RANSOMWARE ATTACKS
EMERGENCY RESPONSE GUIDE

cyber.gov.au
So, you’ve been held to ransom?

You’re not alone. Ransomware is one of the most frequent and damaging types of cyber attack affecting Australians today. It works by locking up or encrypting your files so that you can no longer access them. It can also steal a copy of your files to coerce you to pay the ransom by threatening to publicly leak or sell your data. Some types of ransomware are designed to stop your computer from working entirely.

The good news is, this guide steps you through simple ways you can limit the damage caused by a ransomware attack.

**STEP 1: Disconnect devices**
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, 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 clear incident details while it is still fresh in your mind for better outcomes, and to assist with any professional assistance you may engage to help you.

**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**
We recommend reading the ACSC Ransomware Attacks – Prevention and Protection guide to help avoid this happening again in the future.

**A CASE STUDY: Ransomware attack scenario**
The Croft Family
Follow the fictional story of the Croft family and the steps they took when they fell victim to a ransomware attack that affected their devices.
Introduction

What’s happening?

Maybe you’re locked out of your device, a cybercriminal is demanding payment from you to access your files, or files have been encrypted. We understand you may be feeling pressured, panicked or stressed. Keep calm, follow this guide, and remember:

NEVER PAY A RANSOM!

There is no guarantee that cybercriminals will restore your files, stop attacking you, or that they won’t leak or sell any of your information.

What you can do right now?

The Australian Cyber Security Centre has a 24/7 Hotline: 1300 CYBER1 (1300 292 371).

Please call now if you have experienced a ransomware attack, especially if you have already paid a ransom. In the meantime, keep calm and read this guide. It steps you through what you can do right now to limit the damage.

Do these steps now

Follow these steps to take simple and immediate actions to reduce the impact of ransomware on what’s important to you: your money, business, information and reputation.
Before you do, figure out how you will access this guide once your devices are disconnected. We suggest using an unaffected device to view the guide at cyber.gov.au or print out a hard copy.

A. Disconnect the infected device from the internet, other networks and external storage devices.

B. Do this by physically removing network and data cables and disabling wireless connections (Wi-Fi, cellular data and Bluetooth) from your device.

C. Repeat the above steps for any other infected devices on your network, where possible. Fast disconnection of your devices from each other and the internet (ransomware source) disrupts communication and the potential spread of ransomware.

At this stage, DO NOT connect your external storage devices. If your backup solution includes a networked backup, locate any network storage devices and disconnect them.

### Step 1

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect infected devices from the internet, other networks and</td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td>external storage devices.</td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
</tbody>
</table>

Using a checklist to record your actions in response to a ransomware attack may be mandatory for insurance, banking or legal purposes.

### Need further assistance?

For more detailed information on how to disconnect your device, read the ACSC’s Step-by-Step Guide: Disconnecting your Device from a Network (PC & Mac), available at cyber.gov.au.
Before you do, write down or take a photo of the details in the ransom note, web link, email or Bitcoin address.

A. If you have a Windows 10 device, if possible, identify and terminate the ransomware. If you have a macOS device hold down the power button until it shuts down and proceed to Step 3: Malware scan and removal.

B. Do this by opening Task Manager on Microsoft Windows, by pressing Ctrl + Shift + Escape on your keyboard.

C. Click on the suspicious, unwanted activity and select ‘End Task’ to stop the program. Typically, these programs will have very high disk or network usage in Task Manager.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document details of the ransom note, web link, email or Bitcoin address.</td>
<td>Ø</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>Stop/close/quit any unusual, suspicious or unwanted activity running on your device(s).</td>
<td>Ø</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
</tbody>
</table>

Need further assistance?

For more detailed information on how to terminate ransomware using Microsoft Windows, read the ACSC’s Step-by-Step Guide: **Terminate Ransomware Programs with Task Manager (For Windows 10)**, available at cyber.gov.au.
Malware scan and removal

Malware is any software that is specifically designed to disrupt, damage or gain unauthorised access to a device. Use a malware scanning tool to find and remove the ransomware.

A. Do this using the malware scanning tool on your device. You may already have a malware scanning tool that came with your device. If you don’t know the name of your malware scanning tool, you can search for it.

B. Type the name of the malware scanning tool. Or press the Windows key on your keyboard for Windows 10 and start typing. Suggested search terms: Antivirus, Microsoft Defender.

C. Once you have found your malware scanning tool, follow the instructions to run a scan and delete any ransomware identified.

While in progress, take notes or photos of any suspicious software applications, files, pop-ups or other key details you encounter.

Ransomware is a type of malware. A malware scanning tool is only as effective as its last update. If your device and its software applications are not updated regularly, the malware scanning tool may be unaware of, and unable to detect, newer forms of ransomware.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
</table>
| Run the malware scanning tool to find and remove the ransomware. | ❌ | ___ /___ /___  
| | | ___ : ___ am/pm |
| Document details of the malware scan, such as suspicious software applications, files, pop-ups or other key details. | ❌ | ___ /___ /___  
| | | ___ : ___ am/pm |

Need further assistance?

For more detailed information on performing a malware scan, read the ACSC’s Step-by-Step Guide: Performing a Malware Scan with Microsoft Defender Antivirus, available at cyber.gov.au.
Step 4

Note down key details

We understand there are still steps to minimising the damage to your device caused by ransomware, and that you may be keen to continue. But while your malware scan is running, now is a good time to write down everything that has happened so far, as well as take any additional photos of ransom note details, suspicious programs and files, email addresses, Bitcoin addresses and so on.

Recording clear and detailed notes can result in better outcomes and assist you in:

- Asking for help later on from a professional
- Insurance, banking and legal claim processes that may follow after the ransomware attack
- Advising your customers and authorities that there has been an issue.

<table>
<thead>
<tr>
<th>What happened?</th>
</tr>
</thead>
<tbody>
<tr>
<td>When did you first notice?</td>
</tr>
<tr>
<td>What devices were affected?</td>
</tr>
<tr>
<td>When did you start to take action?</td>
</tr>
<tr>
<td>Did you seek help? If yes, from whom?</td>
</tr>
<tr>
<td>Did you recover using a recent backup?</td>
</tr>
<tr>
<td>Did you report to the ACSC?</td>
</tr>
<tr>
<td>Did you adhere to regulatory / legislative or professional reporting obligations?</td>
</tr>
<tr>
<td>Did you write down or take a photo of the details in the ransom note, web link, email or Bitcoin address?</td>
</tr>
</tbody>
</table>
Step 5

Get professional assistance

The steps you have taken have helped to limit additional harm, but there may be further recovery required.

If you still feel worried or need further help, consider seeking professional assistance.

Asking early could help avoid further loss or harm.

Professional incident response services could help you with resetting your devices and restoring your files:

• Backing up any encrypted files (if needed later on)
• Resetting your device(s)
• Restoring your files.

How much will it cost?

Assess whether this amount will guarantee the outcome you want – recovered information and more resilient devices.

How to find the help you need

There are plenty of information technology service providers out there. To find them we suggest searching a telephone or web directory of businesses. Also consider, do any of the service providers you identify have a history of resolving ransomware attacks like yours?

Before asking for professional help, consider:

What do you need from the service provider? For example, recover lost data such as: customer databases, sales history, emails or software applications.
Get professional assistance (Cont’d)

What you need to tell them

When you have found a service provider, explain to them that your files have been encrypted with ransomware.

Ask them to:

- **Backup your files** – Create a backup of your files onto an external storage device – whether those files have been encrypted or not. Follow the professional’s advice on how to safely store and use this backup if required. (A decryption tool may be available or become available in the future which can be used to recover your files.)

- **Remove the ransomware** – Confirm that the ransomware has been removed from your device.

(This may involve a factory reset. A factory reset will delete all your information and revert the device back to when it was new. To get your device back to a working state, this may also require reinstallation of the operating system.)

- **Reconnect your device and update** – Reconnect the unaffected device to your network and any external storage device and download the latest updates for your operating system and software applications.

- **Restore from backup** – Restore your backup. (If you have an existing backup free of ransomware to provide them with.)

- **Decrypt your encrypted files** – If necessary, look for a decryption tool that may be able to unlock your files. We recommend using [www.nomoreransom.org](http://www.nomoreransom.org) to look for available tools.

Other actions and services to consider:

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have been the victim of identity theft contact IDCARE, <a href="http://idcare.org">idcare.org</a> or 1800 595 160. It is a free government funded service to assist you.</td>
<td>[ ]</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>If you have cyber insurance, contact your insurer. Be prepared to answer questions covered in Step 2.</td>
<td>[ ]</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>If a software application or cloud service has been affected, consider contacting the supplier or service provider.</td>
<td>[ ]</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
</tbody>
</table>

REMEMBER: If you’re having trouble understanding the content within this guide, you can contact the Australian Cyber Security Centre 24/7 Hotline on 1300 CYBER1 (1300 292 371).
Step 6

Notify and report

If you’re a business, and depending on the severity of the ransomware compromise, you may have to notify your customers or authorities.

Maintaining business trust

If your business holds sensitive information (such as financial or personally identifiable information), or is part of a government supply chain, you may be obligated to report the incident to regulators or notify victims.

If you are concerned that you may be subject to these requirements/obligations, you should consult with legal or government support, referring to the information you recorded in Step 4.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact your financial institution for assistance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>if you think your bank account or credit card details have been exposed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>They may be able to stop a transaction or temporarily disable your account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>Contact your legal provider to assist you in contacting customers, clients and suppliers.</td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>Contact anyone affected by the compromise including staff, colleagues, family and friends.</td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>Report the ransomware attack to the Australian Cyber Security Centre at cyber.gov.au/acsc/report or call the ACSC 24/7 Hotline on 1300 CYBER1 (1300 292 371).</td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>Report (if required under law) any data breach to the Office of the Australian Information Commissioner <a href="http://www.oaic.gov.au">www.oaic.gov.au</a>.</td>
<td>❌</td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
</tbody>
</table>
Step 7

Protect yourself from future attacks

WHAT NEXT?
Now that you have responded to your current ransomware attack (as best you can), we recommend reading the ACSC Ransomware Attacks – Prevention and Protection guide to help avoid this happening again in the future.

Available at cyber.gov.au.

The ACSC is here to help make Australia the most secure place to connect online. The Australian Cyber Security Centre, as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia.
A Case Study

Ransomware Attack scenario

The Croft Family

Tania, Daniel, and their three children share a family desktop computer. It runs on Microsoft Windows 10. They use it for homework, storing family photos, and playing video games. They also use an iPad for social media.

Tania and Daniel each have a work laptop that they bring home every day and connect to the home Wi-Fi.

The incident

One of the Croft children wanted Tania to proofread a school assignment. Tania sent the document from the home computer to her work email account. She edited it from her work laptop before sending it back to the home computer.

When Tania reopened the assignment on the home computer, she noticed that the file asked her for a password. Tania did not password protect the file, so she thought this was odd.

A few minutes later, instructions to pay a ransom of 1 bitcoin displayed on the screen.

Armed with a hard copy of the ACSC’s Ransomware Attacks – Emergency Response Guide, Tania performed the following steps:

1. She did NOT pay the ransom.
2. She immediately disconnected all of the family’s devices from the home Wi-Fi and disabled other connections such as Bluetooth (instructions on page 2).
3. Tania took a photo of the ransom note on her screen.
4. With the internet now disconnected, she opened Task Manager and noticed a program she did not recognise was using most of the computer’s disk usage. She terminated the program using Task Manager (instructions on page 3).
5. Tania ran a full scan with Microsoft Defender Antivirus (instructions on page 4).
6. Tania spoke to her children and found out one of them turned off automatic updates months ago as it was slowing down their video games. This was unfortunate as there was a system update for Microsoft Windows 10 which would have detected and stopped this particular ransomware from running.
7. Feeling overwhelmed and now ill-equipped, Tania used her iPhone to seek professional assistance. She searched ‘computer virus experts near me’ and contacted a service provider that offered help with ransomware attacks (instructions on page 7).
Ransomware Attack scenario (Cont’d)

8. She explained to them that her files had been encrypted with ransomware and asked that they:
   • Create a backup of their family’s files – encrypted or otherwise.
   • Remove the ransomware from their device.
   • Restore backup files after they cleaned the device, using a backup drive Tania provided. Unfortunately the backup made was a few months old, so some files were lost.

9. While the home computer was with the service provider being fixed, Tania and Daniel checked their work laptops and other devices for any irregularities, but found no other changes.

10. Tania then reported the incident to the ACSC using ReportCyber (instructions on page 5).

11. Once the home computer was returned safely from the service provider, Tania reconnected it to the internet and followed the ACSC’s Ransomware Attacks: Prevention and Protection Guide to help protect her devices from any future ransomware attacks.

After the ransomware attack

The family decided to never turn off automatic updates or Microsoft Windows Defender.

They also agreed to backup files to an external storage device every fortnight.

One year later, Daniel told Tania that decryption tools for the Shade ransomware were released on the website www.nomoreransom.org. Daniel used the user guide on No More Ransom to safely decrypt the hard drive containing all the files that were encrypted and recovered the information that was previously inaccessible.
Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2020

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).