Internet Scams and Fraud

Information Security & Privacy Office
Before We Start…

• I need your help

• I have a large sum of money that I’m trying to get out of the country

• For your help, I’ll gladly pay you a percentage or about 1.5 million dollars
I NEED YOUR URGENT ASSISTANCE (CALL ME:Tel:+27789042775)

FROM: From Nkosi Family of Zimbabwe

From Samuel Nkosi
Johannesburg South Africa
Telephone:+27789042775
21/January/2009

Please reply only on this our confidential
Email address: nkosifamily@gmail.com

Good Day,

How are you today? My name is Mr. Samuel Nkosi, the elder son of Dr. Teddy Nkosi of Zimbabwe. This might be a surprise to you about where I got your contact address. I got your address from the South African Chamber of Commerce/Industry in Johannesburg, South Africa in my earnest search for a reliable company or individual that can assist me in transferring this reasonable sum of money abroad.

During the current war against the white farmers in Zimbabwe from the supporters of our President Robert Mugabe to claim all the white-owned farmlands to his party members, war veterans and his followers, he ordered all white farmers to surrender all farms to his party members, war veterans and his followers. My father's Company is One of the best Company in our country and because he did not support Mugabe’s ideas, Mugabe’s supporters invaded my father’s Company and burnt everything in the Company, killing my father and made away with a lot of items in my father’s Company.

Before his death, my father had deposited with one of the Security/Finance Company in Johannesburg, South Africa the sum of US$27,000,000 MILLION UNITED STATES DOLLARS. After the death of my father, we decided to move to the Republic of South Africa where he had deposited the money in the Security Company with code as "family valuables only. So I decided to you so that you will assist me to move this money out of South Africa because as asylum seekers we are not allowed to operate any Bank Account within South Africa.

We have agreed to offer you 25% of the total sum for your assistance, 5% will be mapped out for any expenses that may be incurred in the course of this transaction while 70% will be for me and my family to invest in your country. South Africa is very bad due to our refugee condition and we were recently assaulted and beaten in the recent xenophobic attack to foreigners, please we need your urgent help urgently.

Please contact me on the above Telephone numbers. Note that this transaction is 100% Risk free and absolutely confidential and upon receipt of your response, I will let you know the next step to be followed. God bless you and your family.

Please reply only on this our confidential Email address: nkosamuel@gmail.com

Best Regards
MR. Samuel Nkosi (Tel:+27789042775)
Nigerian 419 Scam

• A wealthy foreigner who needs help moving millions of dollars from his homeland promises a hefty percentage of this fortune as a reward
  – Claims to be Nigerian official, businessman, or the surviving spouse of former government honchos
• If you respond, you may receive “official looking” documents and asked to provide your bank account numbers, as well as some money to cover transaction and transfer costs and attorney’s fees
• AKA “4-1-9 fraud” (after the section of the Nigerian penal code that addresses these schemes)
Today’s Objective

• Learn to recognize online scams

• Don’t be a victim
What is a scammer’s goal?
Money!

- Money they can get directly from you!
- Information that can be sold for money!
- Control of your PC that could be used to generate money!
  - By using your PC to send spam
  - By using your PC to launch DDoS attacks
Advanced Fee Fraud

• Class of fraud where scammers convince victims to pay a fee to receive something of value
  – But scammers never deliver
M B C LOTTERY  P O BOX 1010
LIVERPOOL, L70 1NL
UNITED KINGDOM
(Customer Services)
Ref. UK/9920X3/2011
Batch: 085/06/FSX09

BTL NOTIFICATION DESK

We happily announce to you the draw (#1070) of the M B C LOTTERY, online Sweepstakes International program held on Wednesday 14th September 2011. Your e-mail address attached to ticket number: 139573490206 750 with Serial number 1395/09 drew the lucky numbers: 04 17 26 30 34 bonus number 09, which subsequently won you the lottery in the 1st category i.e. match 6.

You have therefore been approved to claim a total sum of J1,000,000,00 (One Million Pounds) in cash credited to file ZXT/1395700117/09.

This is from a total cash prize of J10,000,000 shared amongst the (10) lucky winners in this category i.e. Match 6. All participants for the online version were selected randomly from World Wide Web sites through computer draw system and extracted from over 100,000 unions, individuals, associations, and corporate bodies that are listed online. This promotion takes place yearly.

Please note your lucky winning number falls within our European booklet representative office in Europe and your paying bank will be from our Representative as indicated in your play coupon. In view of this, your J1,000,000.00 (One Million Pounds) would be released to you by our Attorney (Bar., Steven Smith) in England upon clearance and clarification from our payment offices in Europe. Do send us your full name and contact number and you will contacted by our attorney.

Our European agent will immediately commence the process to facilitate the release of your funds as soon as you contact him. For security reasons, you are advised to keep your winning information confidential till your claims is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

Congratulations from me and members of staff of M B C LOTTERY.

Yours faithfully,

Mrs. Tracy Utter
Foreign Lottery AFF Scam

• Congrats! You’ve won a large sum of money in a foreign lottery (that you never entered)
  – But you need to send a small “transaction fee”

• You may even get a check as proof of your winnings… but the check bounces
Need a Job? Work from Home!!
Work-at-Home Scam

• Advertisers offer kits that enable home workers to make money posting links on the Internet
  – You need to pay $2 for a kit

• What often happens?

• Terms and Conditions state you authorize $80 monthly charge to bank account or credit card
Protection Strategies

• It’s unlikely an African official knows you and needs your help

• Sorry, but it’s unlikely you won a lottery you didn’t enter
  – And don’t pay fees for winning something

• Don’t pay a company to hire you

• Read the fine print
“Click Here” Scams
Why Click – Malware Goals

• Get your identity or account credentials
  – Keystroke loggers

• Get control of your PC to create a big network of “robot” computers (a botnet)
  – Viruses and worms
  – Botnets are used for spam and launching distributed denial-of-service attacks
Typical “Click Here” eMail

DHL notification

FROM: DHL
TO: irbychristen@yahoo.com

FRIDAY, MAY 27, 2011 6:44 AM

DHL Express Delivery
tracking number # 203058410

Good morning
Parcel notification

The parcel was sent your home address,
and it will arrive within 3 business days.

More information and the parcel tracking number are
attached in document below.

Thank you

DHL Express Delivery system (c)
153 James Street, Suite100, Long Beach, CA 90800

Attachments

Download All

DHL mail.zip
Variation on a Theme

UPS Express Delivery
tracking number #714611

Good morning
Parcel notification

The parcel was sent your home address.
And it will arrive within 2 business days.

More information and the parcel tracking number are
attached in document below.

Thank you.

UPS Express Delivery system (c)
Copyright © 1994-2011 United Parcel Service of America, Inc. All rights reserved.
Important "Click Here" email

UNIFORM TRAFFIC TICKET #535504

FROM: Police agency
TO: issacnjia200@yahoo.com

New York State — Department of Motor Vehicles
UNIFORM TRAFFIC TICKET

NEW YORK STATE POLICE
Local Police Code

THE PERSON DESCRIBED ABOVE IS CHARGED AS FOLLOWS

Time: 7:25 AM
Date of Offense: 07/02/2011

IN VIOLATION OF
NYS V AND T LAW

Description of Violation
SPEED OVER 55 ZONE
TO PLEAD, PRINT OUT THE ENCLOSED TICKET AND SEND IT TO TOWN COURT, CHATAM HALL, PO BOX 117

Attachments

Ticket.zip

Information Technology Services
"Connecting Phoenix to Information"
IRS notification letter

FROM: IRS Support

TO: jppain@yahoo.com, lwilke@yahoo.com, maricopa.1314@yahoo.com

Department of Treasury Internal Revenue Service

Important information about your tax return

We are unable to process your tax return

We received your tax return. However, we are unable to process the return as filed. Our records indicate that the person identified as the primary taxpayer or spouse on the tax return did not provide all the required documents shown on the tax form. Our records are based on information received from the Social Security Administration. Based on this information, the tax account for the individual has been locked.

What you need to do
Print out the attached notification and list of missing documents, fill it in, add the documents and send the following information to the address shown in the attached notification.

List of required documents:
1. A copy of this letter
2. Notification letter
3. A photocopy of valid U.S. Federal or State government issued identification.

Keep this notice for your records. If you need assistance, please don't hesitate to contact us.

Download All

Information Technology Services
"Connecting Phoenix to Information"
Wrong Transaction Scam

• A hotel made a “wrong transaction” while processing your credit card
  – Click here to get a refund

• Variant: Your recent iTunes purchase

• Yep – it installs malware on your PC
Natural Disaster / Current Event Scams

• OMG!!! Something happened and you need to know about it. Click here!!

• Takes advantage of your curiosity

• They’re fast and sophisticated
  – Barely hours after the Japan tragedies, bad guys began using emails, fake websites, and malicious downloads to try to steal money or plant malware on user systems
Examples

- “Bloody Photos of Gadhafi Death”
  - Malware BEHAV-103
- “Osama found!”
  - Malware BOBAX
- “London bomb” CNN message
  - Malware TROJ.DONBOMB.A
- “Tsunami Victim Fund”
  - Phish to get your personal information
- “Michael Jackson suicide attempt”
  - Malware VBS_PHEL.A
About Your Job Application...

• Problem: Accepting email attachments from strangers may contain malware
  – Resumes and job applications

• Example: You post on LinkedIn that you’re looking for a job
  – Scammer targets you
Scareware aka Rogue Software

• Fake security software
  – Gets you to load malicious software AND
  – Gets your personal / credit card info
Classic Protection Strategies

• Pick strong passwords
  – Easy to remember, but hard to guess or crack
• Don’t post too much information about yourself
• Use anti-virus software and keep it up to date
  – Know what your AV warnings look like
• Apply security patches immediately, including those from Adobe and other trusted sources
  – Configure your computer to apply patches automatically
  – Also update your mobile devices (smartphones, tablets…)

Information Technology Services
"Connecting Phoenix to Information"
Oooohhhh – Aaaaahhhhh
Check out the iPhone 5G!

You just got this email...

Click Here!!!
When You Click Here…

• You get redirected to download an application called *iphone5.gif.exe*
  – It’s hosted on a hacked server

• Bad guy takes control of your PC

• Malware contains this text inside it:

  “I wanna be a billionaire so frickin bad!”
You just got this email...

Click on link and go to...

---

Dear PayPal Member,

Unfortunately one of your recent transaction with PayPal is not successful because your PayPal account has been limited. It is a measure taken to protect your account and help ensure the safety of the PayPal platform. We want to help remove this limitation as soon as possible so he can continue to take advantage of the benefits of PayPal.

**How To remove the restriction**

To remove the restriction on the account, to know why and know what features are not used at the time, just 3 easy steps:

1. Click the link below.
2. Login to your PayPal Account.
3. Follow the instructions.

We apologize for the inconvenience and thank you for your cooperation,
PayPal

---

Copyright © 1999-2011 PayPal. All rights reserved. Registered office: 22-24 Boulevard Royal, L-2449, Luxembourg, ROS Luxembourg B 118 349.
Fake PayPal Website
You’ve Been Phished!

- Phishing – “Spoofed” emails and fraudulent websites designed to fool recipients into divulging personal information
- eMails look very authentic with company logos and link to authentic-looking web sites
Protection Strategies

- Check out file names
  - iPhone scam file name is `iphone5.gif.exe`
  - Note double extension!!

- Check out links – Hover your mouse over the link and look at the bottom-left corner of your browser window
  - Phish scam URL is `http://www.mittemaedchen.de/twg176/admin/www.paypal.co.uk/details.php?cmd=_login-done&login_access=1193476743`

- Enter web addresses manually and/or telephone the company using a well-publicized phone number
Before We Continue…

• I feel funny admitting this, but I’m in love with you

• I want to meet you in person – I just don’t have the money to visit you

• But I can’t wait to see you face-to-face

• And feel your arms around me

• I just wish I could afford to come to you
Romance Scams

• Bad guy/gal uses online dating or social networking sites and posts attractive picture
• Communicates and gains victim’s confidence
• Then asks for money
  – Travel expenses to meet in person
  – Medical expenses
  – Information about the fidelity of the victim’s significant other
Scammers’ Tricks

Psychology of a Scam
Scammers Craft Messages to...

• Get you to react (not act)
  – Make you think you’re heading off “impending disaster” or you’re getting a “great deal” by doing what the scammer says
  – Bypass your normal, rational thought process

• Play upon your desire to help
  – Once a person has accepted the helper role, they usually find it awkward or difficult to back off from helping

• Start small and create a “momentum of compliance” by making a series of requests, starting with innocuous ones
Scammers Prey on Our…

Ignorance

Got Lust?

Lust. It does a body good.

Greed

Goodwill
Psychological Trickery

• There are six basic tendencies of human nature that can be exploited
• We have a tendency to comply with and help
  – Authority figures
  – People we like
  – People who have already done something to help us
  – When we’ve made a verbal promise or commitment to do so
  – When the behavior seems to be supported by our peers
  – When the object being sought is in short supply, is creating competition, or is only available for a limited time
Before We Continue…

• Grandma, I’m on vacation in Canada and was in a car accident. Please wire me $3,000 to pay for medical expenses.

• I’m on vacation in London and was mugged. I can’t pay my hotel bill and they’re going to send me to jail. Please wire me $2,500 ASAP! I’ll pay you back when I get home.
Scams Come From Everywhere

- Text message received on Ilene’s cell phone October 5, 2011
You Owe Money!!

- A man telephones victim at work claiming to be from Parker and Parker law firm
- He demands that she pay $1,000 to settle a payday loan, which she never took out
- Caller is extremely aggressive, refusing to hang-up the phone when a co-worker asked that he call back at a later time
  - Caller also had the consumer’s Social Security and Drivers License numbers
Windows Service Center

• Setup: Receive phone call from a man claiming to be from Microsoft’s “Windows Service Center”
  – Caller says my computer has lots of malware on it, which is showing up at Microsoft
  – Man will clean it up for me
• Talks me through opening the Windows Event Viewer to see errors and warnings “proving” my PC needs his help
Windows Service Center

- Man’s name is “Richard Thomas”
  - Man has heavy Indian accent
- Phone number caller ID shows “011”
- Man wants me to allow him to remotely access my computer so he could “clean” my PC
- Hung up on me when I asked his phone number
  - To call back in case we got disconnected
What Would You Do?

- You get a call at work from the Help Desk
- They need your password to fix a network problem
Phone Scam Safeguards

• Don’t immediately respond

• Verify caller’s identity – Get caller’s name and (desk) phone number
  – If claiming to be an employee, look him up in employee directory
    • Does his phone number start with expected prefix?

• Call the organization / company / Help Desk and ask
  – Use the normal, published phone number

• For “family members in distress,” call family / friends to verify
Facebook Survey Scams

• Pointless surveys that make money for scammers via affiliate revenue from unscrupulous marketing firms

• Some surveys attempt to trick victims into signing up for expensive premium-rate texting subscription services

• Some surveys are just ways to gather information about you that can be used to guess your password or target you for a scam
Get More Twitter Followers

• “GET MORE FOLLOWERS MY BEST FRIENDS? I WILL FOLLOW YOU BACK IF YOU FOLLOW ME - [LINK]”
  – Just enter your Twitter username and password

• You’ve just given control of your account to someone else
  – They may then post spam or malicious updates and links, send unwanted messages, or violate other Twitter rules with your account
Shortened (Tiny) URLs

• Problem: Clicking on shortened URLs may go to a malicious site

• Example: @twitterguy, what do you think about what Obama said? http://shar.es/HNGAt
  – Scammers can choose to redirect you to any webpage they like (malicious, porn, phishing)
  – Scammers are also embedding malicious links into tweets with popular hash terms (#term)
Skimmers

- A device that reads and copies card numbers
- Data is then transferred onto cloned credit cards
- Used to withdraw cash at other ATMs or purchase goods
To Spot a Skimmer

- Skimmers are hard to identify!!
- Look for
  - Wrong colors or materials (cheap plastic vs. metal)
  - Glue or sticky spots
  - A card reader “sticking out” more than usual
- Wiggle the slot before sliding a card into an ATM slot
  - ATM slots with skimmers will appear loose, while those without skimmers will not wiggle at all
- Get to know “your” ATM
- Use ones in well lit, public places, especially with surveillance cameras around
INTERNET

It doesn't make you stupid, it just makes your stupidity more accessible to others.

Information Technology Services

"Connecting Phoenix to Information"
Internet Allows Bad Guys to Reach More Potential Victims

<table>
<thead>
<tr>
<th>Traditional Crime</th>
<th>Cyber Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burglary</td>
<td>Hacking</td>
</tr>
<tr>
<td>Deceptive callers</td>
<td>Phishing</td>
</tr>
<tr>
<td>Extortion</td>
<td>Internet extortion</td>
</tr>
<tr>
<td>Fraud</td>
<td>Internet fraud</td>
</tr>
<tr>
<td>Identity theft</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Child exploitation</td>
<td>Child exploitation</td>
</tr>
</tbody>
</table>

Information Technology Services
“Connecting Phoenix to Information”
But Wait – There’s More...

<table>
<thead>
<tr>
<th>Bullying</th>
<th>Cyber Bullying</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stalking</td>
<td>Cyber Stalking</td>
</tr>
<tr>
<td>Vandalism</td>
<td>Computer Virus</td>
</tr>
<tr>
<td>Activism</td>
<td>Hactivism</td>
</tr>
</tbody>
</table>

Greetings, Institutions of the Media.
We are Anonymous.
Internet Crime is a Problem

- Internet Crime Complaint Center (IC3) received 303,809 complaints in 2010
  - Averaging 25,317 per month

<table>
<thead>
<tr>
<th>Type</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Non-delivery Payment/Merchandise</td>
<td>14.4%</td>
</tr>
<tr>
<td>2. FBI-Related Scams</td>
<td>13.2%</td>
</tr>
<tr>
<td>3. Identity Theft</td>
<td>9.8%</td>
</tr>
<tr>
<td>4. Computer Crimes</td>
<td>9.1%</td>
</tr>
<tr>
<td>5. Miscellaneous Fraud</td>
<td>8.6%</td>
</tr>
<tr>
<td>6. Advance Fee Fraud</td>
<td>7.6%</td>
</tr>
<tr>
<td>7. Spam</td>
<td>6.9%</td>
</tr>
<tr>
<td>8. Auction Fraud</td>
<td>5.9%</td>
</tr>
<tr>
<td>9. Credit Card Fraud</td>
<td>5.3%</td>
</tr>
<tr>
<td>10. Overpayment Fraud</td>
<td>5.3%</td>
</tr>
</tbody>
</table>
Hi! My name is Heidi, and I see you have a room for rent.

I’m coming over to the U.S. for a work/study program that’s sponsored by the Swedish government. So there’s no risk of renting to me.

But I only got one check to cover both rent and travel.

So I’ll send you the check. You can deposit it, keep the rent payment, and send me the rest.
Overpayment Scam

- Bad guy sends you a check for more than the correct amount
- Rather than canceling and reissuing the check – since the scammer trusts you – you are asked to deposit the check and refund the difference
- Except the check bounces and you’re liable
Secret Shopper Scam

• Advertisers seek applicants for paid positions as “secret” shoppers
  – But you need to pay fees to purchase training materials, obtain certification, or register with a database of secret shoppers

• Updated version: You get an employment packet with a cashier’s check for about $3,000
  – Your assignment is to pose as bank customer, cash the check, and wire the funds to an address
  – Check bounces and you’re liable for the money
Before We Finish Today…

• *WARNING* *WARNING*
  GAMING FRIENDS – TAKE NOTE !!!

• This was on CNN this morning
• Do not click on a link that says it is a game for Twilight the Movie “BREAKING DAWN”
• Facebook says this is the worst virus ever!!!

• PLEASE FORWARD TO YOUR FRIENDS
Hoax

• Tell-tale hoax signs
  – Threatens dire consequences if you don’t obey
  – Promises money or prize for performing some action
  – Claims it’s not a hoax
  – Contains technical-sounding language and/or specific names and organizations to make the message seem legitimate
  – Urges you to forward the message to EVERYBODY
  – Has already been forwarded multiple times (evident from the trail of email headers in the body of the message)
Be Aware

• Be skeptical!!
• Be suspicious of sensational, upsetting, or exciting (but false) statements
  – Goal is to get you to click / react immediately without thinking
• Be wary of attachments
• Verify (and then ignore) commands and requests for action
  – Verify identity of message sender
  – Hover your mouse over the link and look at the bottom left corner of your browser window
  – Enter web addresses manually and/or telephone the company using a well-publicized phone number
Prevent Donation Fraud

• Know the organization, be sure they’re legitimate
  – Check the Better Business Bureau and other online resources
• Don’t respond to any email donation request
• Never open attached files from people or organizations you aren’t familiar with
  – Like “disaster photos” that may contain viruses
• And most importantly, use common sense
For More Information

• Anti Phishing Working Group
  – http://www.antiphishing.org/

• Internet Crime Complaint Center

• Looks too Good to be True
  – http://www.lookstooogoodtobetrue.com/

• Snopes – Hoax resource
  – www.snopes.com

• U.S. Secret Service

• U.S. Federal Trade Commission
  – http://www.ftc.gov/bcp/consumer.shtm
If You Think You’ve Been Scammed

• File a report with the City of Phoenix Police Electronic Crimes Division
  – Non-Emergency - 602-262-6151

• File a complaint with the Internet Crime Complaint Center (IC3)
  – IC3 reviews each complaint and refers it to the appropriate federal, state, local, or international law enforcement or regulatory agency

• Depending on the type of scam, you may be instructed to take more steps
Common Sense

So rare that it’s a super power.
Questions? Contact

ispo@phoenix.gov
STUPID PEOPLE RULE

without them, life would be boring

Information Technology Services
“Connecting Phoenix to Information”
Buy My Bonds

• A 52-year-old Missouri man made $100 million from selling worthless financial documents

• Used his home PC to create 2,000 “bonded promissory notes”
  – Claimed they were backed by a U.S. Treasury Department account
  – Sold them for a fee at the “Private Bank of Denny Ray Hardin,” which he ran out of his Kansas City home

• “Private Bank” owner convicted September 15, 2011 of 21 federal fraud charges (creating fictitious obligations and mail fraud)
8/29/2011 – A 22-year-old woman in South Carolina McDonald’s parking lot was approached by two men who offered her an iPad for $300
  – Claiming they had bought iPads in bulk, men showed her an actual iPad and agreed to take $180 for it

She was handed one of several FedEx boxes from their car’s trunk
  – She drove home without looking inside

When she opened the box at home, it contained “a piece of wood painted black with an Apple logo”
Verify Your Purchases

• Get names and addresses of companies
• Check with the Better Business Bureau
• Get references
• Get a warranty
• Keep any documentation (evidence)
  – Canceled checks, credit card receipts
  – Emails, chats, texts, or website screen prints
  – Pamphlets or brochures

• If it looks too good to be true, it probably is!