



AUSCERT

# AUSCERT INCIDENT PORTAL

## LOG AN INCIDENT VIA THE AUSCERT INCIDENT PORTAL

The Purpose of the AusCERT incident portal is to allow AusCERT members to submit malicious files or malicious sites to the AusCERT analyst team, in lieu of an email submission.

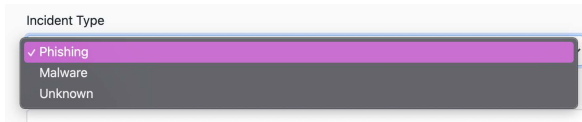
1. Login to the AusCERT Incident Portal (<https://submit.auscert.org.au/>) with your AusCERT Member Portal credentials.

2. Select whether the submission is for a suspicious site or a suspicious file.

3. If the submission is for a suspicious site, please proceed to page two.
4. If the submission is for a suspicious file, please proceed to page three.


## REPORT A SUSPICIOUS SITE

1. Your Member Portal email address will automatically generate at the top of the form.
2. Select from "Incident Type" drop down menu whether the website is phishing, malicious or unknown.



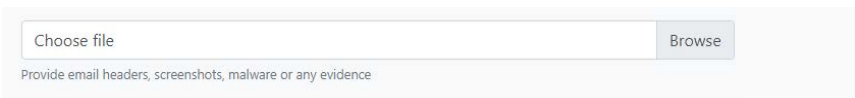
A screenshot of a dropdown menu titled "Incident Type". The menu is open, showing three options: "Phishing" (selected with a checkmark), "Malware", and "Unknown". The background is a light gray, and the dropdown menu has a dark gray border.

3. Input the malicious site's URL.




A screenshot of a form field labeled "Malicious URLs". It is a large, empty text input box. Below the box, there is a small text label that reads "Provide up to 20 malicious URLs here".

4. Input your message for the analyst team.
5. If you would like to receive a response from the team, ensure the "Receive Response" button is selected.
6. If you would like AusCERT to not utilise public tools to scan the submitted files, ensure the "Potentially Sensitive" button is selected.
7. If you would like AusCERT to issue a takedown request for the submitted site, ensure the "Issue Takedown" button is selected.
8. Attach any supporting documentation to the form.



A screenshot of a file upload section. It features a text input field with the placeholder text "Choose file" and a "Browse" button to its right. Below the input field, there is a small text label that reads "Provide email headers, screenshots, malware or any evidence".

9. Once the form is completed, select "Submit" to submit the form to the team.



A screenshot of a blue rectangular button with the word "Submit" in white text.

## REPORT A SUSPICIOUS FILE

1. Your Member Portal email address will automatically generate at the top of the form.
2. Input your message for the team.
3. If you would like to receive a response from the team, ensure the “Receive Response” button is selected.
4. If you would like AusCERT to not utilise public tools to scan the submitted files, ensure the “Potentially Sensitive” button is selected.

☐ Receive Response  
If checked, you will receive a response from an AusCERT analyst

☐ Potentially Sensitive  
If checked, AusCERT will not scan this file using public tools.

5. Attach any supporting documentation to the form.

Provide email headers, screenshots, malware or any evidence

6. Once the form is completed, select "Submit" to submit the form to the team.

**07 3365 4417**

**MEMBERSHIP@AUSCERT.ORG.AU**