CBSW
TAX & BUSINESS ADVISORS

Providing you professional direction

Monthly Information Newsletter – Tax & Super

March 2020

Security online: More important than ever

Communication over an online channel has certainly become the default these days and dealing with the ATO is no exception. In fact, the transition to online has plainly been developing over some years.

More and more transactions and interactions are taking place, for example, over the government's initiative myGov — not just the ATO, but Medicare, Centrelink, JobSearch, Veterans' Affairs and many more. Even the way tax and super professionals deal with the various regulatory bodies is changing — using a more secure channel called myGovID.

However, most of us realise that hand-in-hand with the ease and benefits of online transactions comes the very real danger of scammers and criminals. And although the ATO and the government has very efficient security measures and software to ensure the privacy of your personal information, data and transactions, a huge part of your ongoing protection relies on the end user.

As a taxpayer, you play a big part in the ongoing protection of your personal information and making sure it's safe when you interact with anyone online. With emails, text messages or social media posts for example, always be cautious if downloading attachments or clicking a link — even if these appear to be from a legitimate source.

Online services and tools provided by the ATO, for example, should always be accessed via the official website ato.gov.au or through my.gov.au, and not via a link hosted on another site. If there's any question about the legitimacy of an ATO notification, it may be a better option to go directly to the myGov homepage and sign in to check your own inbox for messages.

Of course, you should never share your tax file number (TFN), passwords, bank account details or other sensitive information — even to prospective employers. Some other recommended security steps you can consider include:

- Use multi-factor authentication where possible (using SMS codes as your sign-in option for myGov is a quick and secure way to access ATO online services)
- Only engage with verified ATO pages on social media, and never share information on these platforms
- Back-up your data on an external hard drive or use cloud-based back-up (and don't just leave back-up devices continuously connected to the main unit)
- Disable remote access software until it's needed
- Keep software up to date, including security updates and running regular anti-virus scans.

The processes the ATO uses

For its part, the ATO has steps in place to make sure taxpayer data is kept safe. Part of its process in doing this is to:

- Confirm your details when you contact the ATO
- Logging access to your personal information so that it can identify any unusual behaviour.

The ATO will not:

- ask you for your TFN or bank details via return email, SMS, or on social media
- provide your personal information to anyone without your consent, unless the law permits it to do so
- communicate with you on behalf of another government agency or ask another government agency to represent the ATO.