ATO impersonation scams on the rise

The ATO has recently warned taxpayers to be alert to malicious scammers who are using increasingly sophisticated methods and technology to impersonate the ATO. A new tactic on the rise involves “spoofing”, whereby scammers mimic a legitimate ATO phone number visible on caller ID to call or send SMS messages to taxpayers, or mimic a legitimate email domain to send emails.

The SMSs and emails sometimes ask the recipient to click on a link and provide their personal details in order to obtain an alleged “refund” from the ATO. Alternatively, the scammers may ask the taxpayer to pay a fake tax debt. The ATO warns Australians that these scammers intend to steal not only your money, but also sometimes your identity via your personal information.

The risk of falling victim to a “spoofing” scam is even greater considering that some scammers hold enough personal information about the targeted taxpayer to appear genuine.

How to spot a scam

As the ATO legitimately contacts taxpayers by phone, SMS and email from time to time, it’s important to know how to spot the tell-tale signs of a scammer who is impersonating the ATO.

The ATO does **not**:

* send emails or SMSs asking taxpayers to click on a link to provide details such as login, personal or financial information, or to download a file, open an attachment or install software;
* behave aggressively or threaten taxpayers with arrest, jail or deportation;
* ask taxpayers to pay an ATO debt via iTunes, pre-paid Visa cards or cryptocurrency;
* ask for payment of a debt by direct credit to a personal bank account – the ATO will only ask taxpayers to transfer money into an account with the “Reserve Bank of Australia”; or
* use its social media accounts (eg Facebook, Twitter and LinkedIn) to ask individuals for personal information such as tax file numbers.

What to do if you’re targeted

If you are unsure whether a communication is legitimate, do not respond or click on any links or open any attachments. You can call the ATO’s scam hotline on 1800 008 540 and they can tell you whether the communication was legitimate.

If you have made a payment to someone you later suspect is a scammer, you should report this to the ATO; contact your bank or financial institution; make a formal police report; and report the scam to SCAMwatch or the Australian Cybercrime Online Reporting Network (ACORN).

If you have provided personal information such as your tax file number to a suspected scammer, you should also call the ATO scam hotline as soon as possible.

Be alert to scams

Everyone needs to be vigilant about unexpected communications from the ATO. Contact us today if you have any doubts about a recent communication you have received from the ATO or if you have any concerns that you may have fallen victim to an impersonation scam.

Thomson Reuters Tax & Accounting