Media Statement: iiNet cyber incident

19 August 2025: iiNet has been impacted by an incident involving unauthorised access to its order management system by an unknown third party.

Upon confirmation of the incident, we acted quickly to remove the unauthorised access to the system. External IT and cyber security experts have been engaged to determine the full scope of accessed information.

We understand these incidents are concerning, which is why we are proactively contacting customers to provide more details, apologise and offer support.

At this time, the unauthorised access appears to have been contained to the iiNet internal ordering system which is used to create and track orders for iiNet services, such as NBN connections. Early investigations suggest the unauthorised access was gained using stolen account credentials from one employee.

We can confirm no credit, banking or financial information have been compromised. No driver's license numbers, ID documentation details, or bank account details were disclosed as a result of this incident.

“We unreservedly apologise to the iiNet customers impacted by this incident,” said TPG Telecom chief executive officer, Inaki Berroeta.

“We are continuing our investigations to ensure we understand all details surrounding this incident. We will begin contacting customers to make them aware of the incident, apologise and provide details on the support available.”

iiNet will provide further updates if more information becomes available.

What we are doing:

Upon confirmation of this incident on Saturday, 16 August, we enacted our incident response plan, began work to ensure the security of the system and to determine what occurred. We have engaged external IT and cyber security experts to assist with our response to the incident.

Our teams have been working around the clock to understand the full scope of customer data affected by this breach, and how this might impact them.

We are making direct contact with affected customers to inform them of this incident, and to provide support and guidance on what to do next.

We have actively engaged with the Australian Cyber Security Centre (ACSC), the National Office of Cyber Security (NOCS), the Australian Signals Directorate (ASD), the Office of the Australian Information Commissioner (OAIC) and other relevant authorities in response to this incident.

What personal information has been accessed in this incident?

Based on the current evidence from our forensic experts, historic data related to iiNet service orders was accessed without authorisation.

Most of this data is of a non-identifying nature and used to authenticate and activate orders for iiNet services.

While our investigation is ongoing, at this time it appears a list of email addresses and phone numbers was extracted from the iiNet system. The list contained around 280,000 active iiNet email addresses and around 20,000 active iiNet landline phone numbers, plus inactive email addresses and numbers. In addition, around 10,000 iiNet user names, street addresses and phone numbers and around 1,700 modem set-up passwords, appear to have been accessed.

Importantly, no credit card, banking details or customer ID documents (passport or driver's licence) are held in this system.

What should customers do?

We will be taking immediate steps to contact impacted iiNet customers, advise of any actions they should take and offer our assistance. We will also contact all non-impacted iiNet customers to confirm they have not been affected.

We urge customers to remain vigilant, especially to any suspicious communications received via email, text or phone call.

If in doubt, contact iiNet directly or seek independent advice from trusted sources, including the Australian Cyber Security Centre at cyber.gov.au.

We have set up a dedicated hotline at 1300 861 036 so customers can reach us if they have any concerns.

A dedicated information page on our website (https://help.iinet.net.au/information-on-cyber-incident) has also been established to provide the latest updates about the incident.

We will continue to share updates direct with customers, on our website and via the media and our social channels.

- ENDS -

Media requests

media@tpgtelecom.com.au