Financial
Intelligence Centre

TYPOLOGIES

SEPTEMBER 2018

CONTENTS

INTRODUCTION.....2

1. CYBERCRIME AND RANSOMWARE ATTACKS 3
2. COURIER SERVICE SCAMS 4
3. SOUTH AFRICAN INHERITANCE FRAUD 6
4. FOREIGN EXCHANGE FRAUD 7
5. FAKE ON-LINE SHOPPING STORES 8
6. ONLINE GAMING FRAUD.....9
7. KIDNEY DONOR CHARITY SCAM 10
8. CRYPTOCURRENCY BASED INVESTMENT AND PONZI SCHEMES.....11
9. FAKE JOB SCAMS.....13

INTRODUCTION

ABOUT THE FIC

The Financial Intelligence Centre (FIC) was established in 2003 as South Africa's National Centre for the gathering and analysis of financial data.

The FIC'S primary role is to identify the proceeds of crime, combat money laundering and terror financing. In this way, the FIC contributes to safeguarding the integrity of South Africa's financial system and its institutions.

ABOUT THIS BOOKLET

Using actual case studies, we provide insight on some of the methods criminals use to abuse the financial system.

1. CYBERCRIME AND RANSOMWARE ATTACKS

HOW IT WORKS

Internet users constantly face the prospect of cybercrime attacks. And, cybercrime will continue to surge due to easy-to-use online tools combined with a low threshold of technical knowledge required for criminals to deploy and use ransomware to conduct these crimes.

Ransomware is increasingly posing a risk to internet consumers, business and organisations.

Criminals send Trojan horse virus programmes via e-mail in the form of an attachment or link. These programmes are disguised as legitimate files. Once opened, the ransomware will launch when the user downloads or opens the file. The user is then threatened with the online publication of his/her data or is denied access to their computer files unless a ransom is paid. In most instances, the criminals demand digital currencies as ransom, making it difficult to identify, trace or prosecute the perpetrators.

Apart from personal computers, ransomware perpetrators are now beginning to target mobile device operating systems. Recovering data without a decryption key is very difficult and can sometimes prove impossible.

THREATS TO THE PUBLIC

- Loss of valuable data
- Organisational and personal reputational damage
- Impaired economic/business activity
- Eroded public confidence
- If a victim pays a ransom for the release of the data, criminals could reactivate hidden encryption programmes on the victim's system for further ransom money.

WHAT YOU NEED TO DO

- ☑ It is essential that individuals enhance their awareness, education and training regarding cybersecurity
- ☑ Keeping regular "offline" backups of data stored in locations inaccessible from any potentially infected systems on external storage drives will counter these attacks.
- ☑ Victims should report such incidents to the Cybersecurity Hub of South Africa which strives to secure the internet where all residents in South Africa can communicate safely, socialise, and conduct business in confidence. To contact the hub, visit: https://www.cybersecurityhub.gov.za

2. COURIER SERVICE SCAMS

HOW IT WORKS

Criminals are known to establish internet infrastructures by registering authentic looking domain names purporting to be international couriers. These criminals then create and use “sock-puppet” accounts on social media and singles dating websites to target victims.

A “sock-puppet” is an online identity used for purposes of deception or a false identity assumed by criminal gangs about themselves while pretending to be another person. They use their “sock-puppet” accounts mainly to contact and target single women and win their trust by establishing an online friendship. They obtain personal details, whereabouts and personal interests of their target over time. Based on trusted relationships, they also have access to social media accounts and photos of their victims and associates. Operators of these “sock-puppet” accounts promise their victims that “trusted” international courier services will deliver high value goods (for example jewellery, handbags, cell phones or laptops) as gifts.

In the meantime, the same gang members also register website domain names for courier services. Although these webpages look authentic, the credentials and referrals used on these webpages are fake. Criminals use the “services” of these fake courier services to give credibility to false promises made regarding the delivery of these non-existing goods to their targeted victims. Victims then receive telephone calls and e-mail messages from these fake courier services to pay “clearance” and “delivery” fees for the parcel. Sceptical about the fee, victims call their “sock-puppet” account holder for reassurance. The “sock-puppet” account holder will feint surprise when contacted, that a fee is requested to release the parcel. The victim will be reassured with promises that money paid will be refunded. After making the payment, the victim receive frantic calls from these fake couriers informing them that the South African Revenue Service has identified foreign currency in the parcel, and that the National Treasury has been notified of this. Official looking documentation from the Revenue Service and National Treasury are sent to victims demanding further payment before they can release the parcel. As part of the fraudulent activities, these couriers also claim that South African custom officials will arrest their “delivery agents/staff” if they do not pay “custom fees”. These claims force victims to pay additional fees.

Victims also receive requests for the payment of a fine and insurance money to release these “parcel”. Should victims fail to pay these fees, they will receive telephone calls and letters of demand from non-existing attorneys. Payment requests continue until these criminals have extorted as much money as they can from victims.

THREATS TO THE PUBLIC

- Financial loss
- Impaired credit rating
- Due to embarrassment victims are often reluctant to report scams to the authorities and this assists in perpetuating these scams.
- Criminals use the victim's identity, personal details, photos, documents, banking information and other social preferences to conduct further financial crimes.

WHAT YOU NEED TO DO

☑ Internet users should always try to protect themselves. Never send money to someone you have not met or know in person.

☑ Be cautious when sharing personal pictures or videos with online acquaintances, especially before having met them in person. These criminals blackmail their targets using compromising material.

☑ Never send money or provide credit card details, online account details or copies of personal documents to anyone you have not met.

☑ Remember, SARS and the National Treasury will never ask anyone to pay money into a personal bank account or via a money transfer service.

☑ Government institutions will not request anyone to complete their personal information on forms via e-mail messages.

☑ People who receive notice of a parcel delivery should request a copy of the courier waybill. Verify the courier company details reflected in the waybill before making any payment.

☑ Internet users who suspects that they have provided their bank account details to scammers should contact their financial institution immediately.

☑ Victims who suffered financial loss can report the matter to the South African Police Service.

3. SOUTH AFRICAN INHERITANCE FRAUD

HOW IT WORKS

Criminals contact their victims via e-mail, text messages or social media messages. They inform their victims that they can claim a large inheritance from, for example, a wealthy South African couple who are about to die from cancer in a hospital in Asia. Fraudsters then distribute falsified South African identity documents of fictitious people to potential victims claiming that they have left a large sum of money with the United Nations. The United Nations' Foreign Exchange Unit will then apparently release the funds to the targeted victim based on a (non-existing) ruling by the North Gauteng High Court, Pretoria.

These criminals then pose as lawyers, bankers and government officials indicating that, for example, the Ferreira family died and left no beneficiaries to victims who respond to these messages. Victims receive official looking identification documents, banking details of the deceased and other documents claiming that they are legally entitled to claim the inheritance. The criminals posing as lawyers inform the victim that they will start the claims procedures on behalf of the victim. Procedures by these criminals include the introduction of a second and third person posing as so-called tax-agents or bankers to assist in facilitating the legal and financial aspects of the transaction. Victims are instructed to make advance payment to facilitate the release of the funds. As part of the criminals' deception, they collect personal information of their victims in order to perpetrate other financial crimes.

THREATS TO THE PUBLIC

- Financial loss
- Identity theft
- Due to embarrassment victims are often reluctant to report scams to the authorities and this assists in perpetuating these scams.

WHAT YOU NEED TO DO

- ☑ Internet users should avoid any arrangements with strangers that ask for up-front payments through money orders, international fund transfers, pre-loaded card or crypto-currencies such as Bitcoin.
- ☑ Victims who provided any personal account details, identification numbers, personal information or addresses to fraudsters should contact their financial institution immediately.
- ☑ Notify the South African Police Service of financial losses suffered, to initiate possible investigations.

4. FOREIGN EXCHANGE FRAUD

HOW IT WORKS

Opportunists exploit economic hardship and advertise non-existent jobs on the internet. These criminals will claim that they will teach people how to make their fortunes. Conferences and training seminars are organised with well-dressed speakers. These speakers try to impress attendees with their expensive lifestyle and posh vehicles. Speakers try to convince attendees to invest in a once in a lifetime opportunity to make large amounts of money.

Attendees are encouraged to, for example, invest in a software solution which is supposedly able to predict foreign currency fluctuations. The potential success rate associated with using this software is grossly overstated to the potential victims of the scam. Victims are further pressured into making additional payments for follow-up seminars and training sessions. This comes with the promise of maximising supposed profits.

Fraudulent activities include:

- Strategies of executing trades for an investment account to generate commission from the account
- Selling overstated software that is supposed to guide the customer to large profits
- Harmful business practices
- False advertising
- Ponzi schemes and fraud.

THREATS TO THE PUBLIC

- The software solutions offered by these organised criminal groups hardly ever yield the desired results and in some instances have been known to completely deplete accounts within a few days of trading.

- It has also been found that the owners of this software were linked to other discredited software. It would appear as if they have been relaunching their failed service in another country or using other methods.

WHAT YOU NEED TO DO

☑ Trading foreign currencies can be a challenging and potentially profitable opportunity for investors. However, before deciding to participate in the foreign exchange market, one should carefully consider personal investment objectives, level of experience, and willingness to participate in high financial risks.

☑ Most importantly, do not invest money one cannot afford to lose.

☑ Inexperienced or new foreign exchange traders should cautious not to utilise the trading platforms of unknown and unverified financial service providers.

☑ The old adage always applies, if the returns sound too good to be true it probably is.

5. FAKE ON-LINE SHOPPING STORES

HOW IT WORKS

Internet based fraudsters create and use fake retail websites to advertise goods at low prices. Usually these websites offer clothing, electronics, jewellery, etc. to internet users. Although a sophisticated design and shopping cart may contribute to the website's legitimate appearance, the payment process will be suspect.

Scammers often ask for payment via money order/transfer and do not use secure online payment systems. Legitimate vendors will never discount a price excessively.

THREATS TO THE PUBLIC

- Internet consumers order these deflated priced goods online, but never receive any products.
- Victims surrender personal information and banking information by completing authentic looking online forms at these fake websites.
- This leads to financial loss and identity theft, used by criminals to conduct other financial crimes using the stolen identity.

WHAT YOU NEED TO DO

- ☑ Always check these online stores and their websites for unusual grammatical inconsistencies. Commonly, fake websites will be produced in countries where English is not the most common spoken language. Do not trust online shopping websites with spelling and grammatical errors.
- ☑ Double-check the legitimacy of a business before dealing with them. Where possible, only conduct business with local online shopping brands. Search the website of the Companies and Intellectual Property Commission to check whether a company is registered. Visit the CIPC website on: http://www.cipc.co.za/products_services/name_search.asp
- ☑ Beware of websites that do not list their company details and contacts:
  - Verify all published details
  - Contact telephone numbers
  - Physical location and
  - E-mail addresses.
- ☑ Change all passwords immediately once you suspect that a website is not trustworthy.
- ☑ Victims should notify their bank immediately of the transaction.

6. ONLINE GAMING FRAUD

HOW IT WORKS

Virtual, online role-playing games are popular ways to connect and play with other participants across the world.

To secure a competitive advantage at these role-playing games, players need to purchase virtual items for their online gaming characters. This can include virtual items such as clothing, tokens, special abilities, weapons or even protective gear. Players invest extensively in these virtual items for their online games. Both player characters and non-player characters populate Massively Multiplayer Online Role-playing Games (MMORPGs). Interactions between people around the globe are crucial to the player's experience.

Well organised and technology savvy criminals exploit gamers who simply want to be the best at their chosen games. These criminals masquerade as players in the universe of MMORPGs and approach player characters offering to sell them virtual items that would ensure their success in a particular online game.

In many instances criminals set up websites as shop fronts to get the attention of gamers looking to purchase in-game currency and other virtual items with real world cash. By investing in in-game currency, players are able to obtain items they usually would have to play (farm) for days or even weeks. These activities can also be used to fund other illegal cybercrime activities.

THREATS TO GAMERS

- Financial loss. MMORPGs are so popular that people sell game items (virtual, non-tangible items, such as armour, weapons, rare battle equipment, etc.) online for real money.
- No case will be opened. If consumers lose money or virtual items during fraudulent transactions, investigative authorities will be reluctant to deploy resources for investigations of this nature. South African legislation only caters for tangible objects and not for virtual items lost during fraudulent transactions.
- Reputational risk.

WHAT YOU NEED TO DO

- ☑ Passwords used for gaming should not reveal any personal information and should be very difficult to crack.
- ☑ Always use strong security software. Keep firewall software turned on at all times.
- ☑ Consumers should purchase virtual items from reliable in-game sources, and not from unknown individuals.
- ☑ Do not download files from unknown sources.
- ☑ Do not share personal information with other players. Young children are prone to share personal information and parents should be vigilant to this behaviour.
- ☑ Parents must evaluate all games before allowing children to play these online games and monitor participation of children during online gaming.

7. KIDNEY DONOR CHARITY SCAM

HOW IT WORKS

Organised internet based criminals recruit bank account holders in several countries to receive funds generated from advanced fee fraud and fraudulent organ transplant schemes on their behalf. These criminals create anonymous e-mail accounts in different countries that are difficult for law enforcement to track down to identify the real subscribers. They then use these anonymous e-mail accounts as fictitious identities to create small advertisements and/or websites to promote the purchase of kidneys from victims desperate or in dire need for money.

The actual collection/harvesting of kidneys never occurs. Internet users who fall victim to these schemes never receive any payment. Instead, they pay money to criminals for promises and/or services that never materialise.

Criminals avoid any physical meetings or contact with their victims. They conduct all financial arrangements with victims by e-mail correspondence. This contributes to their anonymity preventing law enforcement from identifying them or their location.

THREATS TO THE PUBLIC

- Criminals exploit the opportunity to create an illusion of a patient waiting for a kidney, knowing that there is a worldwide shortage of transplantable organs. This increases the desperate victim's expectation of receiving a large sum of money for harvesting their kidney.
- Instead, the victim has to pay for non-existing administration fees, travel fees and services that never materialise.
- This leads to financial loss.

WHAT YOU NEED TO DO

- ☑ Organ donations in South Africa are done for altruistic reasons. Donors donate their organs out of free will with no expectation of monetary compensation.
- ☑ Internet users should avoid any arrangements with strangers offering to provide an organ matching service to supposed patients abroad. E-mail messages of this nature should be ignored and deleted immediately.
- ☑ Victims who provided any personal account details, identification, personal information or addresses to fraudsters should contact their financial institutions immediately.
- ☑ Notify the South African Police Service of financial losses suffered, to initiate possible investigations.

8. CRYPTOCURRENCY BASED INVESTMENT AND PONZI SCHEMES

HOW IT WORKS

Cryptocurrencies are decentralised global currencies and digital payment platforms. These systems operate as peer-to-peer networks, where users conduct transactions without any intermediaries. Network nodes verify these transactions and record such transactions in a public distribution ledger on the internet, known as the block chain.

Criminals register internet domain names, associated with multi-level international investment or Ponzi schemes. Internet Service Providers (ISPs) outside the jurisdiction of South Africa host or facilitate most domains linked to Ponzi schemes that promote trade with cryptocurrency. Ponzi schemes are fraudulent systems that require people to invest in them with a promise to make large profits in return. They require their investors to advertise their systems as a way of making more money. Local organisers and participants strictly trade with cryptocurrencies to evade detection by authorities, financial institutions and law enforcement agencies.

These Ponzi schemes are very hard to identify because they often appear to be legitimate businesses. Only the first few internet users who join will benefit from such a scheme.

Newly recruited investors encourage their family and friends to join the scheme. Once exposed, organisers vanish, taking with them all the money of their investors.

In other instances, organisers pretend to offer cryptocurrency exchange services. The victim is promised that after paying an initial contributing fee, their investment will double within a short time. These fraudsters succeed because they are able to broadcast their activities to many unsuspecting people through social media. They widely advertise their services and manage convince a broad spectrum of victims to participate in their scheme. Organisers require small investments from their victims to entice them to make bigger deposits in the future. Once victims invest large amounts of digital assets, criminals steal their investor's cryptocurrency.

THREATS TO THE PUBLIC

- Cryptocurrency transactions are irreversible once confirmed via the block chain. Unlike credit cards, which can often recover money lost through fraud, these transactions lack consumer protection against fraud.
- It is very difficult to regulate the use of cryptocurrencies and to assist users to avoid these harmful financial practises or schemes. It is important to note that cryptocurrencies by their nature are decentralised and self-regulatory.

WHAT YOU NEED TO DO

- ☑ It is very difficult for authorities to trace cryptocurrency once it leaves the owner's cryptocurrency wallet. This is why most cyber criminals prefer using cryptocurrency-based Ponzi schemes and related fraud. Consumers should not easily trust online dealers who promise to provide any cryptocurrency services without establishing their identity.
- ☑ Internet users must avoid all schemes that promise to make them rich within a short time period. These schemes will invariably result in financial loss to the consumer and other associates participating in the scheme.
- ☑ Internet users should avoid cryptocurrency exchanges with hidden identities.
- ☑ Consumers should conduct business only with legitimate, reputable and registered investment brokers.
- ☑ Where possible, investors should research sites well before they invest in cryptocurrencies. It is important to identify reputable cryptocurrency exchanges and research their history of users before conducting any transactions. This will help users to distinguish between those who are genuine and those who are not.

9. FAKE JOB SCAMS

HOW IT WORKS

Criminals target South African internet users with promises of lucrative career opportunities or job listings abroad. The perpetrators of these scams offer employment and jobs on the internet that do not exist. Usually, these career listings target young people with higher-level qualifications. At first glance these online postings appear to be completely legitimate. The perpetrators prey on unsuspecting job seekers desperate to find better employment opportunities abroad.

Internet-based criminals use a fabricated career or job listing as a ruse to attract employment seekers and obtain their personal information. Such information includes identity numbers, credit card information, bank account information and the curriculum vitae of the victim.

Once a prospective victim has made contact via the fake online job listing, criminals notify them that a position abroad has become available. They then conduct a telephonic, Skype or instant message job interview. These interviews contribute to the illusion that the job offering is real. Applicants receive notices that their qualifications have been accepted and that their interview has been successful. The victims are responsible for the cost of the supposed required background checks and credit score ratings after the interview. Victims are also responsible for their own travel costs and visa applications to the relevant foreign jurisdictions.

THREATS TO THE PUBLIC

- Internet Service Providers (ISPs) do not control the content on web pages published from their web services. They will only react and facilitate the removal of fraudulent content, based on complaints received from victims. ISPs will then contact the fraudsters (their clients) to remove the content. However, this does not remove the threat since fraudsters will only move their scam to the next ISP.

- Criminals use personal information provided by victims to perpetrate other impersonation fraud schemes. Criminals disappear with money provided to them for credit checks and background checks.

- Upon reaching their destination, criminals discontinue further communication with their victims. Authorities abroad treat these stranded victims as illegal immigrants and detain them.

- Victims can suffer financial loss due to having resigned their current position in order to take up the advertised position.

- Possible financial loss due to identity theft.

WHAT YOU NEED TO DO

- ☑ It is difficult to distinguish between fraudulent and legitimate employment offerings. If victims believe that they have encountered a website designed to look like a legitimate website to steal personal information, they can report the matter to the Internet Service Providers Association in South Africa. Visit their site on: http://cybercrime.org.za/docs/Advisory_on_Reporting_Cybercrimes_April_2013.pdf
- ☑ Potential job seekers must conduct thorough research on the company or organisation in the country they wish to work.
- ☑ Making contact with the resident diplomatic mission of the country in South Africa would be a good way to verify the procedures and conditions of employment in the host country.
- ☑ Keep in mind that foreign countries have strict policies when hiring foreigners. Work seekers must familiarise them with the average salary, working hours and visa requirements. Offerings that double an average salary for half the working hours should be considered suspicious.
- ☑ Always check on internet for blacklists or articles on the prospective employer, business or organisation. Search for websites, telephone numbers and e-mail addresses of the prospective employer. Be aware that criminals will use a posting or advertisement, using the name of a reputable and well known company or organisation. Check the e-mail address of correspondence received, against the domain of the company or organisation. Reputable companies or organisations publish their e-mail addresses on their official websites, matching their domain names. Always refrain from corresponding with a recruiter who uses an anonymous e-mail or free mail service.
- ☑ Avoid sending money to recruiters before arriving in the foreign country for work. Be wary of requests for cash payments via international money remittance service providers in exchange for securing an offer of employment.
- ☑ Report any financial loss to the South African Police Service to initiate a criminal investigation.

Making South Africa's

Financial System Intolerant to Abuse

T +27(0)12 641 6000

F +27(0)12 641 6215

www.fic.gov.za