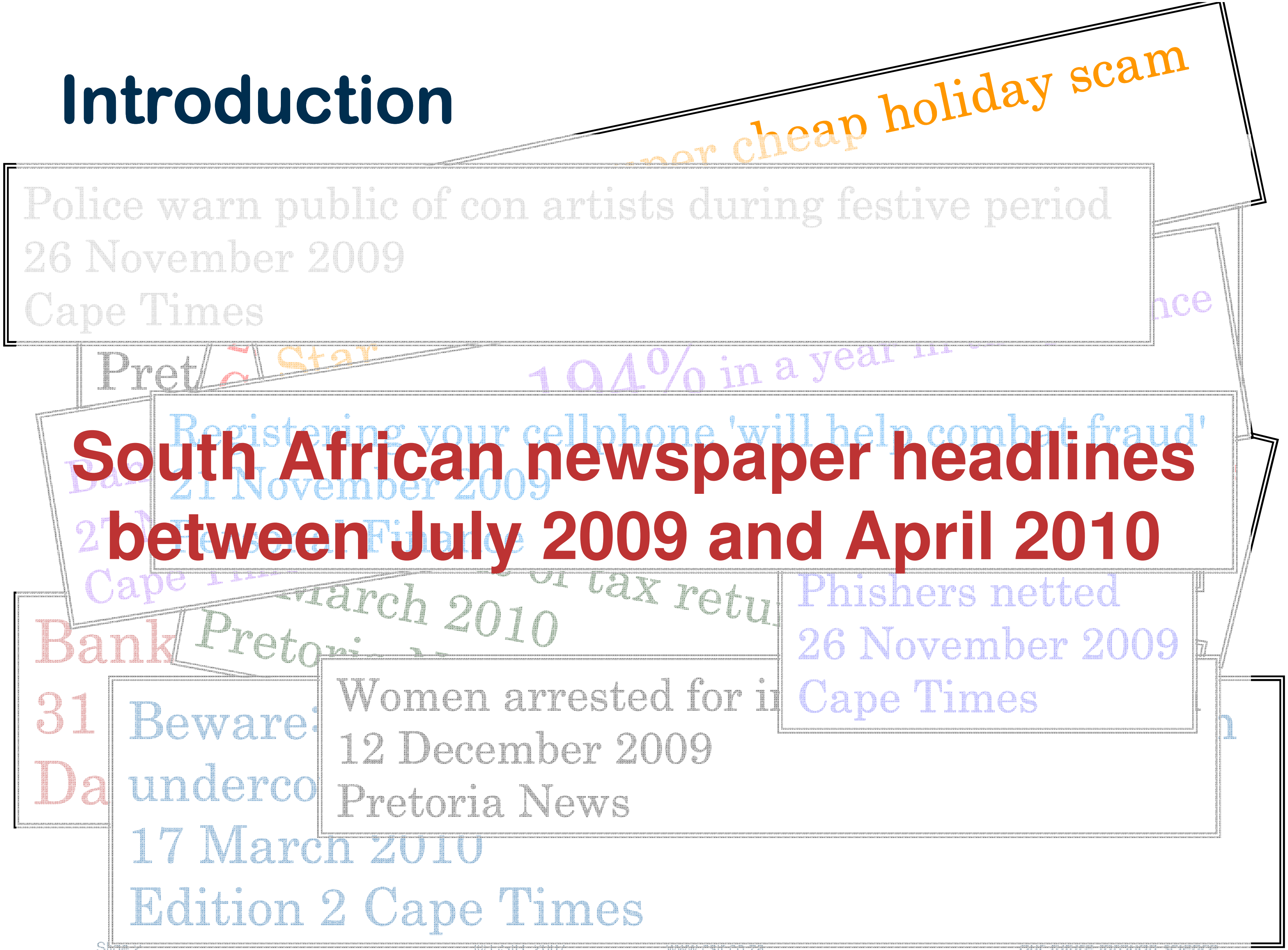
Interfraud's impact on Africa

Dr Marthie Grobler

Council for Scientific and Industrial Research,
Pretoria, South Africa

our future through science

Introduction


per cheap holiday scam
Police warn public of con artists during festive period
26 November 2009
Cape Times
Pret
Star
194% in a year in
nce
Registering your cellphone 'will help combat fraud'
21 November 2009
Personal Finance
Ba
2
Cape Tim
March 2010
of tax retu
Pretoria N
Phishers netted
26 November 2009
Cape Times
Bank
31
Da
Beware
underco
17 March 2010
Edition 2 Cape Times
Women arrested for i
12 December 2009
Pretoria News

South African newspaper headlines between July 2009 and April 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

our future through science

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

our future through science

Global interfraud tendencies

Fraud type 1: Advance fee scam

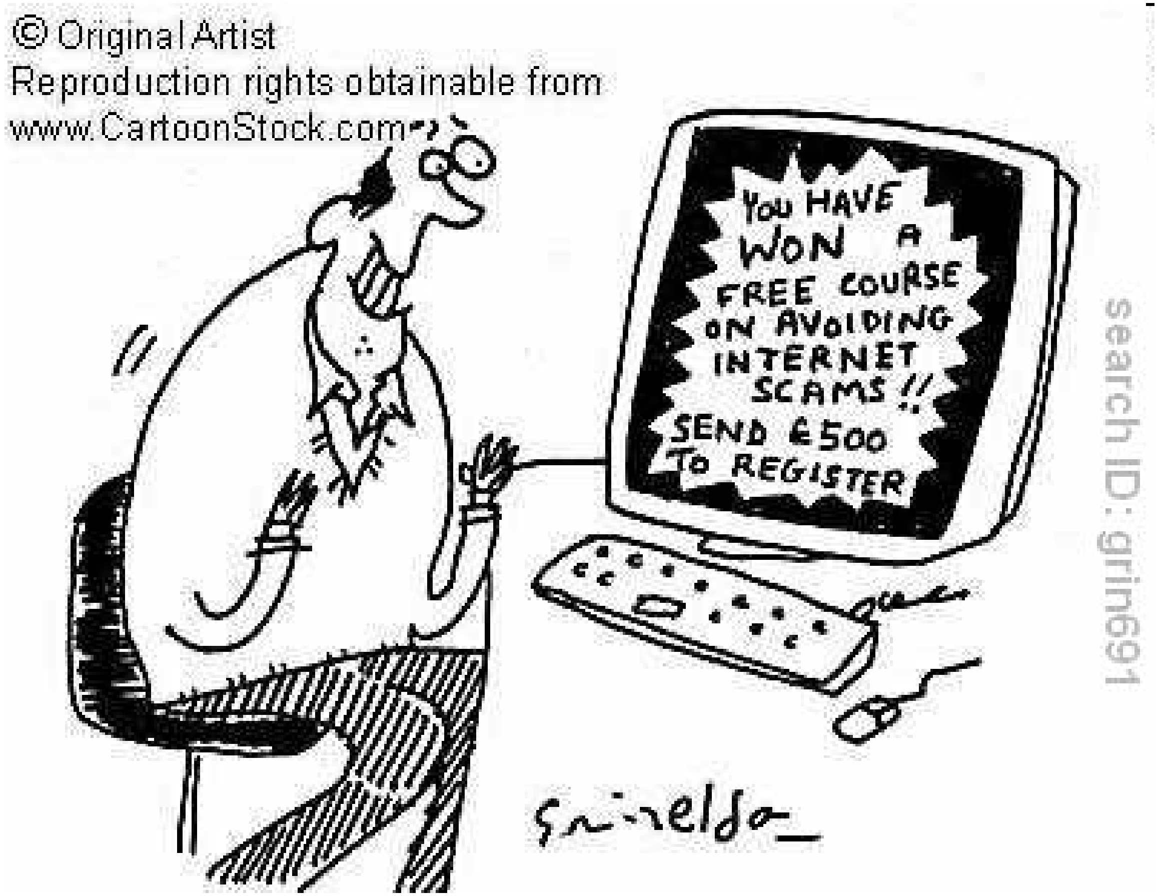
- Confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a significantly larger gain
- Variations: Nigerian Letter, 419 fraud, Spanish Prisoner, black money scam, Russian/Ukrainian scam, work from home scam

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

our future through science

Fraud type 1: Advance fee scam

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


© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
YOU HAVE WON A FREE COURSE ON AVOIDING INTERNET SCAMS!!
SEND £500 TO REGISTER
search ID: grin691
Grizelda

our future through science

Fraud type 1: Advance fee scam

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

You won’t get rich quick

Hang on to your money

our future through science

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

- **<u>Variation 3: Romance scam</u>**
  - 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"*

http://www.romancescam.com/forum/viewtopic.php?t=326

our future through science

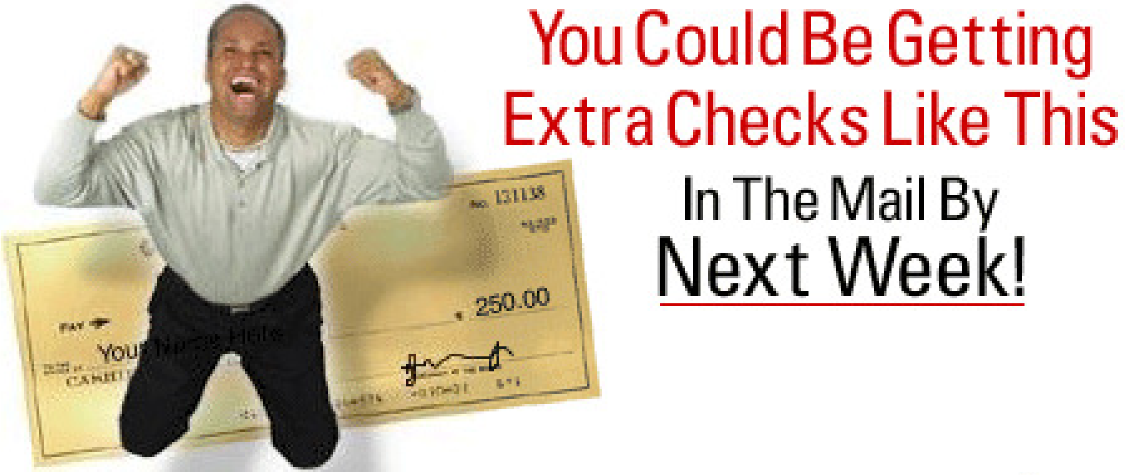
Fraud type 1: Advance fee scam

- **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

our future through science

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"*

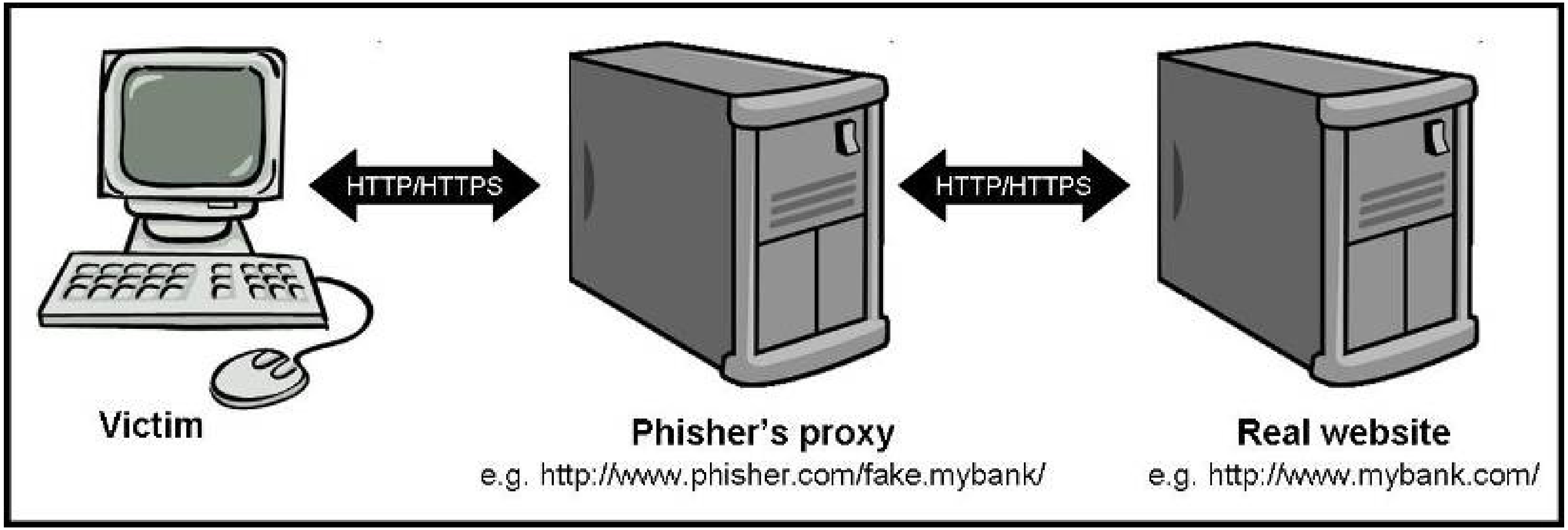


Fraud type 2: Phishing

- 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**


HTTP/HTTPS
HTTP/HTTPS
Victim
Phisher's proxy
e.g. http://www.phisher.com/fake.mybank/
Real website
e.g. http://www.mybank.com/

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.*

our future through science

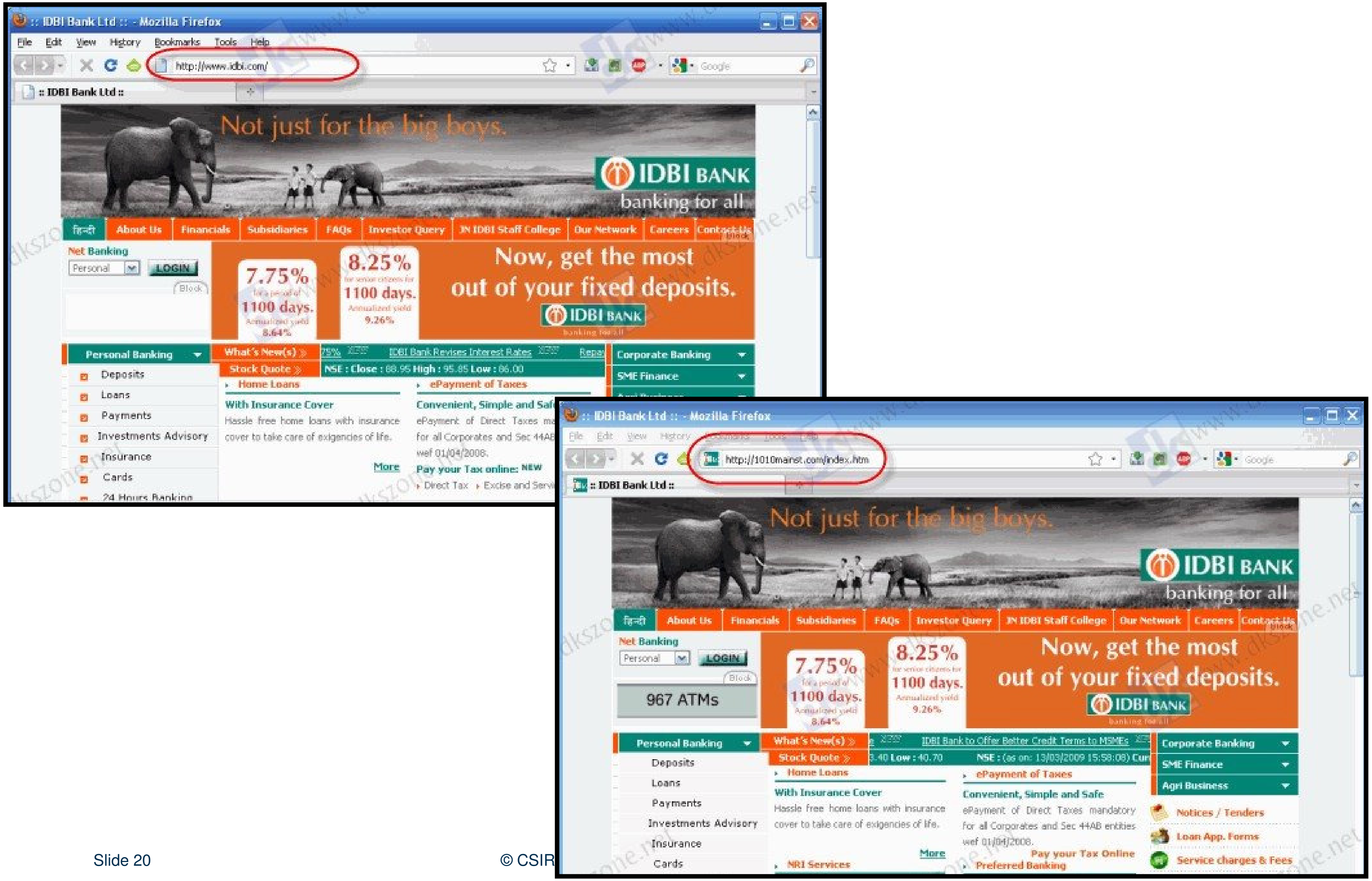
Fraud type 2: Phishing

- **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



:: IDBI Bank Ltd :: - Mozilla Firefox

http://www.idbi.com/

:: IDBI Bank Ltd ::

Not just for the big boys.

IDBI BANK banking for all

हिन्दी | About Us | Financials | Subsidiaries | FAQs | Investor Query | JN IDBI Staff College | Our Network | Careers | Contact Us

Net Banking

Personal | LOGIN

7.75% for a period of 1100 days. Annualized yield 8.64%

8.25% for senior citizens for 1100 days. Annualized yield 9.26%

Now, get the most out of your fixed deposits.

Personal Banking: Deposits, Loans, Payments, Investments Advisory, Insurance, Cards, 24 Hours Banking

What's New(s) | IDBI Bank Revises Interest Rates

Stock Quote | NSE : Close : 88.95 High : 95.85 Low : 86.00

Home Loans

With Insurance Cover

Hassle free home loans with insurance cover to take care of exigencies of life.

More

ePayment of Taxes

Convenient, Simple and Safe

ePayment of Direct Taxes mandatory for all Corporates and Sec 44AB entities wef 01/04/2008.

Pay your Tax online: NEW

Direct Tax | Excise and Service

Corporate Banking | SME Finance

:: IDBI Bank Ltd :: - Mozilla Firefox

http://1010mainst.com/index.htm

:: IDBI Bank Ltd ::

Not just for the big boys.

IDBI BANK banking for all

हिन्दी | About Us | Financials | Subsidiaries | FAQs | Investor Query | JN IDBI Staff College | Our Network | Careers | Contact Us

Net Banking

Personal | LOGIN

967 ATMs

7.75% for a period of 1100 days. Annualized yield 8.64%

8.25% for senior citizens for 1100 days. Annualized yield 9.26%

Now, get the most out of your fixed deposits.

Personal Banking: Deposits, Loans, Payments, Investments Advisory, Insurance, Cards

What's New(s) | IDBI Bank to Offer Better Credit Terms to MSMEs

Stock Quote | 3.40 Low : 40.70 | NSE : (as on: 13/03/2009 15:58:08) Cur

Home Loans

With Insurance Cover

Hassle free home loans with insurance cover to take care of exigencies of life.

More

NRI Services

ePayment of Taxes

Convenient, Simple and Safe

ePayment of Direct Taxes mandatory for all Corporates and Sec 44AB entities wef 01/04/2008.

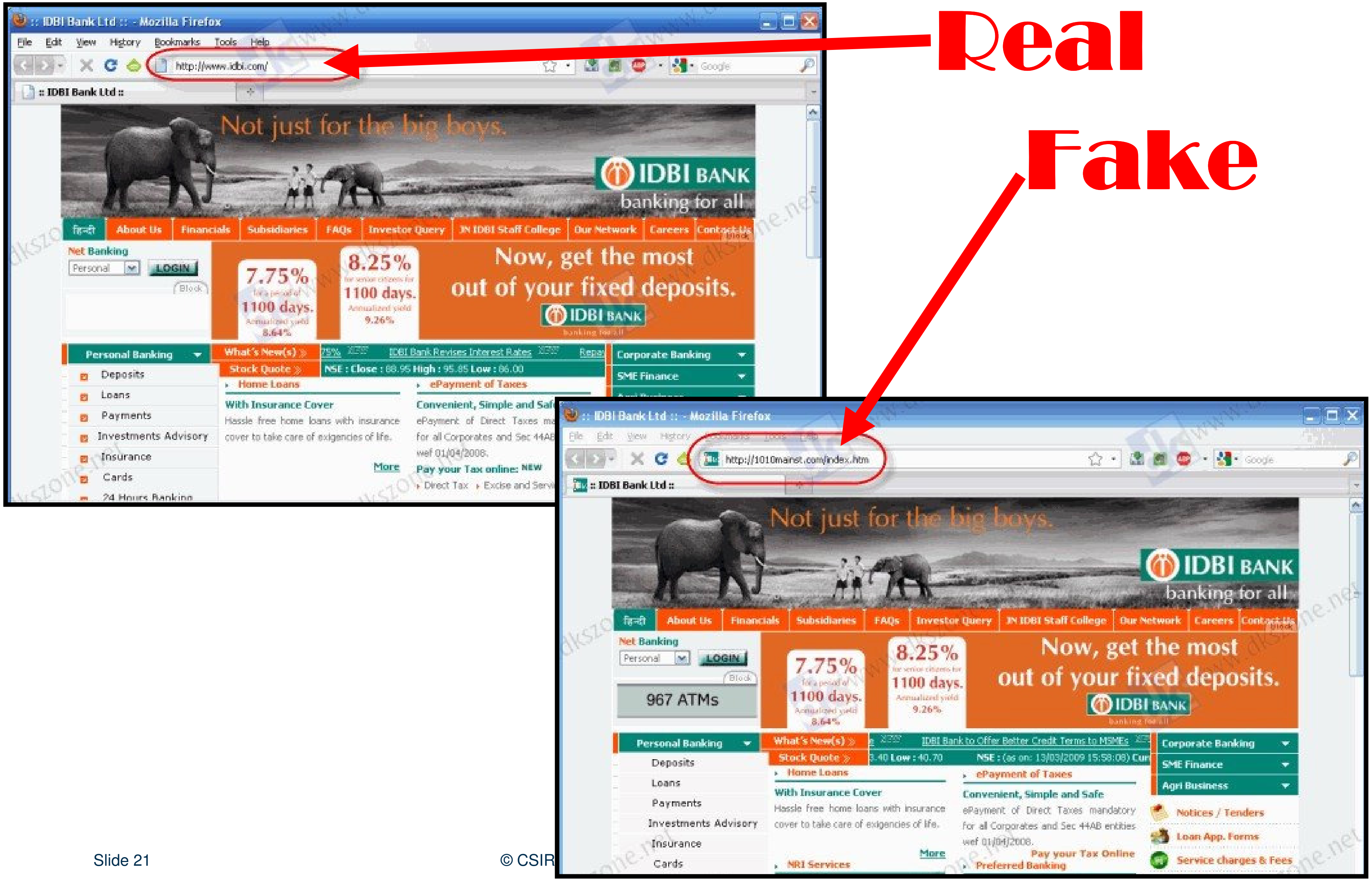
Pay your Tax Online

Preferred Banking

Corporate Banking | SME Finance | Agri Business

Notices / Tenders | Loan App. Forms | Service charges & Fees

Fraud type 3: Pharming



:: IDBI Bank Ltd :: - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.idbi.com/

:: IDBI Bank Ltd ::

Not just for the big boys.

IDBI BANK banking for all

हिन्दी | About Us | Financials | Subsidiaries | FAQs | Investor Query | JN IDBI Staff College | Our Network | Careers | Contact Us

Net Banking
Personal LOGIN

7.75% for a period of 1100 days. Annualized yield 8.64%

8.25% for senior citizens for 1100 days. Annualized yield 9.26%

Now, get the most out of your fixed deposits.

IDBI BANK banking for all

Personal Banking: Deposits, Loans, Payments, Investments Advisory, Insurance, Cards, 24 Hours Banking

What's New(s) | IDBI Bank Revises Interest Rates

Stock Quote | NSE : Close : 88.95 High : 95.85 Low : 86.00

Corporate Banking | SME Finance

Home Loans — With Insurance Cover: Hassle free home loans with insurance cover to take care of exigencies of life. More

ePayment of Taxes — Convenient, Simple and Safe: ePayment of Direct Taxes mandatory for all Corporates and Sec 44AB entities wef 01/04/2008. Pay your Tax online: NEW

Direct Tax | Excise and Service Tax

:: IDBI Bank Ltd :: - Mozilla Firefox

http://1010mainst.com/index.htm

:: IDBI Bank Ltd ::

Not just for the big boys.

IDBI BANK banking for all

हिन्दी | About Us | Financials | Subsidiaries | FAQs | Investor Query | JN IDBI Staff College | Our Network | Careers | Contact Us

Net Banking
Personal LOGIN

967 ATMs

7.75% for a period of 1100 days. Annualized yield 8.64%

8.25% for senior citizens for 1100 days. Annualized yield 9.26%

Now, get the most out of your fixed deposits.

Personal Banking: Deposits, Loans, Payments, Investments Advisory, Insurance, Cards

What's New(s) | IDBI Bank to Offer Better Credit Terms to MSMEs

Stock Quote | 3.40 Low : 40.70 | NSE : (as on: 13/03/2009 15:58:08) Cur

Corporate Banking | SME Finance | Agri Business

Notices / Tenders | Loan App. Forms | Service charges & Fees

Home Loans — With Insurance Cover: Hassle free home loans with insurance cover to take care of exigencies of life. More

NRI Services

ePayment of Taxes — Convenient, Simple and Safe: ePayment of Direct Taxes mandatory for all Corporates and Sec 44AB entities wef 01/04/2008. Pay your Tax Online

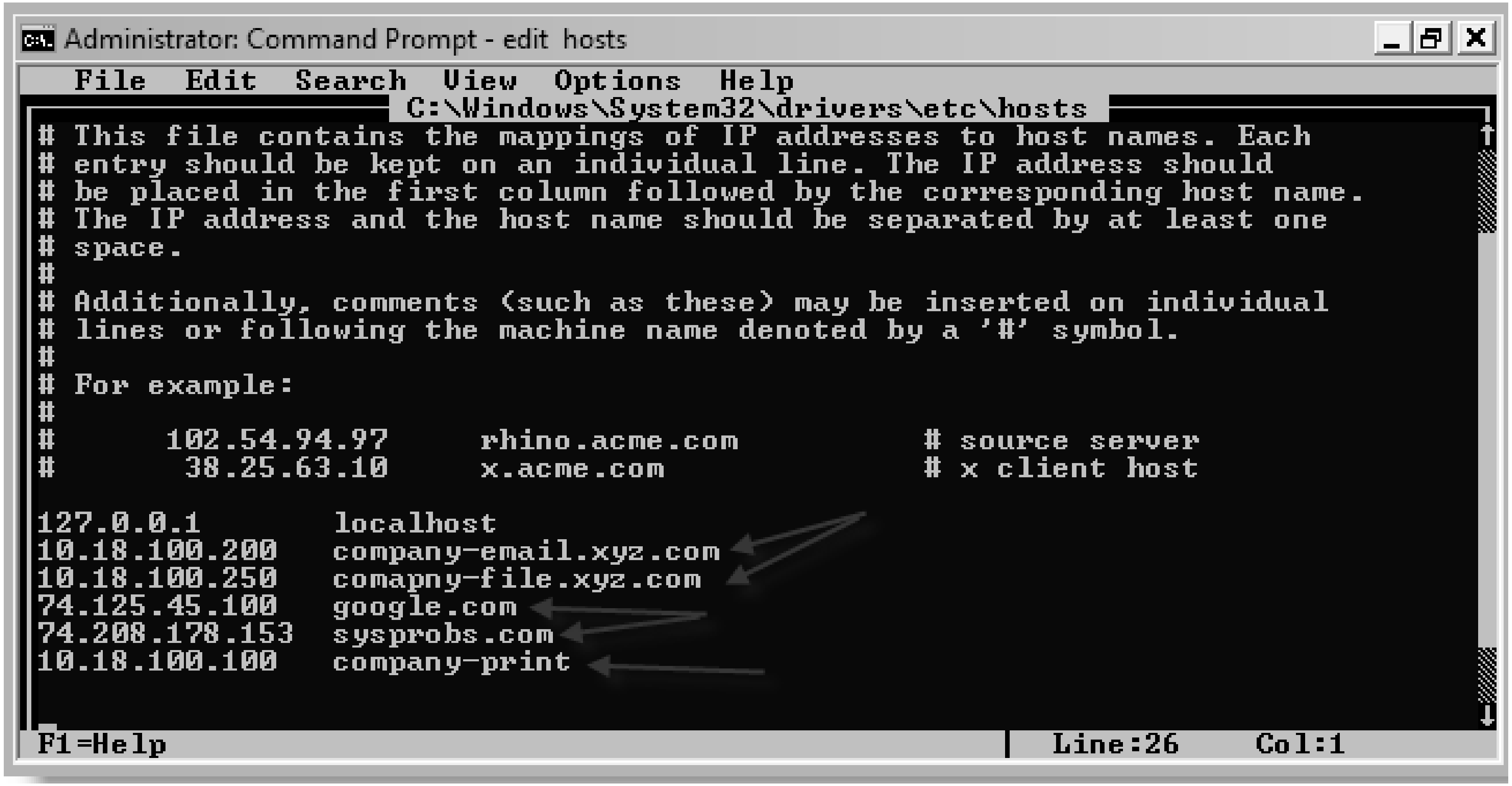
Preferred Banking

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**



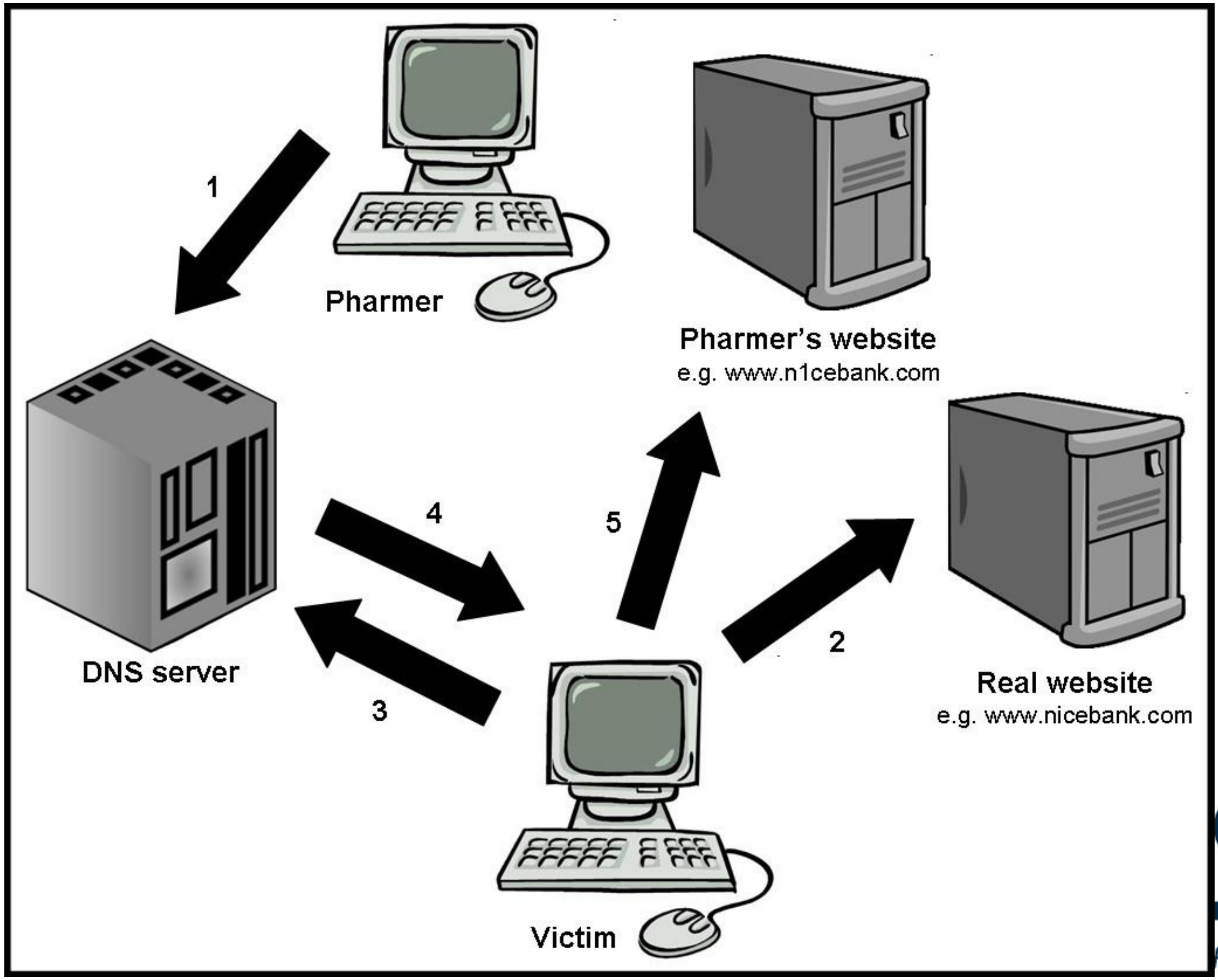
Administrator: Command Prompt - edit hosts
File Edit Search View Options Help
C:\Windows\System32\drivers\etc\hosts

```
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
10.18.100.200   company-email.xyz.com
10.18.100.250   comapny-file.xyz.com
74.125.45.100   google.com
74.208.178.153  sysprobs.com
10.18.100.100   company-print
```

Fraud type 3: Pharming

- **Variation 2: DNS cache poisoning**



future through science

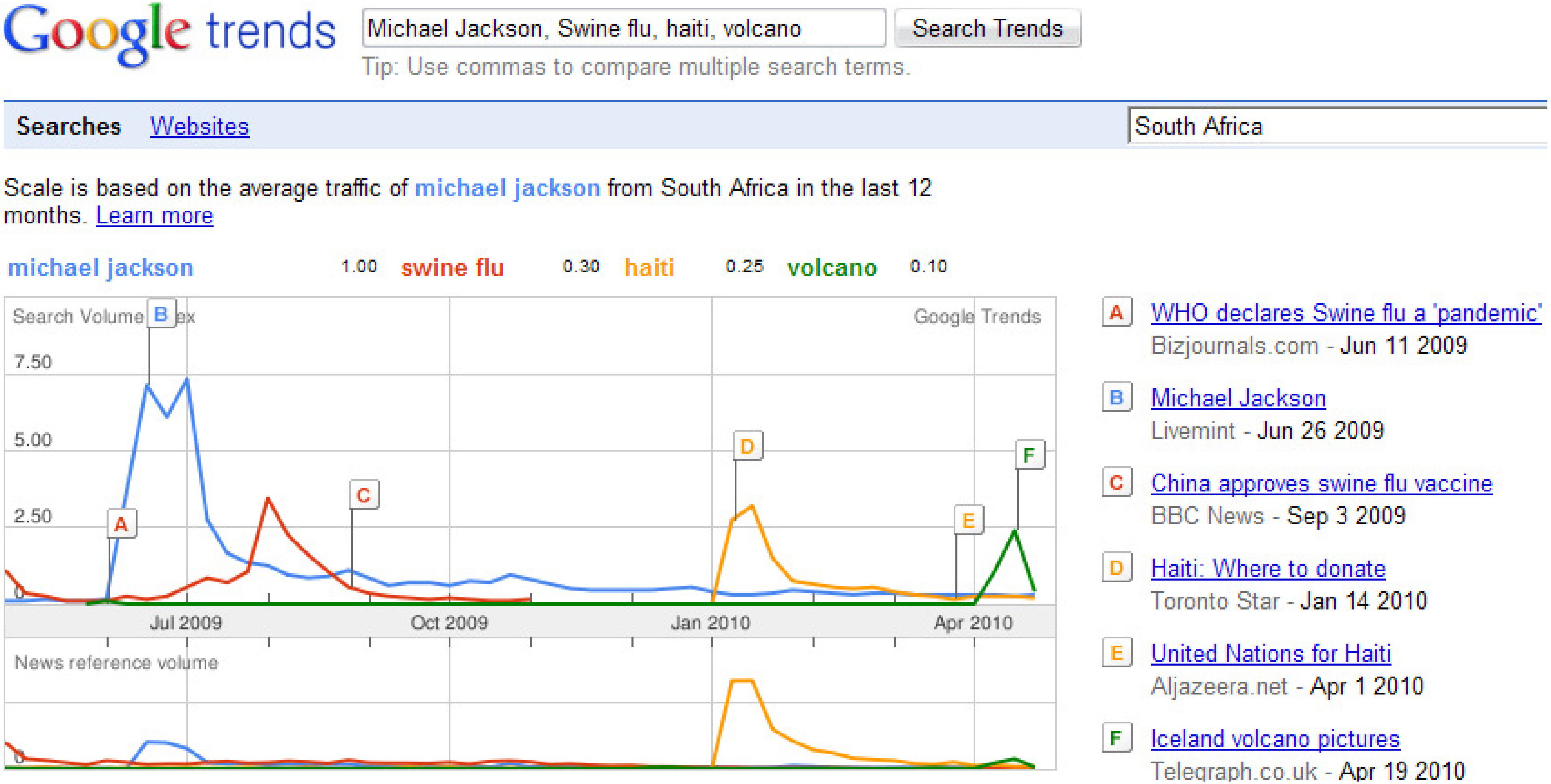
Fraud type 4: Hacking

- 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



Michael Jackson, Swine flu, haiti, volcano

Tip: Use commas to compare multiple search terms.

South Africa

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

michael jackson	1.00	swine flu	0.30	haiti	0.25	volcano	0.10

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

our future through science

Interfraud in Africa

US statistics

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

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)

our future through science

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

our future through science

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

mgrobler1@csir.co.za
marthiegrobler@gmail.com

our future through science