Identity Theft: The Dark Side of Information Technology

Deogratias Nondi

Bidyanguze Ndongwakunzila is a young man from Kigoma, Tanzania who grew up in Insungangwanda village in Nzega district where his father worked in a large mining company. Because of his incredible mathematical talents since his early childhood, his father Mzee Ndongwakunzila Matobo had big dreams about his son. He envisioned him becoming a high profile mining engineer if not a first class pilot of a major airline. So he opened a savings account at an NMBC branch in Nzega and started to save money for Bidyanguze's education since when the boy was only 5 years old; a rare culture in his country.

As expected, Bidyanguze went through the 7-4-2-4 education system in Tanzania, graduating with flying colors at each level. After graduating on top of his Chemical and Process Engineering class at University of Dar Es Salaam, a major gold mining company offered him a full scholarship to study mine processing at the University of Alberta in Edmonton Canada. So here was Bidyanguze with a CAN $ 60,000 cheque that was to cover all his expenses for his master's degree. Barrick Gold had already purchased an air ticket for him to fly to Edmonton.

After finalizing all Waha traditional send-off rituals and receiving a TSh. 5 million worth traveler`s cheque as a gift from his father's savings account, Bidyanguze boarded a plane to Edmonton to start what would be the major part of his and his family's dream. On his arrival in Edmonton he opened an account at a famous commercial bank and deposited all his cheques. Assured that the money was safe, Bidyanguze went back to Hub Mall and started reading different pamphlets he collected during his tour of the University campus. He received a few phone calls from people who introduced themselves as University employees trying to help new comers settle comfortably. They asked a few questions and Bidyanguze, knowing that this is a developed country and with his Tanzanian culture of politeness and cooperation, answered all the questions faithfully.

A month later, Bidyanguze received a note from the University informing him that his tuition fees cheque had bounced because of insufficient funds in his bank account. Convinced that the bank had made an error and that he had much more money to cover all his education than a single semester tuition fee check, he immediately went to talk to the bank manager. At the bank, a smiling bank clerk told Bidyanguze; "Sir you used all your money in the last three weeks. You paid for a new car, bought furniture and withdrew cash for the remaining amount. Only CAN$2,500 is left in your account and this was not sufficient for the cheque you wrote to the University".

Not knowing what to do, Bidyanguze called TANA president and explained what happened. The president told him that this could be a result of identity theft and that he should check with the police and the bank immediately. It was later realized that someone had impersonated Bidyanguze and went away with all the money.

We don't know whether the police or the bank could help Bidyanguze but we were informed that the university decided to suspend his studies until when he is able to pay his tuition fees and other university bills. **What a bad luck for the young Tanzanian!**

Deeply touched by what happened to Bidyanguze, the TANA president asked one of his members to write an article on identity theft on the TANA DIGEST; a monthly bulletin that carries articles on various issues in the community. And this is what went out on the TANA DIGEST:

Be Cautious: Identity Theft Is on the Rise

WHAT IS IT?

Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's identifying information for the purpose of fraud or other criminal activity. Such data may include name, date of birth, social insurance, passport, driver's license and credit cards numbers.

Identity theft is a crime that affects many Canadians by depriving them their hard earned savings, destroying their credit histories and causing stress and hatred in families. People whose identities have been stolen spend a lot of money and many valuable hours to clean up the mess identity thieves have made of their good names, relations and credit records. Victims of identity theft may lose job opportunities, be denied loans for education, housing or other important needs because of negative information on their credit records. They may even be arrested for crimes they did not commit.

WHAT CAN THIEVES DO WITH STOLEN IDENTITIES?

Credit card fraud

Identity thieves may open a new credit card account using the victim's name. When credit card bills are not paid, the delinquent account appears under the name of the victim. Criminals can also change the billing address of the victim so that the victim no longer receives bills. This allows them to use the card for a long period before the victim realizes that there is a problem.

Utilities fraud

Thieves may use the victim's name to open phony accounts and get utility services like electricity, heating, cable TV etc. using victim's name.

Financial fraud

Identity thieves may open bank account using victim's name and write bad checks, authorize electronic money transfers and drain victim's savings or they may take a loan using victim's name.

Document fraud

Thieves may file tax returns, get driver's license, identity cards or government benefits using victim's name.

Others

Other forms of fraud that identity thieves can make are getting jobs using victim's social insurance numbers, rent houses or get medical services using victim's name, and they may even give victim's name to the police during an arrest and this could lead to a warrant for arrest being issued to the identity theft victim.

INVESTIGATION COSTS

Investigating identity theft frauds is a very costly task. In the US, for example, all law enforcement organizations have reported very high investigation costs on identity theft. The executive office of the United States attorneys estimates the cost of prosecuting a white-color crime case is $11,443. The Secret Service estimates the average cost per financial crime investigation is $15,000, while the FBI estimates the average cost per financial crime investigation is $20,000. Since most of the fraud resulting from identity theft lead to financial crimes of some sort, the numbers above should be a good indicator of how costly this crime could be.

HOW DOES IT OCCUR?

Phishing

A phishing attack occurs when an offender seeks to obtain Personally Identifiable Information (PII) or other sensitive information like user names, passwords, credit card information, date of birth etc, from an individual in order to commit fraud by masquerading as a trustworthy person or organization in an official communication, such as an email, instant messaging or social networking tools like FaceBook, MySpace, YouTube, etc.

Pharming

Using pharming methods, a hacker can impersonate a legitimate website so that he can redirect users to a fraudulent site. Differences between the legitimate site and the imposter site are easy to overlook as a fraud. Therefore users of the website (online shopping for example) would believe that they are sending financial information (credit or debit card) to a legitimate entity while actually it goes to a criminal. Pharming is normally accomplished through emails where a user would receive an email with a link to what looks like a genuine website. Most of the time emails would appear as originating from a well known source to the intended target. Clicking on this link directs a user to a fraudulent website.

Hacking, Cracking

The hacking or cracking identity theft occurs when an offender gains unauthorized access to a victim's computer or online account. Advancement in technology has enabled criminals to easily get access to victim's system through the Internet especially when victims' systems are not properly secured or updated.

Spyware, Worms, and Keyloggers

Spyware, computer worms, and keyloggers are all examples of malicious applications that can be installed on an individual's computer in order to collect sensitive information and send it back to the identity thief. An identity thief will most likely use phishing or another identity theft tactic in order to coax the victim into unknowingly installing the malicious program. Malicious applications have also been found in popup advertisements and can be designed to look like a trusted application.

Scripted VoIP Attacks

VoIP attacks exploit the voice over internet protocol (VoIP) which allows users to talk on the phone using their internet connection. Offenders use special techniques to hack one of the protocols (rules) used to implement VoIP. Once the offender obtains control of the connection, he or she can eavesdrop on phone conversations and record PII in order to commit identity theft. Due to the increased use of VoIP, it is expected that VoIP attacks will gain popularity in the near future.

ATM Skimming

ATM skimming involves the identity thief obtaining PII from bank consumers who use an ATM machine in order to commit identity theft. The offender would use a device called an ATM skimmer, which can be installed directly on the ATM. Consumers will use the ATM without noticing the device and PII will be read off the ATM cards and sent to the identity thief.

Social Engineering

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or internet to trick a person into revealing sensitive information or getting them to do something that would let the social engineer obtain sensitive information.

Dumpster Diving

Personal information found in the trash may be used to steal sensitive information.

Shoulder Surfing

Simply looking over someone's shoulder when using an ATM or paying for groceries by debit card at the supermarket or gas station can yield sensitive information like user ID, passwords, and other confidential data. Therefore, protect your PIN when making these transactions.

Other Methods

Stealing and misappropriating information media (DCs, DVDs, thumb drives etc), recovering used and discarded computer hard drives, and stealing laptop computers can all lead to identity theft.

How can you protect yourself against Identity Theft?

The following practices can help you avoid identity theft:

- **Shred** financial documents and paperwork with personal information before you discard them.
- **Protect** your Social Insurance Number. Don't carry your Social Insurance card in your wallet or write your Social Insurance number on a check. Give it out only if absolutely necessary or ask to use another piece of identification.
- **Don't give out** personal information on the phone, through the mail, or over the Internet unless you absolutely know who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date.
- **Don't use** an obvious password like your birth date, your mother's maiden name, or last four digits of your Social Insurance Number, your phone number or your address.
- **Keep** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.
- **Pay attention to signs that require immediate action** like bills that do not arrive as expected, unexpected credit cards or account statements, denials of credit for no apparent reason, calls or letters about purchases you did not make
- **Inspect your credit report.** Credit reports contain information about you, including what accounts you have and your bill paying history.
- **Inspect your financial statements.** Review financial accounts and billing statements regularly, looking for transactions you did not make.

What should you do if you fall victim?

In case your identity is stolen or you suspect that it has been stolen, do the following:

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The two major credit reporting companies have toll free numbers that you can call for help (**Equifax: 1-800-278-0278** and **TransUnion: 1-800-663-9980**).
- **Close accounts.** Close accounts that have been tampered with or established fraudulently. Call the security or fraud departments of each company where an account was opened or changed without your consent. Follow up in writing, with copies of supporting documents.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.

In conclusion

Criminals believe that Identity Theft is a safe crime as it does not involve much physical work. It is therefore very hard for a criminal to be identified while at the same time the payoff is huge. They see this as a great opportunity and most criminals are likely to shift from other crimes to identity theft. Research has shown that Identity Theft is becoming an organize crime and it is expected to grow fast throughout the world. Watch out!

At this time of the year when all Canadians are filing tax returns and when the world economy is struggling, be sure to report any fraudulent activities you notice as they can happen to anyone not just Bidyanguze. **Be cautious!**

Biological Errors, Ignorance and Failure of Common Sense

Deogratias Rweyongeza

In light of recent killings and commercial exploitation of Albinos in Tanzania, it is time to explore the underlying reasons for such barbaric acts. Killing of Albinos and trade in their body parts in Tanzania has appeared in many news outlets (radios, televisions and websites) in North America and Europe. The Tanzanian government is seen as being either slow in confronting the problem or even reluctant to prosecute the perpetrators.

I once read in one of the Tanzanian internet newspapers the argument by the University of Dar Es Salaam law professor that the government was reluctant to prosecute Albino killers and those who buy their body parts because the government does not believe in the existence of witchcraft. Thus, to be able to prosecute witchcraft related crimes, the government would first have to recognize the existence of witchcraft and designate witchcraft a crime. In a different news article, Jenerali Ulimwengu argues that the government is reluctant to prosecute Albino killers because politicians and some bureaucrats consult mediums before contesting for their positions or making crucial decisions. If Mr. Ulimwengu's argument is true, the Tanzanian government is reluctant to prosecute Albino killers for two reasons, that is, fear for revenge attacks from witches, and cutting off its own pool of experts (Mr. Ulimwengu call them *Fundis* or technicians) from which

the government supposedly owes its existence. If both the University of Dar Es Salaam law professor and Mr. Ulimwengu's arguments are true, then the actions of the government of Tanzania to stop Albino killings would only be limited to pretending to act hopping that condemnation from the international community will eventually go away, or the country will eventually run out of Albinos and the killings automatically stop. As part of its efforts to stop Albino killings, the government of Tanzania has recently asked the public throughout the country to secretly name witches involved in Albino medicine and their customers. However, in a country where politicians and the public are supposedly fearful of witches, it is inconceivable that such a measure would succeed, since those witches to be named would presumably know those who secretly name them by some form of remote control.

The tragedy of Albinos in Tanzania is the intersection of a biological error, public ignorance and failure of common sense by the public and government. Albinism is a mutation whereby a child inherits an error in a gene responsible with production of normal human skin colour. The normal human skin colours are white for *Caucasians* or *Caucasoids*, which include all native people of Europe, Western Asia and Arabs; dark for *Negloids*, which are native people of the Sub-Saharan part of Africa (also called blacks in North America) and the so called yellow for *Mongoloids*, which are native people of East Asia and native people of the Americas (also called Orientals). Because of the racial nature of these anthropological classifications and the racist epithets derived from them, I would advise you not to use them in your daily vocabulary.

Albinism is a result of a gene mutation whereby an individual is unable to produce the enzyme *tyrosinase* that metabolize the amino acid *tyrosine* to produce *melanin*, which is a natural biological chemical responsible with production of normal skin, eye and hair colour in humans and other animals. Because the genetic language of character determination and regulation from DNA, through gene, amino acids, proteins, enzymes and hormones is universal among organisms, Albinos exists in humans, domestic and wild animals, and plants. Therefore, like all other Albinos, human Albinos including those in Tanzania are products of an inborn error of metabolism, and there is nothing mystic about them and their body parts.

The scientific cause of Albinism is easy to explain to educated minds and to uneducated minds inclined to despise primitive beliefs. To many Tanzanians, especially those closest to the lowest margins of wealth, education, monotheistic faith, and civilization, the act of being Albino is translated as being white from black parents. As impossible as this might be, it engenders a possibility for procession of a unique and probably mystical power through which difficulties of daily life can be solved.

Ignorance is a state of being uninformed about something. It follows that each of us has a form of ignorance for things we are not trained of, things we have never seen or heard of, places we have never been, equipment we have never operated, food we have never eaten, religions we have never been part of, emotional experience of a person of a different gender, and many more. However, ignorance is not a justification for committing horrible actions such as killing someone because of the way he looks like or he/she appears to be unique among many. Therefore, it appears that there are some thresholds of common sense within which our ignorance of things cannot be excused. At some levels of our human existence, we owe it to ourselves to acquire basic understanding of what we have not been trained to know.

Here I define common sense as that level of deductive thinking merely from what is considered practical. We can expect that if any part of an Albino body was a source of wealth and luck, Albinos who already own those parts would be the richer and luckier than normal coloured individuals who buy those parts. We can also argue that if witchdoctors have power to create wealth and help someone attains political and professional success, they would be rich and successful before they can help someone else. Here we see the failure of common sense in part of those who buy Albino body parts at the advice of witchdoctors.

There is also a failure of common sense in part of the government of Tanzania when it comes to stopping Albino killings. If the argument by the University of Dar Es Salaam law professor that the government has to accept that witchcraft exist before prosecuting witches and their customers is true, witches can be prosecuted through indirect means. Many countries and I presume including Tanzania have laws that prohibit hate crimes. Racial, ethnic and religious incitements that potentially endanger individuals or groups of citizens are normally prosecuted and punished. There is no situation that meets this threshold than the killing of Albinos for commercial purpose in a country like Tanzania.

Stopping Albino killing in Tanzania needs to be approached differently from other primitive acts that Tanzania fought against after independence. Unlike the campaign to educating people in some parts of the country to use toilets instead of bushes, killing of Albinos need a strong hand where force is first and education second. Here, protecting lives is primary and educating the public in second. Because killing of Albinos is part of the large problem of witchcraft, all witchdoctors regardless of their pseudo-medical specialization should be persecuted through controlled intimidation, denial of

access to public facilities and public humiliation. Although there is no documented data in Tanzania, it is obvious that in parts of the country where the belief in witchcraft is rampant, levels of education, civilization, and material development are low. Therefore, witchcraft is bad for the overall development of Tanzania.

The act of politicians and professional to consult mediums in search of success is very reprehensible. It is also a testimony that education alone cannot defeat witchcraft in the country. The cause of such a problem is partly a need for quick fix of problems that only need hard work, and lack of connection between hard work and material success. Again this calls for defeating witchcraft by outlawing witchdoctors in the first place.

Congratulations

Congratulations to Dr. Louise Rolingher for completing her graduate studies at the University of Alberta. Louise did her research in Zanzibar and has been a very productive member of TANA and she and her family are active participants at most of TANA events.

Contact Information

Deogratias Rweyongeza (President): Tel.

780-293-2234, Email: drweyongeza@shaw.ca

Deogratias Nondi (Secretary General): Tel. 780-905-6334, Email: dgratius@hotmail.com

Jane Moshi (Treasurer): Tel. 780-479-2236, Email: jmoshi@ualberta.ca

Jesca Rushubirwa (Secretary, TANA Women Group), Tel. 780-433-6005, Email: jescarushu@gmail.com

Editorial and Submission of Articles

Email: drweyongeza@shaw.ca