BIZCOMMUNITY

Tax season is coming amidst a shocking rise in cybercrime

By Dan Thornton

1 Jun 2022

Cybercrimes spiked globally over the past pandemic years. South Africa has been particularly hard-hit and is rising in the ranks of countries in the world most impacted by cybercrime. This was not unexpected, criminals typically rise to the fore in turbulent times looking to take advantage of large-scale disruptions, stressors and distractions. The sudden pivot to remote working exposed businesses to unforeseen risks; the fear-driven seeking of Covid information led individuals into waiting for phishing traps; breath-taking ransomware attacks and bold data breaches compromised the personal data of millions of South Africans.

Dan Thornton, GoldPhish CEO | image supplied

It would be a mistake to think that these are somehow 'victimless' crimes; businesses suffer not just serious financial, but also severe reputational damage; some never recover. Individuals lose their hard-earned money, and sometimes their identities. Breached data has a snowballing effect because it is frequently used to commit further cybercrimes such as identity theft, phishing and government impersonation scams.

In the lead up to tax season, SARS (South African Revenue Services) has already warned of a sharp increase in scams targeting taxpayers aimed at getting us to disclose personal information that can be used to defraud us, as well as SARS.

While the disaster of the pandemic has somewhat abated, economic woes are accumulating globally; geopolitics remains on a knife-edge with war in Europe ongoing and a worldwide food catastrophe is looming.

Dis-Chem hit with data breach, 3.6 million records exposed

11 May 2022

Opportunities are rife for cybercriminals, and if you are not cyber-savvy, it would be wise to learn about and implement cyber hygiene strategies to properly protect yourself, your money and your personal and financial information.

What is well-known across the cyber security industry is that more often than not, a success for the bad guys happens because there's a good guy who made an unfortunate, but preventable mistake. It's important to note that over the next month or two, criminals will unleash a volley of bogus schemes and scams. They view every honest taxpayer as potentially easy prey. We need to be on guard all the time and help others in our lives to protect themselves.

Tax season scam tactics

Tax season is a prime opportunity for identity thieves to approach people with realistic-looking emails, SMSs and WhatsApp messages about their tax returns and refunds. But taxpayers need to be wary of these SARS impersonation scams, where criminals pose as SARS agents with the intention of stealing their victim's money or personal information. The latter can lead to identity theft — which allows scammers to file tax returns in their victims' names and steal their tax refunds, in addition to other negative financial implications.

Common fraud tactics used by cybercriminals during tax season include SMS scams ('smishing'), email scams ('phishing'), phone scams ('vishing') and refund scams. Be on the lookout for professional-looking 'tax return' phishing emails impersonating SARS, which is in fact fraudulent communications enticing one to disclose specific information such as bank account details.

Sars workers picket for salary increases ahead of nationwide strike

Marecia Damons 24 May 2022

These email addresses may appear legitimate, for example they could be from returns@sars.co.za or refunds@sars.co.za so that they give the impression that they are legitimate. These emails contain links to mock-up forms and fake websites made to look like the "real thing", but with the aim of fooling people into entering personal information which the criminals can then utilise in various ways. Links can also contain malware, and if you click, your device and all your data can be compromised.

Another tactic is to try to convince you that you are entitled to a rebate or refund from SARS.

The scammers, pretending to be from SARS, will ask you to make a small initial payment to cover administration fees or taxes, in order to claim the amount owed to you.

How to protect yourself

- Verify the identity of the contact by calling the relevant SARS branch directly or find them through an independent source such as an online search. Do not use the contact details provided in the message sent to you.
- Remember, SARS will never contact you asking you to pay money upfront in order to claim a rebate.
- Never send money or provide credit card details, online account details or copies of personal documents to anyone you don't know or trust and never by email. SARS will never request your banking details in any communication that you receive via post, email or SMS. However, for the purpose of telephonic engagement and authentication purposes, SARS will verify your personal details. Importantly, SARS will not send you any hyperlinks to other websites – even those of banks.
- Avoid any arrangement with a stranger who asks for upfront payment via money order, wire transfer, international funds transfer, pre-loaded cards or electronic currency. It is rare to recover money sent this way.

- Protect your identity — your personal details are private and invaluable. Always be sceptical before handing over personal information via the phone, email or online form.

Check the SARS Scams and Phishing webpage for their updates on the latest bogus schemes. Report any suspicious contact or communication you receive to the SARS Fraud and Anti-Corruption Hotline on 0800-00-2870. To report or get information on phishing, you can email phishing@sars.gov.za.

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...