News Release
ANZ Scam Safe

For Release: 30 May 2024

ANZ reminds customers to be alert to business email compromise and fake invoice scams

ANZ is warning customers to be aware of the tell-tale signs of business email compromise and fake invoice scams – commonly referred to as payment redirection scams.

According to the ACCC's *Targeting scams* report, Australians reported combined losses of $91.6m to payment redirection scams in 2023. Small and medium sized businesses are the most common targets, as their systems are usually less complicated for cyber criminals to infiltrate. The scammer hacks into the system of the legitimate business, then may alter the details on a payment request, so the payee pays the scammer rather than the legitimate business.

ANZ Scams Portfolio Lead, Ruth Talalla said: "Scammers use increasingly sophisticated and use targeted methods to exploit Australian consumers who are trying to pay legitimate businesses for goods or services.

"It can be easy to miss a minor change to an invoice or email and pay a scammer instead of the intended business or person. It's important to remember to check invoice details with the person or company you want to pay before submitting payments, especially for first time payments or when their account details seem to have changed. It's preferable to use PayID for payments when that's an option, so you know who you're paying."

Criminals may pose as a legitimate business, or representatives from those businesses, and email requests for the urgent transfer of funds to a new account; raise false invoices with fraudulent details; or ask a business' contacts to update banking details with fake account details.

How to spot these scams:

- **Unexpected contact method or requests:** Be wary if someone you do not usually have email or social media messaging contact with reaches out with a personal or payment request (for example on WhatsApp).
- **Modified payment details on an invoice:** Check payment details against previous invoices from that business and question any changes to payment details direct with the company or individual you're paying.
- **Dodgy domains:** A cybercriminal will often pick up an email domain that closely resembles the true sender – compare the email to the company domain online to be certain.
- **Poorly written text or inconsistent message formats:** Check for grammatical or spelling errors and look out for anything in the tone that does not match the way the sender usually writes (though a well written message does not mean it is from the legitimate sender).
- **A missing or faked email signature:** More often than not, cybercriminals will not have the legitimate company's or individual's email signature. Check for any inconsistencies with the legitimate company's or individual's email signature.

Tips to avoid these scams:

- Never call the phone number given in a suspect email or message. Use a phone number you received independently and talk to the person you have previously dealt with if possible.
- Check new or updated account details with the legitimate company on a phone number you have independently sourced, before sending funds.
- If you receive an email or message that creates a sense of urgency don't rush.
- Use PayID to make payments when available, so you know who you're paying.
- If you're intending to pay a large amount, send a small amount first then check the legitimate company or individual received it before sending a larger amount.

For media enquiries contact:
Will Watson +61 403 878 269

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 *Scam Safe* series.

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

To stay *Scam Safe,* ANZ encourages customers to learn their security ANZ's:
A: Always be wary
N: Never share personal information, with anyone
Z: Zoom in on the details, they matter