BIZCOMMUNITY

How to guard against identity theft

By Alain Tshal.

10 Jul 2020

Everyone is fair (and likely) game when it comes to identity theft. That is true at the best of times, but the Covid-19 pandemic has only intensified cyber fraudsters' hunt for the susceptible and vulnerable.

Photo by cottonbro© from Pexels

According to a recent study by the Association of Certified Fraud Examiners (ACFE), 90% of surveyed anti-fraud professionals reported an increase in consumer scams due to Covid-19. Fifty-one percent believe the increase has been by a significant amount.

Just the other week, the Financial Sector Conduct Authority (FSCA) warned that the Covid-19 pandemic had directly resulted in a marked rise in investment scams targeting unsuspecting South Africans. It pointed to an example known as ‘identity hijacking’ whereby a prominent person’s identity is used fraudulently by criminals, posing as well-known financial institutions, to extract money from individuals.

Worryingly, the true scale of the identify theft problem is difficult to gauge in Africa as, according to World Bank figures, the continent accounts for half of the 1.1 billion people in the world unable to prove who they are. This alone makes it extremely fertile hunting ground for identify scammers.

With Covid-19 continuing to embolden the scammers, now is the time to take charge and proactively guard against identity theft.

Here are some best practice tips to help keep you safe:

Use a password manager

The average person has around 70 to 80 passwords, which inevitably results in hand-written notes. Worse still, according to a Harris Poll conducted by Google, two out of three users admit to reusing passwords across multiple accounts.

A password manager is your friend here, helping to create strong, unique passwords for each account. It also encrypts and stores them in a secure password vault – you only need to remember one master password. It is possible for attackers to hack a password manager app, but your encrypted passwords will be useless. If you keep your master password safe, you should be too.

Those still unconvinced about password managers should, at the very least, start creating unique passphrases that use the maximum number of characters allowed. Remember to reset a password immediately if an account is breached.

As a general rule, don't allow your browser to memorize passwords for accounts, and never use your credentials from one site (such as social media) to create an account or sign in to other (third-party) sites. Wherever possible, create usernames that do not include your name, email address, or birthdate clues. This just gives cybercriminals half of the information they need to crack your accounts.

Use multifactor authentication

Get over being annoyed by the "inconvenience" of multifactor authentication, which requires you to enter a code sent via text message after supplying a username and password. It's an effective, additional layer of security that should be used for every account that makes it available to you.

Stop oversharing online

Rethink how and what you share online. Nothing makes you an easier target for identity thieves than a wealth of voluntarily shared personal information. Combine that digital bounty with all the "quiet" data that's been piling up behind the scenes, and there are criminals that can assume your identity in minutes.

To stay safe, it is a good idea to scrub social media and networking accounts of personal information (date or place of birth, maiden name, mother's maiden name, address, phone number, pet's name, hobbies, etc.). Only use the most stringent privacy settings, choose your "friends" carefully (including reporting duplicate friend requests). Resist social media quizzes or games (most are designed to collect personal information).

Don't download apps from unknown sources and be wary of links and/or ads in your social media feed, including those from people you know (since their accounts may have been hacked). Disable location tagging and avoid sharing content like photos if you're not at home. It is of course impossible to list every precaution, but try to continually ask yourself "why

is this information needed? Who does it benefit? Could it hurt my privacy or compromise my identity?”

Protect your privacy at home

Secure your home wireless network. Only use IoT devices that let you change the password and manage security settings, and securely dispose of old phones, laptops, and storage devices. Furthermore, it is important to not overlook “lo-tech” measures like securing your mailbox, collecting your mail daily, opting out of direct mail advertising, and using a crosscut or microcut shredder to discard all documents with personal information (including junk mail). As ever, double check that you don’t leave valuables (i.e. passports, ID cards, wallets) in cars or other publicly accessible places.

Protect your privacy in public

It’s hard to believe anyone needs this reminder, but public Wi-Fi is incredibly susceptible to eavesdropping. Never use it for online banking, shopping (any activity that involves a credit card), or medical- and health-related services. Do not share private information (such as credit card numbers, date of birth, social security number, or any membership numbers) on voice calls when in public places. You should also protect PINs, membership numbers, and other identifiers when using point-of-sale systems. Pay attention when you swipe a card (beware of hard-to-spot skimmers!) and, remember, cash still works in most places.

Avoid being an easy target

Consumers are often baffled, frustrated, or shocked by the endless variety of clever schemes fraudsters devise to pull off scams. Such is the constant drip-feed of news on the subject that the average person can end up feeling overwhelmed and, in some cases, helpless.

In an ideal world, that should never happen and taking a few simple steps (such as those listed above) can make a huge difference. Scammers don’t like obstacles, so the more stumbling blocks you put in their way, the better. The key is to avoid becoming an easy target. Know what you need to do (within your realm of possibility) and remain vigilant about doing it. Nowadays, doing nothing is not an option.

ABOUT THE AUTHOR

Alain Tshal, District Manager Sub-Sahara Africa at F5 Networks