So, you've been held to ransom?

Ransomware is one of the most frequent and damaging types of cyber attack affecting Australians. It works by locking up or encrypting your files so that you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files, or to prevent data and intellectual property from being leaked or sold online. Some types of ransomware are designed to stop your computer from working entirely.

NEVER PAY A RANSOM

There is no guarantee your files will be restored, nor does it prevent the publication of any stolen data or its sale for use in other crimes. You may also be targeted by another attack.

This checklist guides you through simple ways you can limit the damage caused by ransomware.

STEP 1 — Disconnect the device
Immediately disconnect the infected device from the internet, other networks and external storage devices to disrupt the potential spread of ransomware.

STEP 2 — Stop the ransomware
Use Task Manager on Microsoft Windows to 'force quit' suspicious or unwanted activity on your device.

STEP 3 — Malware scan and removal
Use your device's malware scanner to find and remove any malware, including ransomware. This may take several hours.

STEP 4 — Note down key details
Record details while it is still fresh in your mind for better outcomes. This will help with further assistance you may require.

STEP 5 — Get professional assistance
Professional incident response service providers could help you with backing up your data, resetting your device(s) and restoring your files.

STEP 6 — Notify and report
If you're a business and hold sensitive information (such as financial or personally identifiable information) you may have to notify your customers and authorities. You should also report the incident to the ACSC through **ReportCyber** at **cyber.gov.au**.

STEP 7 — Protect yourself from future attacks
Read the **ACSC's Ransomware Attacks – Prevention and Protection guide** to help avoid this happening again in the future.

Do you have some feedback on this product? Go to **cyber.gov.au** and let us know.