CBSW
TAX & BUSINESS ADVISORS

Providing you professional direction

Monthly Information Newsletter – Tax & Super

July 2022

Scam myths

In the past 12 months, the ATO has identified and taken action against 595 websites impersonating its online services. These fake sites are designed to steal passwords, personal information and identity documents, such as passports and driver licences.

Currently, the ATO is seeing many SMS and email scams leading to fake myGov sign-in pages –more than 360 of these scams have reported to the ATO since April 2022. However, there many different types of tax and super scams happening year-round, not just in the lead up to Tax Time.

Scammers are always looking for new ways to convince unsuspecting taxpayers into divulging personal information, such as bank details, usernames and passwords.

This year, the ATO has taken out the guesswork and busted some scam myths to help people stay protected:

Myth 1 – Only older people fall for scams

In the past three years, younger Australians have fallen victim to the most tax scams. In 2021, people aged 25 to 34 reported the most amount of money lost to tax scams, closely followed by those aged 18 to 24. In contrast, those aged 55 and above were among those who reported the least financial losses to the ATO. The ATO's Assistant Commissioner Tim Loh says:

> *We want Gen Z and Millennials to know they need to watch out too, as they are just as susceptible to falling for scams, especially those that involve fake tax debts or threats about alleged fraud*
>
> *If you get a phone call saying it's from the ATO and it doesn't sound right, hang up. Check in with someone you trust, like your registered tax agent. Even better go to the ATO's website where we have a listing of all the current ATO scams or call us on our dedicated scam hotline 1800 008 540.*

Myth 2 – Scams are easy to spot, you'd be a fool to fall for one!

"Email and SMS scams are not always full of typos, bad grammar, and promises of riches from foreign royalty. We are seeing many more sophisticated scam messages using official language and fraudulent websites that mimic online services" Mr Loh said.

"We've seen some very convincing email and SMS scams that would trick even the most cautious people."

The ATO does send emails and SMS to taxpayers to share general information or reminders, or to ask people to check their myGov inbox or get in touch with them. However, here are some tell-tale signs to look out for if an email or SMS says it's from the ATO. The ATO will never:

- send an unsolicited message requesting personal information via a return email or SMS,
- send an email or SMS with a link to log in to their online services,
- ask you to pay a fee in order to receive a refund.

Myth 3 – Scams only happen during tax time

While you may only focus on your tax when it's time to lodge, scammers are constantly looking for ways to steal your personal details and financial information. The ATO sees different types of tax and super scams happening year-round.

It's important to always stay vigilant to potential scams, and to keep your personal and financial details safe.

Some common year-round scams involve scammers:

- phoning people about a fake tax debt, and threatening that they'll be arrested if they don't pay it straight away

- sending texts to people saying that they're suspected of being involved in cryptocurrency tax evasion. If you receive this text, don't click on the link.
- sending emails impersonating the ATO and asking for people to update their financial information so their tax refund can be processed.