

The Sydney Morning Herald

Technology [Cybersecurity](#)

Internet provider Tangerine suffers cyberattack

[David Swan](#) and [Sumeyya Ilanbey](#)

February 21, 2024 – 4.24pm



Listen to this article

4 min

Internet service provider Tangerine has suffered a data breach, with the full names, dates of birth, email address and mobile phone numbers of more than 200,000 customers taken by hackers.

Tangerine said in an email to customers that their personal information was disclosed in a breach on February 18, which was reported to management two days later.



Tangerine co-founders Andrew and Richard Branson.

“We are writing to let you know that Tangerine has been impacted by a cyber incident that has resulted in the unauthorised disclosure of some of our customer data,” the company said in a letter to customers.

“We are contacting you as unfortunately, we believe that some of your personal data was disclosed as a result of this incident and have launched a full investigation to determine the cause. Please note that this incident does not affect the availability or operation of our NBN or mobile services – they continue to operate as normal and remain safe to use.”

The company said that while full names, dates of birth, mobile numbers, email and postal addresses as well as Tangerine account numbers were taken, no credit card or debit card numbers were compromised.

“No driver’s licence numbers, ID documentation details, bank account details or passwords were disclosed as a result of this incident,” the company told customers.

“Upon learning of the incident, we immediately began an investigation to determine how this incident occurred. This investigation is ongoing and is being treated with the utmost priority.

“We know that the unauthorised disclosure relates to a legacy customer database and has been traced back to the login credentials of a single user engaged by Tangerine on a contract basis.”

Tangerine has been contacted for further comment.

The phone and broadband provider is headquartered in South Melbourne and is one of Australia’s fastest-growing internet providers. It was founded by brothers Andrew and Richard Branson in 2013 and 232,000 of its current or former customers have been caught up in the breach.

“No one is more disappointed than me. As a founder-led organisation, my brother and I put everything we can into the business along with a very talented, committed team,” chief executive Andrew Branson said in a statement.

“Anything that negatively impacts our loyal customer base hurts, and we sincerely apologise to them for this incident.

“Thankfully, over recent years we’ve taken multiple pre-emptive steps which have included reviewing what data we really need to keep and what we can live without. That’s why we don’t hold any driver’s licences, any ID documents or any credit card numbers.

“Moving forward, we are fully committed to learning from this incident and implementing necessary improvements to prevent similar occurrences in the future.”

The company has engaged a cybersecurity specialist to investigate the incident and is recommending customers be suspicious of any communications claiming to be from Tangerine Telecom. Customers can also contact government support services including ID Care and the Australian Cyber Security Centre.

The cyberattack on Tangerine is the latest in a series of high-profile data breaches. Just last month, Victoria’s court system [was hit by a ransomware attack](#), with hackers potentially accessing archives containing highly sensitive testimonies.

Before Christmas, St Vincent’s Health was hit by a cyberattack, while DP World was forced to shut down its terminals in November after a cybersecurity incident.

Australian business leaders this year nominated [cybersecurity as their top priority](#), according to a report from KPMG, *Keeping us up at night*, which surveyed more than 300 chief executives.

The scale of concern was highlighted in 2022 when hackers stole the details of 10 million Optus customers in September, and a month later accessed sensitive health information of 9.7 million Medibank customers, progressively leaking the data in an attempt to get the companies to pay a ransom.

The Business Briefing newsletter delivers major stories, exclusive coverage and expert opinion. [Sign up to get it every weekday morning](#).



David Swan is the technology editor for The Age and The Sydney Morning Herald. He was previously technology editor for The Australian newspaper. Connect via [Twitter](#) or [email](#).



Sumeyya Ilanbey is a business journalist for The Age and Sydney Morning Herald. Connect via [Twitter](#) or [email](#).
