FAQs for Account Holders

What happened?

On 13 December 2022, iiNet detected unauthorised access to its Business Hosted Exchange service. iiNet's investigations subsequently showed that an unknown threat actor had accessed certain mailbox items, including emails sent and received, and contacts and notes stored in, the Business Hosted Exchange.

What makes you think that my information has been impacted?

iiNet investigations have shown that an unknown threat actor accessed certain mailbox items in its Business Hosted Exchange.

iiNet forensic experts have analysed the mailbox items which they believe were specifically accessed by the threat actor and determined that the impacted data includes certain mailbox items from our Hosted Exchange email service and included some of your information.

What was the focus of the unauthorised access?

iiNet investigation indicates that the threat actor specifically targeted mailbox items which appeared to relate to financial and cryptocurrency information and accounts and therefore, we believe that this information was the main focus of their attention.

We recommend that you/your company take the protective steps outlined in the notification letter.

How did iiNet respond?

iiNet implemented measures to stop the unauthorised access, as well as additional security measures.

iiNet also engaged external forensic assessors and other experts to help with its investigation of the event and its assessment of affected customers and individuals.

We understand that determining which individuals were affected and in what ways has been a complex process. This is because emails and other mailbox items often contained a wide range of information, included different file types and for many of the files, it was difficult to immediately ascertain which individuals and accounts they related to.

iiNet have also notified relevant authorities, including the Office of the Australian Information Commissioner, the Australian Cyber Security Centre, the Australian Federal Police and the Australian Taxation Office.

Why has it taken so long for iiNet to provide me with the details of the impact?

As soon as iiNet became aware of the unauthorised access, it engaged external forensic experts to help with the investigation of the event and its assessment of affected customers and individuals**.**

We understand that determining which customers and individuals were affected and in what ways has been a complex process. This is because emails and other mailbox items often contained a wide range of information, included different file types and for many of the files, it was difficult to immediately ascertain which individuals and accounts they related to.

The assessment of the impacted data has only now been completed and that is why we are reaching out to you.

Over what time period did the breach occur and when was it discovered?

We understand that mailbox items were most likely to have been affected in the period from 14 October 2020 until 19 November 2022.

iiNet's investigations indicate that the threat actor was using keyword searches for mailbox items in the above period which appeared to relate to financial and cryptocurrency information and accounts.

The incident was discovered on 13 December 2022, when iiNet external cyber security experts advised that they had found evidence of unauthorised access to the Hosted Exchange service.

Has my information been disclosed publicly?

iiNet is not currently aware of any evidence that any of the impacted information has been made publicly available, including on the dark web. However, its experts are continuing to monitor this.

My tax file number has been compromised. Have you contacted the ATO?

iiNet have reported the incident to the ATO and are working with them to let them know that your TFN has been impacted as part of the incident so that they can apply protective measures to your account. If

you wish to contact the ATO yourself about your TFN, you can speak to the ATO's specialist identity security team on 1800 467 033 (available 8am to 6pm AEST Monday to Friday).

How do I know that the email service is secure now?

iiNet implemented measures to stop the unauthorised access and further security measures have been put in place to protect the Hosted Exchange service. We are advised that these measures include enhanced threat detection and response tools and capabilities, increased integration into our event management system and further security controls and tools for managing user access. iiNet have also put in place additional monitoring capabilities to help detect and contain threats.

Does this effect any other iiNet products?

This does not affect any other business products or services and does not affect any home or personal iiNet products – such as broadband or mobile.

What steps can I take to keep my information safe and secure

The unauthorised access has been stopped and further security measures have been put in place.

As a precaution and in the interests of best practice cyber security, we recommend that you adopt the following security practices:

- Always ensure that you're using strong, unique passwords for all your accounts including any crypto exchange accounts, and that you update them regularly. If you wish to change a Hosted Exchange mailbox password | iiHelp (iinet.net.au)
- Install the latest software updates and anti-virus software.
- Be vigilant for suspicious behaviour. It's quite normal to see the occasional pop-up ad, spam email or website redirect, and this may not immediately be a cause for alarm, but if you start to notice an increase in certain suspicious actions when browsing the web or checking your emails, it may be a sign that your information has been leaked. Please be wary of unexpected or unusual 'random' emails containing links or attachments.
- Please also watch out for unexpected calls and texts, particularly if they ask for your personal information or refer you to a web page asking for your personal information. If you are ever concerned that a call from a financial institution or other service provider may not be legitimate, end the call without providing your personal information and call the business back on a publicly listed number.
- Harassing or threatening communications should be reported to the police, including in circumstances where someone claims to have access to your information and threatens to release it unless you make a ransom payment. You can also report such messages to the Australian Cyber Security Centre's "ReportCyber" service here: https://www.cyber.gov.au/acsc/report.

Follow up questions

Individuals calling about IDCARE

iiNet have partnered with IDCARE, Australia's national identity and cyber support community service.

They have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused. IDCARE's services are at no cost to you. If you wish to speak with one of their expert Case Managers please complete an online Get Help form at www.idcare.org or call 1800 595160. Note IDCARE specialist Case Managers are available from 8am-6pm AEDT Monday to Friday (excluding public holidays).

When engaging IDCARE please use the referral code **TPG23**.

Individuals calling to take up Equifax subscription

iiNet are offering customers whose ID documents have been impacted the option to take up a 12-month subscription to Equifax Protect at no cost.

Equifax provides a credit and identity monitoring service. If you would like to take up a 12-month subscription to Equifax Protect at no cost, please contact the iiNet support number which is 1300 552 854 from Monday to Friday, between the hours of 9am to 9pm (AEDT) (excluding public holidays). You will need to provide the reference code that was in the notification letter you provided to you.

An Equifax Protect subscription provides you with monthly credit reports and alerts if there are changes to your credit report.