Be vigilant: How to defend your SMSF from cyber attacks

Superannuation

Tim Mackay

At the end of 2019 there was $2.95 trillion in super, of which self-managed superannuation funds comprised $740 billion, or 25 per cent. This huge honeypot is incredibly attractive to every single hacker on the planet.

In 2019, regulators smashed an online fraud syndicate that had allegedly siphoned millions from super and share accounts using identity data bought on the dark web. While they targeted well-resourced, massive industry super funds, similar future attacks on SMSFs are likely.

Most importantly, you must protect your SMSF identity data. This includes your full name, date of birth, address, bank account numbers, tax file number, passwords and details about your ATO login, driver's licence and passport. If you don't zealously protect this data, you are putting your hard-earned retirement savings at risk.

Store this information securely and, if stored electronically, secure it with a complex password.

IT expert Chris Pirillo says: "Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers."

Shred old documents that show key SMSF information. Don't share this information on social media. Consider a post office box for physical SMSF correspondence. When travelling, don't use public Wi-Fi to access SMSF information.

Ensure the security software and spam filters on all your devices are up to date. If you spend more each year on coffee than you do on IT security, consider re-thinking this.

SMSFs were enthusiastic early adaptors of cloud-based services, online trading and online audit and, as the coronavirus spreads through society, it is also likely we become even more reliant on technology.

This sharing of large amounts of SMSF data between multiple organisations has created cost, time and efficiency improvements. However, it has also accelerated the risk of cyber security threats. Check with your adviser, your accountant and other SMSF service providers that they have a cyber security policy. If they don't, why not?

In a positive step, the ATO recently launched an SMS alert service for SMSFs. When changes are made to your SMSF (for example, bank account details), the ATO will text you.

One common problem is that when you receive a seemingly genuine alert from a bank, how do you tell if it's from the good guys or the bad guys?

First, don't click links, open attachments or download files. Also, don't reply to the message. If you think it is legitimate, call your adviser and let them work it out.

If you don't have an adviser, ignore the contact number on the message, look it up yourself and call them.

If you don't think it's legitimate, delete it and move on. Messages that request your account details or refer to cryptocurrency, PayPal or Western Union are fraudulent.

You should also adopt two-factor authentication, which forces you to log on with a password and a number from a token or a text sent to your phone. It may seem a hassle, but it protects you from hackers.

It is incredibly important to regularly check the transactions in your SMSF bank accounts. Most fraud will typically show up as an unusual payment out of your account to an unrecognised account.

If you think you have been hacked, act immediately. If you've lost money, report it to your local police and lodge a fraud report with your bank.

You can contact expert cyber security counsellors at the not-for-profit IDCARE for free advice and confidential support.

Other reputable resources include ReportCyber and Scamwatch.gov.au.

I believe the ATO should require SMSF trustees to not only have an SMSF investment strategy but also an SMSF cyber security and fraud strategy.

You must prepare your SMSF for cyber threats. A big hack of an SMSF is almost certainly a question of when, not if. A bad guy after your retirement savings only needs to be successful once. SMSF trustees need to remain vigilant at all times.

Some measures to get started with include:

- Ensure the ATO has your correct phone number for SMSF text alerts;
- Monitor SMSF bank account transactions;
- Frequently change passwords;
- Invest in IT security software;
- Limit what you share on social media. SI

Tim Mackay is an independent financial adviser at Quantum Financial.