Use this table of contents as a checklist as you work through the steps in this guide.

**STEP 1:** Update your device and turn on automatic updates ........ 3
Run an update on all devices and turn on automatic updates to ensure you always have the most up-to-date security protection.

**STEP 2:** Turn on two-factor authentication ........................................ 4
Add multiple layers of authentication to increase the security of your accounts.

**STEP 3:** Setup and perform regular backups ................................. 5
Automatically copy and store critical information to a backup device by turning on or confirming automatic backups.

**STEP 4:** Implement access controls .............................................. 6
Make your computer more secure and manage who has access to security settings by implementing access controls.

**STEP 5:** Turn on ransomware protection .............................................. 7
If you are using Windows 10, you can enable built-in ransomware protection. If you are using another operating system, source and install a ransomware protection program.

**STEP 6:** Prepare your Cyber Security Emergency Plan .................. 8
Unless you are responding to a ransomware attack right now, fill out the Cyber Security Emergency Plan to greatly reduce stress and time during a cyber security incident.

**STEP 7:** Remain vigilant and informed ........................................ 11
Stay up to date on cyber security threats and trends with the ACSC Alert Service.
Let’s get started

Introduction

Ransomware is a type of malware that locks up your files until a ransom is paid, typically payable using an online digital currency or cryptocurrency such as Bitcoin. 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.

Preventative and protective measures are simple, cost effective and immediately beneficial.
Introduction

Why do I need to protect myself from ransomware?

Your presence in the digital world may be larger than you think. We use the internet for online shopping, banking, entertainment, running businesses, storing and sharing photos and documents, socialising, and so much more.

These services all connect back to you and your sensitive information – this is what cybercriminals want.

The more services you use, the more avenues cybercriminals have to deploy ransomware attacks in an attempt to destroy your important data and records, or steal information about you, your friends and family, and your business.

What can a cybercriminal do with my information?

Once infected with ransomware, a cybercriminal can steal, lock up, and destroy your files and information. Cybercriminals can then hold you ransom by threatening to corrupt your files so they are not recoverable or publicly disclose your information.

What can I do?

Take steps to proactively prevent a ransomware attack on you or your business. The protective measures in this guide are easy to do and can mitigate the risk and reduce the impact of a ransomware attack – saving you time, money and worry.

If you experience a ransomware attack,
NEVER PAY A RANSOM.

Contact the Australian Cyber Security Centre 24/7 Hotline: 1300 CYBER1 (1300 292 371).

Update your device and turn on automatic updates

A. Having an up-to-date operating system (Windows, macOS or other) and security software reduces the chance of a cybercriminal using a known weakness to hack your computer. It also provides security upgrades and protections for your device against other threats.

B. How you turn on automatic updates on your devices can differ depending on your operating system and your software applications (apps).

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
</table>
| Update your operating system and turn on automatic updates for all your devices and software applications to ensure you always have the most up-to-date security protection. | ☐ | ___/___/___  
| | | ___ : ___ am/pm |

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

For more detailed information on how to turn on automatic updates, read the ACSC’s Step-by-Step Guides available at cyber.gov.au:

- Turning on Automatic Updates (For Microsoft Windows 10)
- Turning on Automatic Updates (For iMac & MacBook, and iPhone & iPad)
Step 2

Turn on two-factor authentication

Multi-factor authentication (MFA) typically requires a combination of something a user knows (PIN, password/passphrase) and something a user has (smartcard, physical token) or something a user is (fingerprint, iris scan).

MFA makes it harder for cybercriminals to gain initial access to your device, account and information by making them have to 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.

Two-factor authentication (2FA) is the most common type of MFA. It provides enhanced security to traditional usernames and passwords/passphrases and increases confidence that the user requesting access is actually who they claim to be.

How to activate 2FA is different for each device or software application. For more detailed information on how to turn on 2FA, read the ACSC’s Step-by-Step Guides available at cyber.gov.au.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
</table>
| Turn on two-factor authentication on all devices, software applications and third-party websites storing your data. | [ ] | ___ / ___ / ___  
| | | ___ : ___ am/pm |

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

In cases where two-factor authentication is not available, a strong passphrase can often be the only barrier between adversaries and your valuable information and accounts. Passphrases use four or more random words as your password, and are most effective when they are long, unpredictable and unique.

Find more information on creating strong passphrases at cyber.gov.au.
Set up and perform regular backups

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

Backing up is a precautionary measure, so that your information is accessible in case it is ever lost, stolen or damaged through a ransomware attack. The best recovery method for a ransomware attack is a regular offline backup made to an external storage device and additionally a backup in the cloud.

Regularly backing up your files is recommended. What that looks like, whether it’s daily, weekly, monthly or less often, is ultimately up to you. Backup frequency depends on the number of new files you load onto your device and the number of changes you make to files.

We encourage you to test your backups so you are familiar with the process and ensure your backups are working appropriately.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up and perform regular backups on all devices.</td>
<td></td>
<td><em><strong>/</strong></em>/___</td>
</tr>
<tr>
<td></td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
</tbody>
</table>

Action. Completed

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

For more detailed information on backing up to both external storage devices and the cloud read the ACSC’s Step-by-Step Guides available at cyber.gov.au:

• Backing Up & Restoring Your Computer (For PC)
• Backing Up & Restoring Your Computer (For Mac)
Step 4

Implement access controls

Implementing access controls is an important step in managing who can access what on your devices. This is especially true in a business context, but also applies to any household.

Access controls help minimise the risk of unauthorised access to important information, which then helps to minimise the consequences of ransomware running on devices by limiting the amount of information it can encrypt, steal and delete.

Principle of least privilege

The principle of least privilege is the safest approach for most. It gives users access only to the software applications and files they need to perform their job.

What you can do

- Do not use an administrator account for everyday use.
- Understand what your employees need to complete their jobs and only give them access to those software applications and files.
- Restrict administrator privileges to an as-required basis.
- Do not share account login details such as passwords/passphrases and other login credentials.
- Remember to revoke accounts when employees leave the business, change roles, or will be absent for long periods of time.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
</table>
| Implement access controls on all devices, and where possible, remove administrative access for accounts. | ○ | ___/___/___
| | | ___ : ___ am/pm |

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

For more detailed information on managing account access, read the ACSC’s Step-by-Step Guides available at cyber.gov.au:

- Managing User Account for Microsoft Windows 10
- Managing Accounts for macOS
Step 5

Turn on ransomware protection

Ransomware protection has the ability to prevent many types of ransomware attacks from happening. In the unfortunate event of an attack, ransomware protection can also interrupt the ransomware from encrypting all your data, which minimises the extent of the damage.

If you are using Windows 10, you can enable built-in ransomware protection to protect your files. If you are using another operating system, you will need to source and install ransomware protection for your devices.

There are many types of ransomware protection available. Ask a professional information technology service provider for advice, or friends and family if they have any recommendations.

In addition to installing ransomware protection, the best course of action is to back-up your information (see Step 3). That way, even if an attack is successful, you will at least have your important information accessible elsewhere.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ransomware protection in Windows 10.</td>
<td></td>
<td>___ / ___ / ___</td>
</tr>
<tr>
<td>If you are using another operating system, source and install</td>
<td></td>
<td>___ : ___ am/pm</td>
</tr>
<tr>
<td>ransomware protection on all your devices.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If you are using Windows 10 and are unsure on how to enable its built-in ransomware protection, refer to the ACSC Step-by-Step Guide Turning on Ransomware Protection In Microsoft Windows 10, available at cyber.gov.au.
Prepare your Cyber Security Emergency Plan

Unless you are responding to a ransomware attack right now, fill out the Cyber Security Emergency Plan on the following pages, and print it out, to greatly reduce stress and time during a cyber security incident.

Get to know your critical information and devices

Know what you are willing to live without and what you are willing to go above and beyond to save.

Consider:
1. What you can and cannot replace
2. To what extent you will invest to recover the information or device.
## Protecting your information and devices

<table>
<thead>
<tr>
<th>What is it?</th>
<th>Impact if it is lost?</th>
<th>Where is it?</th>
<th>Do you have copies? Where?</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g. Customer database</td>
<td>Loss of historic customer transactions and details</td>
<td>Main server</td>
<td>Yes – cloud backup and offline external storage device</td>
</tr>
</tbody>
</table>

### Backup – your Plan B

<table>
<thead>
<tr>
<th>Where is it?</th>
<th>How often is it backed up?</th>
<th>How often is it tested?</th>
<th>Is it disconnected from your device?</th>
</tr>
</thead>
</table>

### Devices

- Mobile phones
- Laptops, desktops
- Tablets
- Printers
- EFTPOS machines

### Software and apps

- Shopify
- Office 365
- Facebook
- Squarespace
- Wix
- MYOB

<table>
<thead>
<tr>
<th>Type of device?</th>
<th>Who owns the device?</th>
<th>Used daily, weekly, monthly or rarely?</th>
<th>Name of software applications?</th>
<th>Who has access?</th>
</tr>
</thead>
</table>
Step 6

Protecting your information and devices

<table>
<thead>
<tr>
<th>Emergency contacts</th>
<th>Email accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Bank (fraud)</td>
<td>• Outlook</td>
</tr>
<tr>
<td>• IT company</td>
<td>• Gmail</td>
</tr>
<tr>
<td>• Internet provider</td>
<td>• Yahoo!</td>
</tr>
</tbody>
</table>

Who do you need to notify?

- Manager
- Staff
- Colleagues
- Customers
- ReportCyber
- Cyber Insurance

<table>
<thead>
<tr>
<th>Who</th>
<th>Contact</th>
<th>When to notify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Remain vigilant and informed

While it is one thing to have built up your defences to protect your information, it is best to remain on the lookout for evolving cyber threats and trends which could impact you at any time. Sign up to the free ACSC Alert Service. This service will send you an alert when a new cyber threat is identified by the ACSC.
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).
For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)