Cyber fraud has steep collective costs

By Dan Thornton

27 Jul 2022

At the root of the vast majority of cybercrime is a simple human mistake - one password used over and over again, your barcoded boarding pass posted on social media, or your entire collection of digital passwords collated in an Excel doc or iPhone notes. Too often, we have an uninformed or lackadaisical approach to our cybersecurity and identity protection - and are also unaware of our potential contribution to the spiralling costs of rampant cybercrime.

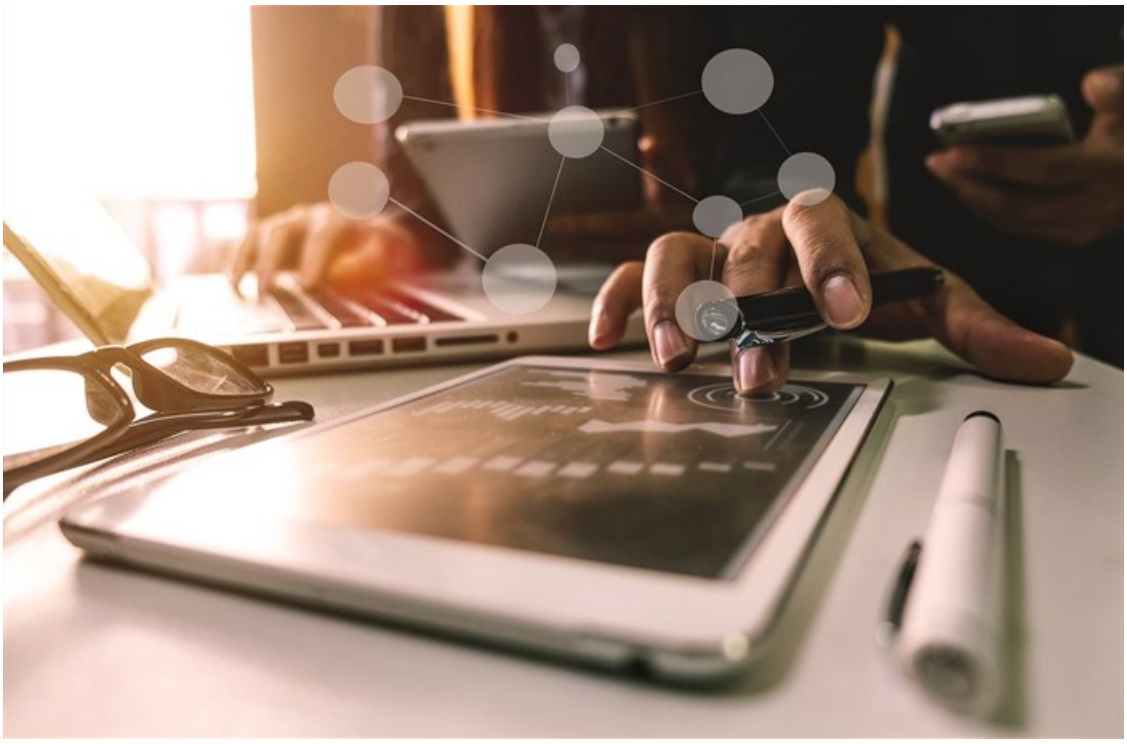

Image supplied

We may believe that cybercriminals have bigger fish to fry than us, or that it is unlikely that a global hacker could stumble upon our missteps in the vastness of the digital realm. These are common misperceptions. What cyber predators are most zealously on the hunt for are the low hanging fruits - the digital accounts and identities of the many people who make basic mistakes when it comes to their cybersecurity. Most cyber criminals are not looking for a wealthy target but an easy one.

Misconceptions also abound when it comes to the potential impacts of cybercrimes. I have heard people say that they don't worry that much about online bank fraud because the banks 'have to pay you back'. This doesn't take into account the months you might wait for bank refunds which can cripple your cash flow and spoil your credit rating in the meantime. And, in cases of identity theft, the repercussions can be much more serious and long-lasting.

Cyber fraud crimes are hard-hitting and difficult to recover from. There's also a large-scale, collective impact. Globally, online bank fraud cases notch up many billions of dollars' worth of losses every year, creating substantial knock-on losses in the insurance sector. Last year, in South Africa with online fraud on the increase and new bank fraud scams emerging, it is estimated that losses exceeded R295m. Somewhere down the line, in the form of rising premiums and charges, you can be certain, we as consumers will most certainly pay for this. As we struggle with Covid recovery and the impacts of supply chain disruptions and war, one of the ways we can all play a part in economic recovery is to act on the power we all have to take our own cybersecurity more seriously.

Most of us manage around 40 to 80 personal digital passwords, including those for our online banking, tax profiles and investment portfolios. Those who are highly digitally active may be operating with in excess of 100 password-protected

online accounts. One of the most common solutions people arrive at to help them cut through the complexity of managing their passwords is to reuse one or a small number of favourites across all their accounts. Of course, cybercriminals know this tendency well - the first thing they do after they confirm a password is in use, is to test how many other accounts it will open.

Here are some basics to help you avoid becoming a victim of cyber fraud or identity theft:

- Create a long but memorable Passphrase for accessing your password manager. A passphrase is a combo of random words that you can remember, but long enough to make it almost impossible for hackers to crack.
- For all other account passwords use machine or algorithm random generated passwords - rather than ones you make up.
- Use a reputable, encrypted password manager app - don't write down your passwords or collate them in unencrypted documents, files or app notes.
- Always enable multi-factor authentication - you may think this extra step is painful, but it is an important layer of protection and worth the short time this step takes.
- Limit what you share online - those who share the most online are most vulnerable to identity theft. Guard your personal details, financials and essential life documents such as passports and visas.
- Never login to sensitive online accounts using public wifi - unprotected networks are one of the easiest ways for hackers to steal your login credentials. Use a VPN or your mobile 4G hotspot.
- If there's any breach or suspected breach of your cybersecurity, change all your passwords promptly.
  One of the riskiest attitudes when it comes to cybersecurity is to think 'it won't happen to me'. Losses from cyber fraud are huge, and they are inevitably impacting on consumers. We need to act on our power as consumers by applying the same vigilance online as we do in our physical world.

ABOUT DAN THORNTON

Dan Thornton, CEO and co-founder of GoldPhish Cyber Security Training, is a former Royal Marine Commandos Officer. During his seven years of service, he was deployed all over the world including multiple operational deployments leading teams in both Iraq and Afghanistan. He then transitioned from the military into a career in Corporate Security Risk Management helping international oil and gas companies operate safely and securely in some of the most high-risk locations around the world, including West Africa, North Africa, and the Middle East.

- SA shoppers warned of online scams ahead of shopping season - 20 Oct 2022
- Building cyber-savvy workplaces in SA - 3 Oct 2022
- Cyber savvy parents keep kids safer online - 22 Aug 2022
- Cyber fraud has steep collective costs - 27 Jul 2022
- Why cybersecurity needs to tighten up as cryptocurrencies plummet - 22 Jun 2022

View my profile and articles...