Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

RANSOMWARE PREVENTION GUIDE

PROTECT YOURSELF AGAINST RANSOMWARE ATTACKS

cyber.gov.au

Introduction

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.

A ransomware attack could block you from accessing your device or the information on it. Take some time to consider how a ransomware attack might affect you. This will help you to invest the right amount of time, effort and money into protecting your systems.

You should consider:

- **What can you replace, for example, files you downloaded from the internet?**
- **What can't you replace, for example, photos that aren't backed up?**
- **What would you spend to recover your information or device after a ransomware attack?**

Follow the steps in this guide to mitigate the risk and impact of a ransomware attack.

Table of Contents

Secure your devices to stop ransomware attacks

Regularly update your devices

Cybercriminals use known weaknesses to hack your devices. Updates have security upgrades so known weaknesses can't be used to hack you. You should always update your system and applications when prompted. You can also turn on automatic updates on some devices and applications so that updates happen without your input.

Read our advice on updates for more information, including how to update your Windows, Apple and Android devices. This can be found at **cyber.gov.au/updates**.

If you have a server or Network Attached Storage (NAS) device in your network, make sure they are regularly updated too. If you are unsure how to update your NAS refer to the manufacturer's guidance or speak to an IT professional.

Set up and perform regular backups

A backup is a digital copy of your most important information (e.g. photos, customer information or financial records) that is saved to an external storage device or to the cloud.

The best recovery method from a ransomware attack is to restore from an unaffected backup. Regularly backup your files to an external storage device or the cloud. Backing up and checking that backups restore your files offers peace of mind.

There are a number of ways to back up your devices. Refer to our advice for backups for more information. This is available at **cyber.gov.au/backups**.

Implement access controls

Controlling who can access what on your devices will help reduce the risk of ransomware. It will also limit the amount of data that ransomware attacks can encrypt, steal, and delete.

To do this, give users access and control only to what they need. This can be done by making sure each person who uses the device has the right type of account.

There are two types of accounts you can set up on Microsoft Windows and Apple macOS; a standard account and an administrator account. Everyday users should have a **standard** account. Only those who need to should have an administrator account. Consider creating a standard account to use as your main account as they are less susceptible to ransomware. It's also important that users don't share their login details for accounts.

If you use a Windows device, follow Microsoft's guidance on adding a new account. Once you have added a new account you will see it appear on the 'Family & other users' settings page. Select the new account, select change account type then choose 'standard account' from the drop-down menu.

If you use a Mac, refer to Apple's guidance on setting up users, guests and groups.

In a business environment, access controls might be managed by your IT provider or IT staff. Speak to them if you are unsure how to action this step.

Use anti-virus software

Anti-virus software can help to prevent, detect and remove ransomware on your device. Make sure you turn on your anti-virus software and keep it up to date. The ACSC has published guidance on choosing anti-virus software. You may also already have an anti-virus tool on your device. Microsoft Windows 10 and Windows 11 come with a built-in anti-virus tool called Windows Security.

Whatever anti-virus you choose, we recommend familiarising yourself with what legitimate warnings look like. Sometimes websites will give you a fake warning to try and get you to click on a harmful link. If you know what your anti-virus warnings look like, you can avoid the harmful links.

Turn on ransomware protection

Some anti-virus products offer ransomware protection. Make sure you enable this function to protect your devices.

For Microsoft Windows devices, you can enable **controlled folder access** within Windows Security. This will prevent designated files on your device from being encrypted by ransomware. For more information visit Microsoft's website.

Disable macros

Microsoft Office applications can execute macros to automate routine tasks. Macros can be used to deliver ransomware to your device so they should be used with caution.

If you don't need to run macros, it is best practise to disable them. If you do need to run macros, consider preventing macros from running automatically and restricting which macros can run.

- Microsoft has published guidance on configuring macros settings on their support website: **support.microsoft.com**.
- The ACSC has published guidance to help organisations with Microsoft Office macro security at: **cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/microsoft-office-macro-security**.

Turn on multi-factor authentication

Multi-factor authentication (MFA) makes it harder for cybercriminals to gain initial access to your device, account and information by making them jump through more security hoops and additional authentication layers. This means that the cybercriminal will have to spend more time, effort, and resources to get into your device before any ransomware attacks can begin.

MFA typically requires a combination of two or more of the following authentication types before granting access to an account:

- something a user knows (PIN, password/passphrase),
- something a user has (smartcard, physical token), or
- something a user is (fingerprint, iris scan).

Prioritise enabling MFA on critical services such as email or remote access (if this is used by your business). Read our guidance on MFA for more information. This can be found at **cyber.gov.au/mfa**.

Use unique passphrases

If your accounts do not have multi-factor authentication then make sure to use a unique passphrase. Never reuse a passphrase across multiple accounts. This could help stop ransomware from spreading or your accounts being compromised.

Extra measures for small business or advanced home networks

Secure your servers

If you use a NAS or other server in your home or business, take extra care to secure them. These devices are common targets for cybercriminals because they often store important files, or perform important functions.

There are many mitigation strategies required to protect these devices from ransomware. For example, it's important to ensure any server or NAS devices are updated regularly and accounts are secured with a strong passphrase or multi-factor authentication. You should also consider monitoring and setting up alerts for high disk activity and account logins on these devices. General mitigation advice is published in the ACSC's 2021 Increased Global Ransomware Threats advisory.

If you need help to secure your NAS or server, including specific mitigation advice, speak to an IT professional.

Minimise external facing footprint

Audit and secure any internet exposed services on your network (Remote Desktop, File Shares, Webmail, remote administration services). Discuss this with an IT professional if you are unsure.

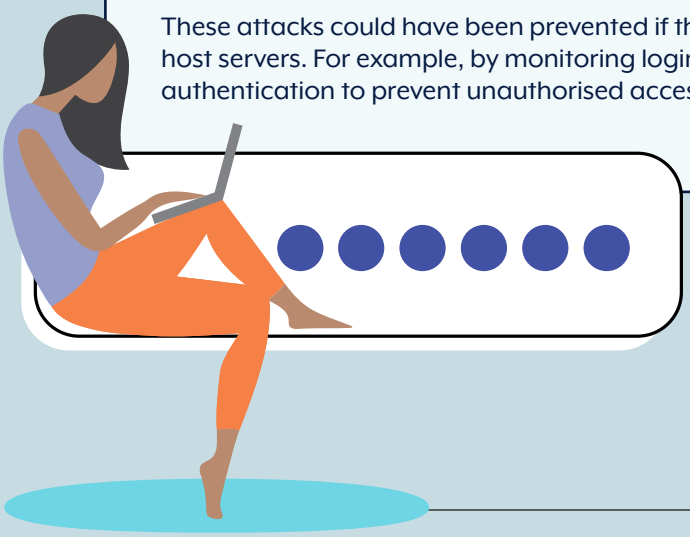
Migrate to cloud services

Consider using online or cloud services that offer built-in security, instead of managing your own. For example, use online services for things like email or website hosting.

Case study – securing host servers

The ACSC has responded to several attacks where cybercriminals have deployed ransomware on Virtualisation host servers. The ransomware encrypted files on the host servers, including the disk files used by virtual machines. These attacks made the business' virtual machines inaccessible, along with all the data stored on them.

These attacks could have been prevented if the businesses had taken steps to secure their host servers. For example, by monitoring logins to the servers and enabling multi-factor authentication to prevent unauthorised access.



Understand how to prevent ransomware attacks

Check messages you receive

Cybercriminals will send you fake messages to try and get you to take some action. For example, they might ask you to click a link, download a file or give away your personal information. If you receive a message that you weren't expecting it might be a way for a cybercriminal to get access to your account or device.

Be careful opening files and downloading programs

Sometimes you need to open a file or download a program from the internet.

Avoid opening files that you receive unexpectedly or from people you don't know. As an example, don't open an email attachment if you don't recognise the email address or weren't expecting to receive it.

Do not download files if they have a different file extension than what you were expecting (for example, a file that ends in .exe or .msi when you were expecting a PDF or image).

Check that software is made by a reputable company before downloading and installing on your device. Always download software from the company's official website or an official app store. If you access software through other means, such as pirating, this could put your device at risk. For example the software may not receive security updates, or it could be malicious. Avoid software that asks for excessive or suspicious permissions.

Avoid links that ask you to log in or reset your password

Sometimes you might receive a link that asks you to enter your credentials or reset your password. Do not enter your credentials after receiving instructions from an unexpected message. This could be a phishing attempt designed to steal your login details.

If you think the message might be legitimate, find another way to action the request. For example, if you need to change your password for an account go to the official website and request to reset your password there. Do not use the links provided to you in an unexpected email or message as these could be fraudulent.

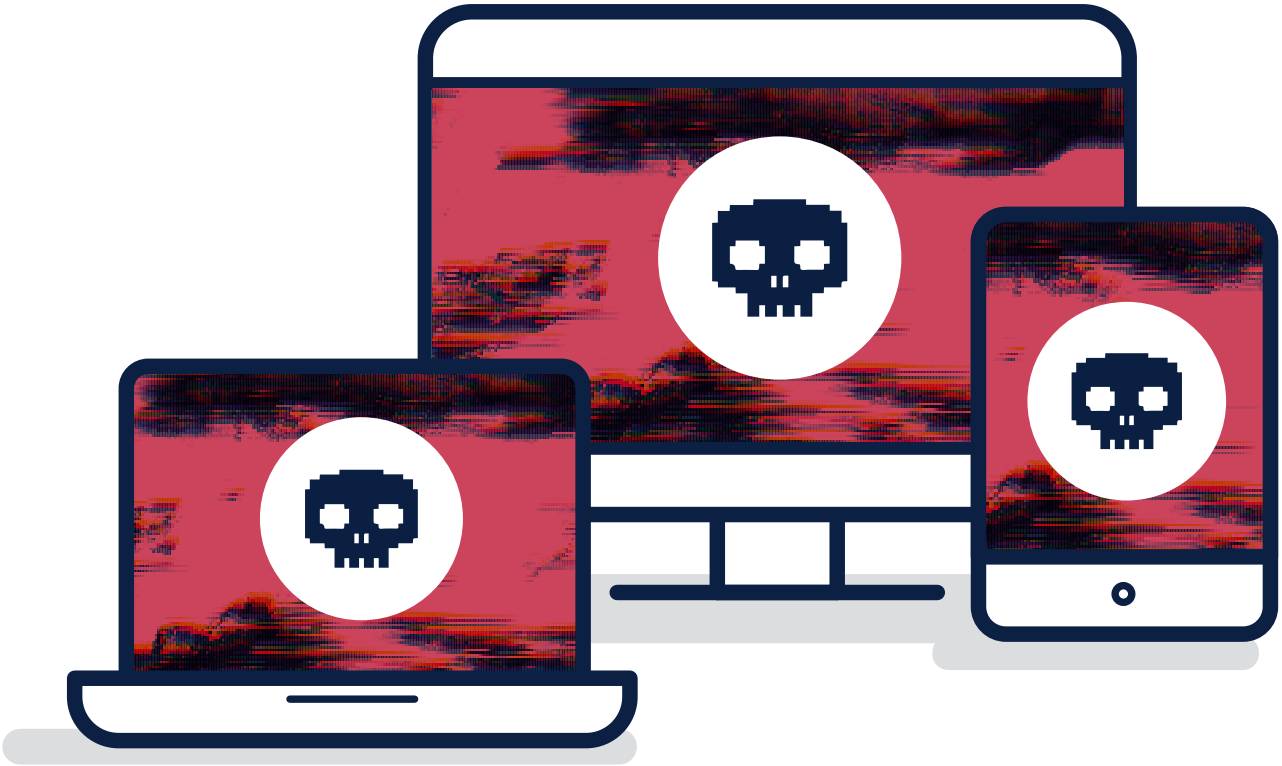
Prepare for a ransomware attack

Prepare your Ransomware Backup and Response Register

'The ACSC has published a **Ransomware Back up and Response Register** to assist businesses to prepare for ransomware attacks. It is important that this register is easily accessible and known to all employees, especially in the event of a ransomware attack. These products can be found by visiting at: cyber.gov.au/ransomware

Remain vigilant and informed

Sign up to get alerts through the free ACSC alert service. This service will send you an alert when a new cyber threat is identified.



If you are held to ransom?

If you fall victim to a ransomware attack, complete the following steps or read **What to do if you're held to ransom** at cyber.gov.au/ransomware for more information.

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.

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

STEP 1	**Record important details.**	As quickly as possible, record important details about the ransomware attack. Take a photo of the ransom note or any new file extensions you have noticed.
STEP 2	**Turn off the infected device.**	As soon as you have finished Step 1, turn off the infected device by holding down the power button or unplugging it from the wall. This is the best way to stop ransomware from spreading.
STEP 3	**Disconnect your other devices.**	If there are other devices on your network, you should turn them off too. Start with your most important devices that store valuable information such as servers, computers, phones and tablets.
STEP 4	**Change your important passwords.**	Some forms of ransomware steal your passwords. As a precaution, you should change the passwords for your online accounts, starting with your most important accounts first.

RECOVER FROM A RANSOMWARE ATTACK

STEP 5	**Recover your information.**	Check your backups for use in Step 7. Make sure not to connect your backup to the infected device or network. If you think your backups may be infected with ransomware, or you don't have a backup, ask an IT professional for support.
STEP 6	**Remove ransomware from affected drives and devices.**	For most people, the best way to remove ransomware is to wipe all infected drives and devices and reinstall their operating systems. 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.
STEP 7	**Restore your information.**	After removing the ransomware in Step 6, it is safe to restore your information. Use the backups from Step 5, but only if you are confident that they are free from ransomware.
STEP 8	**Notify and report.**	If your business holds sensitive information or is part of a government supply chain, you may need to report the incident to regulators. Consult with oaic.gov.au. You should also report the incident to the ACSC through ReportCyber at cyber.gov.au.

PREVENT FUTURE ATTACKS

STEP 9	**Prevent future attacks.**	The ACSC has published advice to help you protect yourself against ransomware attacks, available on cyber.gov.au.

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