Publication: Sowetan (Late Final), Money
Date: Thursday, September 27, 2018
Page: 18

Identity theft is a real threat and is on the rise

By **Patricia Holburn**

ID theft is a big problem that can happen to anyone of us. If fraudsters open an account in your name and it is unpaid, this can result in a judgment against you. /123RF

Beware fraudsters are out to steal from you

Not letting your credit card leave your sight, not sharing too much information on your Facebook account and not readily giving out your ID number too often may not be enough to protect you from identity theft.

Credit cards can be cloned with a swipe across a sleeve, your social media photos can let criminals know you're not at home and your home ownership and loan records are publicly available through the deeds office.

"Crooks do research and there is a lot of publicly available information," Steven Powell, the head of ENSafrica's forensics department told the annual Fiduciary Institute of South Africa's conference held in Sandton recently.

Powell says if you are a victim of ID theft and fraud, the sooner you pick it up the greater your chances of not losing money, but ID theft and fraud are rife.

ID theft is the unlawful use of someone else's information.

Powell explained that the more information criminals have about you, the easier it is for them to steal your ID and commit fraud. And it's not just social media that criminals access – there is a range of easy-to-access information publicly available.

The deeds office has details of where you live (present and past) and your home loan accounts; company registers have details on directors and company owners; credit records show where you have accounts; and the eNatis system shows your vehicle ownership.

At the Master of the High Court, a criminal can find out if you are a beneficiary of a trust or estate.

Added together, this gives criminals a very comprehensive view of your life that they can use to open accounts in your name, change bank account details, and defraud you, often without your knowledge.

"Once a syndicate gets hold of your details they can pretend to be you, create authentic-looking documents to open new credit card accounts to purchase items that can be sold easily for cash," Powell said.

ID theft is a big problem that can happen to anyone. If fraudsters open a retail account in your name, but you don't know about it, and it is unpaid, this can result in a judgment against you. That can end up on your credit report, affecting your ability to get credit in future, he said.

> ***"Syndicates get hold of your details and run up bills in your name***

"When you've got a financial need, and there is weak control, fraud becomes almost irresistible," he said.

Powell illustrated how one syndicate operated. On the way to a taxi rank, a call centre operator physically bumped into a gentleman.

This seemingly innocent chance meeting led to a date, exposing the call centre operator to a lavish lifestyle she had never experienced.

Within three dates she had revealed details of her work and information she had access to and was sucked into a "you can have this too, all you need to do is give us details".

What can you do to protect yourself from identity theft

- Be careful about what you throw away; shred documents that contain your details.
- Check e-mail addresses – "hover your mouse over the address to see if there is an alias".
- Use strong passwords that can't be guessed with numbers, characters and special characters.
- Be attentive at ATMs.
- Check phone numbers and bank details on invoices with the provider or on its website or against those you have used before – don't just go by those on an invoice or e-mail.
- Be careful what you put on social media.
- Check your credit report regularly. You are entitled to one free report from each credit bureau each year.
- Don't give out passwords to people who call you, or put them in an SMS or an email.
- Read your statements – and be wary if you don't receive a statement when you usually do.

If you have been a victim ...

There are three things you must do immediately if you have been a victim of identity theft, says Steven Powell, the head of ENSafrica's forensics department.

- Place a fraud alert on your accounts with your bank, letting them know your ID has been stolen and that any changes to your account, such as the addition of beneficiaries, must be checked.
- Change your passwords.
- Open a criminal case with the police.

How you can become a victim of identity theft

There are a variety of ways in which you can fall victim.

A call centre operator gives your details to a fraud syndicate

Steven Powell, the head of ENSafrica's forensics department, told the Fiduciary Institute of South Africa's recent annual conference that call centre operators in SA have been offered £50 (R945) for a person's details and some have handed the information to fraud syndicates.

Information a call centre might have includes your ID, address, employment, salary slips, contact details, tax number, email accounts and servers, possibly medical information, and also information about whether you are due a claim or refund. These details can be used to change the bank account for payments or open new accounts.

Your credit card is cloned

Powell said cloning devices can be the size of a matchbox, attached to a sleeve cuff or apron, and your card can be swiped with a quick hand movement.

A cloned credit card is a white piece of plastic with a magnetic strip, created using the cloned information, a laptop and laminating machine.

Your bank account details are changed

Your information is used to change your bank details on accounts on which you are due a refund – for example your medical scheme, and the payments are made to the wrong account.

Your Gmail account is hacked

Powell says Gmail is "probably the most hacked form of e-mail", giving fraudsters access to personal e-mails with a lot of information about your accounts and investments.

If you are sending confidential documents via Gmail – password protect them, he says.

An invoice is cloned

When you're expecting an invoice from a lawyer or other service provider you will most likely pay if it looks legitimate.

But, if one or two amendments such as a phone number or the bank account are made – you can end up paying money to the fraudster without realising it.

And then you still owe the original supplier, Powell points out, because paying the wrong account doesn't discharge your debt.

"A debt is only extinguished when the amount hits the recipient's account – not when the payer pays."