Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

RANSOMWARE EMERGENCY RESPONSE GUIDE

RECOVER FROM A RANSOMWARE ATTACK

cyber.gov.au

What to do if you're held to ransom

A guide to remove ransomware, recover your files and protect yourself against future attacks.

Ransomware is a common and dangerous type of malware. 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.

This guide has simple steps to follow if you are a victim of ransomware. The first section will show you how to respond if one of your devices is infected with ransomware. The second section will help you to recover your files and restore your devices.

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.

Call the Australian Cyber Security Centre 24/7 Hotline on **1300 CYBER1** (1300 292 371) if you need cyber security assistance.

Not all ransomware attacks are the same so some of the steps in this guide may not apply to your situation. Use the actions that best suit your case.

Table of Contents

Here are the simple ways you can remove ransomware, recover your files and protect yourself against future attacks. **If you get stuck, find a professional to help you work through a ransomware attack or call the Australian Cyber Security Centre's 24/7 Hotline on 1300 CYBER1 (1300 292 371).**

RESPOND TO A RANSOMWARE ATTACK

RECOVER FROM A RANSOMWARE ATTACK

PREVENT FUTURE ATTACKS

Respond to a ransomware attack

Start here if you are experiencing a ransomware attack.

Work through the steps below as quickly as you can. Acting quickly could stop the ransomware from spreading.

If you get stuck, seek professional help. Ransomware attacks can cause serious damage. It is hard to tackle and overcome them on your own. Consider finding a professional to help you work through a ransomware attack and get back on your feet.

Step 1: Record important details

It is important to record important details about the ransomware attack to help you:

- ask for help from a professional
- make an insurance, bank or legal claim that may follow after the attack
- make a report to the ACSC through ReportCyber
- tell your family, colleagues or authorities that there has been an issue.

Complete this step as quickly as possible, as the ransomware could still be spreading through your device and network.

What to record

The details you should try to record are:

- if the files that have been affected by ransomware have a new extension
- the name of any new file extension
- the ransom note
- anything else that has changed since the attack.

A quick way to record the information you need is to take a photo of your screen. It's okay if you can't record everything, but you should try to capture as much as possible, as quickly as you can.

Step 2: Turn off the infected device

As soon as you have recorded details about the ransomware attack, turn off the infected device by holding down the power button or unplugging it from the wall. For most people, this is the best way to stop the ransomware from spreading.

Step 3: Disconnect your other devices

Ransomware can spread across networks. If there are other devices on your network, you should turn them off too. Start with the devices that are most important to you. Important devices typically include things like Network Attached Storage (NAS) devices, servers, computers, phones, tablets, and any other devices that store valuable information.

Step 4: Change your important passwords

Some forms of ransomware steal your passwords. It can be difficult to know what information ransomware has accessed so, as a precaution, you should change the passwords for your accounts as soon as possible. Start with your most important accounts first.

What's important will be different for everyone, but important accounts typically include:

- cloud storage accounts
- email accounts
- bank accounts
- business accounts.

The ACSC has published guidance on using password managers and guidance on creating passphrases (a strong type of password). These resources are available at **cyber.gov.au/passphrases**.

As you change your passwords, consider enabling multi-factor authentication on supported accounts. Multi-factor authentication makes it harder for cybercriminals to get access to your accounts. The ACSC has published guidance on enabling multi-factor authentication. This is available at **cyber.gov.au/mfa**.

Recover from a ransomware attack

Now that you've responded to a ransomware attack, it's time to recover your information, restore your infected devices and report the incident.

Note: At the end of this guide, you will be given guidance on reporting the incident. In some cases you may need to make reports urgently, for example, to meet obligations to your customers or your insurance company. Consider if you have any urgent reporting requirements before you begin the next step.

Step 5: Recover your information

Check your backups

The ACSC recommends you keep backups of your information as a precaution against things like ransomware attacks.

If you have backups, make sure they are free from ransomware to avoid re-infecting your device. Your backups may be infected with ransomware if they are saved on your infected device or were on the same network as your infected device at any point since the infection. Your backups should be secure if they were never connected to the infected device or to the same network as the infected device.

If you think your backups may be infected with ransomware, don't try to access them, ask an IT professional for support.

If you have backups that are free from ransomware, make sure you don't connect them to your infected device or network. Remove the ransomware from the infected device or network first using the guidance in Step 6.

What to do if you don't have a secure backup of your information

If you do not have a secure backup, it may still be possible to recover your information but you will likely need professional help. Consider how important the affected information is to you and how much you are willing to pay for professional help to restore it.

Remember, 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.

Step 6: Remove ransomware from affected drives and devices

Ransomware can be difficult to remove. For most people, the best way to remove ransomware is to wipe all infected drives and devices and reinstall their operating systems. **Be aware that this step will permanently delete all of your information so make sure you've completed Step 5 and recovered what information you can first.**

Remember that ransomware can spread across a network. We recommend following this step for all drives and devices that were on the same network as the infected device at any point since the infection.

The steps to wipe your drives and devices vary across manufacturers. The manufacturer of your drive or device will have guidance on their website. We've listed some resources below.

Apple iPhone, iPad or iPod: support.apple.com/HT201252
Apple Mac devices: support.apple.com/HT212749
Microsoft Windows devices: support.microsoft.com (Search for the article "Recovery options in Windows")
Samsung phones: samsung.com/au/support/mobile-devices/factory-data-reset-samsung-phone/
Google Pixel phones: support.google.com/pixelphone/answer/4596836

Step 7: Restore your information

Now that you have removed the ransomware from affected drives and devices, it is safe to connect them to your backups and restore your information. Remember the guidance in Step 5; only restore information from a backup if you are confident that it is free from ransomware.

The ACSC's guidance on backups includes information on restoring your information. This is available at **cyber.gov.au/backups**.

Step 8: Notify and Report

Report the incident to the ACSC through ReportCyber at **cyber.gov.au/acsc/report**. Submitting a report helps to disrupt cybercrime operations and make Australia the most secure place to connect online. Include the information you recorded in Step 1.

Additional reporting responsibilities for businesses

If you're a business, depending on the severity of the ransomware compromise, you may have to notify your customers of the attack.

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

If you think you need to make a report, consult with the Office of the Australian Information Commissioner at **oaic.gov.au** or seek legal or government support.

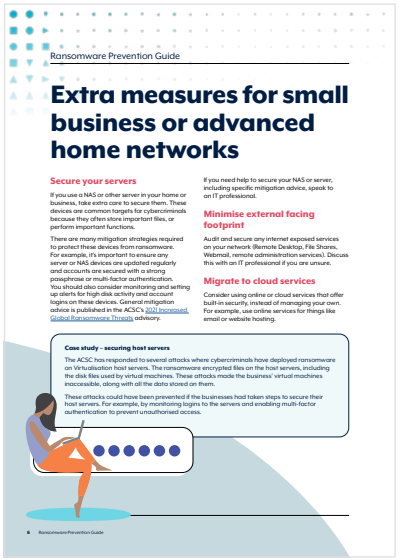
Prevent future attacks

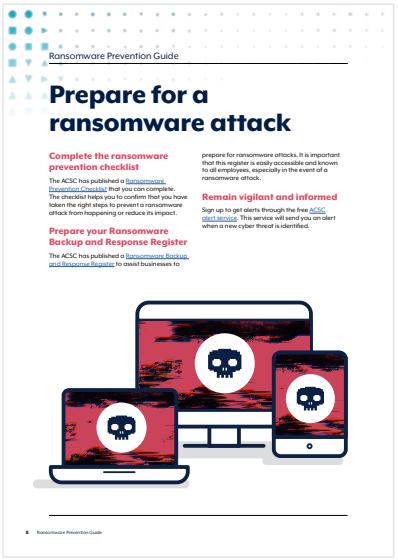
Step 9: Prevent future attacks

Take some time to consider how your device was infected with ransomware so you can prevent the same thing from happening again.

The ACSC has published advice to help you protect yourself against ransomware attacks at **cyber.gov.au/ransomware**.

This advice outlines precautions you can take to reduce the impact of ransomware attacks or prevent them from happening in the first place.





Notes

Notes

Notes

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.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre