Business

ANALYSIS

JACKSON HEWETT: Qantas cyber hack the latest of many to come

Jackson Hewett The Nightly
Wed, 2 July 2025 3:39PM Comments

Jackson Hewett

The hack on Qantas is one in a growing trend. The Nightly Credit: The Nightly

Monday's attack on a Qantas call centre in Manila is the latest in a slew of cyber attacks that appear to be growing in both sophistication and frequency.

According to the Global Anti-Scam Alliance, $US1.03 trillion ($A1.57t) was lost globally in 2024, finding nearly half of global consumers experiencing a scam attempt at least once a week.

With six million customer records potentially stolen during the breach, Australians were likely to be among those whose personal data could be used to hack financial accounts or to commit identity theft fraud.

Australia continues to be a lucrative destination for scammers, drawn by high balances in bank accounts and superannuation funds.

In April this year, some of the largest super funds in the country, including including AustralianSuper, Hostplus, REST and Australian Retirement Trust were subjects of a "credential stuffing" scam, which relies on people using the same password across multiple accounts.

AustralianSuper, which has more than 3.5 million customers and $367 billion in funds under management said four accounts in the pension phase were defrauded of a combined $500,000. In many instances the super funds had not turned on multi-factor authentication, which requires users to verify their identity using two or more different factors, such as a password and a code sent to their phone.

Australians are becoming better at recognising scams however, and despite it costing an estimated $2b last year, the Government's National Anti-Scam Centre said losses were down by 25 per cent on their peak of $3.1b in 2022.

The number of scam reports fell almost 18 per cent over the same period from 601,803 in 2023 to 494,732 in 2024.

The top five losses, accounting for 80 per cent of total losses were led by investment scams at almost $1b, followed by romance scams, payment redirection, remote access and phishing.

FEDERAL POLITICS

Taylor says Wong coming home ‘empty-handed’ after US visit

Kimberley Braddish and Peta Rasdien

In January the National Anti-Scam Centre launched the ‘Stop. Check. Protect.’ campaign to encourage Australians to confidently identify, avoid and report scams.

Matt Warren Credit: supplied

But while Australians appear to be getting the message, scammers are using artificial intelligence to become more sophisticated.

Matt Warren, director of the RMIT University Centre for Cyber Security Research, said scammers are now using AI to polish their messages, eliminating the spelling and grammar mistakes that used to act as red flags. This makes scam emails harder to detect, especially when people are distracted or in a hurry, with Mr Warren noting “those warning signs aren’t as obvious anymore”.

CELEBRITY

Valance in line for major settlement after billionaire split

Kimberley Braddish

Mr Warren said scammers were already using digital tools to target people at scale, focusing on the “five per cent or so” of victims who were susceptible to spoof communication.

But Daswin De Silva, professor of AI and Analytics and Director of AI Strategy at La Trobe University said AI was enabling scammers with far more impressive tools, such as the ability to mimic recognisable voices, for fooling potential victims.

“The Qantas attack was likely driven by impersonation attacks or social engineering, and with artificial intelligence, we can do this in droves,” he said.

“We already have examples of deep fakes being used impersonate individuals. These attacks are not that sophisticated, but the attack surface and the intensity and complexity of the attacks definitely can increase with AI.”

As companies collect more and more consumer data in pursuit of increasing levels of personalisation, the threat expands.

Daswin De Silva Credit: supplied

“Companies will use AI to determine certain buying patterns, certain behaviours, but AI can also be used to derive more personalised information than what we would have typically disclosed to a commercial organisation,”Mr De Silva said.

“So there is also that risk that with increased data collection about us and how we live, scammers can develop more ways to trick us.”

Mr De Silva said Australia lagged the European Union, which had introduced the General Data Protection Regulation in 2018 which gives individuals more control over how their personal data is collected, used, and stored, and imposes strict rules on organisations that handle such data, including third parties.

It also makes companies accountable for infringements, with fines of up to 4 per cent of annual worldwide turnover. In the US, which is far more supportive of innovation than regulation, data protection is governed by a patchwork of Federal and State laws.

“We want to be in the middle between the EU and the US, where there is a healthy balance of supporting, enabling innovations, but also securing and looking after the rights, the privacy, the confidentiality of individuals,” Mr De Silva said.

It is not just individuals that were at risk from identity theft, with government transfers an increasingly lucrative scam for criminal gangs.

TRAVEL

Australian Government issues global travel warning

Max Corstorphan

Last week the Federal Bureau of Investigation announced it had seized $US245m and charged hundreds of citizens and medical professionals as part of a widespread identity fraud targeting the US healthcare system that may have resulted in as much as $US15b in losses.

Mr Warren said Australia’s Medicare system would be a valuable target using similar identity theft techniques.

The attack on a third party provider also called into question the security processes expected by companies looking to outsource costly activities like call centres, to providers who may not have made the appropriate investment in their systems.

Mr De Silva said stronger regulation could help close cybersecurity gaps by requiring third-party technology providers to meet minimum standards, including mandatory audits and system checks, training, and hiring practices.

“There is definitely opportunity for tighter regulation that ensures the safety of data and individuals,” he said.