News Release
ANZ Scam Safe

For Release: 11 January 2024

New year, new habits: why January is the perfect time to safeguard your personal information for 2024

The new year may be the perfect time to rest and reset, but for scammers, the beginning of the year presents an ideal time to strike. According to ScamWatch, individual scam reports peak in January each year, with 57,000 reports made in the first two months of 2023 alone.

It's always important to remain vigilant to scammers, but the beginning of a new year presents the perfect opportunity to update and defend personal details by switching to tough-to-crack passphrases and activating two-factor authentication to thwart the efforts of opportunistic cybercriminals.

Phishing and recruitment scams are two common tactics used by scammers to target victims, particularly jobseekers in the early months of the year. They will send too-good-to-be-true job offers through email, texts, and social media, containing links and job listings that look legitimate. Through these links, scammers can gain access to personal information, passwords and account numbers.

ANZ Senior Manager, Fraud Analytics, Jess Bottega said: "We encourage everyone when looking for new jobs online to protect their personal information and to beware of any offer made through social media."

"Young people and recent school leavers can be particularly vulnerable to recruitment scams, with the promise of making quick money the biggest lure."

According to ScamWatch, Australians aged between 25 and 44 report the biggest losses to recruitment scams.

Ways to protect your personal information online:

- **Enable Two-Factor Authentication (2FA) –** 2FA uses a second factor to double check your identity when logging into personal accounts such as banking, email or social media.
- **Use passphrases over passwords –** A passphrase is a sentence like string of words, making it longer and more complex than a traditional one-word password. Passphrases are easier for humans to remember, but harder for technology to crack.
- **Turn on automatic updates –** Regular updates are critical to maintaining the security of digital devices, and act as great ammunition against unauthorised access.
- **Be social media savvy** – Always keep your social media posts and privacy settings in check to guard your digital footprint. Seemingly benign details, like a workplace, photos with location details or a birthday can be a goldmine for scammers. With these details, cybercriminals can develop impersonation profiles and commit identity theft.
- **Beware of unexpected messages** – The best way to identify a scammer is to watch for unexpected or strange messages, particularly those demanding urgent action, containing links or requesting personal information.
- **Keep email addresses private** – Protect your email from spam and malicious emails by not sharing addresses online unless vital. As much as possible, have separate email accounts for personal and business use and set up accounts to filter and detect spam emails.

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

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 or visit us at http://www.anz.com.au/security/report-fraud/ for more information.

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

About ANZ Scam Safe: To assist the community in remaining aware and alert to the constantly changing scams and fraud environment, ANZ has launched a new *Scam Safe* series.

Scam Safe will highlight the latest cyber security and fraud issues impacting the community and what ANZ is doing to help protect our customers.