Australian Competition & Consumer Commission

SCAMWATCH

Steer clear of tax scams

The Australian Competition and Consumer Commission is urging Australians to hang up on and delete tax scams after more than $1 million was reported lost to Scamwatch already this year, with over 300 people reporting that they lost money to tax scams in the first half of the year. This is compared with 400 people who reported losing money in the 12 months previous, with $1.6 million lost in total.

These incessant scams come in many guises but generally claim that you have underpaid your taxes and are required to repay the tax debt immediately or face frightening repercussions such as arrest.

“Tax scammers are particularly aggressive so many people feel pressured to pay quickly without questioning them. The most threatening scammers even say that police are on their way to arrest you but can be stopped if you pay immediately,” ACCC Deputy Chair Delia Rickard warned.

These scams often use personal information they found online to try and convince you they’re legitimate. They usually ask for payment for an “unpaid debt” via wire money transfer, credit card, direct debit cards or even iTunes cards. The call looks like it comes from a local phone number but most use voice over internet protocol

(VOIP) phone numbers to disguise the fact that they are calling from overseas.

The ATO said that while it makes thousands of outbound calls to taxpayers a week, the ATO would never cold call you about a debt, would never threaten jail or arrest, and our staff certainly wouldn't behave in an aggressive manner. If you're not sure, hang up and call the ATO back on 1800 008 540.

The ATO would never request the payment of a tax debt via gift or pre-paid cards such as iTunes and Visa cards, nor will it ask for direct credit to be paid to a personal bank account.

Other scams using the busy tax time to slip under your radar include phishing emails, which aim to get your personal details. These scammers tell you that you are owed money by the government but to collect it, you must first pay a small fee.

The ATO said that while it does communicate with people via bulk email, it would never request personal details, such as banking information. If such personal details were required, you would be redirected to ATO Online services.

"If you receive a call or email out of the blue from someone claiming to represent the ATO and that you are entitled to, or owe money – just hang up or press delete. You can check whether they're the real deal by calling the ATO on its official contact number: 1800 008 540," Ms Rickard said.

"Any unusual requests to send money via money transfer, gift card or other digital currency should be treated as highly suspicious. Your personal details, including your Tax File Number, credit card or bank details are valuable and should never be provided to a stranger. If you hand over your personal information to a scammer, they can use it for identity theft or to commit other crimes."

The ATO advises that from time to time it will send taxpayers emails, SMS messages or official social media updates about new services. However, the ATO will never request personal or financial information by SMS or email.

Protect yourself

If you receive an email or phone call out of the blue from 'the ATO' claiming that you are entitled to a refund, that you owe money or asking you to confirm, update or disclose confidential details like your tax file number, press 'delete' or just hang up. Verify the caller or sender by contacting the ATO on its official contact

number: 1800 008 540.

The ATO advises that you should be very careful with whom you share your tax file number (TFN). Never put your tax file number (TFN) on your resume – only give it to your employer after you have started your job. Never share your TFN, myGov or bank account details on social media.

You should also change your passwords if you have shared them with anyone, including family and friends.

The ATO also advises that if you use a tax agent, make sure they are registered by checking at www.tpb.gov.au/onlineregister.

Don't reply to suspicious emails, open any attachments or click on any links – they may take you to a bogus website or contain a malicious virus.

Always keep your computer security up to date with anti-virus and anti-spyware software and a good firewall. Only buy computer and anti-virus software from a reputable source.

If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.

You can report suspected ATO email scams by forwarding the original email to ReportEmailFraud@ato.gov.au.

You can also report scams to the ACCC via the Scamwatch report a scam page or by calling 1300 795 995. You should also spread the word to your friends and family to protect them.