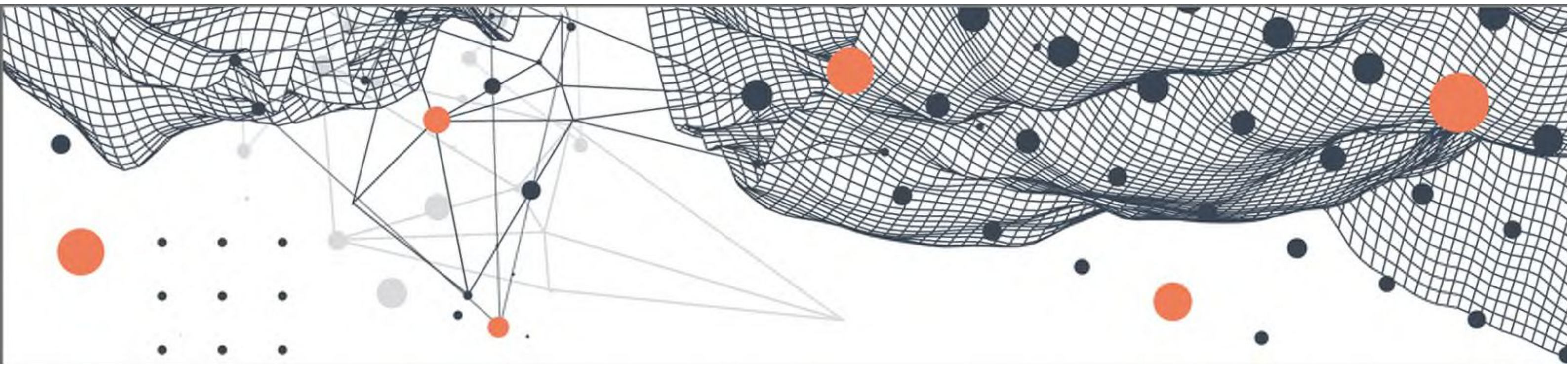
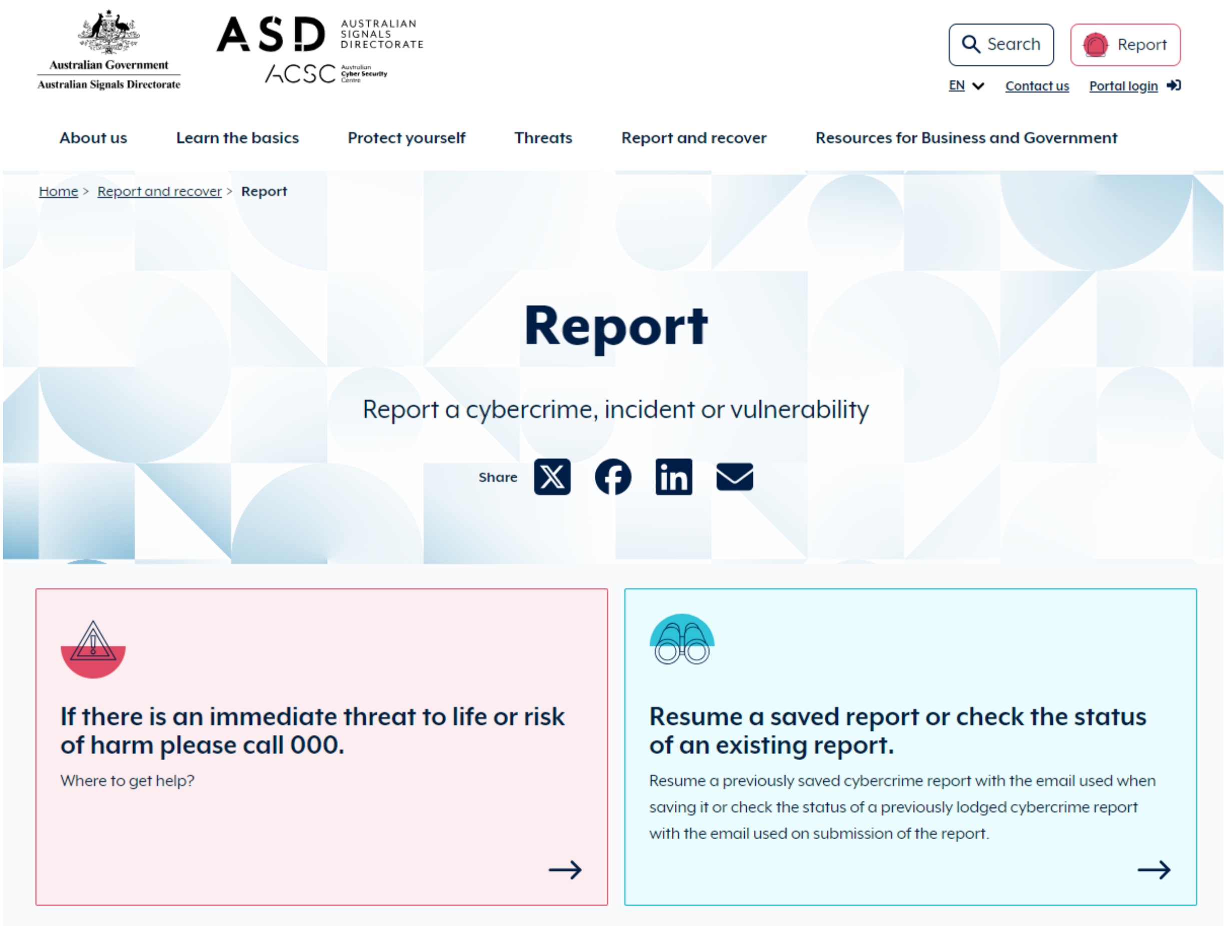


HOW TO MAKE A REPORT

Mandatory ransomware and cyber extortion payment reporting is active **from 30 May 2025**

Step 1: *ReportCyber* landing page

You can access the ransomware and cyber extortion payment reporting form through the landing page on *ReportCyber* found at: https://www.cyber.gov.au/report-and-recover/report.


Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre
Search
Report
EN
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government
Home > Report and recover > Report
Share

Report

Report a cybercrime, incident or vulnerability

If there is an immediate threat to life or risk of harm please call 000.

Where to get help?

Resume a saved report or check the status of an existing report.

Resume a previously saved cybercrime report with the email used when saving it or check the status of a previously lodged cybercrime report with the email used on submission of the report.

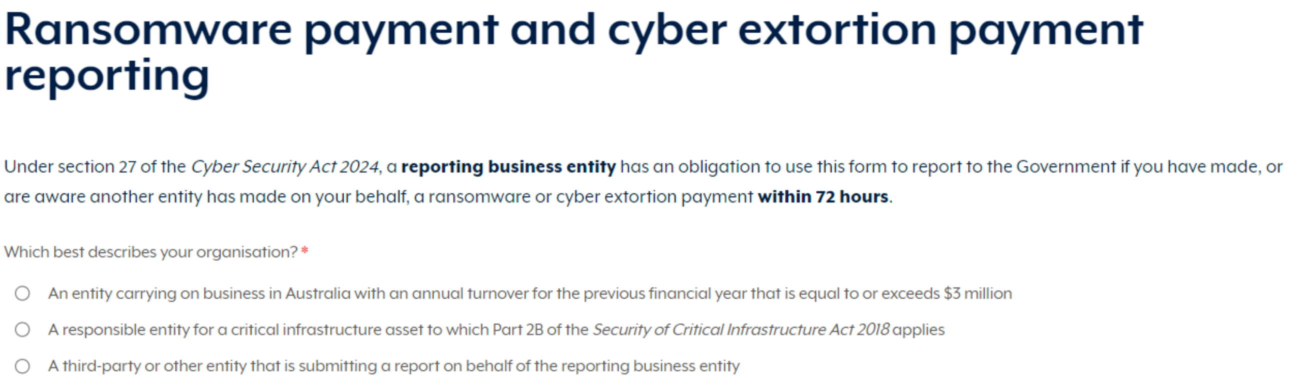
Scroll down and under the section ‘Who are you reporting on behalf of?’ select ‘A business or organisation.’ This is the same button you would use if you were reporting a cybercrime to the Police, a cyber security incident or a cyber security vulnerability to ASD’s ACSC.

Once you have identified whether you are a ‘Large Organisation’ or a ‘Critical Infrastructure entity’ or not, you can scroll down to the end of the list and select ‘**Ransomware payment and cyber extortion payment reporting**.’ Move on to Step 2.

Step 2: Ransomware payment and cyber extortion reporting landing page

You will be taken to another webpage where you will identify whether you are:

- **An entity carrying on business in Australia with an annual turnover for the previous financial year that is equal to or exceeds $3 million;**
- **A responsible entity for a critical infrastructure asset under Part 2B of SOCI;**
- **A third party or other entity submitting a report on behalf of the reporting business entity.**



Ransomware payment and cyber extortion payment reporting

Under section 27 of the *Cyber Security Act 2024*, a **reporting business entity** has an obligation to use this form to report to the Government if you have made, or are aware another entity has made on your behalf, a ransomware or cyber extortion payment **within 72 hours**.

Which best describes your organisation? *

○ An entity carrying on business in Australia with an annual turnover for the previous financial year that is equal to or exceeds $3 million

○ A responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies

○ A third-party or other entity that is submitting a report on behalf of the reporting business entity

Once you have made a selection, scroll down and move onto Step 3 to commence the form.

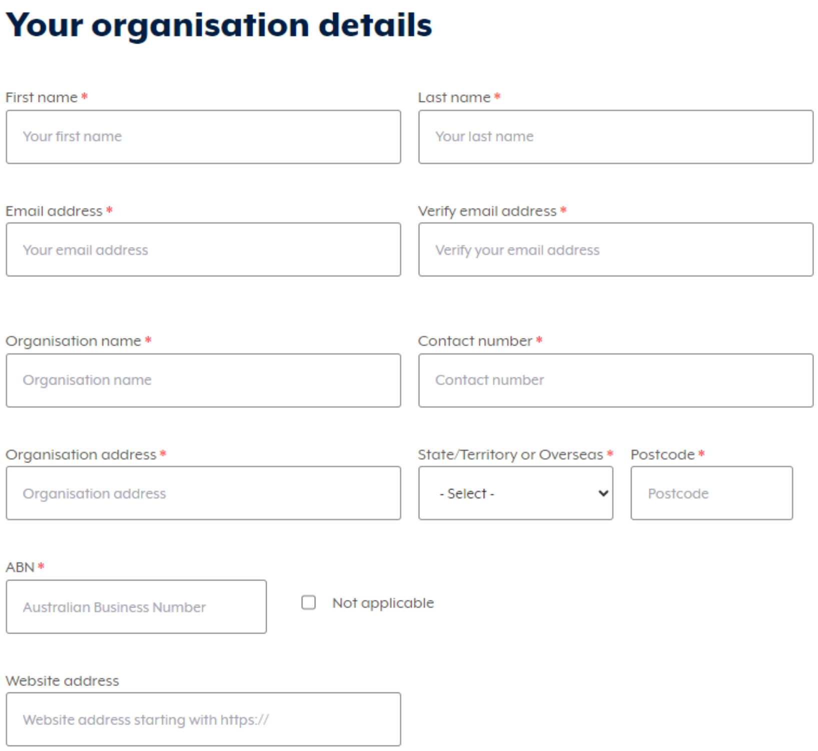
Step 3: Your organisation details

Fill out the contact details for your business. Note, fields with a red asterisk marked next to them are **mandatory** and you must fill these fields out in order to submit the form.

If you are the responsible entity for a critical infrastructure asset under Part 2B of the *Security of Critical Infrastructure Act 2018*, select what critical infrastructure sector you belong to (there is an ‘Other’ option if your sector is not listed) and what ‘critical infrastructure asset’ you are the responsible entity for.

If you are a third-party submitting a report on behalf of the reporting business entity, a new section will pop up. You must fill out information on the entity you are reporting on behalf of.

Once all fields are filled out, move onto Step 4.



Your organisation details

First name * — Your first name

Last name * — Your last name

Email address * — Your email address

Verify email address * — Verify your email address

Organisation name * — Organisation name

Contact number * — Contact number

Organisation address * — Organisation address

State/Territory or Overseas * — - Select -

Postcode * — Postcode

ABN * — Australian Business Number

□ Not applicable

Website address — Website address starting with https://

Step 4: Cyber security incident details

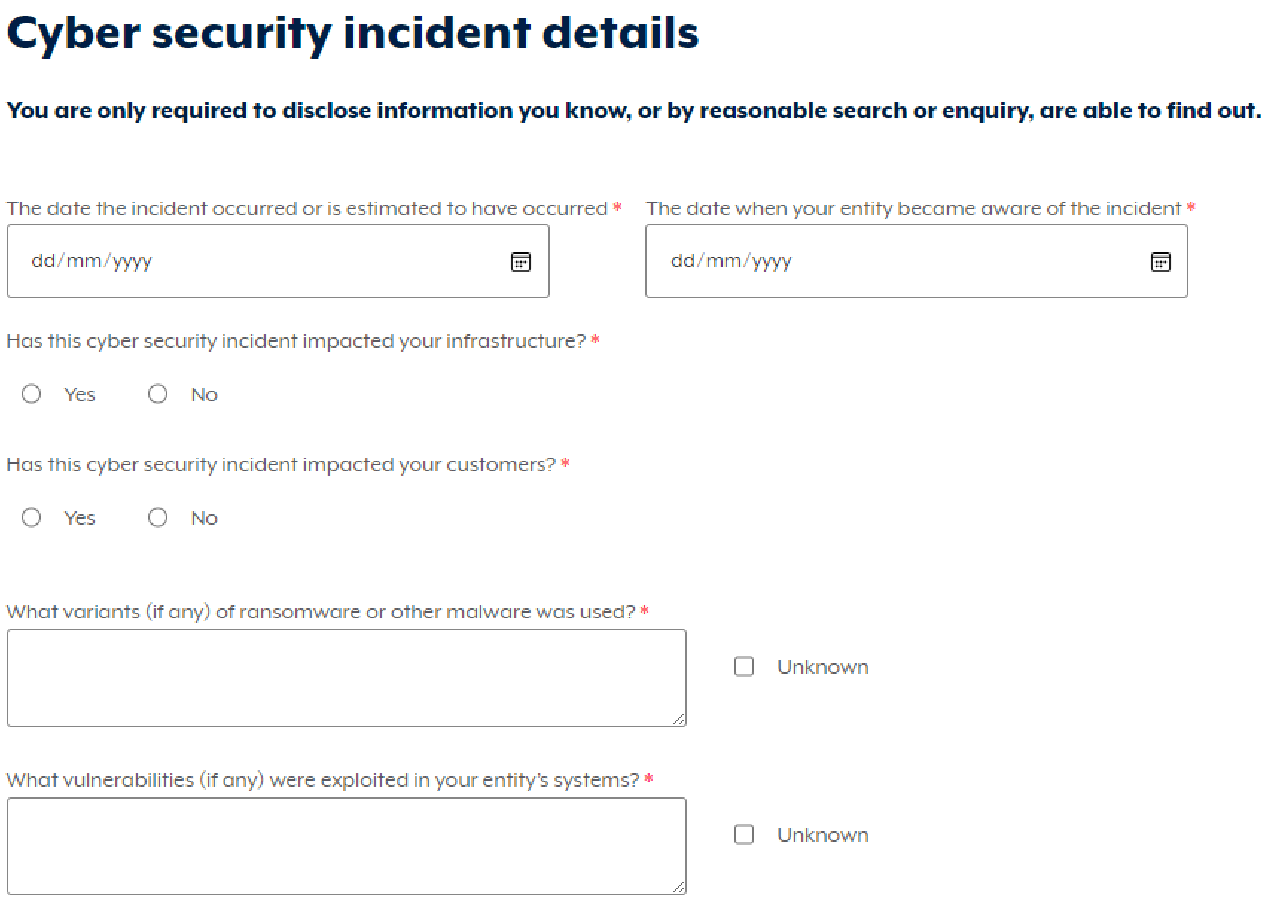
Now you must provide details on the cyber security incident, including the date the incident occurred, or is estimated to have occurred, the impact on your infrastructure and customers, the date your entity became aware of the incident and details on:

- the variants of ransomware (if any) or other malware used; and
- the vulnerabilities that were exploited in your entity’s systems.

Remember, you only need to provide information you know, **or by reasonable search or enquiry**, are able to find out.

You may select ‘Unknown if you do not know what variants of ransomware or other malware were used, or if you don’t know what vulnerabilities were exploited in your entity’s systems at the time you make your report.

If the cyber security incident has had an impact on your infrastructure and customers, you must provide a brief description of this impact the field that appears.



Cyber security incident details

You are only required to disclose information you know, or by reasonable search or enquiry, are able to find out.

The date the incident occurred or is estimated to have occurred *

dd/mm/yyyy

The date when your entity became aware of the incident *

dd/mm/yyyy

Has this cyber security incident impacted your infrastructure? *

○ Yes ○ No

Has this cyber security incident impacted your customers? *

○ Yes ○ No

What variants (if any) of ransomware or other malware was used? *

□ Unknown

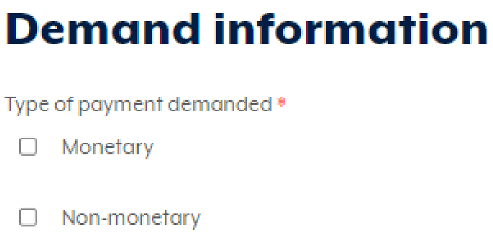
What vulnerabilities (if any) were exploited in your entity’s systems? *

□ Unknown

Once you have filled out all mandatory fields, please move on to Step 5.

Step 5: Demand information

You must provide information on the ransomware or cyber extortion demand on the extorting entity (if it is known or relevant to your report).



Demand information

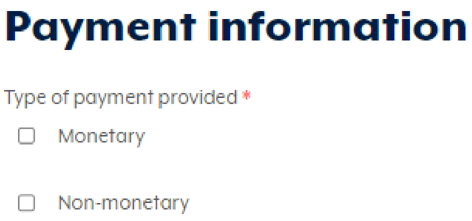
Type of payment demanded *

□ Monetary

□ Non-monetary

All reports need to provide information on the amount of payment demanded and the method of payment demanded if the type of payment demanded is monetary. Where demands relate to non-monetary goods or transfers of information, you must provide a description of any non-monetary benefits that are demanded by the extorting entity and the method of payment demanded. If demands are both monetary and non-monetary in nature, provide information for both. Once completed, move onto Step 6.

Step 6: Payment information



Payment information

Type of payment provided *

□ Monetary

□ Non-monetary

All reports need to provide information on the amount of payment and the method of payment if the type of payment demanded is monetary. Where payments relate to non-monetary goods or transfers of information, you must provide a description of any non-monetary benefits that are paid by the reporting or other entity along with the method of payment. If payments are both monetary and non-monetary in nature, provide information for both. Once completed, proceed to Step 7.

Step 7: Extorting entity information

If you have communicated with the extorting entity in any way, through any medium, you must also provide brief descriptions of:

- **date and timing of those communications**, for example, on Friday 30 May 2025 at 12pm and 3pm;
- **the communications themselves** and include the method of communication for example, occurring over email;
- **any pre-payment negotiations undertaken in relation to the demand or payment**, for example, you attempt to change the behaviour of the extorting entity in any way by offering information or more money.

At the end of this section, you may provide any additional information you think will assist the Commonwealth in responding to, mitigating or resolving the cyber security incident that you believe is not already captured by the form.

When you have filled out all mandatory fields, click ‘Submit’ and your report will be sent to ransomware.reporting@homeaffairs.gov.au