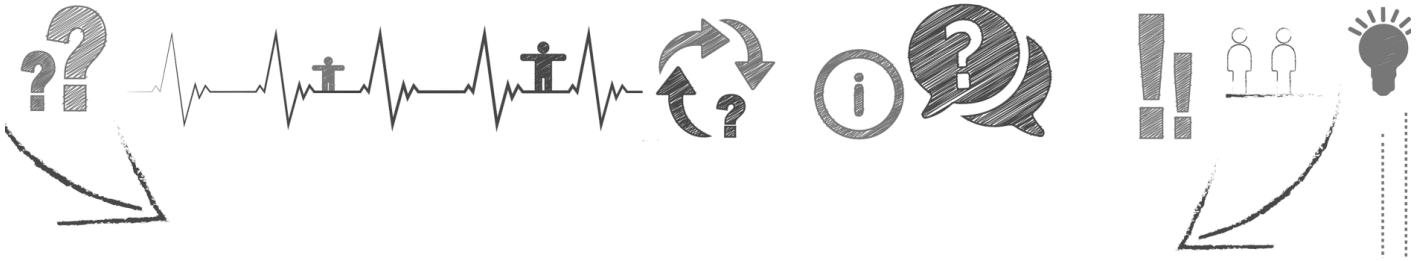
Financial
Intelligence Centre

ONLINE
SCAMS



CONTENTS

INTRODUCTION

The Financial Intelligence Centre is committed to increase the utilisation of financial intelligence using a variety of methods – including creating awareness on scams – in an effort to enhance the intolerance of the abuse of South Africa's financial system.

This public awareness document provides information to assist the reader against becoming a victim of cybercrime. As much as people use cyber technology for honest work and play, there are cyber criminals doing the opposite. The evolution of cyber technology has also increased the risk of business and ordinary citizens alike being exploited by those involved in cybercrime.

POPULARITY OF SCAMS

Why are scams via cyber networks increasingly such a popular modus operandi for criminals? There are manifold reasons including but not limited to:

ANONYMITY – Criminals can operate virtually anonymously accessing their victim's business and/or private information. From the victim's perspective it may be difficult to tell whether an e-mail pleading for funds to aid families dying of starvation in an earthquake struck region is genuine or not.

DATA IMPROVEMENT – Continuous improvement in data and information analysis is a boost for criminals. Gathering information and drawing analysis helps criminals build profiles on the movements, worth, value and status of their target.

TACTICAL ADAPTABILITY – Using cybercrime, criminals are able to adapt and plug into their target's desires like instant wealth, helping those in need, economic and social freedom and so on. Typical examples will be during the holiday season where criminals will run holiday scams. During floods and other national disasters, they will use these ordeals to skim off their monies. Legitimate charities to end child labour; curb animal mistreatment; support victims of war and others are easily misguided.

EASE OF ACCESS – As technology evolves and improves the lives of users, it also paves the way for criminals. Transnational financial transactions, for example, has made international banking commonplace and increased trade across continents. It has eased the possibility of illicit money moving more easily between jurisdictions.

GEOGRAPHICAL ADVANTAGE – Technology allows criminals to create domains in one country, operate in another and target victims in a third. This while law enforcement agencies and/or courts of law often have limited jurisdiction over cross-border cybercrimes.

STAY INFORMED & BE ALERT

The best approach to protect yourself.

Cyber criminals want to obtain your identity number, your bank account details, your PIN (personal identity number), passwords and/or any other particulars that will give them access to further information on you, on your bank account(s), access to your current or potential earnings, to that of your family if possible, to the grant or pension money you receive, to any other information or details on you which would tell them more about you.

It is vital that you remain alert and protect your private and personal information from anyone seeking to use your information for criminal purposes.

WHAT YOU CAN DO

PRACTICAL STEPS

- **PERSONAL DETAILS** – Do not provide your personal details unless you are absolutely sure that the person/organisation/business/retailer/bank/website etc. asking for it is genuine and that they have a legitimate reason for asking the information requested. If you have any doubts, do not answer any questions and shut off contact.
- **DO NOT BE SWAYED** – Cyber criminals can be charming, persuasive, convincing, and making you believe that if you do not take action immediately you will lose a fortune. Remember, if what anyone is saying sounds too good to be true it is most likely not true. This includes that a donation to a person or a cause will secure a special reward from a long lost love, an ancestor, a religious leader or a spiritual healer.
- **SHORTCUT TO WEALTH?** – It is unlikely that a stranger whom you have never heard of, never contacted or never come across before in your life would consider giving or offering you considerable wealth. Should they make direct or indirect contact with you, and if you choose to listen to them, listen with a great deal of scepticism. You are unlikely to become wealthy from the contact; more likely they will be benefiting from your intentions.
- **EVERYONE IS FAIR GAME** – When they seek out their victims, criminals do not distinguish between educated/uneducated, employed/unemployed, poor/rich, old/young, healthy/sick. Do not believe they will never target you. Remain cautious, alert and wary – it is your best protection.

This booklet touches on some cybercrime case studies to help you understand how these incidents can occur, how the criminals operate and how you can protect yourself against these scams.

MOBILE APPLICATIONS

HIDDEN MALWARE

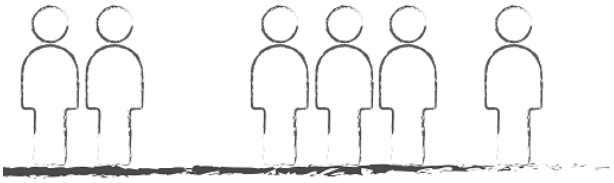
Smartphone users receive SMSs containing hyperlinks directing them to malicious websites. Once they click on the hyperlink they are redirected to websites containing malicious software created by cyber criminals. Unwittingly, users download this software when they click on the hyperlinks on their smartphone. This enables the cyber criminals to access any information stored on the handset for criminal purposes (e.g. banking details, contact details). They can even freeze the handset and demand a ransom in exchange for restoring the owner's access.

MODUS OPERANDI

Criminals realise that by redirecting users to websites masquerading as legitimate websites, the public would be vulnerable to having their personal information stolen. This would enable the cyber criminals to bypass security without the mobile subscriber's consent or knowledge in order to fraudulently generate an income.

The malicious code that is distributed by the criminals appears as software required in order to view an e-mail attachment. Once installed, the malware sends SMS messages to premium-rate numbers or services. Premium-rated numbers are numbers that charge a higher rate to the person who made the call or sent the SMS resulting in a high cell phone account.

Alternatively the infection process can happen in the background and then the victim would not even be aware of having become the criminal's target. The mere act of browsing a website hosting malicious software can expose the user's device to being infected, thereby providing the cybercriminal with access to personal information.



THREATS TO THE PUBLIC

Mobile device users may see unexplained increases in their data consumption, airtime usage or unwanted value-added services such as additional ringtones, wallpapers, horoscopes or traffic updates.

WHAT YOU NEED TO DO

- ☑ Avoid downloading applications from websites not officially endorsed by your mobile service provider or cell phone brand.
- ☑ Do not install applications from untrustworthy sources.
- ☑ Smartphone users, turn off your data connections when not using your applications. Otherwise, your applications continue to run in the background.
- ☑ Carefully read and pay close attention to ALL mobile data SMS notifications to decide before accepting instructions.

FAKE FINANCIAL SERVICES

On a daily basis the Internet is being used for legitimate and fraudulent transnational transactions. Fake financial entities create web pages on the Internet, and these websites are hosted in jurisdictions outside South Africa. Alternatively, contact details displayed on these websites show false physical addresses in South Africa.

Scams of this nature targets businesses working with foreign suppliers and companies that regularly perform electronic banking and fund transfers. The scam is carried out by encouraging the user to subscribe. In the subscription process the user's personal details are gathered for future fraudulent use, such as unauthorised transfer of funds to the cyber criminal.

MODUS OPERANDI

Cyber criminals use intermediaries to register untraceable and anonymous domain names on the Internet. The true Internet identification of these domain registrars is not available on publicly accessible databases. Furthermore, foreign Internet service providers protect the privacy of their customers and also do not make their domain holders' credentials accessible.

Criminal web designers download templates and forms from websites and customise them. Logos and trademarks of banks, businesses, companies, government departments and others are then copied and embedded in the fake website to create the home pages set up by criminals.

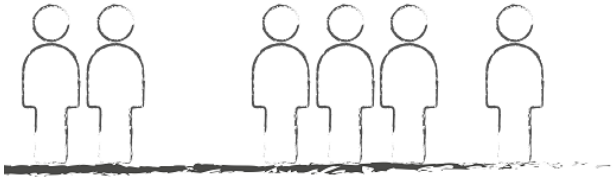
These websites record the browsing habits, operating system details and browser information of potential victims. With such information criminals can evaluate the Internet security posture of their potential victims and exploit their computer systems.

Criminals, known as "E-mail harvesters" collect e-mail addresses of potential victims over the Internet. Potential victims are selected and targeted based on their Internet presence, e-mail addresses and available information are profiled by syndicate members. Pre-formatted documentation is then sent by e-mail to potential victims, where additional personal data is collected by criminals.

The personal data is then sold off to other criminals to enable further fraudulent activities.

To obtain loans and other bogus financial services, victims often have to pay advance fees. Once the victims pay these fees, the amounts paid are reflected on a databases created by criminals. Login credentials to the website are provided to victims as confirmation that money was received.

Online money mules are used to receive money from victims and conduct electronic transfers to fraudsters and their associates. The money provided by victims is never paid into the bogus financial service. Rather it will go into the pockets of criminals.



THREATS TO THE PUBLIC

Financial loss: Fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise. In some instances, victims of fraud may be contacted by criminals over and over again.

Criminals pretend to be lawyers, government officials, police or law enforcement agency representatives that are there to help you recover your money but also want a fee to get it back. In these instances the victim's loss is often compounded.

Reputation: Fraud can seriously damage the reputation of a business or organisation. If the matter is reported to the authorities, their loss and security incompetence might reach the public domain. People might not want to engage in business ventures with them in future.

WHAT YOU NEED TO DO

- ☑ Internet users must learn how to spot common scams and fraud. Personal information should only be provided over encrypted websites. Never provide personal details in response to an e-mail or pop-up message or a website containing links from an e-mail to a web page.

- ☑ Business must know their buyers and sellers. It is essential for businesses to conduct background research on their online clients so that they can know whom they are dealing with.

- ☑ Internet users who believe that a company needs their personal information should call to check this by using a number for the company as it appears on their legitimate website or telephone directory.
  Users should not call the number or links used in an e-mail as displayed on a fraudulent website.

- ☑ If any financial loss is suffered, the matter should be reported to law enforcement. If banking information was provided to fraudsters, victims should alert their bank immediately. ■

3G POCKET-PORT DEVICES UTILISED BY CRIMINALS

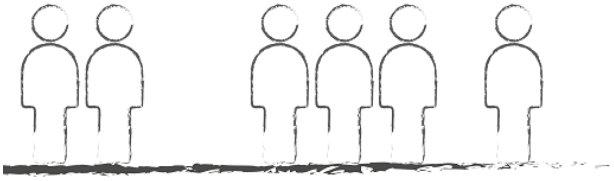
Criminals in South Africa are importing hardware devices (3G mini routers) to connect to targeted networks. A virtual connection is established from a remote location through cellular networks from anywhere in the world to the targeted network. This enables the cyber criminals to access the victim's computer network and to remotely transact without the victim's knowledge or consent.

MODUS OPERANDI

Criminals use the device to establish the physical location of financial and/or other systems with sensitive information in an organisation. So-called physical keyloggers will be installed on targeted computers with the assistance of unknowing staff or through social engineering techniques. Criminals may infiltrate businesses by posing as ICT support contractors.

Keyloggers are used to intercept usernames and passwords. Usually, criminals deploy keyloggers for only a day or two on targeted systems before removing the device. Once usable user names and passwords are collected, a small pre-programmed external hard drive or USB device is connected to the targeted computer. A copy or clone is made of the targeted computer's hard drive.

Afterwards a PocketPORT is placed anywhere on the targeted segment of the network out of sight. Usually the device is placed within the cable ducting or places where it is not visible to personnel or security. The virtual connection between the two devices is then established for the collection of sensitive and financial data.



THREATS TO THE PUBLIC

Primary targets are government departments, businesses, banks and financial institutions. These devices provide access to personal data hosted on targeted systems. Once in place, intruders are able to use these devices to change computer settings without user or administrator consent. This enables them to further their collection of user names, passwords, surfing habits and files from other systems on the network.

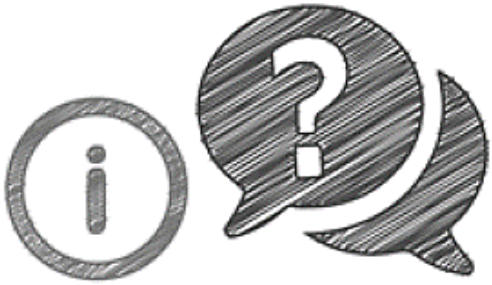
Physical surveillance can be conducted by criminals, activating the web cameras and microphones of targeted computers on the network.

Based on access to targeted computers on the network, financial data can be obtained and used by criminals. Electronic funds transfers can be conducted from targeted computer systems on behalf of the user without their knowledge.

Financial data and other information can be altered and/or manipulated without the knowledge of the user.

WHAT YOU NEED TO DO

- ☑ As modern communication technology advances and becomes increasingly complex, there are more and more opportunities for criminals and eavesdroppers to access and steal information.
- ☑ With criminals using keyloggers to primarily target government and financial institutions, it is important that these organisations invest in technical surveillance counter measure (TSCM) capabilities.
- ☑ Regular physical security inspections of computer systems and computer user awareness is essential. ■



BLUE WHALE – ONLINE SUICIDE GAME

An online suicide game called Blue Whale, has periodically come to the forefront since 2016. The game consists of a series of tasks assigned to players over a 50-day period and as the ultimate challenge, the player is required to commit suicide. The game was reportedly invented by Philip Budeikin from Russia and has been associated with the death of several teenagers world-wide.

MODUS OPERANDI

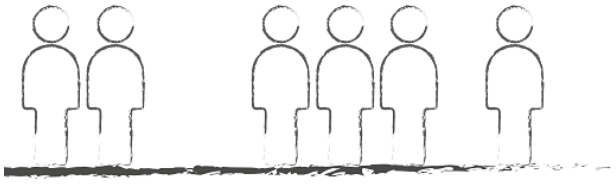
Internet users have to sign-up to participate in the game. Once entered into the game, the user is assigned to an administrator or curator who issues tasks over the next 50 days.

The game starts off with simple tasks such as listening to a certain song and in time progressing to watching unsettling videos. Extreme requests such as cutting words and symbols into the skin are included in daily tasks to the participant.

Children are requested to complete each task diligently and are encouraged not to reveal the activities to anyone. Administrators threaten participants who indicate that they do not want to continue with the game at any stage. They claim they have personal and location information on participants and that they will “go after” the victim.

After each task the participant is required to upload photographic or video proof of completion to the administrator.

If any fake, tampered, altered photographic proof or video material of self-infliction is uploaded for review by the administrators, they immediately stop replying to the victim.



THREATS TO THE PUBLIC

Ultimately, suicide by minors and young people.

WHAT YOU NEED TO DO

- ☑ Parents should be on the lookout for behavioural changes in their children. Important indicators include strange carvings, cuts and marks on the body. Children are also instructed to wake up early in the morning, especially at 04:20. Children have to watch psychedelic and horror videos regularly.
- ☑ Parents should also take careful note of children who change their music preferences to strange music provided by the curators.
- ☑ Be on the lookout for children who regularly visit high places, such as bridges and buildings to overcome acrophobia.
- ☑ Children participating in these games will say they are increasingly “talking to whales”. ■

CYBERBULLYING

Children's increased access to mobile platforms and the Internet has increased their exposure to cyberbullying.

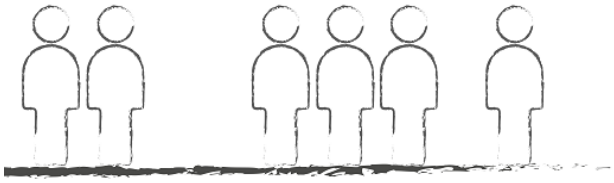
Young people are using social media to bully and humiliate other young people. Such activities have a wider reach, due to the fact that other people are exposed to comments, pictures distributed and video content.

Cyberbullying is playing a major role in teenage suicide in South Africa and around the world.

MODUS OPERANDI

Cyberbullying is perpetrated through text messages, mobile phone calls, e-mail messages, chat rooms, Internet gaming, pictures and/or video clips sent from mobile phones.

Victims are subjected to serious violations of dignity and publication of material intended to cause humiliation or reputational damage.



THREATS TO THE PUBLIC

Suicide by young people.
Victims usually suffer from anxiety and depression.

WHAT YOU NEED TO DO

- ☑ Parents need to be engaged and present as far as possible in all aspects of their child's life.
- ☑ Victims of cyberbullying and their parents are encouraged to report these matters to their local law enforcement departments, the Department of Basic Education, the Department of Social Development and the Department of Justice and Constitutional Development.
- ☑ Any victim can apply at the nearest Magistrates' Court for a protection directive in terms of the Protection from Harassment Act, 2011 (Act 17 of 2011). ■

INTERNET-BASED PET SCAMS

Internet fraudsters are creating fake websites advertising expensive and non-existent exotic pets for sale.

Sometimes non-existing animals are even offered for adoption at no cost. Victims have to pay only for the shipping and travel arrangements.

MODUS OPERANDI

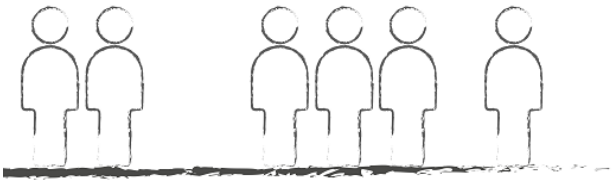
Using false credentials, criminals are registering several Internet domain names. In some instances, advertisements are placed in newspapers or on online platforms like OLX and Gumtree.

In authentic looking web pages, the criminals claim they are breeders of pets. Specific keywords are placed within the source code of the web pages to optimise searches on specific keywords related to pets.

During communications with victims, criminals call the pets their “babies” and insist that they only want a loving and caring home. Sometimes they send the potential victim a list of questions about how the new owner will take care of the pet. The victim also receives photographs of the animal they are interested in. This is to hold victims’ attention and to convince them to buy the advertised animal.

Secondary websites are published on the Internet where non-existing courier businesses are established. Authentic looking displays with airline information are sent to victims from these “animal courier” websites. Victims are requested to make payment for the transport and delivery of these animals. Sometimes, online “tracking numbers” from secondary websites are provided to victims to view the delivery of the animal online. Again, this is to convince the victim that the business is legitimate.

Once payment is made, victims are requested for additional fees because the animal needs a different crate; a health inspection or insurance before the pet can be delivered. If the victim stops the payments, they are threatened with “legal charges” for animal abandonment, kennel fees and additional feeding, due to delays caused by them. Victims have to pay recurring fees to these fraudsters mostly through Western Union or MoneyGram payment systems.



THREATS TO THE PUBLIC

In reality there is no pet or courier service and victims have been lured into an Internet based pet scam. Victims falling for this scam suffer financial loss.

WHAT YOU NEED TO DO

- ☑ Before engaging in financial transactions for the purchase of a pet, insist on a physical inspection of the pet.
- ☑ If you have been a victim of these scams, do not delete text messages, call logs or e-mail messages sent or received. All of this is supporting evidence which must be reported to your closest South African Police Service office.
- ☑ The information should also be provided to the South African Cyber Security Hub at incident@cybersecurityhub.gov.za. ■

PROPERTY / TIMESHARE / HOLIDAY ACCOMMODATION SCAMS

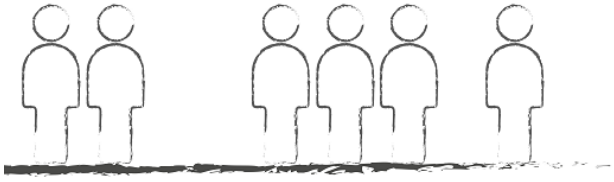
Internet based fraudsters impersonate property managers of holiday resorts in South Africa. Non-existing holiday accommodation is provided by these criminals to victims. In some instances, criminals will convince their victims to sign perpetual contracts, supposedly paying holiday clubs large amounts of money for shares of holidays which never materialise.

MODUS OPERANDI

Online classified advertisements for holiday accommodation are placed on the Internet on websites such as Junk Mail, Gumtree and others.

Criminals exploit the joint ownership of holiday facilities, such as timeshare and holiday point systems. Interested clients are presented with "once-off" holiday packages and pressured into signing contracts without them having read the contracts.

Should victims attempt to cancel contracts, the criminals demand cancellation fees exceeding R20 000.



THREATS TO THE PUBLIC

The scams for holiday accommodation occur when victims respond to fake advertisements and hand over money, only to discover that the accommodation, unit or timeshare for which they paid, does not exist.

WHAT YOU NEED TO DO

- ☑ If any holiday offer sounds too good to be true, it probably is. The public should avoid paying deposits before having viewed a property and read with understanding any contract related to it before signing on the bottom line.
- ☑ Scammers are going to great lengths trying to part people from their money. Potential victims should be careful about completing application forms or sending any personal information. It is essential that you ask as many questions as possible, such as who is the property owner.
- ☑ Request detailed information pertaining to the property. Check the Internet for complaints and/or reported fraud.
- ☑ Verify the address of the accommodation and whether it actually exists by conducting an online search using Google Street View.
- ☑ Be wary of advertisers using web-based e-mail addresses. These accounts can be created quickly with fake information by anyone with access to the Internet.
- ☑ Be cautious when requested to make an urgent payment to secure such booking.
- ☑ The public should avoid the temptation of completing and sending application forms containing personal information ahead of time.
- ☑ When dealing with an agent, always ask to see their Fidelity Fund Certificate and check the number via the Estate Agency Affairs Board website. ■

FAKE JOB SCAMS

nternet users are targeted by scams that involve fake career or job listings. With fake employment scams, scammers list jobs that do not exist.

MODUS OPERANDI

Internet based fraudsters use a career or job listing to attract employment seekers and obtain their personal information. Such information includes identity numbers, credit card information and/or bank account information. The information is often used to impersonate the victim to purchase online goods.

Employment seekers are notified that a position has become vacant and a telephonic, Skype, or instant message interview will be conducted. Applicants are then notified that they would be responsible for the cost of the background check. Victims are instructed to purchase a pre-paid debit card and to send it to the interviewer to pay for the supposed background check.

In other instances, potential victims are notified that a fictitious company is interested in the qualifications as indicated on the victim's application. Victims have to pay to get their credit score checked. Afterwards the applicant is directed to a website where they surrender their personal information such as full names, surname, physical address, identity number, banking details and contact details. This information is then abused by criminals.

THREATS TO THE PUBLIC

Internet Service Providers (ISPs) do not have control of 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.

Personal information provided by victims is abused by criminals in other impersonation and identity theft scams. Criminals disappear with money provided to them for credit checks and background checks.

In some instances, these criminals will request that jobseekers send their CVs to a fax number. Unknown to the jobseeker, the fax number would be set up to charge higher than standard rates. After the CV has been sent, the charges are then debited to the victim's telephone account at much higher than usual rates.

WHAT YOU NEED TO DO

- ☑ It is difficult to distinguish between scams and legitimate employment offers. If victims believe that they have encountered a website designed to look like a legitimate website to steal personal information, the matter should be reported to Google Inc., The Campus, Bryanston, Johannesburg.
- ☑ Fraudulent activities can also be reported to the Internet Service Providers Association in South Africa. See: http://cybercrime.org.za/docs/Advisory_on_Reporting_Cybercrimes_April_2013.pdf
- ☑ Financial loss should be reported to the South African Police Service to initiate a criminal investigation. ■

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 CONTRIBUTE TO SAFEGUARDING THE INTEGRITY OF SOUTH AFRICA'S FINANCIAL SYSTEM AND ITS INSTITUTIONS.

THE FIC'S MANDATE IS THE IDENTIFICATION OF FUNDS GENERATED FROM CRIME AND COMBATING MONEY LAUNDERING AND TERROR FINANCING.

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