OUTBACK PHARMACIES
C.P Peoples Chemist, Tembys Day Night Pharmacy, Netting Chemist, Westside Plaza Pharmacy, Good Price Warehouse Broken Hill

Outback Pharmacies Group
325 Argent Street
Broken Hill NSW 2880
ABN: 32 264 862 317
info@outbackpharmacies.com.au
www.outbackpharmacies.com.au
08 8087 3326

6th January 2026

Outback Pharmacies Cyber Incident

Outback pharmacies recently experienced a cyber incident and unfortunately, due to the nature of the incident, we may be unable to determine the precise information impacted. For this reason, we are informing our customers on a precautionary basis to provide guidance that you may wish to consider taking to protect your personal information against potential misuse.

We understand this news may be concerning. The notification below outlines what happened, the findings of our investigation to date and what information may have been found to be involved. This information has been provided in the spirit of transparency and out of concern for our customers & community, which we serve and to which we belong.

WHAT HAPPENED?

In November 2025, Outback Pharmacies experienced a cyber incident involving unauthorised third-party access to a portion of our IT environment.

As soon as this incident was detected, a response team was quickly mobilised, and work began to ensure the security and integrity of our systems. We would like to assure you that we have implemented measures to ensure the security of our systems and to reduce the risk of recurrence.

While our investigation is ongoing, it has unfortunately discovered that a portion of our environment has been accessed, however due to the impact of the incident on our systems, we are unable to determine the specific data involved. We appreciate that the concern that this uncertainty may cause and as member of the local community, we have taken this step to issue this precautionary notification to all our customers as a demonstration of our commitment to you.

IMPACTED PERSONAL INFORMATION

Please consider if you have previously provided information to us and review the following guidance:

- ***What information of mine may be involved?***

  We set below the types of personal information which we may have collected from you:

  - Contact information
  - Health Information

  The remedial advice with respect to the above types of personal information is contained within the below 'Questions and Answers' section. This remedial advice has been provided on a precautionary basis only, as we are unable to confirm or rule out whether your personal information was specifically involved in the incident due to the impact on our systems.

- ***What if I haven't provided some/any of the information below?***

  In this case, your personal information is <u>not involved,</u> and you are not required to take any further steps.

We appreciate that this notification may be concerning. We are committed to providing you with the support and assistance you need.

We set out guidance below on steps that you may want to take in response to this incident, and support services available to you.

WHAT ACTION HAS OUTBACK PHARMACIES TAKEN?

Since discovering the incident, we have secured our systems and put in place additional security measures to prevent reoccurrence.

We have also conducted an investigation to better understand what happened, however at this point we anticipate that it will likely not be possible to confirm exactly what data was involved.

We have also informed the relevant government agencies and law enforcement authorities including the NSW Police, the Australian Cyber Security Centre (**ACSC**) and the Office of the Australian Information Commissioner (**OAIC**) of the incident.

WHAT STEPS CAN YOU TAKE TO PROTECT YOUR INFORMATION?

As noted above, please carefully read this communication and the below '*Questions and Answers'* section, which provides detailed advice on steps you can take to protect your information against potential misuse on a precautionary basis.

Should you have any questions once you have reviewed this notification, please do contact us at info@outbackpharmacies.com.au

We recommend you remain vigilant against the risk of phishing emails and scams, which are often the most likely risk associated with any unauthorised access to contact information.

Scam calls and phishing emails are becoming increasingly sophisticated and can appear to come from legitimate email addresses or phone numbers with local area codes. They will often claim to be contacting you from a reputable organisation, such as a government entity, bank, or telecommunications agency. They will also create a sense of urgency to try to get you to disclose sensitive information or to elicit funds from you.

What precautionary steps can I take?

There are some steps you can take to help protect yourself against these scams. We recommend you take the following steps:

Contact information (name, address, email address and/or phone number);

Where a third party has accessed and disclosed your contact information, it is important to consider the following:

- **Phishing**: cybercriminals try to trick people into handing over personal information. This can be done through fake emails or text messages that appear to be from a person or organisation you trust. Phishing can lead to a loss of information, money or identity theft as a result of your online banking logins, credit card details or passwords being stolen. If you think you've been the target of a phishing attack, visit the cyber.gov.au phishing advice page to understand the steps you should take;
- **Website addresses/ URLs:** when on a webpage asking for your login credentials, take note of the web address or URL ('Uniform Resource Locator'). The URL is located in the address bar of your web browser and typically starts with 'https://'. If you are suspicious of the URL, do not provide your login details. Contact the entity through the usual channels to ensure you are logging into the correct web page. Please note that we will never contact you to ask for your username or password;
- **Passphrases**: when compared to a **password**, a passphrase is a memorable sequence of words that offers stronger protection due to its length and complexity. Create strong and unique passphrases of 14 or more characters long for every account. You can check the strength of your passwords/passphrases on the NSW Government password checker website: https://www.nsw.gov.au/id-support-nsw/passwords;
- **Multi-factor authentication**: activate this for your online accounts where possible, including your email, banking, and social media accounts to add an extra layer of security; and
- **Software updates and anti-virus software**: update your software regularly and install anti-virus software on any device you use to access your online accounts.

Health information

Some of your health information, specifically prescription information, may have been subject to unauthorised access.

For context, cyber-criminals typically seek to misuse information that can be easily manipulated for financial gain (such as credit cards and identity documents for identity theft). For this reason, health information by itself is generally not useful to a cyber-criminal.

We know that it will be concerning to learn that your health information may have been accessed in this manner. Should you experience any anxiety or distress in relation to this, please seek medical advice from your regular treating physician or GP.

Who can I contact for more information about cyber security?

Additional general resources on identity and cyber security support can be found here:

- **OAIC**: The OAIC offers data breach support and resources on its website: https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/data-breach-support-and-resources.
- **IDMatch**: Commonwealth, state and territory governments also provide free guidance on how to protect government issued documents in connection with a data breach: https://www.idmatch.gov.au/individuals/data-breach.
- **Scamwatch**: The National Anti-Scam Centre provides further information about phishing and how to recognise, avoid and report scams here: https://www.scamwatch.gov.au/.
- **ID Support NSW**: Information, support and advice on cybersecurity and identity misuse prevention: nsw.gov.au/departments-and-agencies/id-support-nsw
- **ASD**: The Australian Signals Directorate's Australian Cyber Security Centre provides advice and information about

how to protect yourself online here: https://www.cyber.gov.au/.

- **ReportCyber**: You can report a cybercrime or incident by calling 1300 292 371 or online here: https://www.cyber.gov.au/report-and-recover/report.
- **Mental health support**: Call 000 in an emergency. A number of free government and community services provide online or by phone mental health support or see your doctor.
    - Lifeline – 13 11 14
    - Kids Helpline – 1800 55 1800
    - Mental Health Crisis Assessment and Treatment Team in your state/territory
    - Beyond Blue – 1300 224 636
    - MensLine – 1300 78 99 78
    - SANE Helpline – 1800 187 263
    - Headspace – 1800 650 890

If you have any other questions, please contact our team at cyberincident@outbackpharmacies.com.au