Interfraud's impact on Africa

Dr Marthie Grobler
Council for Scientific and Industrial Research, Pretoria, South Africa
South African newspaper headlines between July 2009 and April 2010

- Police warn public of con artists during festive period
  26 November 2009
- Taken in by a super cheap holiday scam
- Phishers netted 194% in a year in the province
  29 March 2010
- Women arrested for internet fraud of R2m
  31 March 2010
- SARS warns of tax return phishing scam
  26 November 2009
- Beware: your new Facebook friend could be an inside job
  12 December 2009
- Banks must fight online fraudsters
  21 November 2009
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
- Phishers netted R24 000
  26 November 2009
- Women arrested for internet fraud of R2m
  31 March 2010
Interfraud
What is interfraud?

• Any fraud scheme that uses one or more online service to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme
  • target large number of victims for small per-victim losses
  • target small number of victims for large amounts of per-victim losses
What is interfraud?

• The Federal Trade Commission reported that interfraud has been the top consumer complaint for the past four years
• 292,799 reports of fraud in the global media during 2009
• $559.7 million were lost last year to Internet-based scams and fraud, more than double the figure for 2008
• Also referred to as dot con
Global interfraud tendencies
Fraud type 1: Advance fee scam

- Confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a significantly larger gain
- Variations: Nigerian Letter, 419 fraud, Spanish Prisoner, black money scam, Russian/Ukrainian scam, work from home scam

* 419 refers to the article of the Nigerian Criminal Code (part of Chapter 38: "Obtaining Property by false pretences; Cheating") dealing with fraud
Fraud type 1: Advance fee scam

- Variation 1: Purchasing goods and services
Fraud type 1: Advance fee scam

- **Variation 1: Purchasing goods and services**

  You won’t get rich quick
  Hang on to your money
Fraud type 1: Advance fee scam

- **Variation 2: Job opportunity scam**
- **Admin needed asap**

On Tue, Feb 9, 2010 at 9:46 PM, Ref! <r.nkele@gmail.com> wrote:

HI we are really pretty impressed on your CV you had attached in your last mail you had sent to us we really appreciate that you would like to work with us. We have a lot of other Job Applications and emails referring to this job coming to us everyday and most of the senders aren't serious at all and actually are time waster so we ask for you to purchase a R55 worth of vodacom airtime and mail it to us when you read this email, then we can know that you're really serious/desperate to get this job as the amount per month is about 32K a month and ask you to come over for interview or to review the workplace and see available cars as that is the benefit when getting into the job.

Please reply asap with the airtime required and for us to schedule for you to come in today as we need someone to fill up on the position as soon as possible!
Fraud type 1: Advance fee scam

- **Variation 3: Romance scam**
  - Exploit free online dating websites
  - The victim is approached on an online dating service
    - 1) The offending party claims to be interested in coming to visit the victim, but needs some cash up front in order to book the plane, hotel room, and other costs
    - 2) The offending party claims to have travelled and has been arrested by corrupt officials, or become ill from eating the local food → needs an emergency Western Union transfer
Fraud type 1: Advance fee scam

• **Variation 3: Romance scam**
  - “She said her name is dian white”
  - “just contacted me as elenazv on a site called lavaplace”
  - “She is calling herself Elena and using the e-mail address elenasunflower@mail.ru”
  - “She contacted me using elvirlo@gmail”
  - “she also uses angelok@mail.ru”
  - “Emailed me and called herself Rica, using email Ricalapochka@yandex.ru”
  - “calls her self Nastya”
  - “REGINA KUGUELOVA”
  - “She is calling herself Nina with me, nina-moon@mail.ru”
  - “I have come across her using the name Elvira and email Elvira089@nm.ru”
  - “Ulyana, ulyanayou@yahoo.com”

Fraud type 1: Advance fee scam

**Variation 4: Lottery/Competition scam**

- A Bloemfontein woman received an email in December telling her that she had won a million British pounds in a foreign competition
  - had to pay an initial amount before getting her prize money
  - had to go to London to claim the prize
  - could not go due to work commitments
  - had to pay an agent to claim the money on her behalf
  - she was told that a safe with the prize money had been brought to South Africa and she had to pay an additional amount to have it opened
  - 13 payments totalling R1.2m between January and March 2010
Fraud type 1: Advance fee scam

• Variation 5: Work from home scam
  • Currently a 54-to-1 scam ratio among work-at-home job leads on the Internet → result of recession
  • These jobs offer the convenience of working at home
  • Often offer more than in an average 9-to-5 office job
  • "Make $600 a day wearing your pajamas"
  • "Achieve financial freedom without ever leaving your couch"
Fraud type 2: Phishing

- An attempt by a third party to solicit confidential information from an individual, group or organisation
  - mimic a specific, usually well-known brand and aims to elicit financial gain
  - employ social engineering and technical deception to steal unsuspecting users’ personal identity data and financial account credentials
Fraud type 2: Phishing

• **Variation 1: Man-in-the-middle attacks**

![Diagram of man-in-the-middle attack](image-url)
Fraud type 2: Phishing

- **Variation 2: URL obfuscation attacks**
  - **Bad domain names** - purposeful registration and use of bad domain names
    Instead of http://privatebanking.mybank.com, the following privatebanking.mybánk.com, mybank.privatebanking.com
  - **Third-party shortened URLs** - third-party organisations offers free services designed to provide shorter URLs
  - **Host name obfuscation** - URLs are presented as IP address, and not domain name
    Instead of http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm, the following http://mybank.com:ebanking@210.134.161.35/login.htm.
Fraud type 2: Phishing

- **Variation 3: Capturing customer data**
  - Receive a letter from a national bank card carrier including a new card and information that one of your existing cards had been compromised
  - The recipient has to phone a 800 number to activate the replacement
  - Activation requires knowledge of the old card number, it’s expiry date, the recognition code, and the two digit check code - everything a phisher needs to strip the account
Fraud type 3: Pharming

- Pharming attack misdirects Internet users of trusted brands to false storefronts set up to harvest identities.
- Unlike phishing, pharmers work invisibly and do not rely on spam to lure victims to their fraudulent websites.
- Pharming is a form of domain spoofing, where pharmers change a local DNS server to redirect the victim's web request to a fake website - pharming attacks direct victims to a fake website even if they typed the correct address of the intended website into their browser.
- If the pharmers designed the fake website to look like the legitimate website, the victim has no way of knowing it is a fraudulent website.
Fraud type 3: Pharming
Fraud type 3: Pharming
Fraud type 3: Pharming

- **Variation 1: Altering the victim computer's host file**
  - Locally stored files, hosts files, contain a mapping between an alphanumeric domain name and its IP address
  - The host file is an easily altered text file that contains IP addresses separated by at least once space and then a domain name, with each entry on its own line
Fraud type 3: Pharming

- **Variation 1: Altering the victim computer's host file**
Fraud type 3: Pharming

- **Variation 2: DNS cache poisoning**

![Diagram showing the process of Pharming with steps 1 to 5 labeled accordingly.](image-url)
Fraud type 4: Hacking

- Suspected cyber hackers have stolen a total of R5.5m from the Mpumalanga education department’s bank account, presumably with inside help
  - changed the bank details of existing beneficiaries as a smoke screen
  - transferred the money to registered beneficiaries
  - money was paid into seven different accounts on August 24, August 25 and September 24 2009
  - several transfers were made, ranging between R864 000 and R989 000
- The fraud came to light when a Nedbank clerk noticed huge amounts paid into a woman's account, outside her normal financial profile
- R1 543 345 could be saved
Fraud type 5: Actuality exploits

- Any major world event triggers a flood of internet attacks and spamming campaigns
- Take advantage of people's interest in actuality topics to improve their success rate of spam campaigns
  - Michael Jackson’s death
  - Swine flu outbreak
  - Haiti earthquake
  - Volcanic eruption
Fraud type 5: Actuality exploits

Google trends

Scale is based on the average traffic of michael jackson from South Africa in the last 12 months.

- Michael Jackson, Swine flu, haiti, volcano

Searches

- michael jackson: 1.00
- swine flu: 0.30
- haiti: 0.25
- volcano: 0.10

High points:

A. WHO declares Swine flu a 'pandemic'
   Bizjournals.com - Jun 11 2009

B. Michael Jackson
   Livemint - Jun 26 2009

C. China approves swine flu vaccine
   BBC News - Sep 3 2009

D. Haiti: Where to donate
   Toronto Star - Jan 14 2010

E. United Nations for Haiti
   Aljazeera.net - Apr 1 2010

F. Iceland volcano pictures
   Telegraph.co.uk - Apr 19 2010
Interfraud in Africa
Interfraud in Africa

- Top 10 cyber crime perpetrator list
  - 1\textsuperscript{st} United States 65.4%
  - 2\textsuperscript{nd} United Kingdom 9.9%
  - 3\textsuperscript{rd} Nigeria 8.0%
  - 4\textsuperscript{th} Canada 2.6%
  - 5\textsuperscript{th} Malaysia 0.7%
  - 6\textsuperscript{th} Ghana 0.7%
  - 7\textsuperscript{th} South Africa 0.7%
  - 8\textsuperscript{th} Spain 0.7%
  - 9\textsuperscript{th} Cameroon 0.6%
  - 10\textsuperscript{th} Australia 0.5%

\textbf{NOTE} Statistics may be skewed due to unreported incidents
Interfraud in South Africa

- "The government has identified at least 27 cases where a syndicate has swindled more than R199-million from government departments in four provinces over the past three years - using cyber-spyware…” (Mail & Guardian 2008)
Interfraud in South Africa

- Historically low broadband penetration limit the probability of cyber attacks
- 2010 seems to be the turning point
  - Symantec’s Internet Security Threat Report shows that countries introducing pervasive broadband experience an immediate increase in threats (see Brazil, Turkey and Poland)
  - As the host of the 2010 FIFA World Cup, South Africa has become a prominent target (see France, Korea and Japan)
Interfraud prevention

- Be wary of email messages asking for personal information
- Only enter personal information using a secure website
- Do not use links in an email message to load a web page
- Check your bank accounts regularly
- Use the latest version web browser and security patches
- Purchase items via the Internet by credit card
- Learn as much as possible about the seller
- Ask the seller about when delivery can be expected and if there is a problem with the merchandise is it covered by a warranty or can you exchange it
- Obtain a physical address rather than merely a post office box
- Call the seller to see if the number is correct and working
- Consider an escrow or alternate payment service
- Check the address in the address bar
- Report to FraudWatch International
Conclusion

"Fraud today has a technological twist, but is really old wine in new bottles. The internet is a great tool for the con artist, though also a tool for law enforcement because it provides a trail" – John Stark