The complete guide to protecting yourself when **buying and selling online**

fraudcheck

Foreword

In a world where e-transacting is becoming more the norm than the exception, it is to be expected that criminals will show up online, just as they do in our shopping malls, shops and on the street.

As long as you are aware and understand who the cyber criminals may be and how they operate, you are in a position to **protect yourself** from harm while enjoying all the fun and ease of online transacting.

This book EBook will teach you to **identify potential scam artists** or **fraudulent online transactions** and give you tips to stay safe while shopping or selling online, so that you can enjoy the benefits of the e-world without the risk.

Introduction

Cybercrime is on the increase globally. Recent findings presented by Grant Thornton reveal that cybercrime is taking a serious toll on business globally with businesses losing in the region of US$315bn over the past 12 months. A survey in the Grant Thornton International Business report this year found that 1 in 6 businesses globally had been the victim of cyber-attacks.

South Africa has not avoided **cybercrime**. According to the Centre for Strategic and International Studies (CSIS), cybercrime costs South Africa approximately R5.8 Billion rand per annum. The Southern African Fraud Prevention Service (SAFPS) estimates that identity theft alone costs South Africa R1 billion rand per year.

> “Cybercrime is taking a serious toll on business globally with businesses losing in the region of US$315bn over the past 12 months”

Cyber criminals take advantage of the public’s lack of knowledge about their methods and lack of awareness about cybercrime generally. In order to stay safe it is important to equip yourself with at least a general knowledge of the risks associated with transacting online, as well as some **simple and basic prevention methods** that will protect you from becoming one of the thousands of victims of online fraud every day.

1. What is online or cyber fraud?

Any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them” -The Electronic Communications and Transactions Amendment Bill, 2012

Broadly speaking cybercrime is any criminal activity carried out using a computer, the internet, any public network or other computer technology such as a smart phone or tablet. **The computer may be the tool used to commit the crime or it may be the target of the crime.**

Cybercrimes include:

- Computer misuse for example **hacking, viruses, spam email,**
- Financial fraud such as **phishing, online theft and scams**,
- **Identity theft** and **identity fraud** and
- Offences against other persons such as **cyber bullying** and **trolling**

2. I love online shopping, how could I become a victim of online fraud?

Online shopping is convenient and fun; nothing beats crowd-free shopping from the comfort of your own lounge, mug of coffee in hand and the knowledge that whatever you order will be delivered straight to you. Unfortunately, there are **risks** associated with online shopping. While we may be sitting in the safety of our own homes, we are in reality engaging with the world at large, albeit virtually.

1. Identity Fraud

It is simple to set oneself up as a seller online. Online shopping portals such as OLX or Gumtree make it possible for anyone to sell or purchase goods online. This makes it very difficult to determine whether the person you are transacting with is who they claim to be and if they are a legitimate seller. Criminals frequently pose as honest sellers in order to **defraud innocent buyers.**

2. Sales Scams

Con-artists and scammers may pose as legitimate sellers in order to trick honest buyers into parting with their hard earned money. Some scammers may not have the goods they claim to be selling at all; still others may be selling stolen goods claiming that they are selling their own property. The product may be of an inferior quality compared to what is advertised and when the purchaser tries to return it for a refund the company or seller has disappeared!

> “Con-artists and scammers may pose as legitimate sellers in order to trick honest buyers into parting with their hard earned money.”

Frequently these scammers have a believable online profile accompanied by photographs of the goods they claim to be selling. They may even offer you a telephone number to call to confirm the goods. This telephone number of course goes straight through to an accomplice who verifies the transaction. Typically the con-artist **will require payment up front and refuse to allow you to collect the goods**, promising to deliver them, but never does.

Popular examples of online shopping scams of this nature include the sale of scarce breeds of animals or birds online; sellers insist that the payment be made up front in order to reserve the pet with a promise to deliver when the animal is old enough. **Delivery** is either **never made**, or where a collection **address** is given, it is a **fraudulent** or **non-existent** address.

3. Rental Scams

Another kind of scam involves rental of property or holiday accommodation; **fraudsters advertise a property** as a holiday rental and provide full photographic portfolio of the property. Full payment is required in advance to guarantee the rental. Unsuspecting holiday makers are shocked to discover when they arrive, that the property is either a privately owned home, a corporate hotel or in some cases an empty piece of ground.

4. Special Offers and Vouchers

One of the attractive aspects of online shopping is price; online products are often offered at a lower price to the retail store pricing. However discount vouchers and special offers such as pre-launch offers or extreme discounts are often utilised by scammers to entice buyers into purchasing non-existent or inferior products. **Remember, if it sounds too good to be true, it probably is!**

> “Discount vouchers and special offers such as pre-launch offers or extreme discounts are often utilised by scammers to entice buyers into purchasing non-existent or inferior products.”

3. As an online vendor how could I be a victim of online fraud?

Selling goods online is an efficient, low cost and simple way of transacting. Whether you are a private individual who occasionally sells items online or an organisation with a full online shopping store, **online selling is not risk free**.

1. Credit Card Fraud

The most common risk associated with selling online is financial fraud. Criminals defraud online vendors by using stolen credit cards, particularly for international transactions. Once the stolen credit card is reported, the payment is reversed from the vendor's bank account.

> " Criminals defraud online vendors by using stolen credit cards, particularly for international transactions. "

2. Cheque/Bank Deposit Fraud

Alternatively, the criminal deposits a stolen cheque into the seller's bank account and insists on urgent delivery or collection of the goods. The cheque will reflect as 'to be cleared' by the bank and two to three days later the cheque will be **dishonoured** and the **deposit reversed**, leaving the seller without his merchandise and his money.

A variation on the stolen cheque is the fraudulent proof of payment advice; a small amount of cash is deposited by the fraudster for e.g. R100.00 and the proof of payment receipt is changed to reflect R100 000.00. By the time the seller realises the short deposit the merchandise has already been delivered.

3. Fraudulent Banking Details

> " Fraudsters may provide fake or incorrect banking details for debit order or instalment purchases. "

Fraudsters may provide fake or incorrect banking details for debit order or instalment purchases. The seller loads the debit order and in good faith hands over the goods, only to discover when the debit order run is initiated that the **bank account does not exist** and the purchaser has absconded having also provided **fraudulent personal details** rendering him or her untraceable.

4. Identity Fraud

Fraudsters who commit any type of **banking fraud,** as described above, **combine** it with **identity fraud**. The online shopper may produce fraudulent or stolen identification or proof of address that appears to be legitimate when applying for a debt order credit purchase, or when using a stolen or forged credit card. **Addresses** given for delivery are often **not traceable** to the person or may even be a general collection depot.

4. Other ways in which cyber fraud is committed

Cyber fraud is not only committed during online shopping; cyber criminals have devised a number of ways in which to defraud innocent people!

1. Identity Theft

A significant risk associated with cybercrime is identity theft which occurs when someone uses your **personal identifying information** (e.g., name, address, ID number, banking account number, username or password) to commit fraud.

Criminals obtain copies of **personal** identity **documents**, bank statements or other documents and utilise these **to obtain credit**. Frequently the person whose identity has been stolen is the last to know, and only becomes aware of the theft when they attempt to apply for credit or receive a notification of legal action for a **credit default** that they have no knowledge of. The damage this causes is enormous; **having one's name removed from a credit blacklist is difficult and time consuming.**

> “ The damage this causes is enormous; having one's name removed from a credit blacklist is difficult and time consuming. ”

2. Phishing

Phishing is the fraudulent practice of sending emails **purporting** to be from **reputable companies** with the intention of inducing the person to reveal personal information such as bank account details, passwords, and credit card numbers online. Phishing emails typically instructs the recipient to perform an action by clicking a link to a **fake website** that is designed to look and feel exactly like the site of a familiar and reputable organisation e.g. your bank. Once on the clone website the cyber-criminal is able to **harvest** all your secure login and **password details** needed to access and withdraw funds or to commit further identity fraud.

Spear phishing

Spear phishing is a type of phishing aimed at specific individuals or organisations and the criminals will harvest personal information for inclusion in the email. This type of phishing is currently the most successful and accounts for 91% of all phishing attacks today.

3. Invasion

Cyber criminals may include links in emails or in websites that cause you to inadvertently download spyware or malware. **Spyware** or **malware** are programmes that infect your computer and allow the **hacker** to have **access** to any information, including secure passwords and banking information or other personal identification information. Viruses may also be hidden in ofr example a .jpg picture.

Common examples of this include an email or a telephone call from a tech support agent who claims to be able to fix a problem on your computer or assist you with a repair to your Microsoft computer. **Once you click the link in the email or visit the website the malicious program download is triggered and your information is available to the cyber thief.**

5. Risks of using different computer technology e.g. computers, internet café, mobile telephone or tablet

As mentioned, cybercrime may be committed using **any type of computer technology or network**. Although people commonly assume that viruses and scams would only take place via a PC or laptop,

this is not true.

> “ Cybercrime may be committed using any type of computer technology or network. ”

1. Cybercrime on tablets and smart phones

> “ When stolen, portable devices provide criminals with a wealth of private information about the owner via the address book or other saved documents. ”

Tablets and smart phones may place you at risk of cybercrime in a number of ways. Firstly, these **devices** are **vulnerable to theft** by virtue of their portability. When stolen, portable devices provide criminals with a wealth of private information about the owner via the address book or other saved documents. Moreover because portable devices utilise apps which are often in a permanently logged in state, criminals may be able to access secure apps and **impersonate you**. For example they can send emails on your behalf, access social networks or enter your banking/shopping apps.

Secondly, until recently, it has been believed by many that operating systems of mobile telephones and tablets are protected from virus attacks. This is no longer true; the research team at Palo Alto Networks, an American network security company based in Santa Clara, California has recently discovered a **new Apple iOS malware which has the ability to clone apps and replicate itself through networks onto other devices.**

2. Public computer networks and internet cafes

Perhaps it goes without saying that **using shared computers or internet** café's carries **additional cybercrime** risks. Innocent users may unwittingly trigger or download a virus or spyware onto a public machine which you will later use. Alternatively, fraudsters themselves may pose as users and **intentionally infect** a public computer.

Since you **cannot control the security settings**, firewall settings, or anti-virus software on a shared or public computer, there is **no guarantee** that the computer you are using is 100% clean and that it is safe to insert private or sensitive data such as passwords or personal details. You may be at risk of **identity theft.**

> " At all times be aware of your surroundings and the people around you. Protect yourself, stay vigilant. "

Be awared **Shoulder surfing** the practice of hovering around a person who is working or transacting, in order to see their passwords, is common in internet cafes and at ATMs. At all times be aware of your surroundings and the people around you. Protect yourself, stay vigilant.

3. Mobile storage devices

Mobile storage devices such as **flash drives** and **portable hard drives** are vulnerable to **infection by viruses** and when used on different machines, infect the host computer, which in turn will infect another mobile storage device, possibly yours.

6. How to spot a Fraudster when transacting online

It is not necessary to be a cybercrime expert or a super sleuth to spot some of the common signs that the person you are dealing with may not be an honest seller or buyer.

1. Email style and wording:

Phishing emails can be difficult to distinguish from legitimate emails from a company or website that you are familiar with since they often carry the logo of the company and may appear to come from an official email address containing the name of the company. However there are some tell-tale signs you can look for;

- **Content;** Cyber criminals will take advantage of the online user's fears or hopes to trick them into revealing sensitive confidential information or clicking onto a clone website. Theemails may come from banks, the South African Revenue Service or other companies like Microsoft. The emails will refer to an **urgent problem** with your tax return or your online banking profile that needs to be **fixed immediately** by following the instructions in the mail. Alternatively, the email may **promise a large tax refund or inheritance**. If you are being asked to type in or send banking details and/or passwords you may be dealing with a scam.

- **Spelling or grammatical errors;** large organisations have copy writing departments who proof read corporate emails so you can be sure that spelling or grammatical errors would not appear in an official mail. If you spot any of these you may be dealing with a fraudulent email.

- **Links;** the email will contain a **website link** that looks as though it is **legitimate**. However rolling a mouse over the address without clicking it will reveal the actual address to which the link is pointing which will look nothing like the company it purports to be.

- **Threat;** along with an instruction to **click a link** in the email is a threat that not doing so will cause your account to be frozen immediately. This kind of email is likely to be a phishing mail.

2. Website addresses

Clone websites can look very similar to the official company website and may be difficult to detect. Look out for the following clues to determine whether you are on the true website.

- **Look and feel:** Cyber criminals **steal corporate logos** from the internet or use poorly rendered copies of logos. If the layout looks a little different to what you are used to on your normal website or if the graphics appear to be fuzzy, misaligned or discoloured, you are probably on a clone site. If you have never used this company's website in the past, do some research by asking for references or doing wider internet searches on the company in blogs or forums.

- **Security encryption:** Before entering any banking or credit card information ensure that the padlock appears in the website address bar and that the address begins with https://. Without these, it means that your information is not secured. Any major retailer or online payments company will use these security measures as a matter of course.

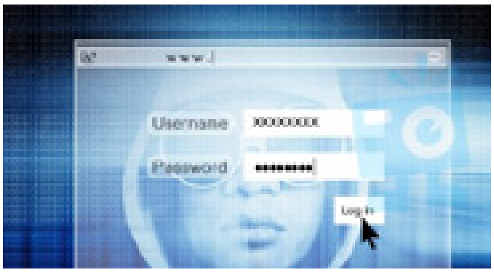
3. Sales Scams

Sales scammers also give themselves away with tiny details.

- **Pressure to pay:** A legitimate seller will not **pressurise** you to pay or **threaten** you in any way. If a seller is insistent on payment of a deposit to view the goods, you may be dealing with a scammer.

- **Emails:** Sales scammers often use a **poorly drafted confirmation email** that asks you to deposit money and promises delivery. These emails contain poor spelling or grammar and may appear as though they have been badly translated, or changed from a previous mail. The email may also come from an address that contains **strange characters** for example **'jones4@vsljp9c.com'.**

Despite the seriousness of cybercrime it is possible to keep yourself safe while transacting online. Making use of these simple tips will **protect** you from the most common forms of online fraud.



7. Ten tips to stay safe online

1. Install recognised anti-virus and anti-spyware software and ensure that regular updates keep your antivirus up to date with the latest threats.

In order for any fraud prevention measure to be successful it must be one step ahead of the would-be fraudsters. Hackers and virus creators generate new ways to beat security systems daily. It is important that your security software performs **regular scans** and that it updates itself to keep in line with the latest known threats. **Be aware of certain free anti-virus or anti-spyware software offered on the internet.** Some of this free software is actually a **virus** that once downloaded and running on your computer steals your information or damages your computer. Only use software from a reputable, recognised company.

Finally, most banking websites offer a **free software download** which is able to **detect** a **cloned** bank site. Protect yourself by using this software.

2. Turn your firewall on

Most operating systems contain a built-in firewall that will prevent unwanted access to your computer. Find out how to use this and make sure that it is turned on.

3. Treat all unsolicited emails with suspicion

Even if an email purports to come from someone that you know, be wary if you are not expecting the email. Cyber criminals **hack** into email systems or **steal passwords** and are able to send emails from addresses that appear to be correct. If the email is unexpected or the content is unusual, **delete it**. A legitimate sender will contact you again if you have deleted a genuine email.

Viruses and spyware are often **embedded** in **attachments** to emails. These malware may attack your computer, steal your information or cause your computer to send spam emails to your email contacts, containing the virus, thus, spreading the virus far and wide. If you are not sure **delete** the email without opening the attachment.

4. Password Autofill

Internet browsers frequently offer the option to "Remember Me". While it is handy to make use of this feature, it also provides **easy access** for any unauthorised person into your password protected websites. Be reminded that identity theft and impersonation even takes place on social media sites with devastating effects.

> "Be reminded that identity theft and impersonation even takes place on social media sites with devastating effects."

Similarly many computers contain an **autofill option** which allows the computer to store information that you regularly type into online forms such as addresses, telephone numbers, identity numbers and suggest that every time you fill in a form. Again, this is a great time saver, however, it means that anyone who has access to your computer can find out your personal details by simply attempting to complete an online form. If you choose to use this feature on your computer, **be vigilant about logging off** every time you step away from the computer.

5. Basic computer safety skills

Always ensure that you are **properly logged off** when you step away from your computer. Do not leave password protected websites, including social media sites, open in your browser if you are not sitting at your computer, particularly if you are in an office environment or using a **computer** in a **public place** such as an internet café. It takes only a few minutes of absence for your identity to be stolen, your bank accounts to be cleared or your reputation to be damaged by criminals or pranksters using your sites.

Most computers, tablets and mobile phones have a **'sleep' function**; after a period of inactivity the unit goes dormant and a password is required to reactivate it. Find out how to set this on your computer; it provides an extra layer of security should you accidentally forget to log off when you step away from your computer or if your laptop, mobile phone or tablet is stolen.

Unless it is an absolute necessity, avoid accessing online banking or shopping sites from another person's private computer or a public computer. Even if you have logged out correctly after the transaction, there may be viruses that you could not be aware of that steal your information or store your passwords. Be aware also of the **risk of transferring** viruses and spy ware between computers using portable storage devices such as flash drives. Only insert your flash into a computer that you are 100% sure is clean and only allow trusted mobile storage devices to be plugged into your computer.

Finally, always **be aware** of your surroundings and the people around you. Be alert to 'shoulder surfing' at ATMs or internet cafes. Cover your hand when typing in a pin or password and if you notice a person or people hanging around you for too long log off and walk away.

6. Do not use the same login and password details on all websites you use.

In today's world we are all required to make use of a number of different websites whether for work purposes or for personal browsing. It is tempting to create a **universal password** for all your websites so that only have one to remember. While this may assist you with management of your sites, it also **leaves you vulnerable to attack**. A cyber-criminal only needs to have one password for free access to all of your personal and browsing information.

7. Never give your personal details such as passwords, date of birth, address or banking details

Do not give any confidential personal information away over the telephone, via email or over a social networking site. Educate yourself and learn how to **manage** your **privacy** settings on social networking sites to ensure that the information you share is only seen by those whom you have chosen. Only submit banking and payment information to **secure sites** that are guaranteed to encrypt your data. Security encrypted sites will show a padlock in the website address bar and that the address will begin with **https://**.

8. Check your statements frequently and shred all documents after their required storage life

It may sound like tedious work, but a simple **monthly check** of your statements to verify all **transactions** may alert you to identity theft or bank fraud against you. Contact your bank if there are unexpected or unusual transactions on your statement.

“ Make sure that you shred any documentation that contains identity numbers, banking details, account numbers or medical aid details after the required storage years have passed. ”

Moreover, criminals are determined; they will go through rubbish bins or other disposals to find documents containing your personal information. Make sure that you shred any documentation that contains identity numbers, banking details, account numbers or medical aid details after the required storage years have passed. Also be on the look-out for individuals sorting through your rubbish bags before they are collected by the refuse removal company.

9. Check your own credit report annually

Identity thieves apply for credit in the name of the person whose details have been stolen. Because these **credit applications look valid** the fraud is often only **discovered** a **long time after** it has taken place, usually when the victim applies for credit themselves and is declined either because of defaults or affordability. By **checking** your credit profile **annually** you will pick up any credit agreements that you did not make and can take action immediately to have your profile corrected.

10. Stay Informed

Cybercrime methods change daily as criminals find new ways to beat the security systems put in place. The best way to stay safe is to educate yourself and stay informed. The South African Portal for resources and **information on cybercrime** is housed at **www.crybercrime.org.za**. Here you will find up to the minute information about latest criminal tactics, reporting of cybercrimes, legislation and news.

> “ Cybercrime methods change daily as criminals find new ways to beat the security systems put in place. The best way to stay safe is to educate yourself and stay informed. ”

8. What to do if you are a victim of cyber fraud

Since cybercrime describes such a wide range of possible illegal activities the **steps** you take as a victim depend on the type of crime committed against you.

1. Contact your bank or credit card company immediately

You need to **alert** your **bank immediately** that you have become aware of a fraudulent transaction of any sort. You must put a stop on all cards that have been affected as well as change any logins, passwords or pin numbers. In certain cases your money may be **refunded**, but not in all cases. In the case of identity theft the bank will require **proof** that you were not party to any credit agreements before they remove them from your name.

> “ You must put a stop on all cards that have been affected as well as change any logins, passwords or pin numbers. ”

2. Alert the ecommerce site where you transacted and that the fraud occurred

All major ecommerce sites such as OLX, Gumtree, and Amazon are aware of online shopping scams and constantly **monitor** their systems for scams and cyber breaches. They need to be **made aware** of any fraud that has taken place via their site in order to stay ahead of the criminals. Notifying the company assists them to **tighten security** where it is needed most and prevent further incidents from occurring.

3. Report the incident to the police

Theft and fraud are crimes whether committed in the virtual world or in the ‘real’ world. One of the reasons that cyber criminals are rarely caught is because the crime is not reported to the authorities and is never investigated. In order to **track down** and **root out** these criminals the **police** must be **notified**. When reporting a cybercrime incident at a South African Police Station you will be required to dictate an affidavit which describes the incident and the type of cybercrime you were a victim of. You will be issued with a **case number** and an investigator will be assigned to the case. You will then be able to follow up with the investigating officer to ensure that the matter is being attended to.

4. Report the incident to cybercrime websites or action groups

Cybercrime action groups collate data, conduct research and predict trends in order to assist businesses, governments and individuals to **stay one step ahead** of cyber criminals. Reporting portals can be found at these addresses;

- Online Technology Risk Advisory Centre website for reporting and getting help
  https://ontrac.org.za/support/
  and
- University of Johannesburg Centre for Cyber Security website for recording statistics
  http://adam.uj.ac.za/csi/ReportCybercrime.php

5. Update your anti-virus software and run a full scan

While this may feel a little like closing the stable door once the horse has bolted, it is critical that you **clean your PC or mobile device** of all malware and spy ware that may still reside in the operating system. Remember to include any portable storage devices in this scan.

6. Talk about it!

People are often embarrassed about having been scammed and keep quiet about it, don't! There is no need to feel embarrassed; cyber criminals are masters of deception, misdirection and trickery. They succeed because they are good at what they do and rely on people's poor understanding of the risks of cybercrime and the ways in which it is committed. By telling as many people as you know, you will be **educating your friends and family** so that they can avoid becoming victims of a similar event.

9. How can FraudCheck help to keep me safe online?

FraudCheck is in the business of protecting its users against fraud by providing the information needed, educating them about ways to **identify fraud** and creating a greater **awareness** of the many types of and ways in which identity fraud is perpetrated. FraudCheck offers a number of services that will enable you to transact online with confidence and peace of mind, knowing that the person you are dealing with is legitimate.

> “FraudCheck offers a number of services that will enable you to transact online with confidence and peace of mind, knowing that the person you are dealing with is legitimate”

1. Identity Verification

When transacting with an individual online you can request their ID number from them. The FraudCheck ID online real-time verification confirms that a **South African ID number** provided is **valid** and belongs to that person. This **real-time** online service provides instant validation; you will instantly know whether or not to proceed with your transaction.

2. Bank Account Verification

Before accepting EFT payments or depositing money into a bank account, give yourself the peace of mind of **verifying** the **validity** of the bank account. Remember, the person you are dealing with may be using a stolen identity. Combining our FraudCheck Bank Verification with our FraudCheck ID online real-time verification ensures your **protection** from the risks of fraudulent/incorrect banking details and also confirms the validity of the South African ID number provided.

3. Credit Reports

It is recommended that every person checks their own credit report annually to ensure that they have not unwittingly fallen victim to identity theft. Moreover, when transacting online and agreeing to receiving payment in instalments it is important to know the **credit history** of the person you are dealing with. The FraudCheck Credit Check in combination with the FraudCheck ID online **real-time verification** confirms the following;

> “It is recommended that every person checks their own credit report annually to ensure that they have not unwittingly fallen victim to identity theft.”

- The **ID number** provided is **valid** and belongs to that person; and
- the **marital status** is as stated, and
- the **address** given is correct and current, and
- whether the **property** is owned by the applicant, and
- any and all **court judgements**, **administration orders** or **sequestration orders**, and
- current and previous **employment history**, and
- current valid **bank details**

To do a full credit profile on yourself or another person FraudCheck offers FraudCheck Credit Check with Payment Profile which provides all NLR (National Loans Register) & CPA (Consumer Protections Act) data i.e.

- All accounts in the person’s name
- Payment behaviour on the accounts

4. Criminal Checks

If you are concerned that the person you are transacting with may be a criminal the FraudCheck Criminal Check will confirm the following;

- **No Illicit activity** on the part of the individual being checked or
- Individual has a history of **illicit activity**

5. Deeds Search

Avoid being caught out by fraudulent property lessors; verify that you are dealing with the person legally entitled to let a property. The FraudCheck Deeds Verification with FraudCheck ID online real-time verification confirms the validity of a South African ID number and details of **all properties associated** with that ID number. This real-time online service provides instant validation; **no waiting** indefinitely to find out if the information you have been given is correct.

> “ Avoid being caught out by fraudulent property lessors; verify that you are dealing with the person legally entitled to let a property. ”

Conclusion

Cybercrime is on the rise and expected to continue to grow. For the cyber criminals, it is a lucrative, low risk enterprise; conviction rates are low. Whilst governments are becoming more aware of the threat posed by cybercrime and the need for legislation to protect its citizens and the economy, the onus rests squarely on the individual person or business to educate and protect themselves from all kinds of cybercrime. Making use of the tips above, reporting all incidents of cybercrime and being active and vigilant will ensure that the criminals do not win!

fraudcheck