



419 SCAM

notes

What is it?

A form of “advance-fee” fraud. Measured by monetary losses, 419 fraud is the world’s most prevalent scam.

The 419 scam originated in the early 1980s in Nigeria, and is named after a section of that country’s criminal code. This scam is no longer confined to Nigeria – 419 fraudsters are arrested throughout South Africa and around the world.

How it works

Today, 419 scams typically make use of the internet. They commonly begin with an email with the aim of persuading the recipient to advance money to the sender, with the promise of a large future payoff. The author often claims to be royalty or fabulously wealthy, and promises large amounts of money if the sender will pay a small sum first, or forward their bank details.

Perpetrators of the fraud advance a range of claims to explain why they need the recipient’s help: funds are said to be trapped in central banks due to political unrest; massive inheritances hard to access because of government restrictions or taxes; and so on.

Scammers ask the victim to pay fees and taxes, or give bank account details to help them transfer the money. These fees may initially be small amounts, but the scammer will keep requesting money and the victim will never receive the large “reward” promised.

How to avoid being a victim

- If it sounds too good to be true, it probably is.
- The scam email will emphasise confidentiality and “risk-free” transactions.
- Unknown sources of money and unrealistic value of funds are presented.
- The letter often (but not always) contains grammatical errors.
- Do not give out your bank details or reply to an email requesting such details.
- Know who you are dealing with – research the company or person.



Excerpt from 419 e-mail (spelling as in original)

notes

You may be surprise to receive this message from me since you don't know me in person, but for the purpose of introduction, I am Mr (NAME REMOVED)....

Before the death of my father, he took me to SOUTH AFRICA to deposit the sum of \$25.5 million with a security and finance company as if he knew the looming danger in Angola....

I, my mother and my family ... have decided to transfer this money to a foreign country where we can invest it.... The South African monetary policy/law does not allow such investment hence I am seeking for an asylum or refugee. I must let you know that this business is 100% risk free and the nature of your business does not necessary matter.

So if you are willing to assist us, we have agreed to give you 20% of the total money, 40% will be for a joint business venture I will be doing with you and another 35% will be for me and my family which we shall also invest in your country and the remaining 5% will be mapped out for all expenses we may Incurred during the transaction.

Remember that this is highly confidential and the success of this business depends on how secret it is kept....

**“419” IS AN OLD NIGERIAN CRIMINAL
CODE FOR THEFT UNDER FALSE PRETENCES**



notes

CASE STUDY: 419 SCAM

A 419 syndicate approached a Czech citizen, claiming that financing was needed to fund a project in Europe. The recipient was told he would receive a cut of the project upon its completion.

After depositing about R3 million into the fraudsters' account, the victim was told that the project leader had passed away, but a South African bank would still honour the agreement of the project profit share (\$37 475 000).

The syndicate created fake South African bank documents showing an account in the name of the victim and that funds were available for withdrawal subject to certain provisions. A document with a copied FIC logo stated that the funds were approved for transfer to the victim – all that was needed was a South African Receiver of Revenue certificate after certain taxation fees were paid.

To complete the transfer, the victim paid tax and administration fees. In total, he lost more than \$3 million in various currencies.

The FIC analysed the fraudulent documents, which revealed a cellphone number that was repeatedly used in correspondence with the victim. The cellphone number and fax number led to the identification of other reports, in which the same number was used for the transfer of money to beneficiaries in Nigeria.

The perpetrator's ID document was obtained, revealing a number of suspicious transaction reports filed against him. The perpetrator had married and divorced a South African national to obtain citizenship. Other databases revealed that he had acquired assets that are suspected to have been purchased with the proceeds of crime.

The matter has been referred to the law enforcement agency for further investigation.



SAPS save South Koreans from 419 scam kidnap gang¹
Statement issued by the South African Police Service
9 January 2012

notes

Members of the South African Police Service (SAPS) have arrested six suspects for allegedly kidnapping two Korean nationals lured to South Africa through a 419 scam.

The 65 year-old father and his daughter, who is in her 30s, apparently responded to an email from the suspects promising tens of millions of dollars. The duo arrived in South Africa from South Korea on Tuesday. The suspects allegedly tasked a driver to fetch the victims from OR Tambo airport. The driver and the two Korean nationals were kidnapped and kept at a house in Meadowlands, Soweto.

The driver managed to escape and alert the police. The suspects demanded a US\$10 million ransom from the 65 year-old man's wife (who was back in South Korea), to be deposited into an account in Singapore. The amount was eventually negotiated down to US\$120 000. While the negotiations were on-going, the wife alerted the South Korean embassy in South Africa. Members of the SAPS rescued the captives, before the ransom money was deposited.

Six suspects (five foreign nationals and a South African) were arrested during a rescue operation in the early hours of this morning.

They have been charged with kidnapping.

¹ <http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oId=274248&sn=Detail&pid=71616>