Watch out for tax scams

The Federal Budget is behind us, and amid the celebrations over tax cuts (around $500 annually for low to middle income earners if proposals are legislated), now is the time to be mindful of scammers pretending to be from government bodies – especially the Australian Taxation Office (ATO). In some cases, scam victims have lost close to $1 million dollars.

Beware scams posing as ASIC

If previous years are anything to go by, the end of the financial year will bring the inevitable wave of scams. Money watchdog the Australians Securities and Investment Commission (ASIC) for instance, has recently warned about crims posing as ASIC representatives asking victims to pay bogus fees. They often make contact via email, accompanied by an invoice that infects your computer with malware if you click the link.

Protect yourself by looking for warning signs that show an email isn't from ASIC at all. The clues include requests to make a payment in order to receive a refund, or if the email asks directly for your credit card or bank details.

Dodgy emails seeming to come from the ATO

More worrying, the ATO has recently advised that scammers are leaving voicemail messages on their victims' phones, threatening the recipient with arrest due to an unpaid tax debt or suspected tax evasion. It can be scary stuff for those on the receiving end.

Scammers are also sending fake emails asking for completion of a 'tax refund review' form to allow recipients to receive a refund. Apparently, the form asks for online banking details, credit card numbers (and even credit limits) as well as your personal address. The ATO is warning not to click on or save any attachments as they may download malicious malware. Above all, do not disclose the personal information the form is requesting.

Scam victims can pay dearly

Not surprisingly, many people are taken in by these scams, and in previous years up to 48,000 people have reported coming across these scams between the peak tax-time months of July and October.

Hundreds of Australians have collectively handed over millions of dollars to scammers with one victim losing $900,000 borrowed from friends and family. Others have handed over personal details such as tax file numbers, which can lead to identity theft.

Protect yourself – and your money

In many cases, scam emails are easily spotted. Hover your computer's mouse over the email address of the sender and it will show the true source. Have a close look through the email, and you'll typically find that scam messages are poorly written with some pretty obvious spelling mistakes. The email may ask you to click what appears to be a link to the ATO website but when you hold the mouse over the link, it won't have the official ato.gov.au address.

If you are unsure if a phone call or voicemail is from the tax man, call the ATO on 1800 008 540. Better still, contact your financial adviser before 30 June to connect with a reputable accountant or tax adviser, who could be a valued source of reassurance if you find yourself crossing paths with a scammer.

Source: AMP News & Insights.