Ornico
KNOW HOW. TO GROW

BONA 2016/12/01 Page: 68-69

AVE: 83271.87 (ZAR)

WISE UP

DON'T BE A SCAM VICTIM

Online banking makes your life easier, as does having a cellphone and an ATM card. You also shop, book holidays and even date over the Internet; it's all convenient. But, with scams on the increase, to stay safe you need to be savvy.

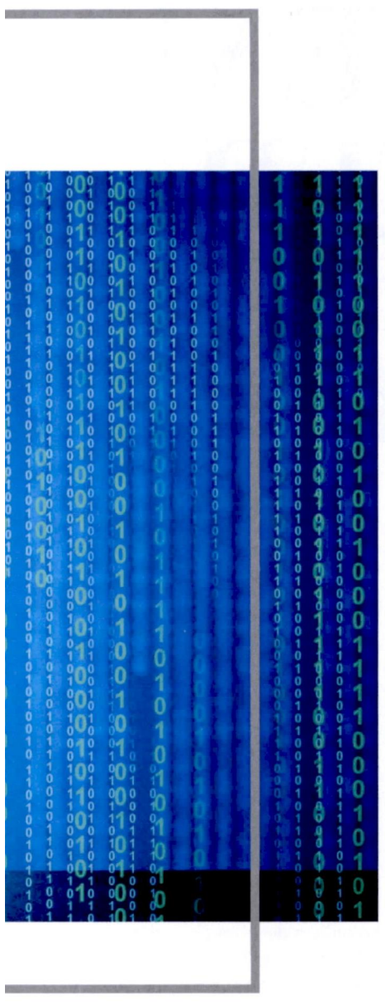
By Françoise Gallet

Your full names, address, cellphone number, date of birth, ID number and bank account details (credit card number, banking passwords and PIN numbers) are like gold to cyber criminals, warns Jacky Fick, executive head of forensic services at Cell C.

Typically, fraudsters fish for this information by sending deceitful emails (phishing), SMSs (smishing) or resorting to a call (vishing) that looks and sounds legitimate, and has some kind of 'hook' to cloud your judgement. If you fall for their bait and share your personal and banking details, fraudsters can wreak havoc in your life. They can open store accounts or buy luxury cars in your name, steal funds from your bank accounts or use them in money laundering activities, implicating you in the crime, explains Roy Retief, operations manager of the Southern African Fraud Prevention Services (SAFPS).

A healthy suspicion of all emails, calls and SMSs requesting personal information is a good first-line defence, suggests Jacky. Fraudsters are also relentless in their efforts to bypass security hurdles. The SIM swap scam is a good example, explains Jacky.

Once you unsuspectingly share your sensitive personal and banking information in a phishing, smishing or vishing probe, fraudsters can approach your mobile operator with a request for a SIM swap, pretending to be you. If they succeed, they can intercept the One Time Passwords (OTPs) sent to your cellphone as a banking security measure and take control through your cellphone banking. And, because you gave the fraudster your personal details, you're ultimately liable for your loss. So, Kalyani Pillay, chief executive officer of the South African Banking



So, Kalyani Pillay, chief executive officer of the South African Banking Risk Information Centre, shares these tips to protect your identity:

- Never fill in sensitive personal and banking information if prompted to do so from a link in an email, SMS or via a call.
- When banking online, ensure that you're on the secure website and not a 'spoof' site. Type in the address, look for the security icon on your browser tool bar and ensure that the URL begins with https, not http.
- If you receive a call requesting personal information, do not respond.
- If you lose reception on your cellphone, immediately check what the problem could be, as this may be an illegal SIM swap.

SOME DEALS ARE TOO GOOD TO BE TRUE

With the festive season in full swing, identity theft isn't your only concern. There are plenty of bargains, often for attractively priced and highly sought products such as iPhones and iPads or holiday rentals. But, not all of them are legitimate, Kalyani warns.

And, if you're buying a second-hand item based on an advert, don't part with any money until you've had personal contact with the seller and examined the goods.

When it comes to accommodation scams, be it a holiday or residential rental, fraudsters typically advertise a set of attractive pictures with a hard-to-refuse price, ask for a deposit upfront and then disappear with your money. So, when planning a holiday online, don't rely solely on information provided on one website. "Do cross-checks and references, and if possible, verify the authenticity of the business you are about to purchase your holiday package from with the relevant tourism association," urges Mmatšatši Ramawela, CEO of the Tourism Business Council of South Africa.

Dexter Leite, Pam Golding Properties rentals manager in Cape's Cape Town Metro, has the following advice for finding residential rentals online:

- Be aware of private listings where deposits and rentals are requested upfront, before viewing.
- Insist on viewing the premises – inside and out – before committing to anything.
- It's possible that a fraudster could pose as an estate agent. Check that the agent and agency are registered with the Estate Agency Affairs Board and hold a valid Fidelity Fund Certificate.
- If it sounds too good to be true, it probably is. Proceed with caution!

NOT JUST AN SMS

You also need your wits about you when reading a simple SMS. In the airtime transfer scam, a subscriber receives an SMS informing them that they will receive free airtime by simply punching in a USSD (Unstructured Supplementary Service Data) code, like *102*02*29*0725283185#, onto the handset. This code actually transfers airtime from your account to the number specified in the string, explains Vodacom spokesperson Byron Kennedy.

So, ignore unsolicited messages, especially where they appear suspicious or out of the ordinary, and adopt a position of sensible caution and common sense, suggests Byron.

ALWAYS KEEP AN EYE ON YOUR PLASTIC

Not all fraud occurs online. Information stolen by skimming a genuine bank card – or taken off lost and stolen cards – could give fraudsters the means to paint the town red at your expense.

Advocate Clive Pillay from the Ombudsman for Banking Services has this advice for keeping your card safe:

- Never let your card out of sight when making payments.
- Never accept help from anyone at an ATM.
- Never use an ATM that is tampered with or visibly damaged. This may be a ploy to force you to use another ATM in close proximity on which a skimming device is mounted.

HELP, I'VE BEEN DUPED!

Experts agree that if you suspect you're a victim of a scam, you should call your bank's fraud hotline number immediately, notify your mobile network and report it to the police.

To find out more, call 0860 101 248 or SMS "protected" to 43366 (standard network rates apply).