to the address supplied on the [FraudWatch International](#) website.
- You can also read about 419 scams on the SABRIC website www.sabric.co.za for more information.

ACCOMMODATION SCAMS

Criminals are exploiting potential tourists through falsely advertising accommodation on the internet and demanding large deposits to secure bookings. Once the money has changed hands, the victim cannot reach the booking agent to make further arrangements and learns that the accommodation does not exist. The deposit is then lost.

What to do

- Be very cautious when you are requested to make urgent payment to secure bookings, this is a red flag.
- Do not do business with unknown people. Course as much information about the other person or company as possible, and verify the information before doing business.
- Make sure that you can verify the existence of the accommodation before booking it. Do not accept information provided by the other party, on face value.
- Do not make bookings through entities that are not reputable.

SALE OF COUNTERFEIT AND STOLEN GOODS

The selling and redistribution of counterfeit goods and stolen goods is the only way that criminals can change their illegal gains into cash. This has as severe impact on the economy. Tourists might be enticed to purchase goods such as DVD's, CD's and FIFA 2010 paraphernalia from street corners for reduced prices rather than at legitimate shops.

What to do

- Do not support illicit trade; rather buy from a legitimate trader. If you support illicit trade you will not have the same guarantees and warranties accompanying the product as you normally when purchased from a legitimate dealer. More importantly, you will become part of the money laundering cycle and indirectly be promoting crime in South Africa.

COUNTERFEIT CURRENCY

Visitors to South Africa generally have the need to exchange their currency into local currency. Whilst the local banks, Bureau's de Change and many hotels will be offering this service, the criminal element is always looking for opportunity to launder their own dirty currency alternatively to undermine the financial system through offering better rates on the streets.

What to do

- Tourists are urged not to trade on the black market as they may find themselves in possession of counterfeit currency alternatively guilty of money laundering.
- Always have your passport available to exchange currency as the South African banks or Bureau's de Change will not exchange currency without presentation of a valid passport.

INFORMATION THEFT

Personal information is a valued commodity for criminals. The theft of foreign passports and credit cards is a high risk as criminals will attempt to use them fraudulently for their own gain. Fraudulent purchases with credit cards as well as cash withdrawals at ATMs when the PIN number has also been compromised, pose a huge threat.

What to do

- Tourists are urged to safe guard their personal property and information. Do not carry unnecessary personal information in your wallet or purse or leave luggage un-attended.
- Should a credit card be lost or stolen, it must be stopped immediately using the following numbers:

Amex	0800110929
MasterCard	0800020600
VISA	0800110132
Diner's Club	0800020600

CARD SKIMMING

Card skimming is the illegal copying or stealing of tract data contained on the magnetic tape at the back of a legitimate bank card. This information is then encoded onto another card which is then used illegally. Skimming could take place at point where card payments are made or at an ATM.

What to do

- Tourists are urged not to let their cards out of their sight when making payments. Do not allow your card to be swiped through any device other than the legitimate device to make payment.
- Do not accept any assistance at an ATM; rather seek assistance from inside the bank.
- The Golden Rule: When punching in your PIN both at Point of Sale or withdrawing money at an ATM cover the key pad, so that the fraudsters do not get your pin.

INTERNET BANKING

Phishing sites and e-mails targeting consumers for the purpose of enticing them to disclose personal information are already on the increase. As the soccer world up approaches, there attempts will escalate and it is expected that the communications will assume the look and feel of promotional and marketing material. This will confuse both local and foreign citizens and trick them into disclosing personal information.

What to do

- Your bank will never request card and PIN numbers from you in an e-mail. Do not respond to such requests.
- When doing internet banking always type in the website address (URL) in order to make sure that you visit the correct website. Do not use hyperlinks contained in e-mails.
- Do not make use of internet café's or computers in any public places to do your internet banking as you have no guarantee that these computers are protected against viruses.

EMPLOYMENT SCAMS TARGETING FOREIGNERS

Tourists might fall victim to employment scams, before entering South Africa and during their stay in South Africa. This goes hand in hand with advance fee fraud scams where victims might be requested to pay up front for fraudulent job offers, fraudulent permanent resident permits and like documents.

What to do

When applying for work in South Africa note that:

- Fees are not payable for any applications to be processed.
- There is a minimum wage payable to any employee of a company in South Africa.
- Get familiar with the South African Labour Laws to prevent yourself from being exploited.

Daya Moodley
SABRIC
(011) 847 3147