



Phone: +27 (0)21 528 3420

Fax: +27 (0)21 552 2848

Website: www.bulksms.com

4th Floor South Lobby
Boulevard Place Heron Crescent
Century City 7441 South Africa

PRESS RELEASE BULKSMS.COM

April 2010

Don't be scammed on SMS

Do you know how to spot an SMS 419 scam, phishing attack, or fake payment confirmation? If you value your money, you should know what to look out for.

Although it is encouraging to see more and more businesses using SMS as a communication platform, it's becoming easier for scammers to trick consumers as a result.

South Africa has one of the highest mobile penetration rates in the world, so it is no wonder that local businesses are increasingly using SMS as a means of communication with their clients. There are many benefits to SMS, both for the businesses and the consumers they serve, but there is also a darker side to this method of communication.

Scammers will, and do, try anything to get their hands on your money. One method they like to use is **419 scams** or advanced-fee fraud as they are also called. The 419-scam originated in Nigeria and is named after the article of the Nigerian Criminal Code that deals with fraud.

On e-mail, these scam letters give space for a lot more information and generally speak of an inheritance (worth billions) that the sender is due. The beneficiary, however, needs your bank account in which to deposit the funds and promises the bank account holder a percentage of the inheritance for use of the bank account. As a show of faith, or in order to release the funds, the sender then asks you to deposit a certain amount into another account first. Once you deposit the money, you obviously never hear from the scammer again. They typically get several tranches of money out of victims. The more the victims give, they more they've already committed, and the more they keep giving, up to a point.

The SMS version works in a very similar way, but the message is generally focused around a cash prize you have won, and asks for a deposit in order to release your winnings. "Congratulations!" is a common word used in these advanced-fee scam SMSes. Another identifier is the use of a non-professional e-mail address. The message will pretend that the prize is from a known brand, such as Nokia, but the e-mail address included in the SMS will be a Yahoo or Hotmail address.

Fraudsters have also taken to using SMSes for **phishing attacks**. Phishing also has its origin in e-mail, but banks have very successfully managed to decrease these attacks through user education. This is a big reason why fraudsters have now moved to using SMS for phishing, because users do not generally expect it.

People also make the mistake of assuming that SMSes are more secure than e-mail, because it seems like a more personal communication method. Unfortunately, this is not the case. Just like a bank will never ask for your confidential information over e-mail, they should never ask for them by SMS either.

SMS phishing scams are, in a way, even more dangerous than their e-mail counterparts, because it is often a real person that asks you for your details over the phone. For instance, you may receive an SMS (that has been replicated from the official version) alerting you that you have logged on to your Internet banking.

The end of the message will read along the lines of “If you have any enquiries, please contact (number)”. Of course you will panic if you are nowhere near your Internet banking service, and immediately phone the number provided. The person who takes the call, however, will be a fraudster who will ask you for your Internet banking details. Once they have these, nothing stops them from accessing your banking online and transferring money wherever they want.

A similar scam fraudsters cotton on to involves **fake payment confirmations**. Again, an official bank SMS will be replicated, but this time it will be a typical bank SMS payment confirmation. The scammer will purchase goods from you, send a fake payment confirmation and then you will release the goods to them without knowing that the confirmation was a fraud.

These SMSes are sent from individual phones, via international SMS providers or occasionally via a local wireless application service provider (WASP).

What is being done and what you can do

Some WASPs look out for these types of scams and close them down where possible. Some WASPs automatically pick up fraudulent messages through filtering methods and block them.

At network level, Vodacom has been the most proactive in terms of preventing fraudulent messages originating from international networks, although MTN is quickly following suit.

Because of the large financial risks involved, it is worthwhile for network providers to implement solutions that would block fraudulent SMSes. That said, it is important to keep in mind that it is very difficult to track these fraudsters down, because they use stolen identities in the first place. Even if an IP address is traced and the offending computer identified, it would still need to be proven that the alleged scammer used the computer at the time the fraudulent act was carried out.

The most effective thing to do if for consumers to educate themselves as much as possible on these scams and to keep in mind a few basic tips:

- If it sounds too good to be true, it probably is
- Save the phone number of your bank on your mobile, and always phone your bank to verify potentially fraudulent SMSes.
- Check network operator websites for reports on the latest SMS scams
- Report abuse to WASPA