News Release

For Release: 23 June 2023

ANZ encourages customers to be vigilant to scammers this End of Financial Year

As the financial year comes to an end, ANZ is reminding Australians to be aware of increased scam and fraud activity as sophisticated cyber criminals take advantage of the busy tax period.

In the 2022-2023 financial year alone, the Australian Tax Office (ATO) received 19,843 reports of tax related scams and expect an increase in scam activity this year as Australians prepare to lodge their tax returns.

ANZ Head of Customer Protection Shaq Johnson said: "Technology has made our lives easier and more accessible; customers can now file their tax returns online using a range of tools and services that have transformed the way we manage our tax affairs."

"Towards the end of the financial year, customers share more of their personal and financial information online, with their accountants and their tax agents."

"When you pair this with being the busiest period of the year for most businesses, this can create the perfect opportunity for online criminals to take advantage and catch people off-guard."

Tactics to watch out for at tax time:

- Impersonation of tax officials online, over the phone or on SMS in attempt to gain access to bank details, tax file numbers or other personal information,
- The promise of faster or more substantial tax returns,
- Impersonation of trusted online retailers through mimicking websites,
- Convincing people that they owe the ATO money, and;
- Offering bogus tax refunds to convince people to provide personal information.

Whether it's on the phone, via SMS, email or other communication channels, always be alert to requests for personal information or demands for urgent payment.

Always verify requests are authentic before clicking on links, opening attachments or following instructions, particularly when it comes to your finances or personal information.

Top tips to help protect yourself during tax time:

- Seek confirmation if you receive a request via email, phone or SMS message to change or update payment information. Always confirm by contacting the supplier directly using contact information that you know is genuine, and not contained within the suspicious communications in question.
- Turn on multi-factor authentication for all essential services such as email, bank, social media accounts and any databases holding personal or customer information.
- Access websites directly by typing the URL into a web browser, rather than clicking on a link in an email.
- Remember, if something seems too good to be true, it usually is. Pause and verify before acting.
- Be alert of the latest scams, including myGov tax return and ATO scams.

ANZ's customer protection teams and systems operate 24/7. Customers who believe they may have been a victim of a scam should contact us immediately, on 13 33 50 and report it to the ACCC via the ScamWatch website.

For more information on the types of scams and how to protect yourself visit http://www.anz.com.au/security/types-of-scams and ScamWatch.

For media enquiries contact:
Claudia Filer; +61 401 777 324