Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

Step-by-Step Guide

Turning on ransomware protection for **Microsoft Windows 10**

cyber.gov.au

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.

Table of Contents

Introduction

This step-by-step guide shows you how to turn on **ransomware protection** for **Microsoft Windows 10** devices using controls that are built-in to Windows 10.

For more cyber security advice, visit **cyber.gov.au**

Ransomware

What Certain malware that locks down your computer and files until a ransom is paid

Ransomware attacks are typically delivered to a user via a malicious but legitimate looking email link or attachment. When the user opens the ransomware it will typically encrypt a user's files, then demand a ransom to restore access – typically payable using cryptocurrency, like Bitcoin.

Why Money

Ransom, an age-old and effective crime, is now being committed online. Ransomware offers cybercriminals a low-risk, high-reward income. It is easy to develop and distribute. Also in cybercriminals' favour, most small businesses are unprepared to deal with ransomware attacks.

NEVER PAY A RANSOM.

You are not guaranteed to regain access to your information and may be vulnerable to a second attack.

Who Everyone

Many individuals and small businesses are often less security conscious, are less likely to implement cyber security measures, and spend less on cyber security measures. While medium and large businesses may have some considerations for cyber security measures, they too can benefit from inbuilt system security features – such as Microsoft's ransomware protection.

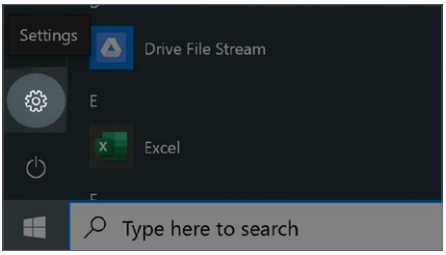
Microsoft's ransomware protection

Ransomware protection is a control on computers to stop a ransomware attack from encrypting access or files that are important to you.

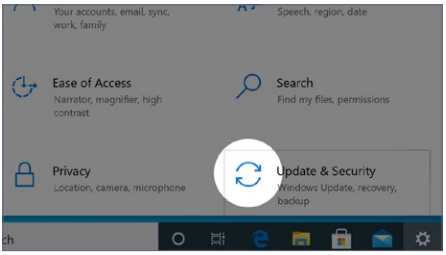
Microsoft has a built-in control to help protect devices from ransomware. It ensures folders you choose cannot be altered which prevents them from being encrypted down by a criminal. This guide will demonstrate how you can configure and use this control to protect your files from a ransomware attack.

While ransomware protection can be useful, having a backup stored offline is important in case you need to retrieve important files or information. For more information on backing up visit **cyber.gov.au**

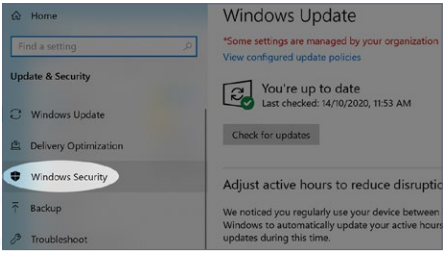
Setting up ransomware protection for Microsoft Windows 10



1. Select the **Windows** icon in the bottom left of your screen and then click on the **Settings Cog** icon.

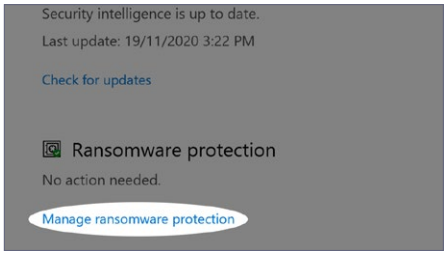


2. Once in Settings, click on the **Update & Security** icon.

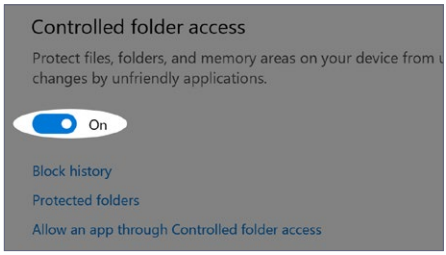


3. Click **Windows Security** tab.

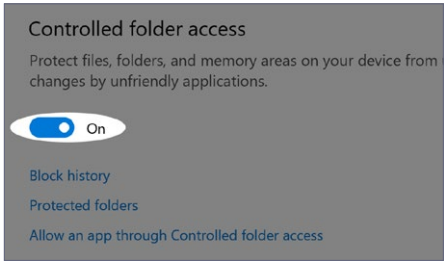
4. Under the **Protection areas** list, click on **Virus & threat protection**.



5. Click on **Manage ransomware protection** under ransomware protection.



6. In many cases, the **Controlled folder access** will be toggled off. If so, click on the **toggle** to turn it on.



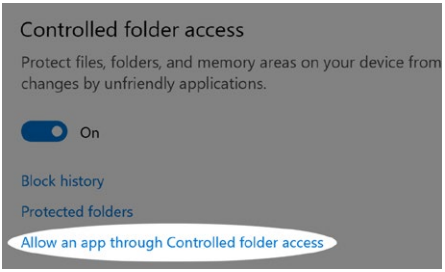
7. Once controlled folder access is turned on, click on **Protected folders**.

   NOTE: You can only use this functionality if you are an administrator.

   If you are a standard account user, you will be prompted to login or authenticate using the administrator account.

   For more information regarding administrator and standard user accounts, please refer to "Step-by-Step Guide – Managing User Accounts on Microsoft Windows 10".

Setting up ransomware protection for Microsoft Windows 10 CONTINUED



8. Click on **Add a protected folder** to select the folder you want to be added to the Protected List.

   By default, the following folders are already included in the Protected List:
   - Documents
   - Pictures
   - Videos
   - Music
   - Favourites

   NOTE – This will restrict applications from accessing any folders in the Protected List.

9. **OPTIONAL** – To allow applications to access files inside folders on the Protected List, go back to the "Ransomware protection" window and click on **Allow an app through Controlled folder access**. Then click **Add an allowed app**.

   NOTE – This step is only recommended for users who are comfortable navigating the Windows folder structure.

   By default, Microsoft has a list of apps that are trusted and included behind-the-scenes. You may have applications such as MYOB or Adobe that are not part of this list.

   Only allow apps that are reputable and trustworthy to access your folders in the Protected List, as this is similar to allowing a technician into your house without supervision.

Notes

Notes

Notes

ACSC Australian **Cyber Security** Centre

For more information, or to report a cyber security incident, contact us

cyber.gov.au

call 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate