STAY SECURE
THIS END OF FINANCIAL YEAR

The end of the financial year is a busy time for organisations and their employees. Cyber criminals look to take advantage of this period, where we might be more likely to overlook the signs of a scam.

> $98M

in losses from Business Email Compromise (BEC)[1]

In FY 2021-22, cybercrime reports increased by nearly

13%[2]

The ACSC received

447 ransomware reports in FY 2021-22[3]

Help keep your organisation safe by staying vigilant to online scams and following the below tips.

01

CONFIRM THE SENDER

Look for the signs of Business Email Compromise (BEC). If you receive an unusual, urgent or threatening request via email, be suspicious and confirm the authenticity by contacting the sender directly through another channel.

02

PAUSE BEFORE YOU PAY

Scammers may impersonate or compromise a trusted supplier's email account and attempt to extort money from businesses by sending invoices that appear genuine but contain the scammers account details. According to Scamwatch, in April 2023, there was $5,023,678 stolen through false billing scams.[4]

03

CALL OUT SUSPICIOUS MESSAGES

At this time of year, scammers may impersonate the ATO and threaten individuals and businesses with tax debt or offer rebates. In Australia, $4,217,895 has been reported stolen through rebate scams so far in 2023.[5] If you're unsure, always contact the ATO directly.

04

STAY UP-TO-DATE

For more information on how to protect yourself and your organisation from cybercrime:

- Visit the ATO at ato.gov.au and search for scam alerts
- Visit the Australian Cyber Security Centre (ACSC) at cyber.gov.au
- Visit the ANZ Security Centre at anz.com.au/security

[1,2,3] ACSC Annual Cyber Threat Report 2021-2022. [4,5] Scamwatch.gov.au

anz.com

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522.
Item No. 98593 06.2023 WZ133034