



Module 12v2

**Professional Practice Program
Cyber Security**



Implementing Cyber Security Resiliency Hardening Guide

Cyber Security Hardening Guidelines For Your Microsoft Windows And Apple macOS Computers

Disclaimer

© Institute of Public Accountants July 2021– all rights reserved.

All the information, skills and concepts contained within this publication are general in nature only. This publication and any part thereof should not be taken as specific advice and may not be appropriate for the reader's circumstances, nor can this publication take into account all possible future developments in this subject matter. It is recommended that the reader obtains independent, specific advice before attempting to implement any concepts contained in this publication. The intent of this publication is to offer a variety of information to provide a wider range of choices recognising that we all have widely diverse circumstances and viewpoints in an ever changing field. Should any reader choose to make use of the information contained herein, this is their decision and the contributors (and their companies), authors, and publishers do not assume, and expressly disclaim, any responsibility or liability whatsoever, under any conditions or circumstances.

Contents

| | |
|---|----|
| A Note To The Reader | 4 |
| What Are The Objectives Of This Manual? | 4 |
| Your Cyber Security Resiliency Hygiene Steps | 6 |
| Microsoft Windows | 7 |
| How To Patch And Update Your Operating Systems and Applications | 8 |
| Keeping Commonly Used Applications Up To Date | 16 |
| How To Implement Endpoint Protection Software..... | 21 |
| Some Common Questions & Answers | 25 |
| How To Implement Secure Email Protection..... | 28 |
| How To Implement Functional Backup / Restore Processes | 35 |
| Performing A Backup | 35 |
| Performing A Restore..... | 45 |
| Miscellaneous - Windows Additional Security Configurations | 48 |
| Remove Admin Rights From Desktops | 48 |
| Apple macOS | 52 |
| How To Patch and Update Your Mac Software and Apps | 53 |
| Updating Third Party Applications Originated From Apple App Store | 55 |
| Updating Third Party Applications Not From The App Store | 55 |
| How To Implement Endpoint Protection For Your Mac | 57 |
| How To Employ Email Secure Best Practices For Your Mac..... | 58 |
| How To Implement Functional Backup / Restore Process | 61 |
| Backup Your Mac with Time Machine | 61 |
| Backup Your Mac with iCloud Drive | 63 |
| Restoring Your Mac From A Backup..... | 64 |
| Restoring From A Time Machine Backup..... | 64 |
| Restoring Both The macOS And Your Files | 67 |
| Miscellaneous - macOS Additional Security Configurations | 70 |
| General Security & Privacy Settings | 71 |
| Turning FileVault On | 72 |
| Turning The Firewall On..... | 74 |
| Checking Your Privacy Settings | 75 |
| Create A Standard Account (non-admin) For Everyday Activities | 77 |

A Note To The Reader

You and Your Computer machine are on the frontline of the cyber battleground. Together, you both represent the most significant entry point for attackers obtaining a toe hold into your business.

Nearly every day, we read stories about companies that have suffered severe breaches due to not taking cybersecurity seriously.

Despite widespread awareness around cybersecurity, there's a reason why cyber-attacks are still so effective. They are always several steps in front of us. These miscreants continue to increase their level of sophistication, and there are now dozens of different ways that they can attempt to get their hands on your valuable and personal information.

Phishing and ransomware represented the top two most significant threats to hit organisations in the past year.

Their motivation is money. Well, your money!

2021 has been a very productive year for cybercriminals. And it's only going to get worse for us! Cybercrime will grow by 15% per year over the next five years, reaching an estimated \$10.5 trillion by 2025 annually. Think about it. This represents the most significant transfer of economic wealth in history. Cybercrime can be viewed as a tax on global growth.

So, What Is Cyber Security Resiliency?

Almost all cybersecurity measures' core function is to guard hardware, software, and data against everything from unauthorised access to malicious attacks and even accidental damage.

As such, the majority of cybersecurity measures needs to be implemented long before an attack occurs.

Everyone should know how important it is to stay safe online. If you fall for a phishing scam or similar, you can end up having your identity stolen, which can have some pretty severe consequences.

Although implementing effective company-wide cybersecurity controls is the aim of the game, it doesn't stop there. You see, being cyber secure doesn't guarantee that you will not suffer a breach. What is more important is how well you recover from such a breach - being cybersecurity resilient needs to be your desired outcome.

What Are The Objectives Of This Manual?

The purpose of this manual is to provide you with a step-by-step process of how to implement the necessary cyber hygiene to give you the best cyber protection as well as cyber resiliency for business as well as yourself.

The manual is divided into two segments:



1. **Segment 1** – How to implement security controls for Microsoft Windows and associated applications; And
2. **Segment 2** – How to implement security controls for Apple macOS and associated applications.

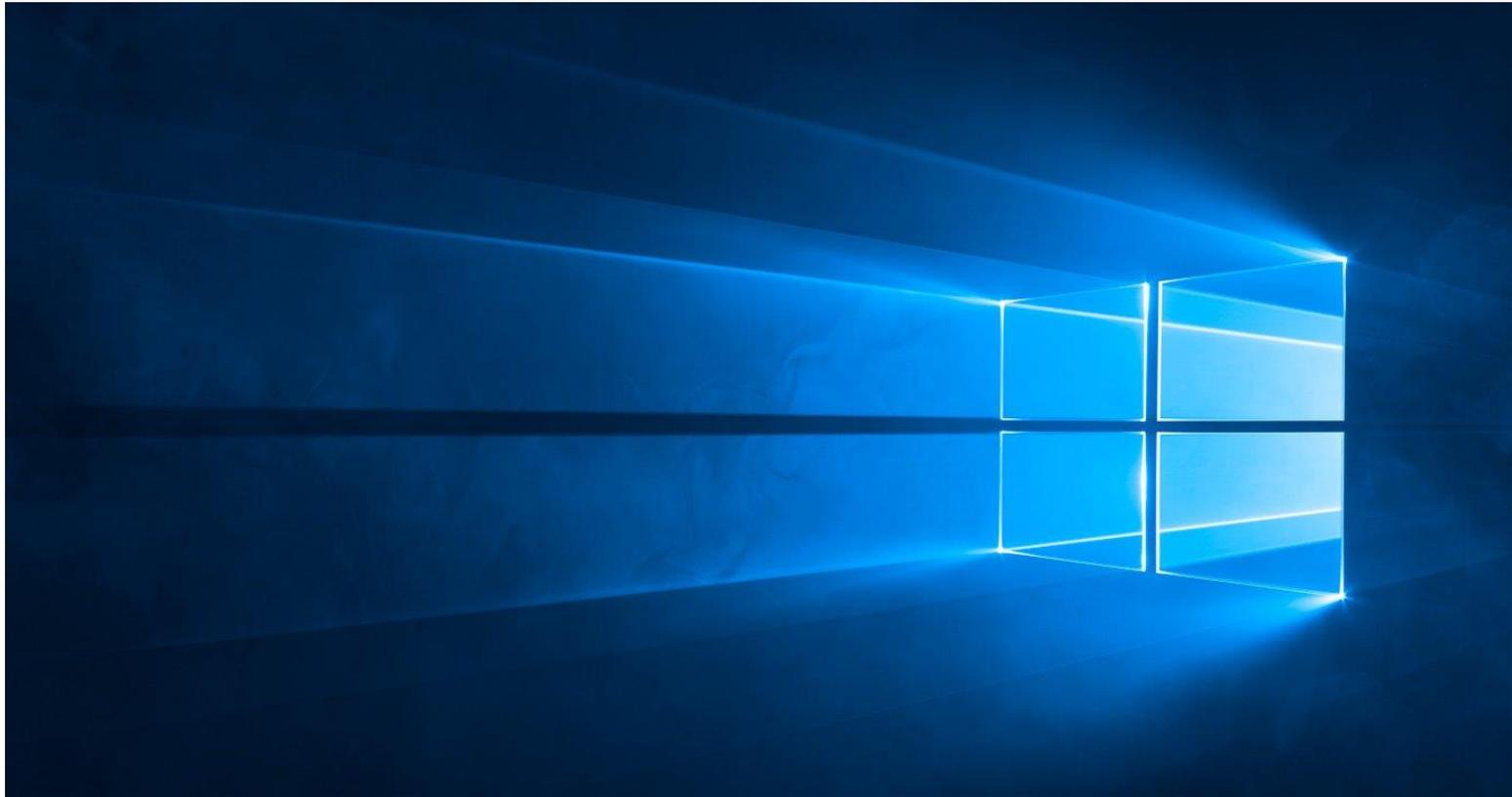
Your Cyber Security Resiliency Hygiene Steps

Every day we do things to safeguard ourselves and our business. For example, when we drive our cars, we buckle up; We brush our teeth daily to maintain our mouth and gums hygiene; We apply sunscreen to our skin to protect ourselves from the harmful rays of the sun; We take car insurance in case of an unforeseen accident.

Protecting your information and digital business worlds need to become your regular day-to-day activity. You must adopt a high level of hygiene practice on a day to day basis, or else you very much endanger your business.

Remember, your BUSINESS is your BUSINESS. Whether you are in business or managing someone else business, you are responsible for its success.

Microsoft Windows



*“I believe that if you show people the problems and you show Them The Solutions,
They Will Be Moved To Act.”*
— **Bill Gates**

The following four subsections are the fundamentals of hygiene practices that you need to employ within your business.

| Section | Page |
|--|------|
| 1. How To Patch and Update Your Microsoft Windows Systems and Applications | 10 |
| 2. How To Implement Endpoint Protection Software | 22 |
| 3. How To Implement Secure Email Protection | 29 |
| 4. How To Implement Functional Backup / Restore Processes | 36 |
| 5. Miscellaneous - Windows Additional Security Configurations | 47 |

How To Patch And Update Your Operating Systems and Applications

If your system seems to be working fine, you may be wondering why you need to apply any updates or patches to either the system or its applications. We have often heard of the saying, *“if it isn’t broke, don’t fix it!”*.

Great quote, but unfortunately, it doesn’t apply for engendering business resiliency from cyber threats.

Malware is continuously adapting. It's dynamic. This means your cyber resilience effectiveness has a direct correlation with the latest system and application updates.

And if you decide not to apply the updates, you might be leaving the door wide open for malware to take advantage of. Malware exploits flaws in your operating system and applications.

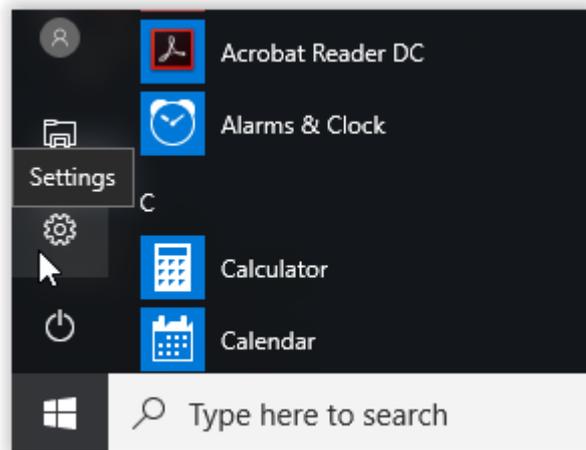
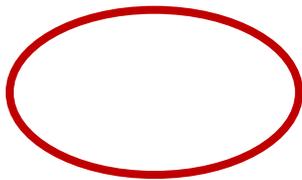
By applying these updates, you minimise the attack surface.

Keeping Microsoft Windows up to Date

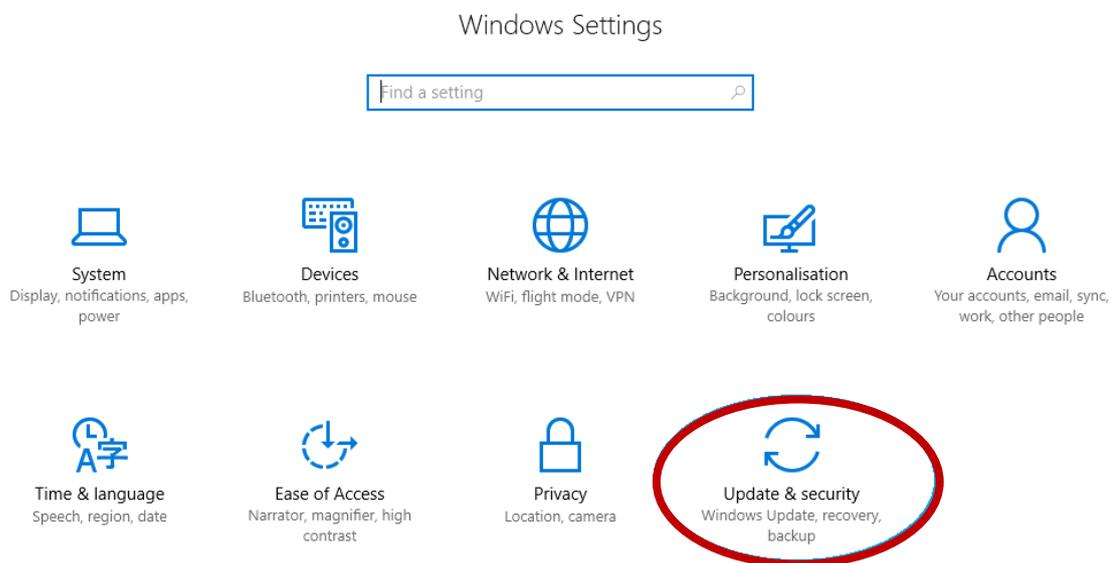
Every computer running windows comes with the windows update functionality. This enables Microsoft to provide machines with the latest software patches that fix security problems within the operating system and the (Microsoft) applications.

One can check the status of the updates by following these steps:

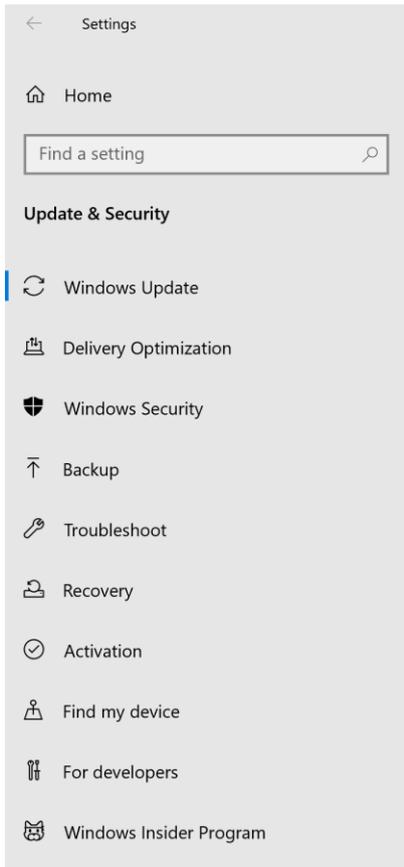
1. Click on the “Windows”  button followed by a click on “Settings.”



2. In Windows Settings, double click on “Updates & Security.”



This will pop up a window and will show the status of “Update Status.”



Windows Update

*Some settings are managed by your organization
[View configured update policies](#)

 You're up to date
 Last checked: Today, 8:36 AM

[Check for updates](#)

[Check online for updates from Microsoft Update](#)

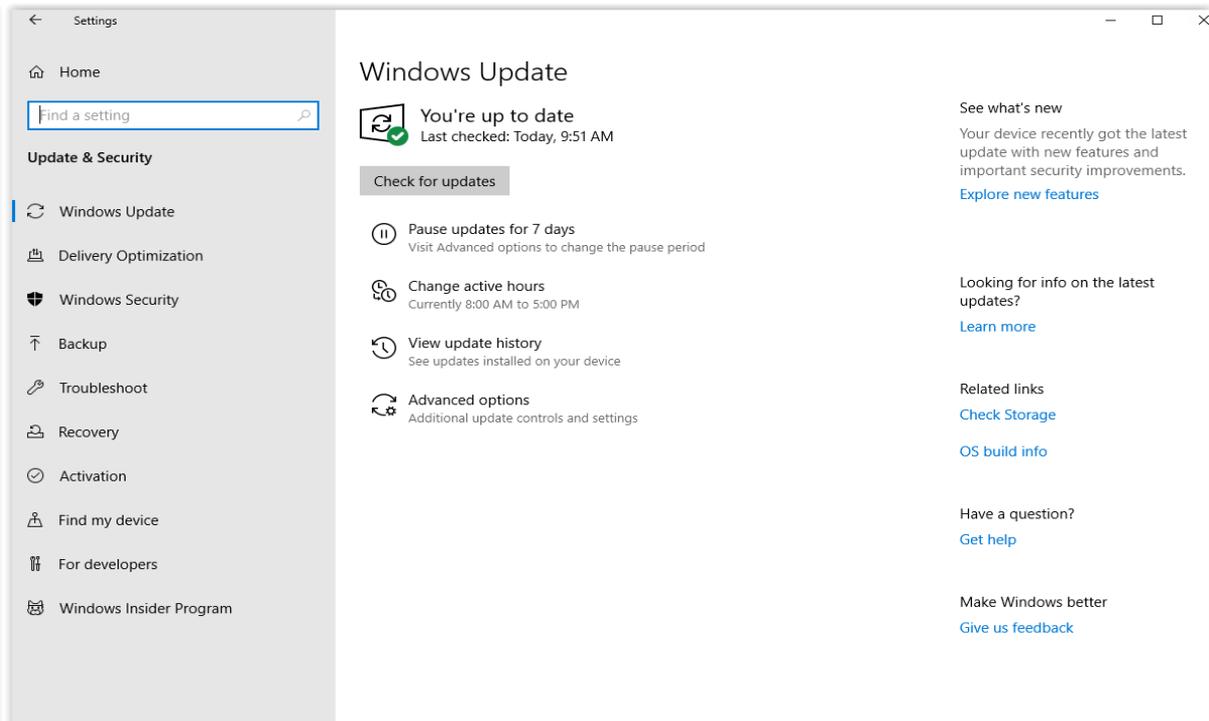
-  **Pause updates for 7 days**
 Visit Advanced options to change the pause period
-  **Change active hours**
 Currently 8:00 AM to 6:00 PM
-  **View update history**
 See updates installed on your device
-  **Advanced options**
 Additional update controls and settings

See what's new

Your device recently got the latest update with new features and important security improvements.
[Explore new features](#)

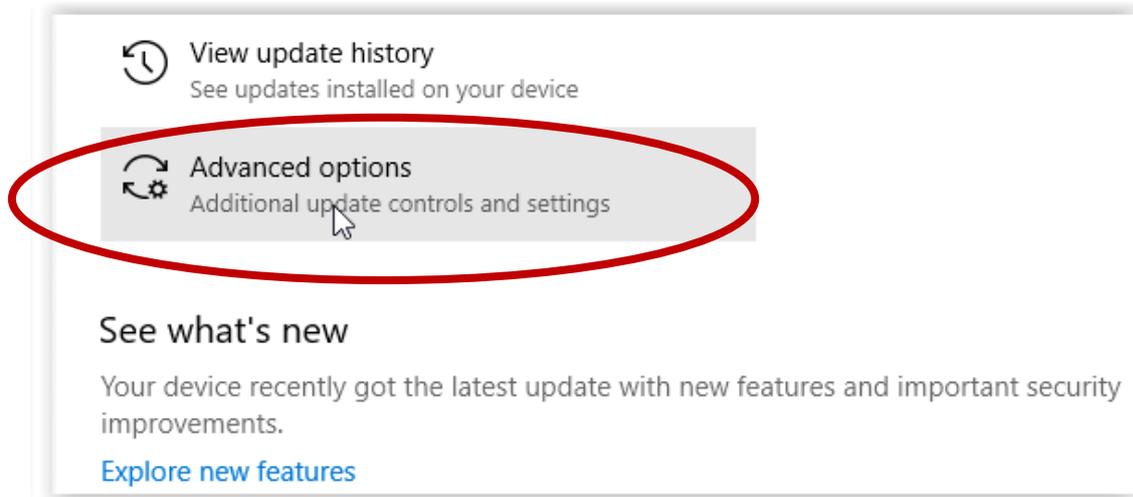
If “Windows update” is centrally managed like in this example, the computer will report that, as can be seen over here.

The following screen is from a computer that’s running without a managed update:

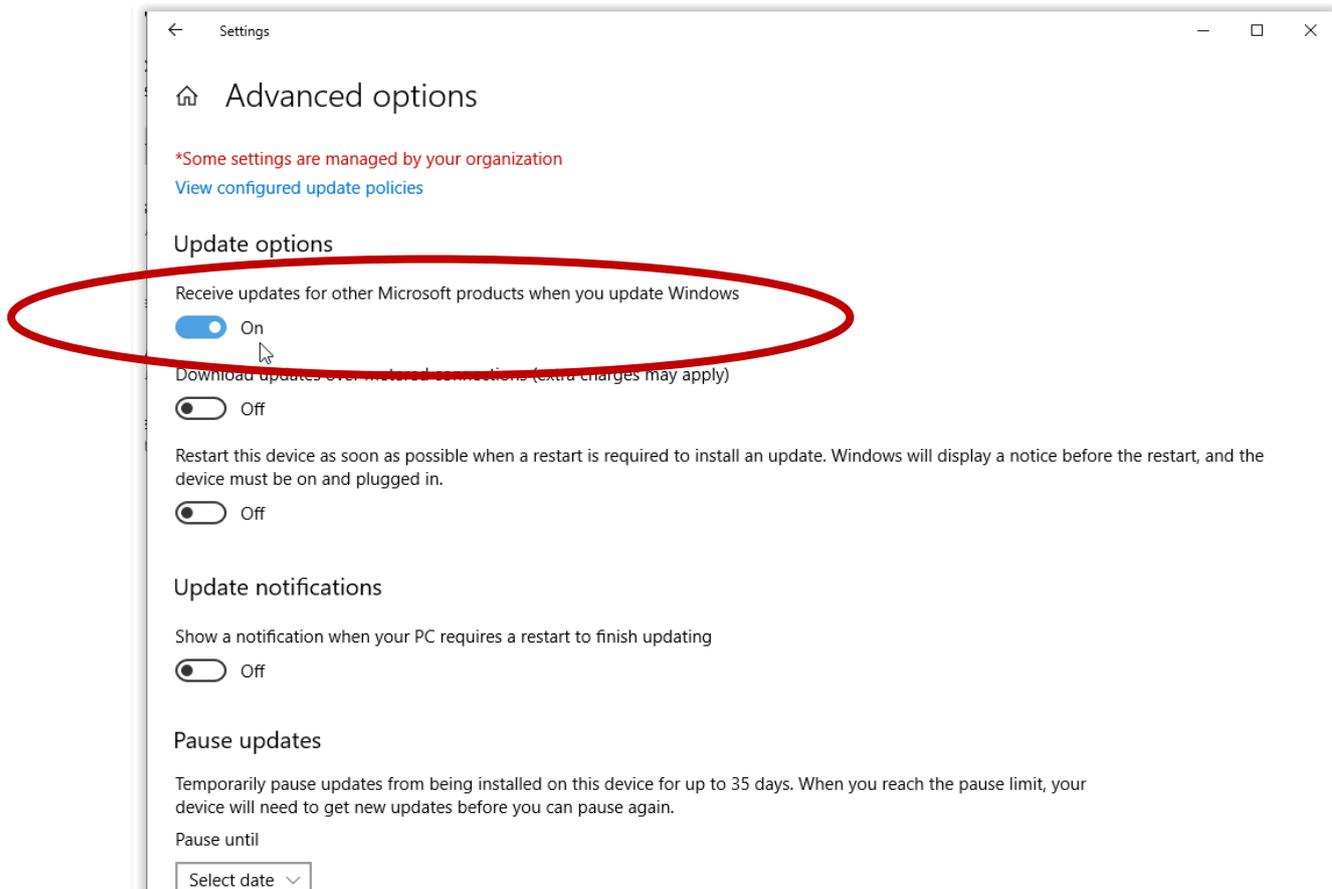


To make sure a computer is getting all the updates for Microsoft products to do the following:

3. Click on “advanced options.”

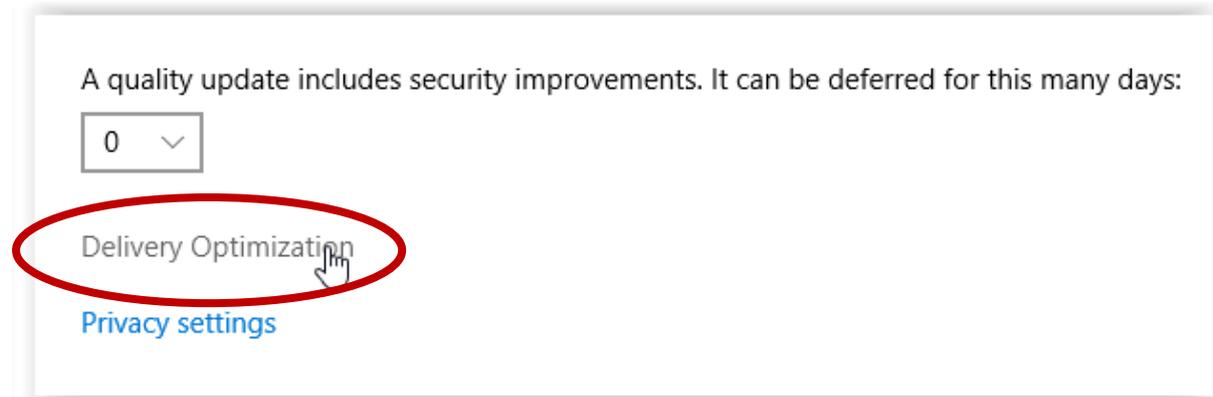


4. Make sure the slider is set to “On” at: “Receive updates for other Microsoft products when you update Windows”, as seen below.



If there are multiple windows computers on the network, it is possible to redistribute the updates internally. This will ensure it makes the most of your internet connection.

Scroll further down in the “Advanced options” screen and click “Delivery Optimization”:



Turn On the slider and Select only “PCs on my local network.”

Delivery Optimization

Delivery Optimization provides you with Windows and Store app updates and other Microsoft products quickly and reliably.

Allow downloads from other PCs

If you have an unreliable Internet connection or are updating multiple devices, allowing downloads from other PCs can help speed up the process.

If you turn this on, your PC may send parts of previously downloaded Windows updates and apps to PCs on your local network or on the Internet. Your PC won't upload content to other PCs on the Internet when you're on a metered network.

[Learn more](#)

Allow downloads from other PCs

On

PCs on my local network

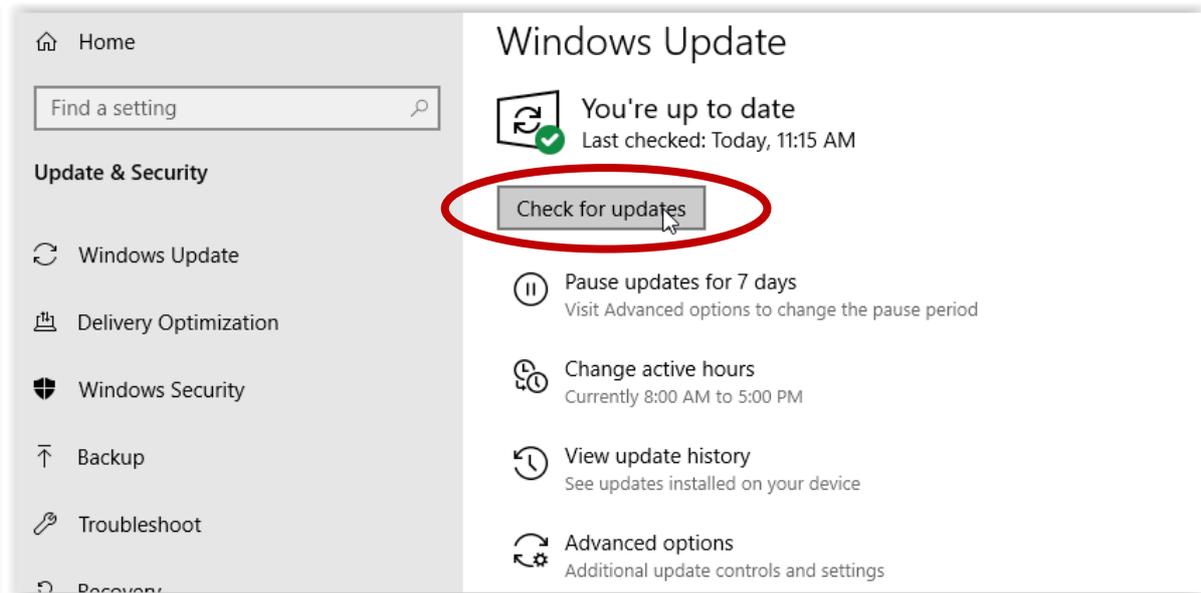
PCs on my local network, and PCs on the Internet

[Advanced options](#)

[Activity monitor](#)

If there is just one Windows computer, this setting can be turned off.

5. To perform a manual update of Microsoft applications and the Operating system, click “Check for Updates.”



Keeping Commonly Used Applications Up To Date

Many commonly available software needed to extend the operating system's functionality tends to come with new updates.

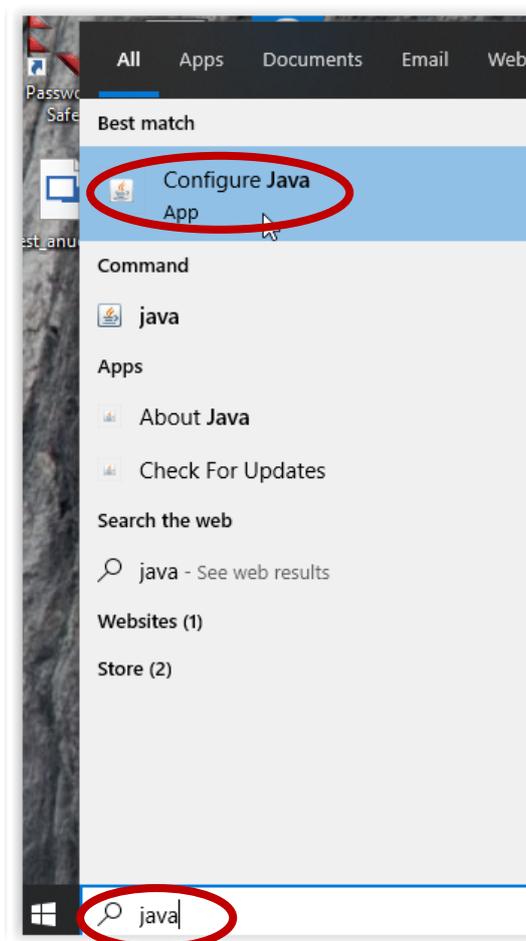
It would be impossible to describe all of them, but these would be the most common ones and targeted a lot by miscreants with malicious intent.

Java

Java is a popular programming language created in 1995. It is owned by Oracle and has been downloaded by more than 3 billion devices. Java is used by desktops, web applications, games, databases and much more.

Unfortunately, Java has had over years numerous security vulnerabilities. For this reason, it is suggested from a best practice point of view to either remove it or at least ensure that it is kept up to date.

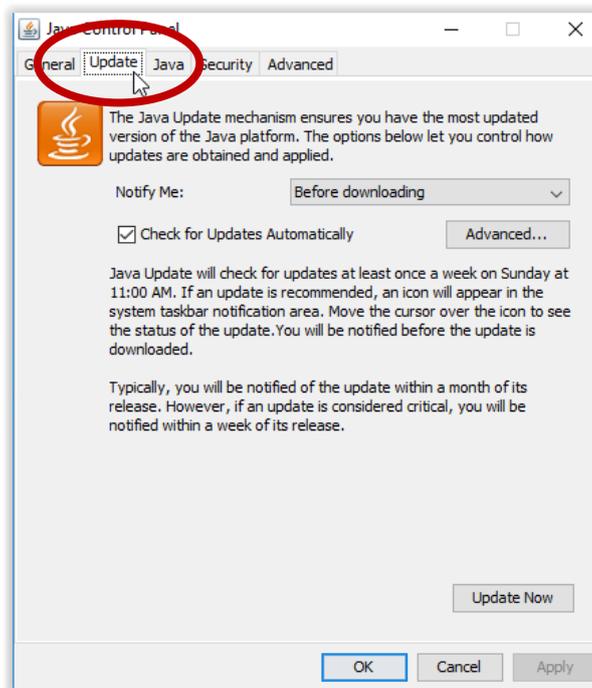
Java has a management tool that can be found in the windows control panel. To access it, start typing “java” in the windows search box and click on “Configure Java.”



An alternative way is to go through Control Panel: Open “Java (32-bit)



Select the “Update” tab in there and check the settings.



The default settings will have auto-update on as well, and there is a button to perform a manual update by clicking: “Update Now.”

JavaScript

JavaScript is a programming language for the Web. It can update and change both the HTML and CSS code. Also, it can calculate, manipulate and validate data. In short, it is a highly capable program.

JavaScript is most commonly used as a client-side to make web development easier and more attractive.

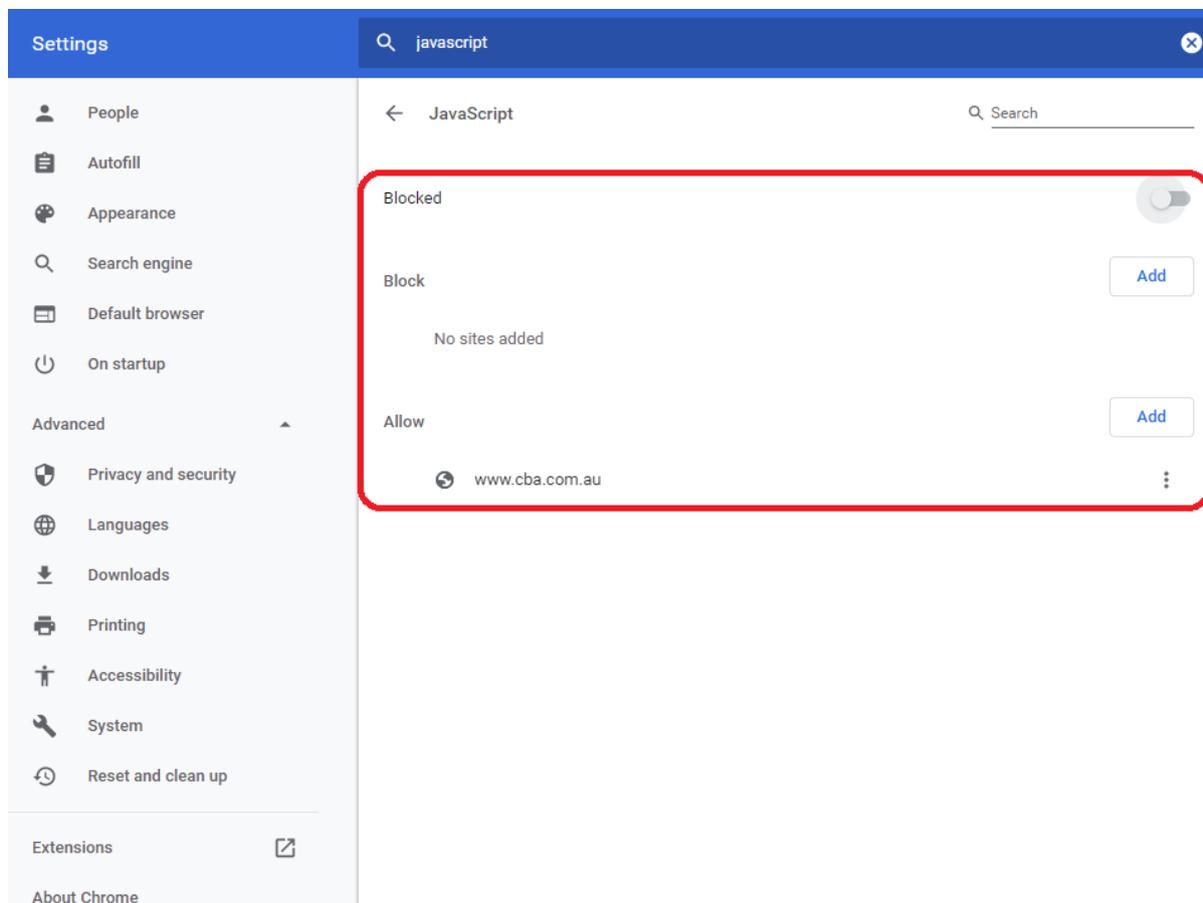
What makes this application so risky is that it allows hackers to inject client-side script into web pages viewed by other users. It's accounted for as much as 84% of all security vulnerabilities on the Internet in the past.

How do you know whether JavaScript is running on your machine? Remember that JavaScript is a "per browser" setting. So you will have to identify whether it is running on each of your browsers.

It is suggested from a best practice point of view to either block it or run on only certain websites of your choice.

You will need to test the browser's functionality and see whether regular day-to-day access is still functional. Interestingly, many banks require JavaScript to be turned on.

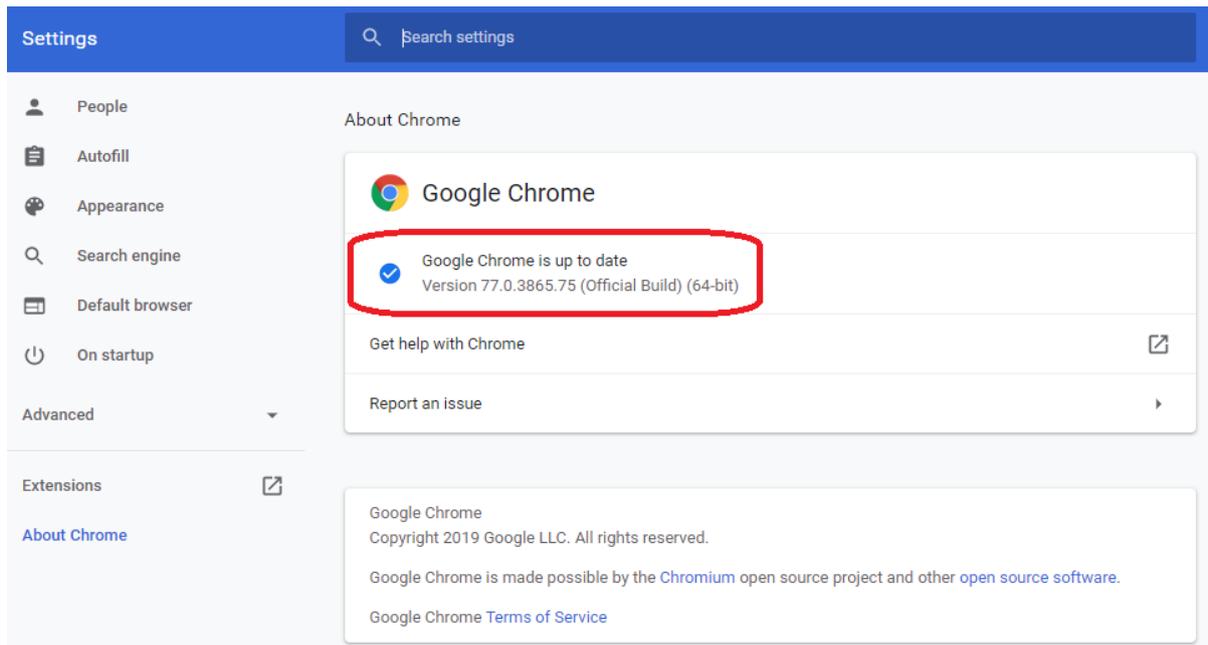
For Google Chrome, it would like something like this.



If you intend to run JavaScript, make sure you regularly update the browser.

- For Google Chrome, type the following command in the URL: <chrome://settings/help>

It will automatically then check that the browser is up to date, as can be seen in the following picture



- For Mozilla Firefox. By default, it is set to update automatically, but you can always do a manual update. Manual update will still let Firefox download an update, but it won't install it until you restart Firefox. Here's how to set it up:
 - Click the menu button , click  Help and select About Firefox.
 - The **About Mozilla Firefox** window will open. Firefox will begin checking for updates and downloading them automatically

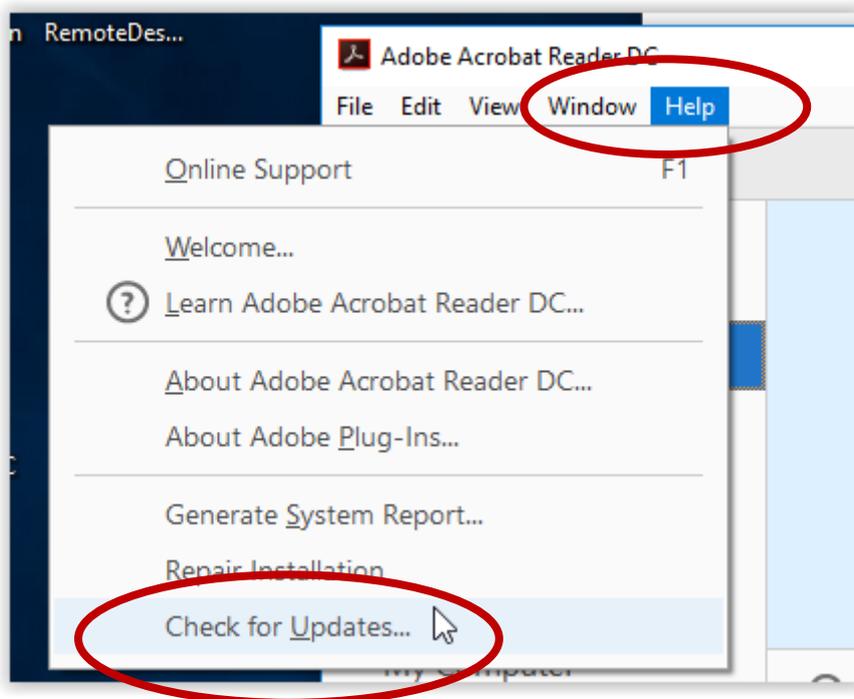


- When downloading is complete, it will ask you to **Restart to update Firefox**

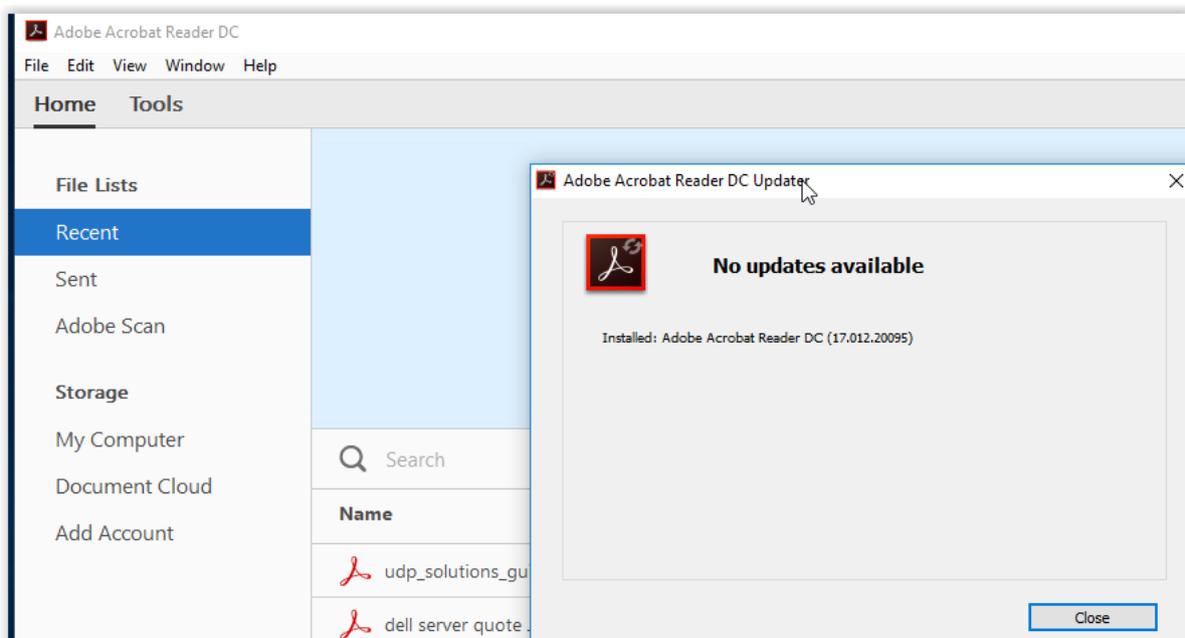
Adobe Reader

Adobe Reader is a tool used to open PDF documents. It's been targeted a great deal by malware creators and other miscreants.

The update can be found in the program itself. Go to "Help" and click: "Check for Updates..."



Running it will either update the software or return the up to date status:



How To Implement Endpoint Protection Software

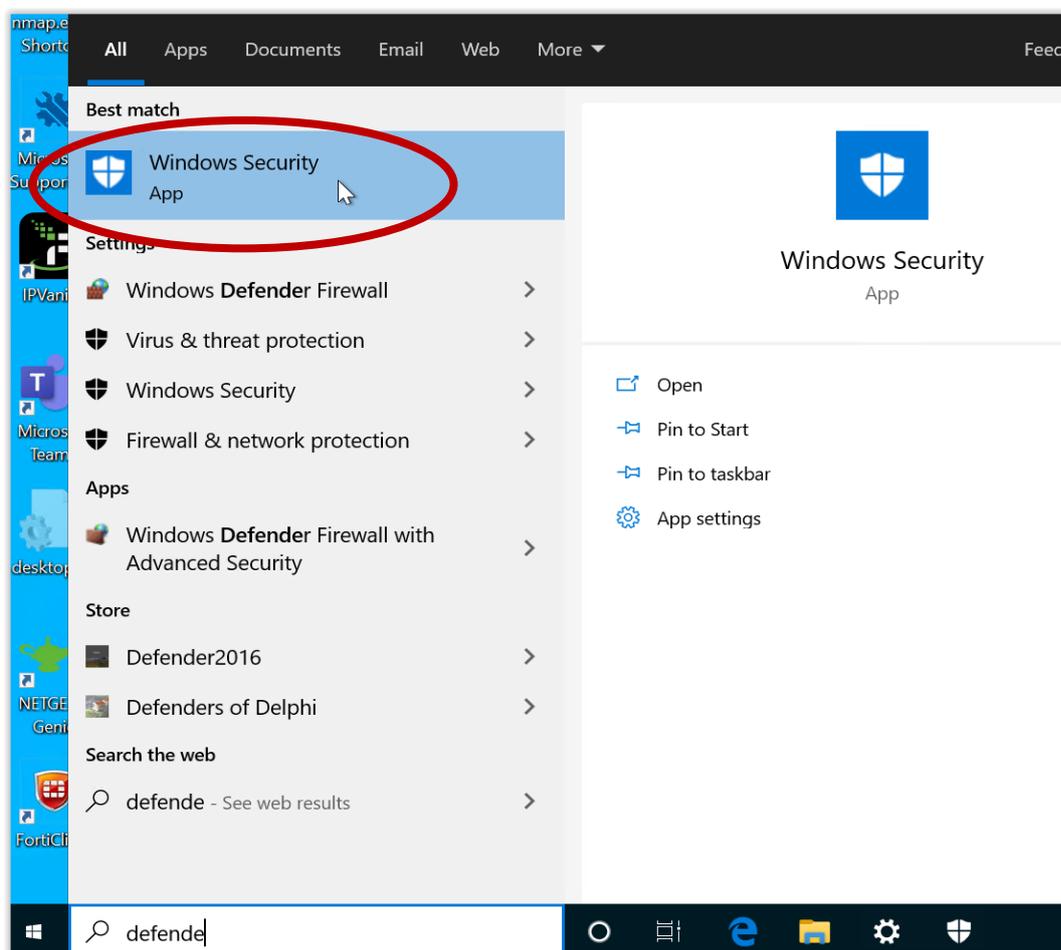
Microsoft Windows has inbuilt antivirus software that helps you identify and remove viruses, spyware, and other malicious software.

Windows Defender Antivirus is built-in to Windows. There's nothing to buy and nothing to install. No configuration and no subscriptions.

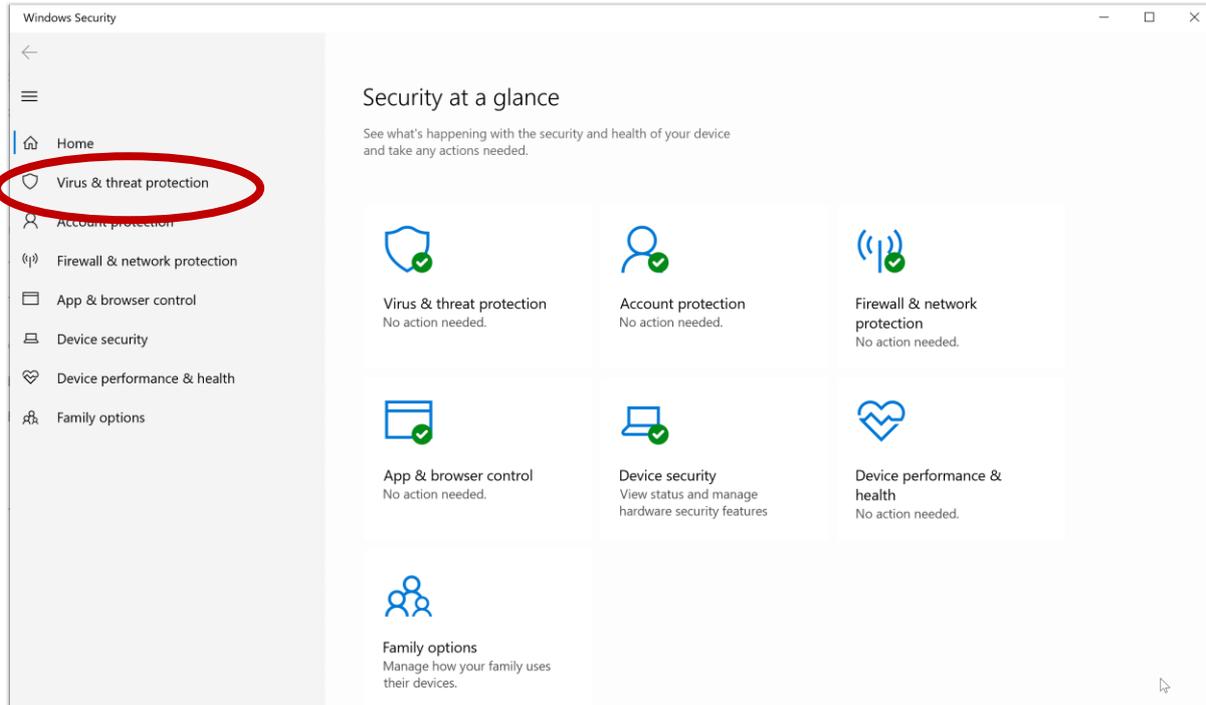
Windows Defender runs in the background and notifies you when you need to take a specific action. However, you can use it anytime to scan for malware if your computer isn't working correctly or if you clicked a suspicious link online or in an email message.

Question: How do I know whether Windows Defender is running or not?

Answer: Just ask Cortana or type "Defender" in the taskbar search box. Click on "Windows Security"

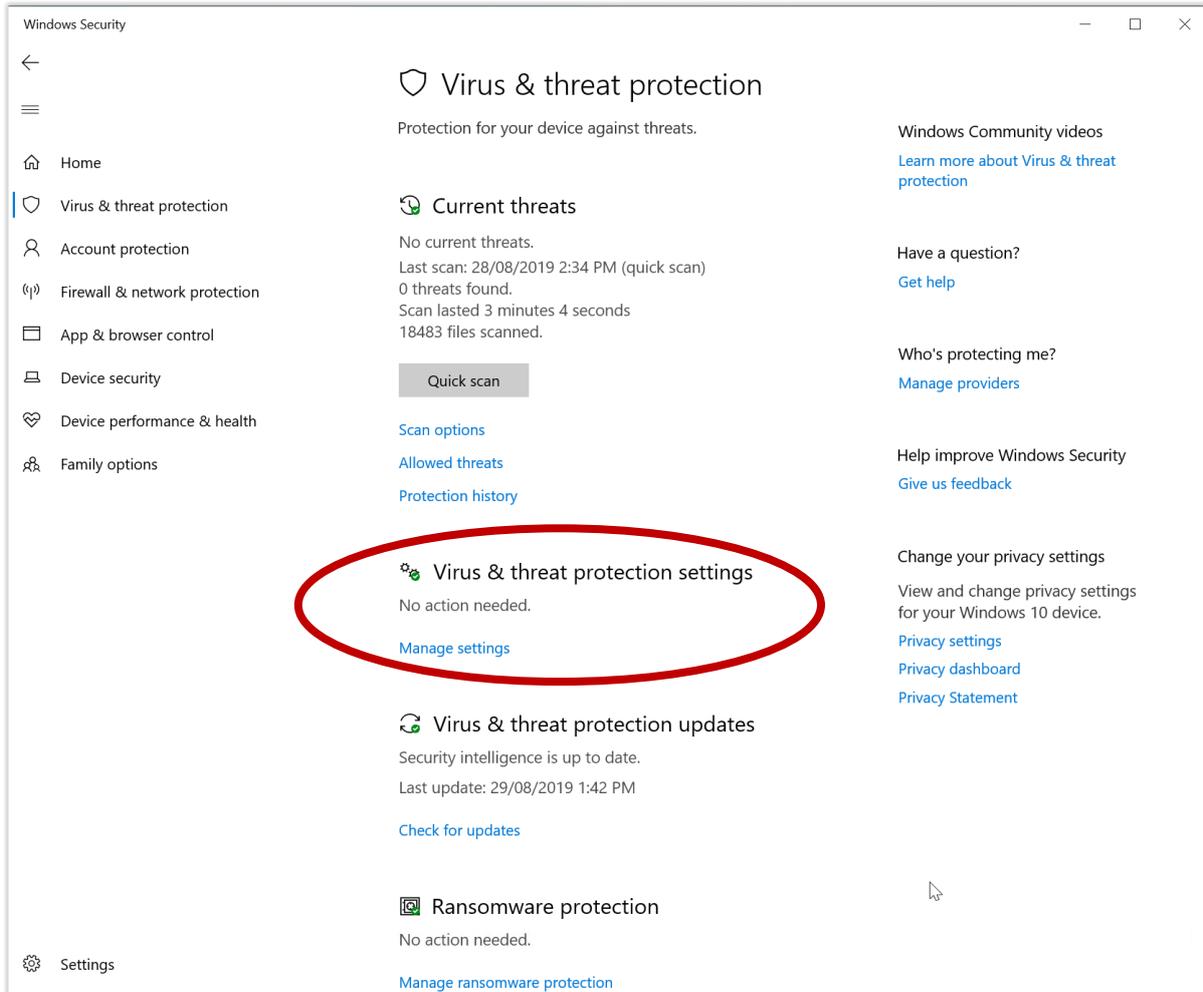


This will provide you with a "Security at a glance" overview of the overall security health of your device.



Next, click on “Virus & threat protection”.

And now click on “Manage settings” under “Virus & threat protection settings.”



Make sure that “Real-time protection” is set to On. This can be found at “Manage settings.”



Microsoft now includes Ransomware protection with its Defender products as well. Make sure it's been turned on (off by default)

 **Virus & threat protection updates**
Security intelligence is up to date.
Last update: 29/08/2019 1:42 PM
[Check for updates](#)

 **Ransomware protection**
No action needed.
[Manage ransomware protection](#)

 **Ransomware protection**
Protect your files against threats like ransomware, and see how to restore files in case of an attack.

Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

 **On**

[Block history](#)
[Protected folders](#)
[Allow an app through Controlled folder access](#)

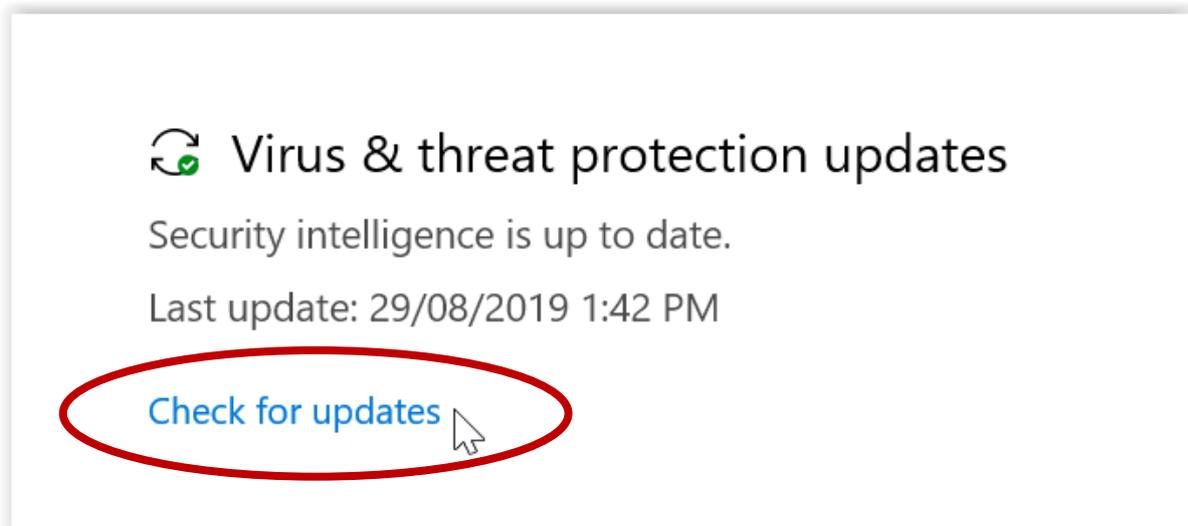
Some Common Questions & Answers

Question: I'm having problems with my Windows Defender running?

Answer: It may be because you may already have another antivirus software. If you want to use Windows Defender, uninstall all of your other antivirus programs, and Windows Defender will automatically turn on. You may be asked to restart your device.

Question: How do I know whether I am up to date?

Answer: You can manually get the latest update by clicking on "Check for updates."



Question: How do you run a scan, and how often?

Answer: It is suggested to run a Full scan on your machine once a week. This is going to be by far more accurate than a Quick scan.

Quick scan

Checks folders in your system where threats are commonly found.

Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

Custom scan

Choose which files and locations you want to check.

Windows Defender Offline scan

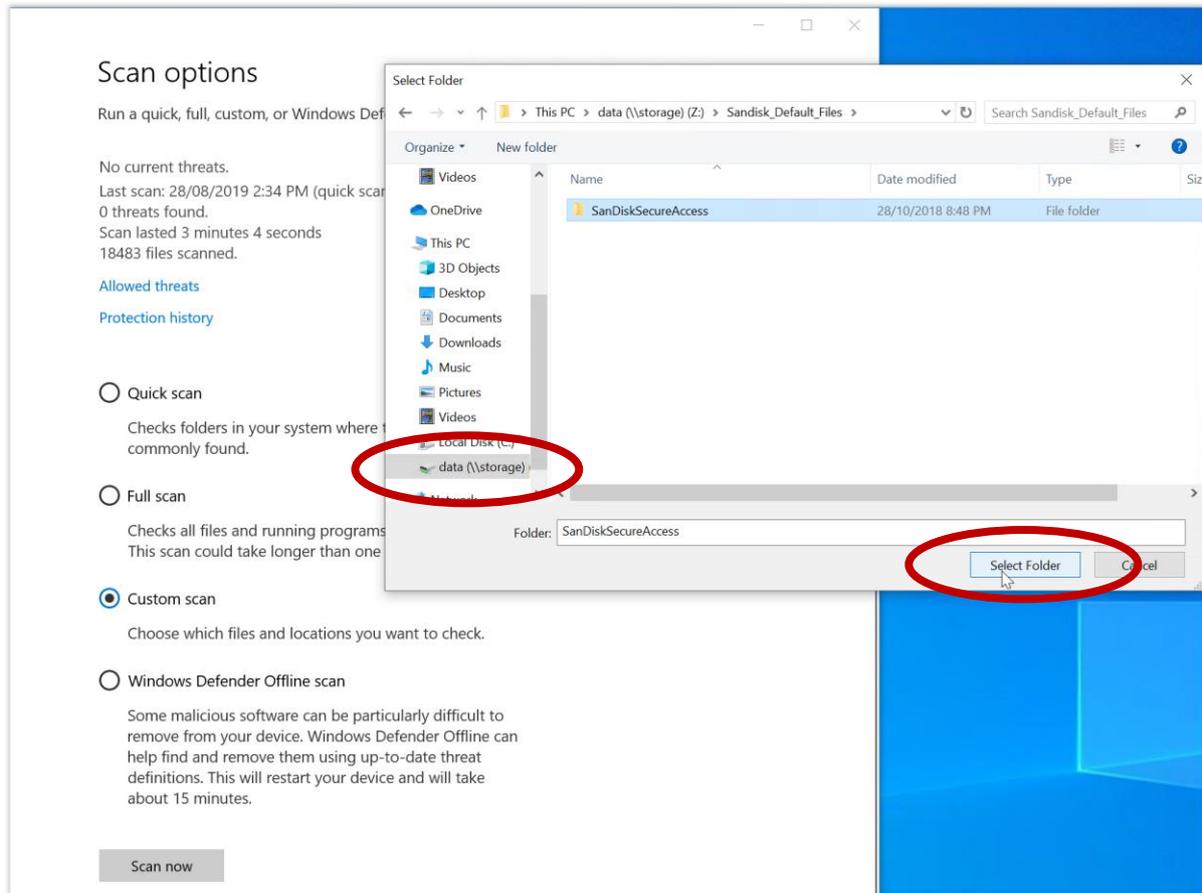
Some malicious software can be particularly difficult to remove from your device. Windows Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Scan now

Question: How do I scan the attached drives?

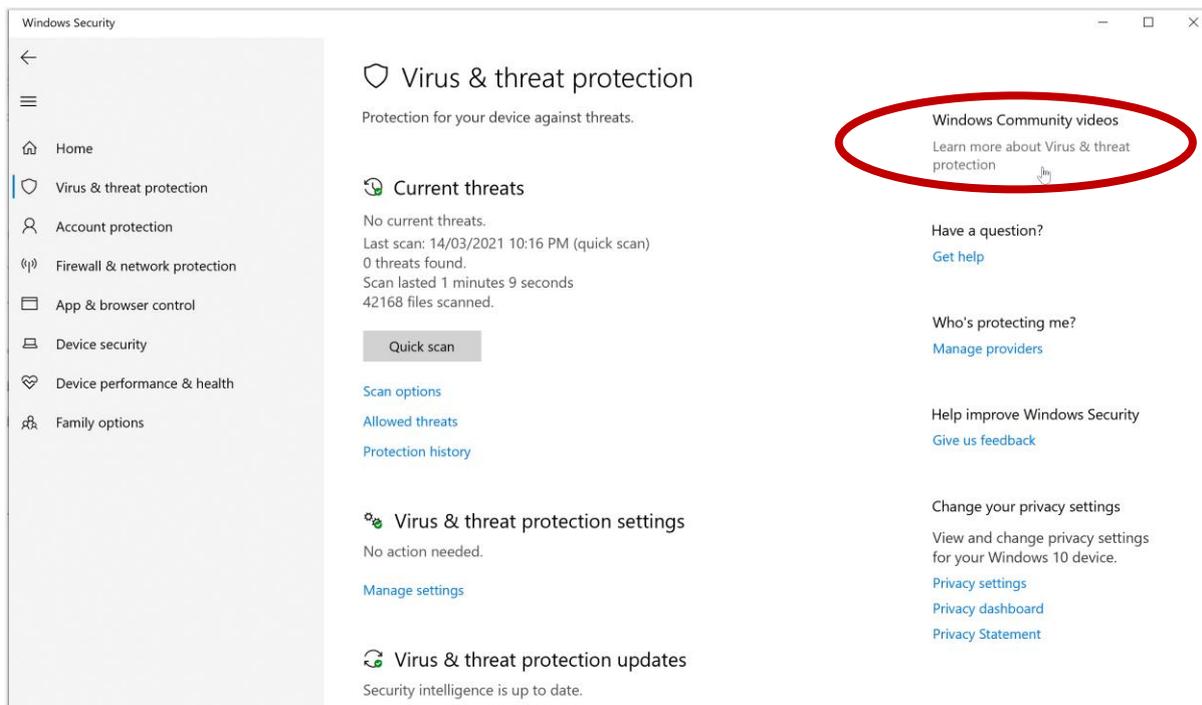
Answer: You can “Custom scan” as shown above in the third option. This will provide you with options of what you want to scan.

Now you will be able to select any attached network share or USB device



Question: Where else can I find more information about Windows Security?

Answer: By clicking on “Learn more about Windows Security.”



How To Implement Secure Email Protection

The security industry widely agrees at large that the majority of all security attacks start with email (around 91%)

The weakest point of security in any organisation is **the users**, either due to a lack of awareness, security fatigue or plain and simple negligence. Attackers know this, and they target users through email because, with a working email address, a malicious but well-crafted attack could quickly get in front of a vulnerable employee.

Since email is the number one threat vector, it comes to reason that our first line of defence should be the protection of the mailbox.

To “minimise the attack surface”, businesses must adopt the following security best practices.

- **Create a strong password for your email account.** You should also make a point of changing your password often and look into any additional security measures your email provider can offer. For example, some email providers can send a text message to your phone if they detect any out-of-character activity, such as someone logging into your account from an unfamiliar geographical location.
- **Check whether you should be scanning email attachments manually.** Email attachments are a huge potential source of viruses and malware. Although many email providers automatically scan attachments for you, if you’re unsure whether this applies to your particular account, then don’t take the risk. Check your account’s ‘Settings’ or your email provider’s documentation to see whether they check email attachments automatically or whether you should be scanning these attachments yourself. And remember that even if your email provider scans all attachments for you, there’s no guarantee that it’ll catch 100% of dangerous email attachments, so you should never open or download anything that strikes you as unusual or outright suspicious.
- **Establish clear rules about email usage.** Setup an Email Acceptable Use Policy (AUP) that applies to all staff (including temporary staff), visitors, and contractors. This policy should be considered part of the conditions of using your organisation systems.
- **Close and forward accounts for ex-employees.** Closing an account ensures that when employees leave your organisation, they no longer have access to your business operations through their account. Forwarding ensures the business they were handling becomes the responsibility of a current employee capable of completing or delegating the continued communication.
- **Watch out for “phishing” emails.**
 - Don’t open attachments. Be wary of any attachment; and
 - Don’t click on links. Be wary of any links.

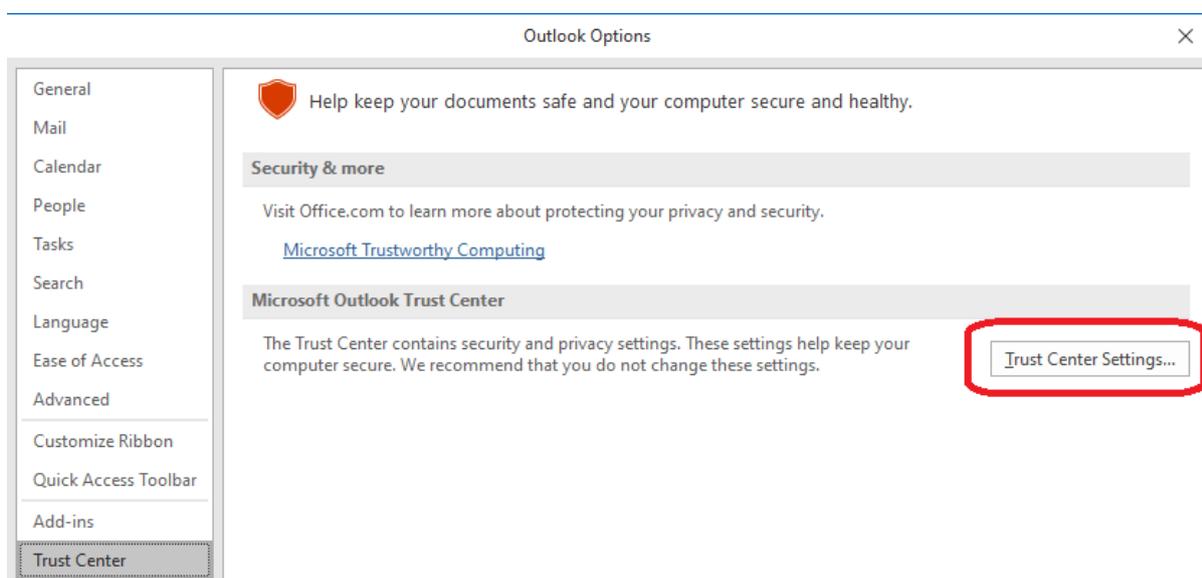
- Do not respond to requests, as this would suggest that you are a natural person behind the email.
- **Do not “unsubscribe” from a spam message.** This tells the hacker that you are a real contact and would also lead to receiving more spam. And some of them may even lead you to a malicious site.
- **Do not send sensitive personal information via email** unless you use specialized tools that can encrypt your message.
- **Whenever you need to email a group of people, use Bcc rather than Cc.** Then, even if this email falls into the hands of potential spammers or hackers, at least they won’t immediately have access to the contact details of everyone on that list.
- **Never access your email using public Wi-Fi.** Public Wi-Fi is never secure, and there are many ways hackers can steal all the information that passes through such a network.
- **Don’t share passwords either with your colleagues or friends.** You wouldn’t share your toothbrush with some else, don’t share your password.
- **Be sure to log out when you have finished work.**

Remember

“Do NOT Respond To Any Emails If You Didn’t Ask For It In The First Place!”

Microsoft Outlook Security Tips

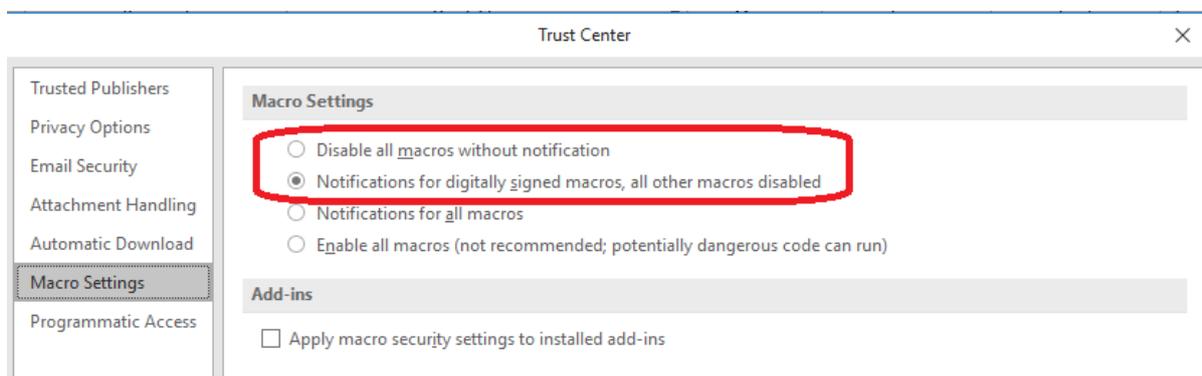
- Microsoft will never ask for your password in email, so never reply to any email asking for personal information, even if it claims to be from Outlook.com or Microsoft.
- Outlook Trust Centre. The Trust Center is where you can find security and privacy settings for Microsoft Office programs.
 - To access Outlook Trust Centre, click “ Options” on the File Tab.
 - Click “Trust Centre’, and then click “Trust Centre Settings.”
 - Click the area that you want (on the left pane) and make the selections you want.



Suggested Settings for Microsoft Outlook

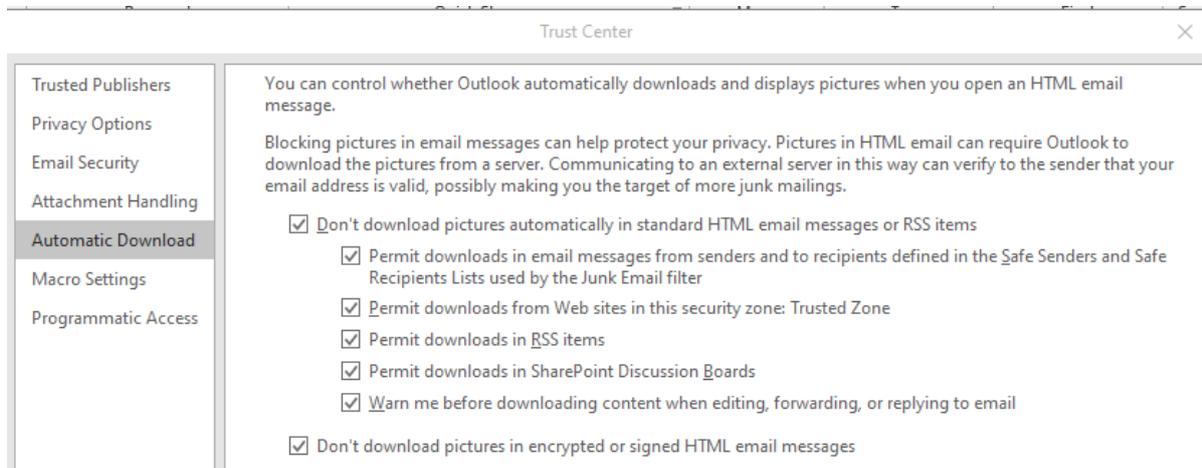
- Macro Settings. Block macros from the Internet and only allow vetted macros either in ‘trusted locations’ with limited write access or digitally signed with a trusted certificate.

Note: Microsoft Office macros can be used to deliver and execute malicious code on systems



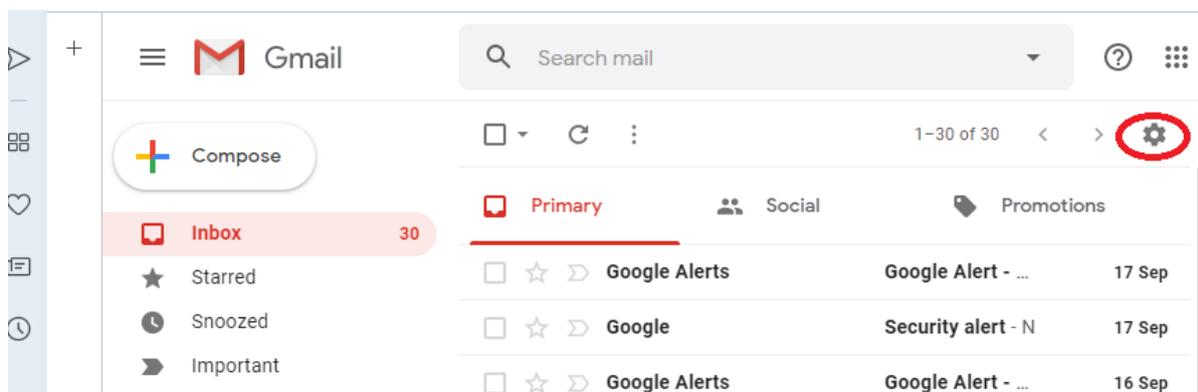
- Automatic Download. Blocking pictures can help protect your computer. It helps keep malicious code from being exploited.

Microsoft Outlook is configured by default to block automatic picture downloads from the Internet.

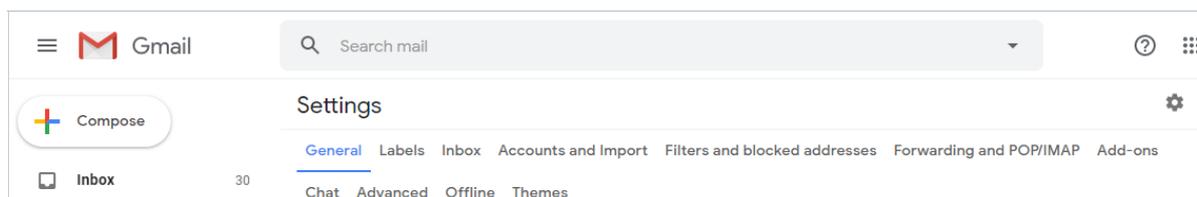


Google Gmail Security Tips

- Verify Gmail settings to see if everything is alright. When you log into your Gmail, click the “gear icon”, then click “Settings.”



It will look like this. Review the settings. Make sure that neither “Signature” or “Out Of Office Autoreply” haven’t been tampered with,



- Click on “Accounts and Import” and verify that the email addresses for **Send mail as:** is you.

Send mail as: **Boaz Fischer <bfcommsnet@gmail.com>** [edit info](#)
(Use Gmail to send from your other email addresses) [Add another email address](#)
[Learn more](#)

Check email from other accounts: [Add an email account](#)
[Learn more](#)

Using Gmail for work? Businesses can power their email with G Suite. [Learn more](#)

Grant access to your account: [Add another account](#)
(Allow others to read and send mail on your behalf) **Mark conversation as read when opened by others**
 Leave conversation as unread when opened by others
[Learn more](#)

- Click on “Filters and blocked addresses”.
 - **Filtered emails:** Make sure that you do not have any additional filters. If you do have a suspicious filter, delete it immediately.
 - **Blocked emails:** You can check all the blocked addresses in this section — you will not receive emails from these addresses, so make sure it doesn't contain any known or essential email address. If it does, unblock it.
- Click on “Forwarding and POP/IMPA”
 - **Forwarding:** Make sure that your emails are not being forwarded to someone else without your permission. If you find such an unknown address, remove it to disallow others from accessing your emails.
 - **POP Download:** Check that POP is not enabled without you knowing about it.
 - **IMAP Access:** You need to check that IMAP is not enabled if you are not using it.

Other suggested security practices

- **Turn on 2-Step Verification.** 2-Step Verification is an additional security strategy that helps to protect your account better as it asks you for a second authentication secret (other than a password)
 - Open “[Sign-in & security](#)” in a browser and click “2-Step Verification”, and then click “GET STARTED” on the following screen

- Home
- Personal info
- Data & personalisation
- Security**
- People & sharing
- Payments & subscriptions
- Help
- Send feedback

Security issues found

Protect your account now by resolving these issues



[Secure account](#)

Signing in to Google



| | | |
|---------------------------|-------------------------|---|
| Password | Last changed 6 Apr 2017 | > |
| Use your phone to sign in | Off | > |
| 2-Step Verification | Off | > |

- Then Google will ask you first to verify that it's you. So you will need to authenticate once again.
- It will then ask you the phone that you want to use

← 2-Step Verification



Let's set up your phone

What phone number do you want to use?

 | _____

Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

Text message Phone call

Don't want to use text message or voice call?
[Choose another option](#)

Step 1 of 3 NEXT

- It will then send you a confirmation that it works.
- If it works, It will then ask you to click “TURN ON”

Great Resource – “Gmail Security Best Of” -

<https://www.hongkiat.com/blog/gmail-security-tips/>

How To Implement Functional Backup / Restore Processes

Performing A Backup

To safeguard against the more common crypto viruses or just data accidental loss, it is essential to have a backup of all files and folders at a location inaccessible to the computer.

A portable hard drive or USB stick with enough capacity should be enough for most small businesses.

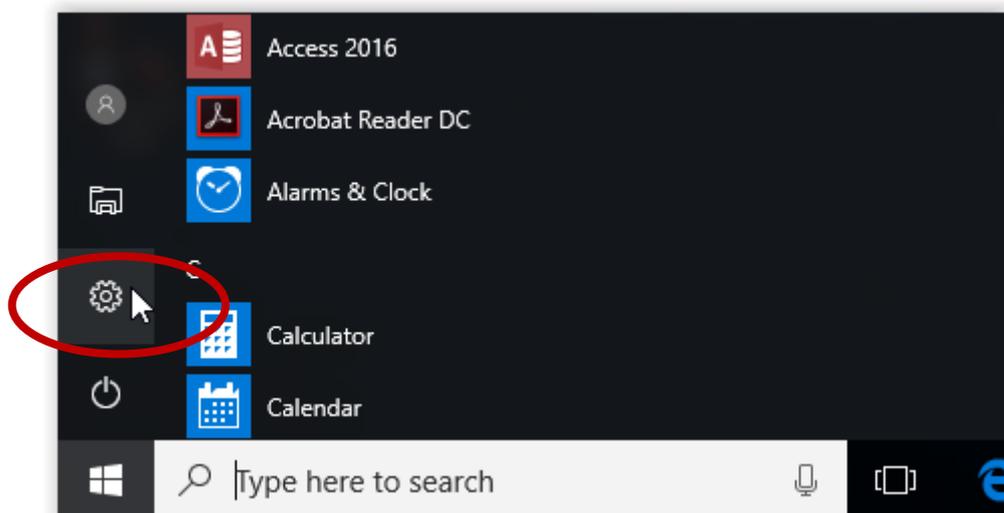
Question: Why do we want to separate the backup from the machine?

Answer: By having a physical separation, you minimise the ability for malware to target your backup.

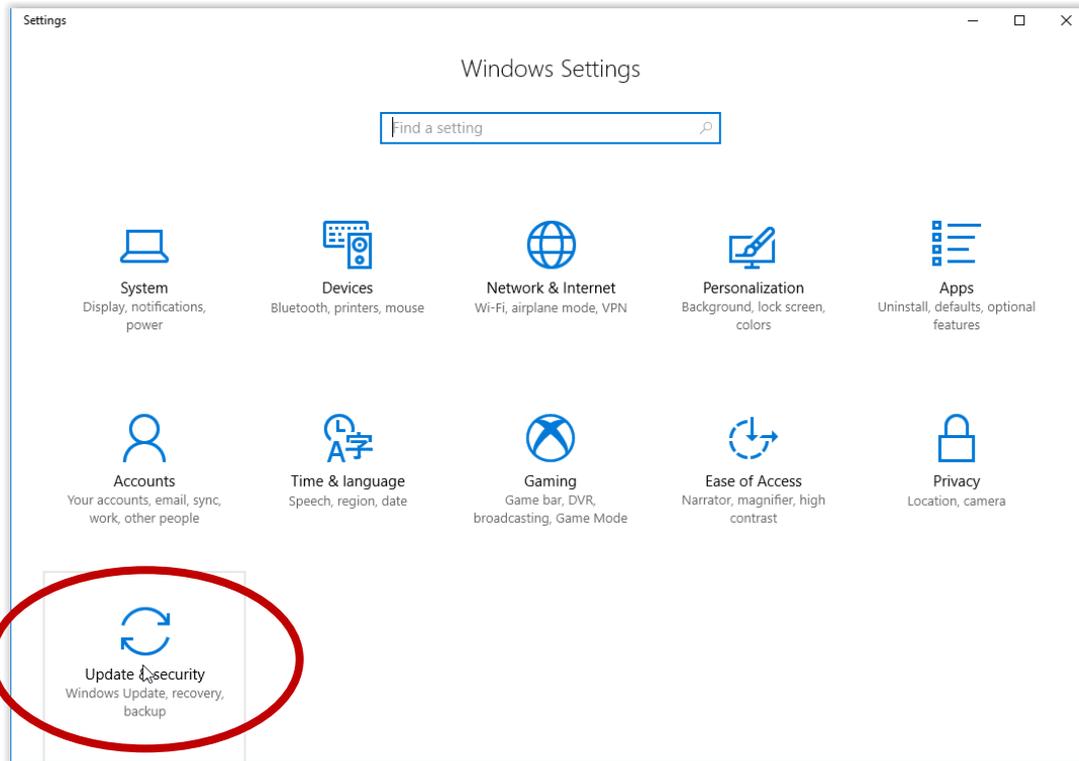
Windows 10 comes with built-in backup functionality that can make use of these portable media.

Insert a portable drive into the computer first.

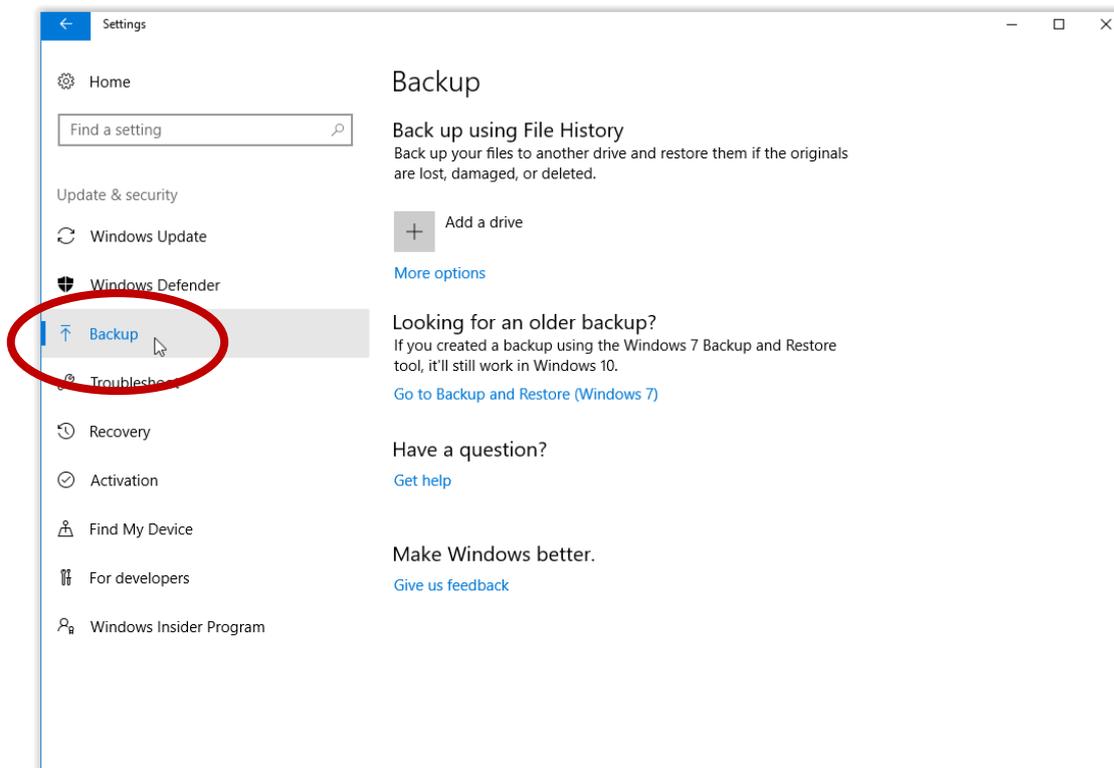
To use it, click the start button and choose “Settings.”



Click on “Update & security”:

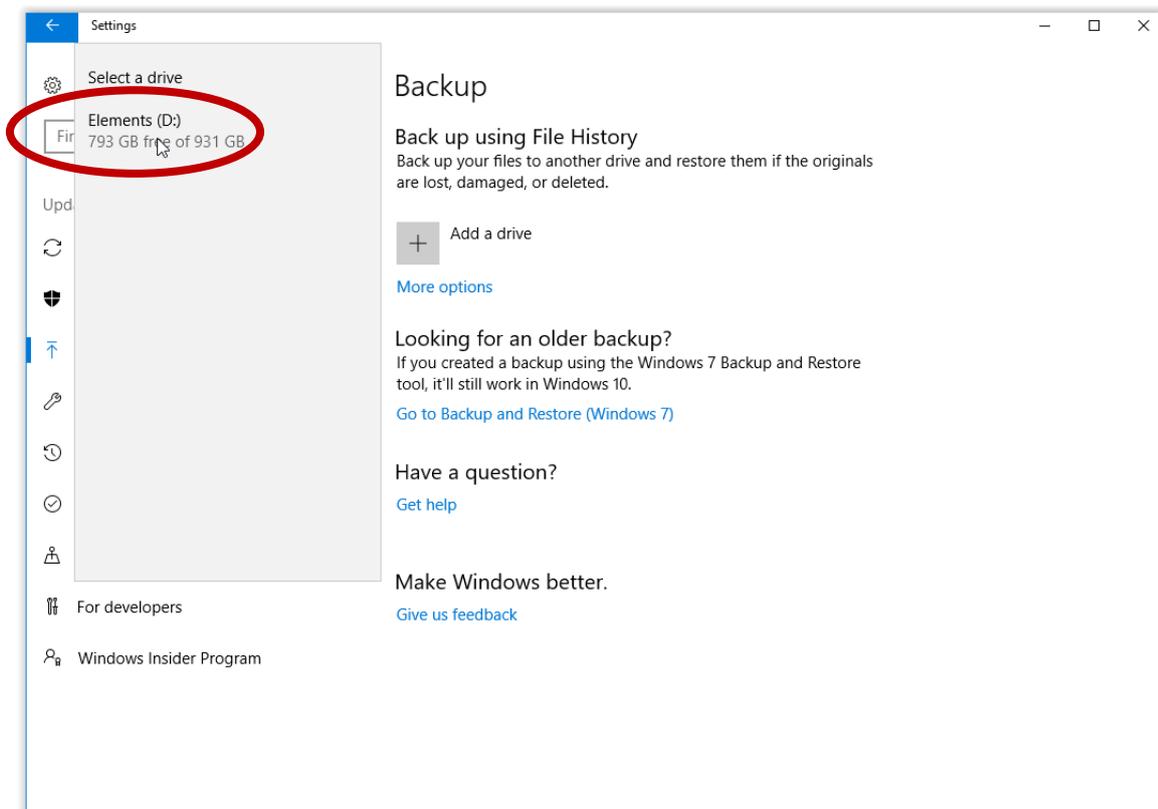


Choose “Backup”

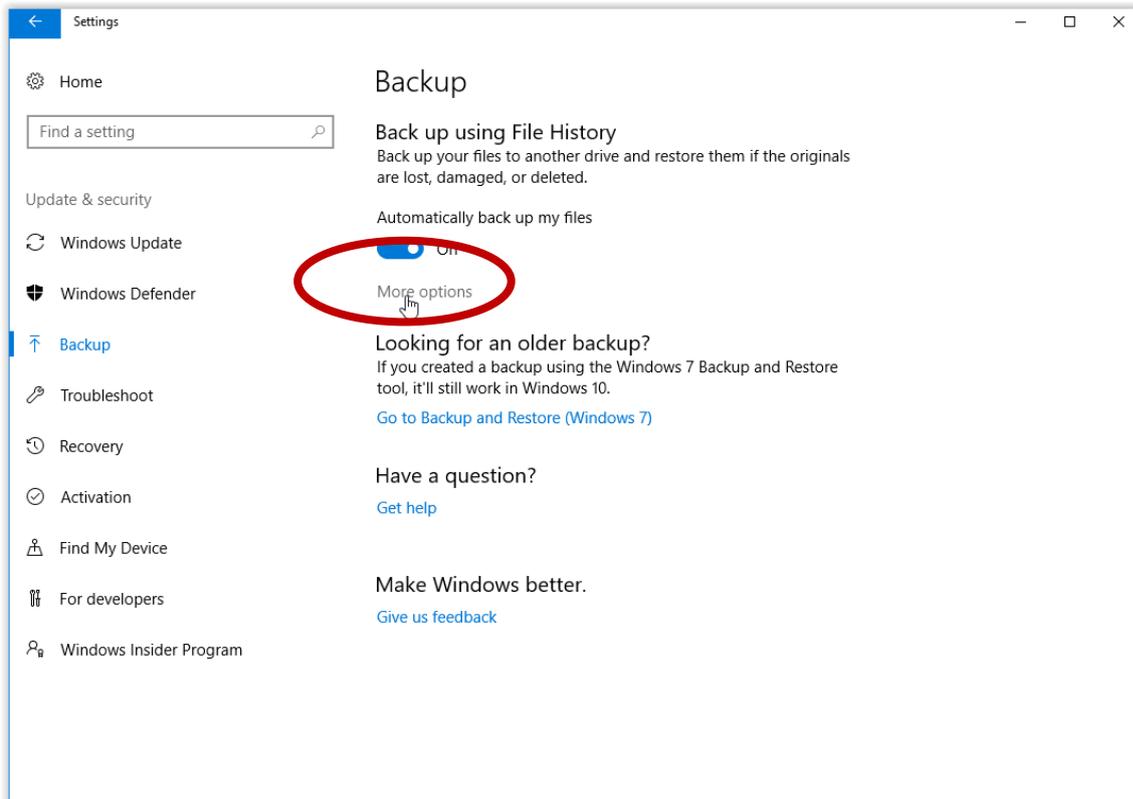


Choose: + Add a drive

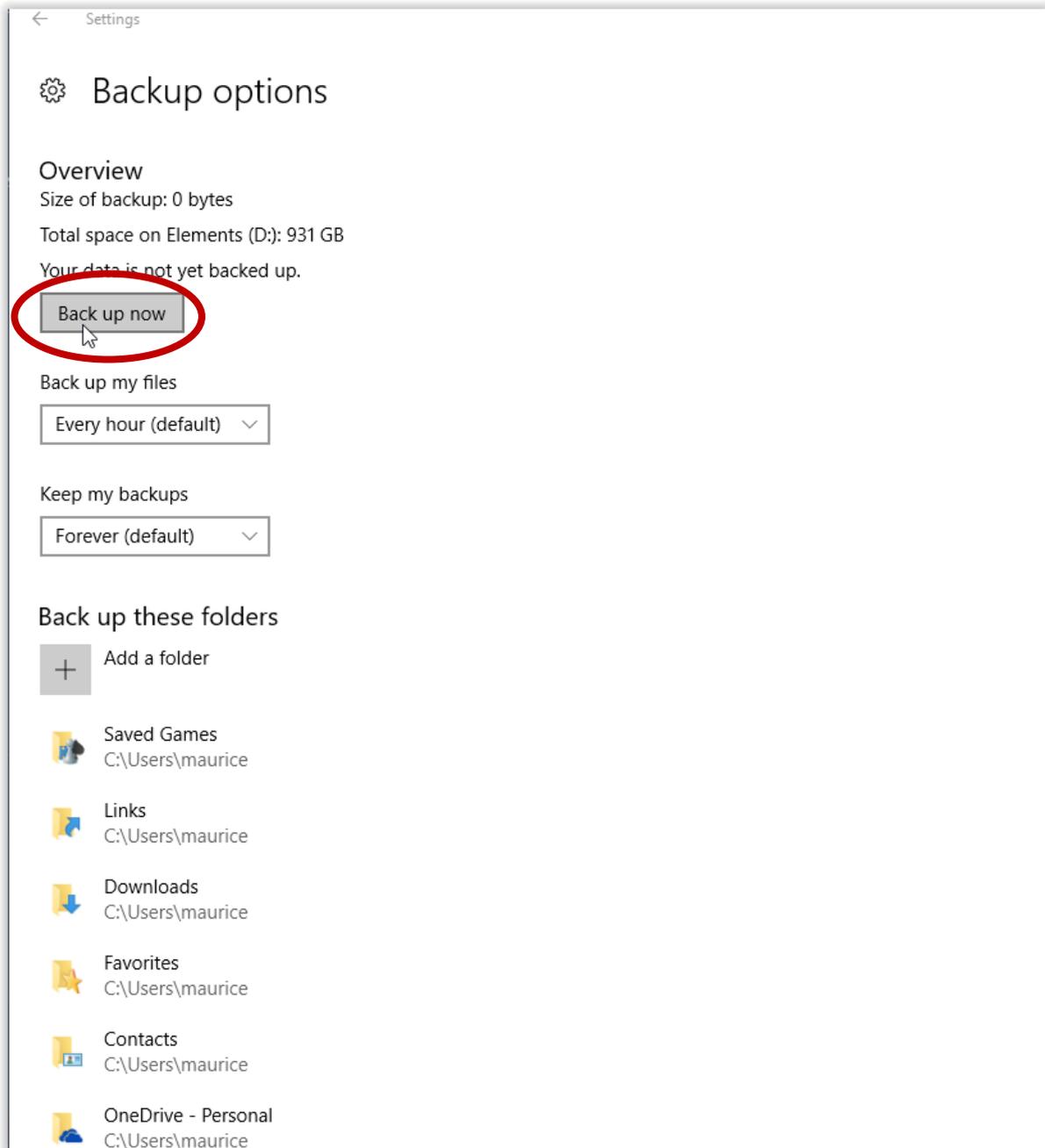
Select the drive that was inserted (It should show up in the list)



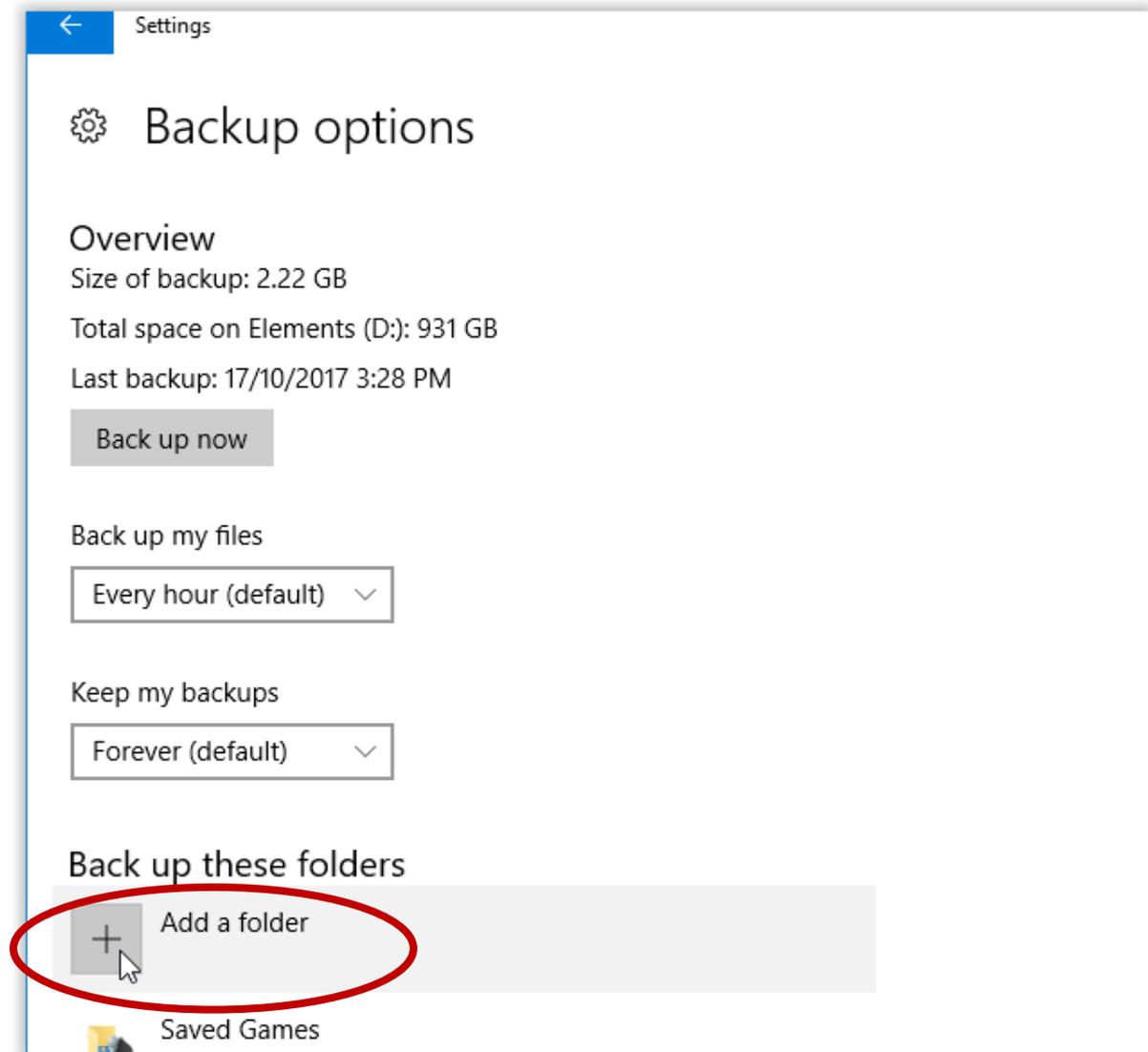
Click on “More options.”



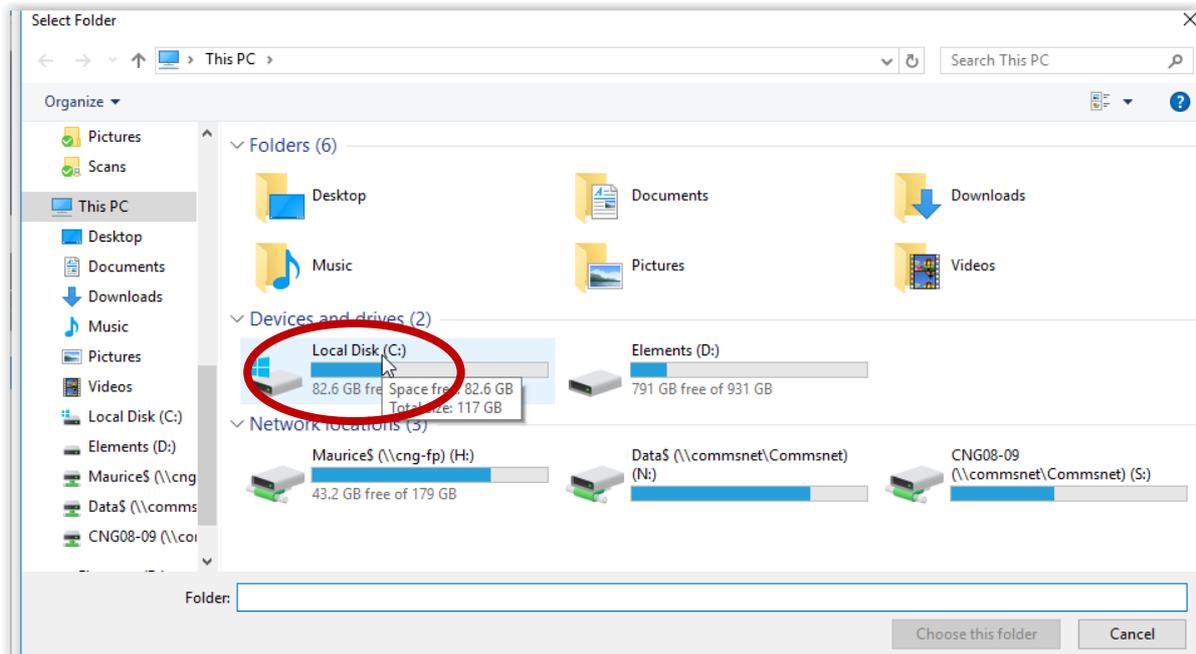
Click on: “Back up now” to create a backup of the selected folders:



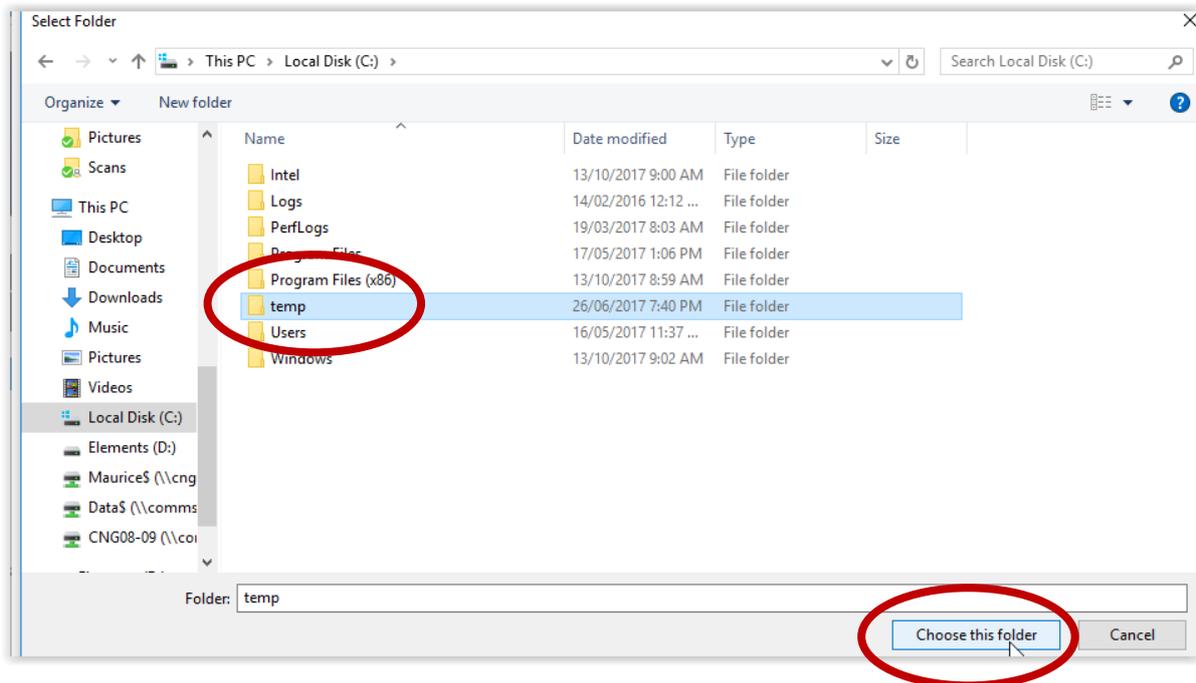
It might be necessary to add other locations used to store data other than Windows's default ones. This can be done by adding these folders to the backup procedure. To do this, click on: "Add a folder":



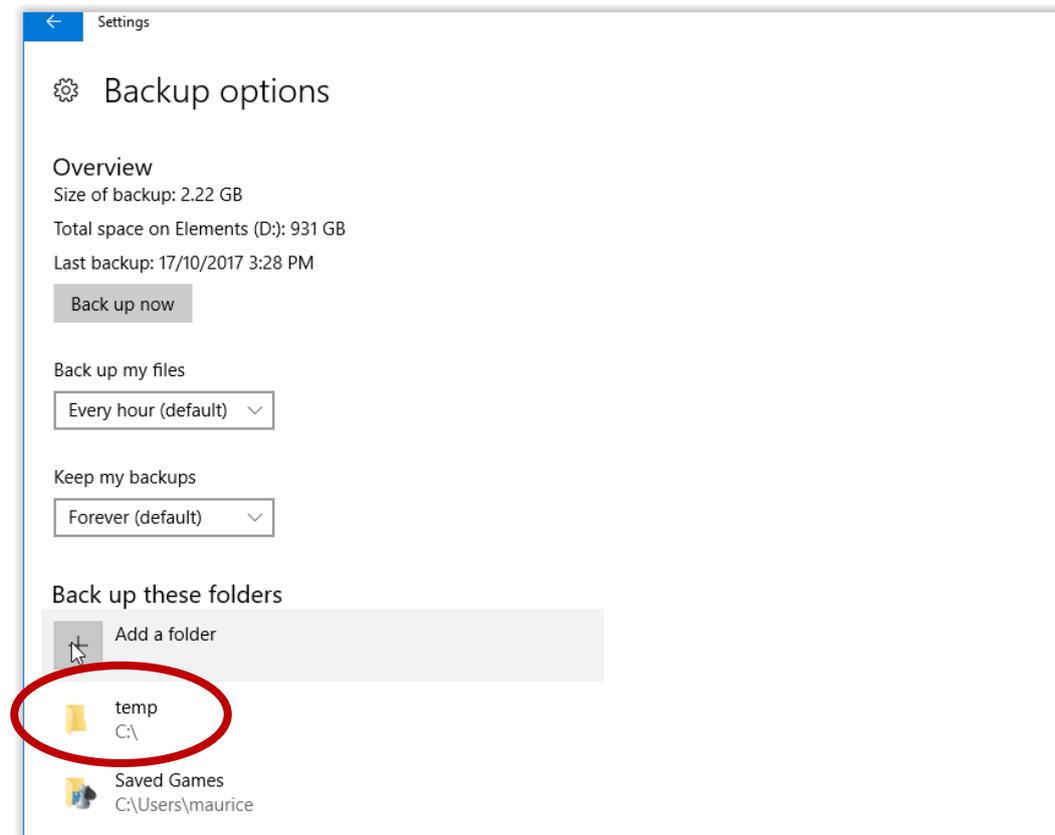
Go to the folder that needs backing up using the browser window:



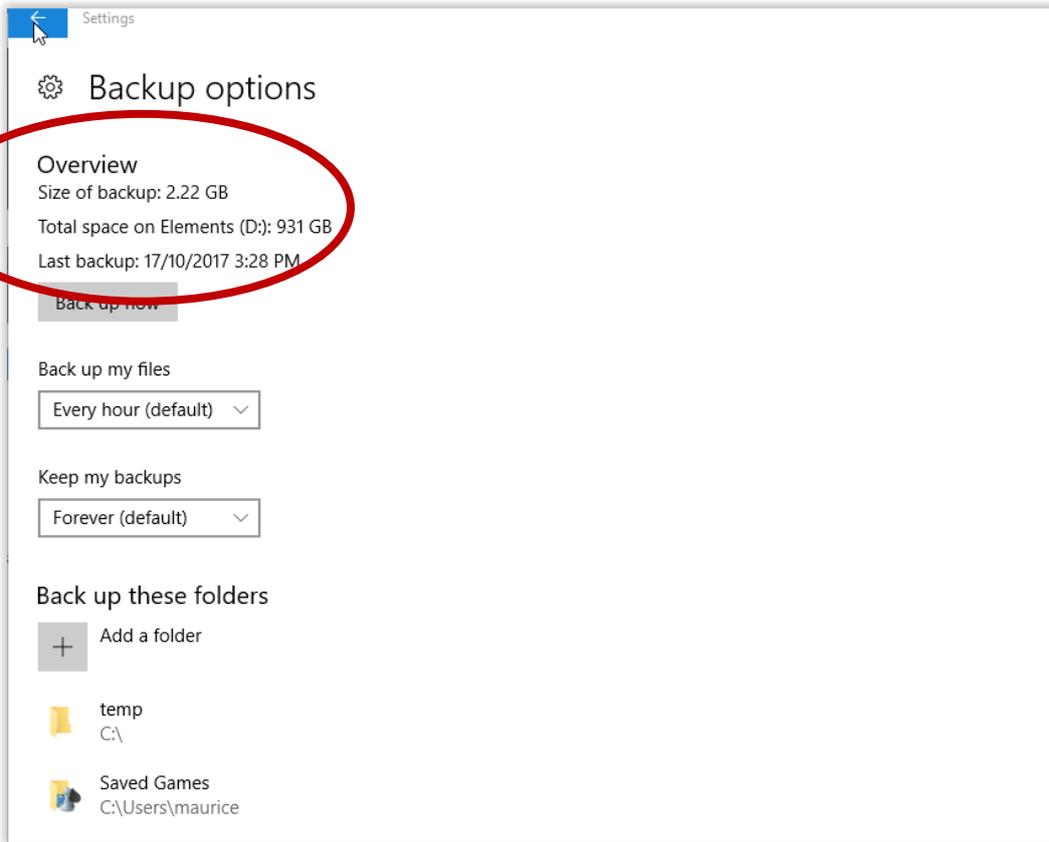
Select the folder required and click on: "Choose this folder."



The folders should now show up in the list of folders:

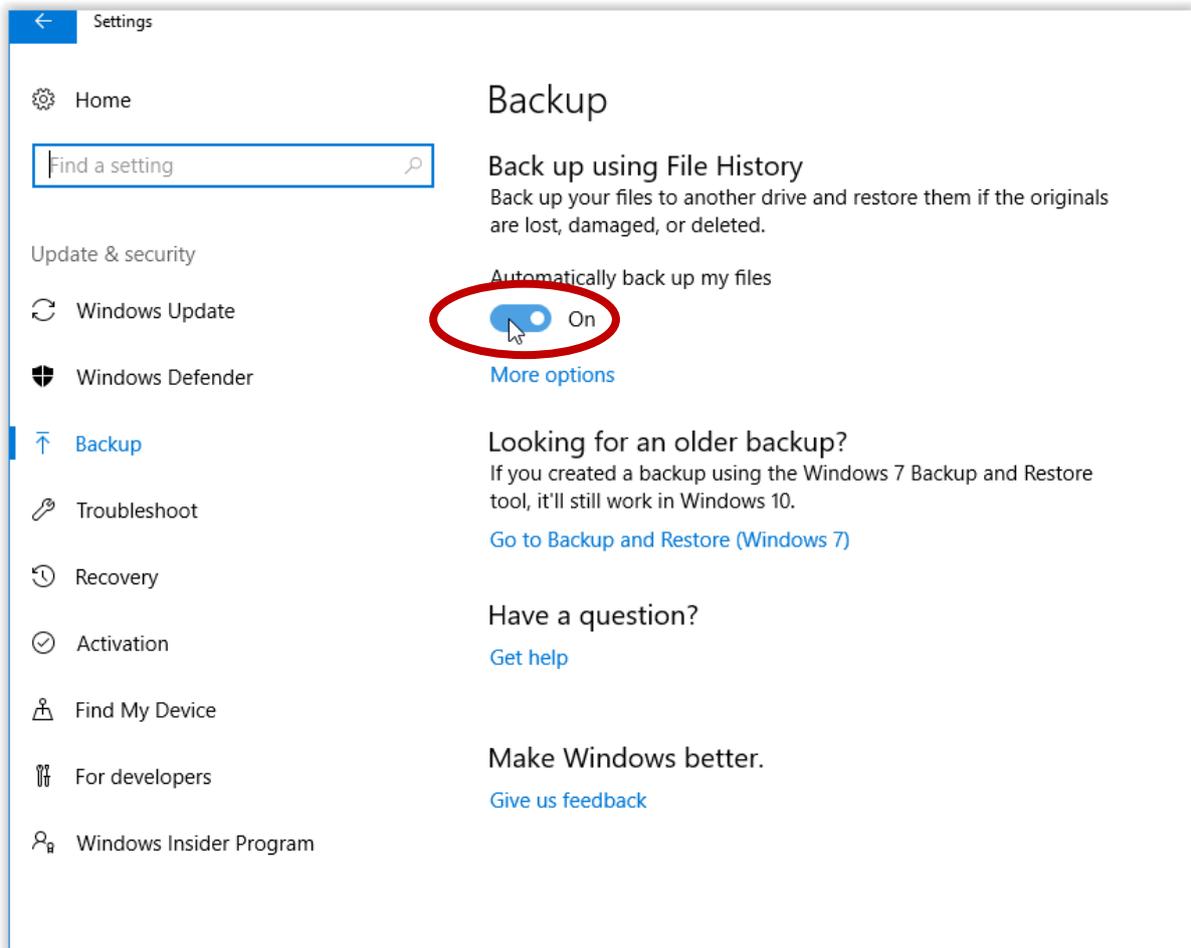


This window will now show the last created backup:



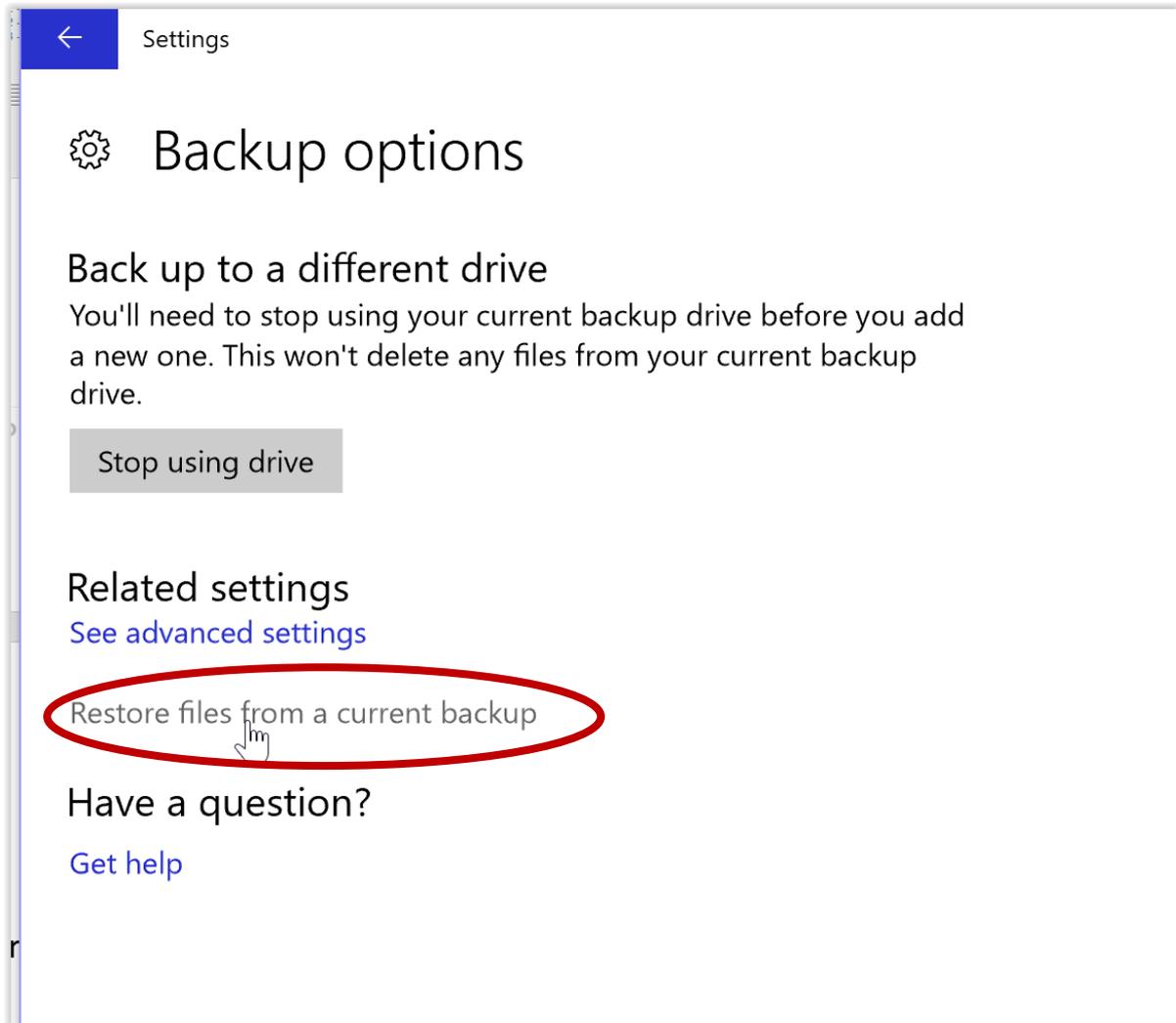
It might be a good idea to disable the automatic backup when the portable drive is removed from the system to secure it against crypto viruses and other malware.

This can be done by moving the “On” slider to the Off position, and this slider will need to be moved back to the “On” position again when creating a backup:

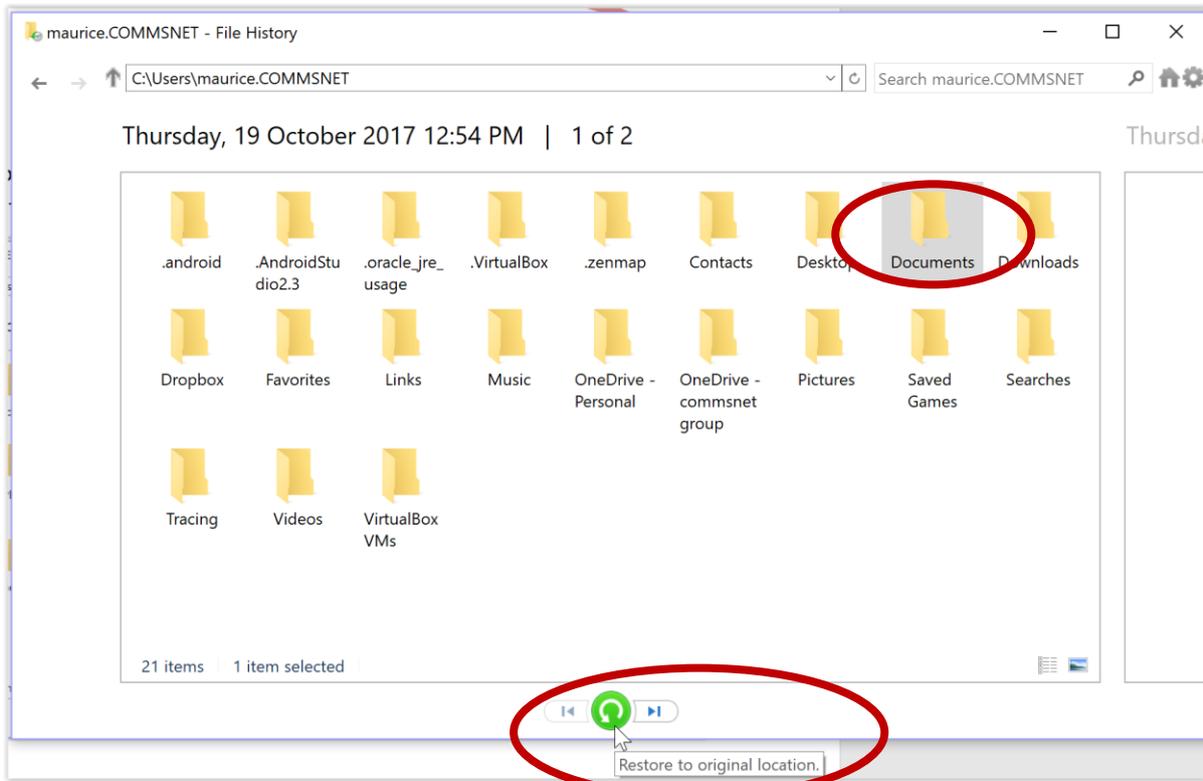


Performing A Restore

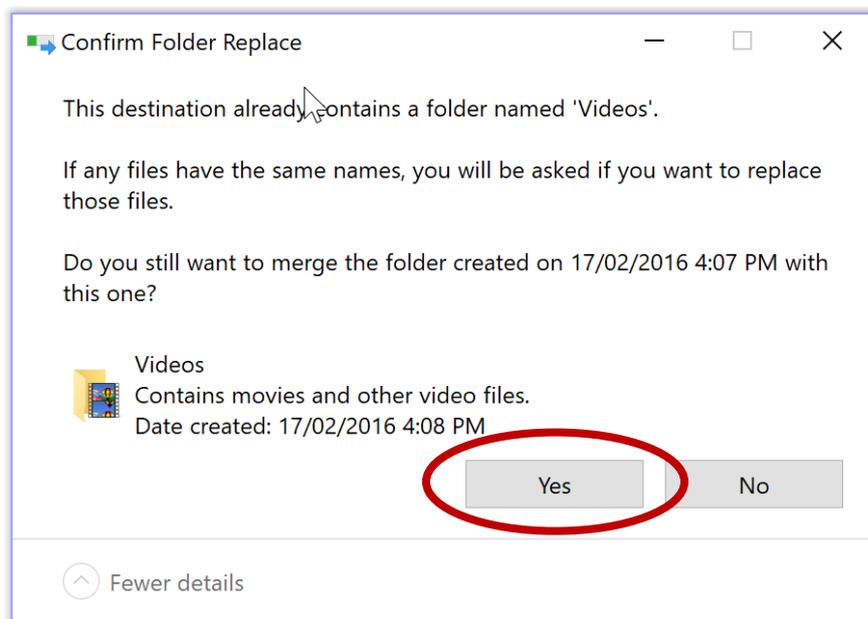
Scroll down in the backup options screen until you reach: “Restore files from a current backup” and click on it



Select the folder you want to restore, and if you want it to be restored to the original location, click on the green button in the bottom midsection



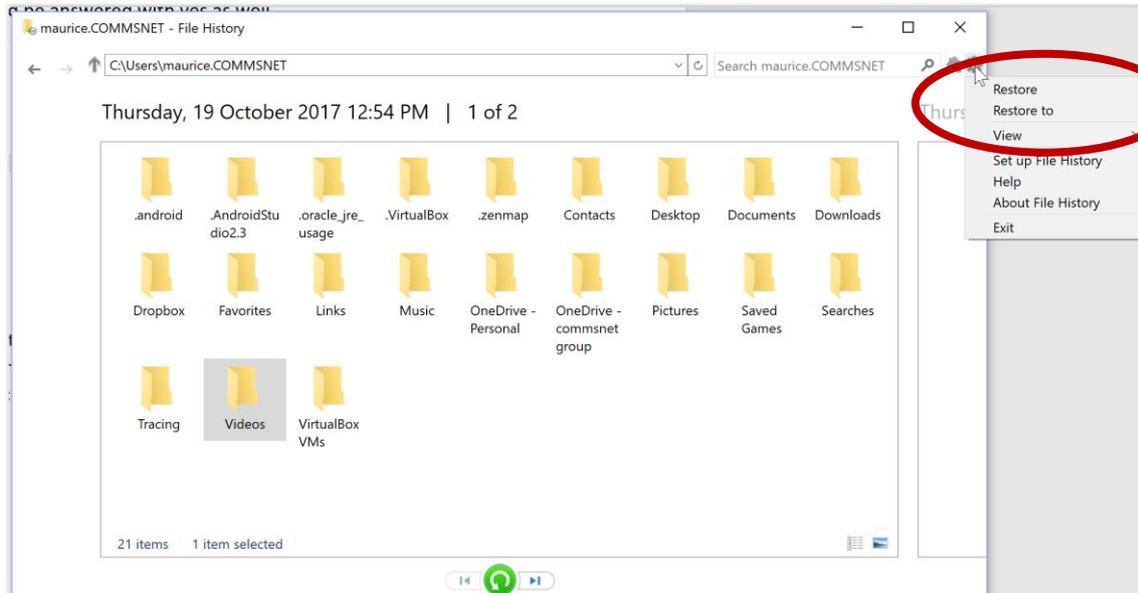
This will pop up a warning. If you want to overwrite, click "Yes":



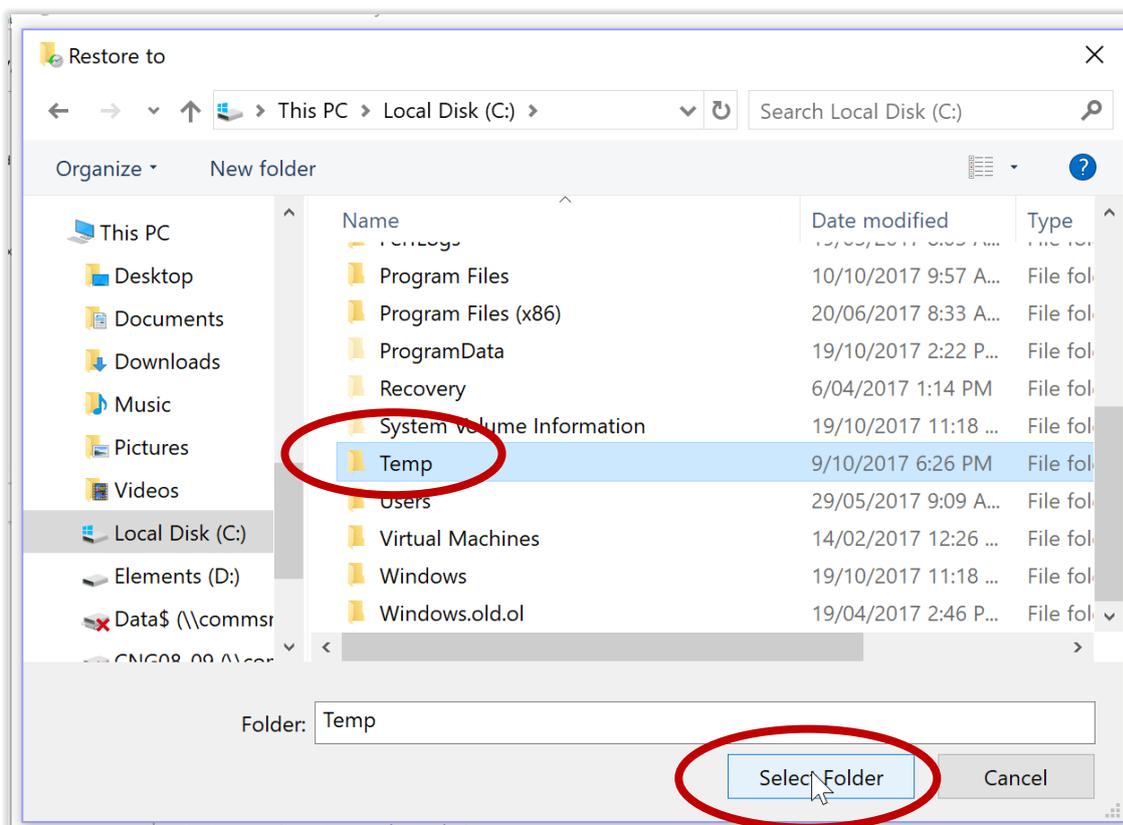
This will restore the files and might ask for confirmation during the process, which should be answered with yes as well.

If you do not want to overwrite the current location (e.g. you want to restore a previous version because you want to compare you can opt for a restore to a

different location, this is done by clicking on the option cogwheel and choosing “Restore to”:



Select the alternative location where you want to perform the restore and click: “Select Folder”:



This will restore the required folder to the selected location and will open it in Windows Explorer.

Close all remaining backup windows afterwards.

Miscellaneous - Windows Additional Security Configurations

Remove Admin Rights From Desktops

When users have local admin rights, they have the power to do almost anything they want to their workstations. They can download any application, use any program, and even ignore or undo anything IT administrators do to their devices. Many users, especially the power users, don't want to feel handcuffed or slighted because they don't have complete control, so organisation management lets users be the masters of their own devices.

So why restrict local administrator rights?

Local admin rights give the user too much power. Endpoints are where many of the greatest risks to organisation security lie, and giving users control over those endpoints only opens networks to more risk.

Malware is around every corner. Regular Web browsing and email phishing put Windows workstations at constant risk. If users have local admin rights, the risk is even greater because malware can veto IT security measures.

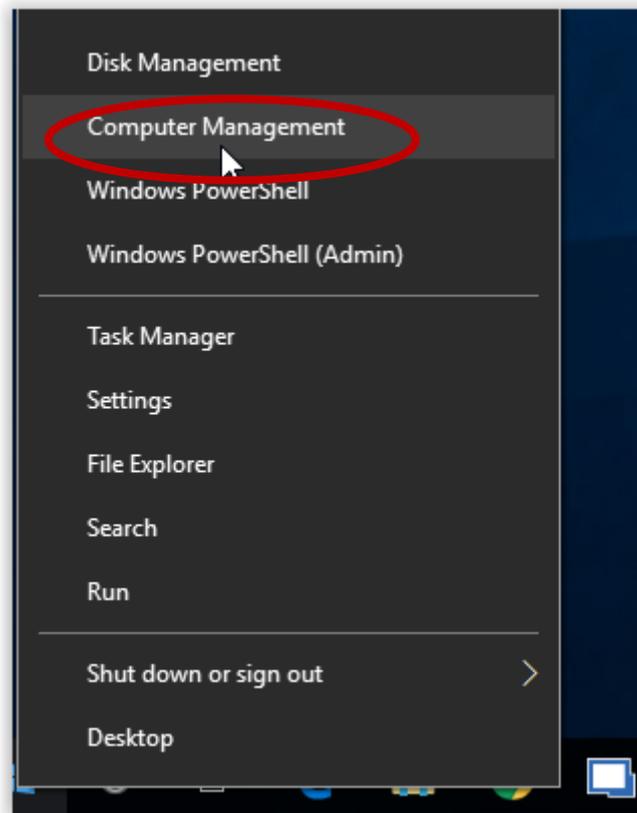
The solution is to make admin rights a software-based approach – not a user-based one. Adopting this approach ensures that if an attacker managed to gain access to a user's credentials through malware or otherwise, they would be limited in the damage they could cause. Once an admin account is breached, the attacker has the keys to the kingdom and can freely gain access to the core network, configurations, documents and data.

What Do You Need To Do?

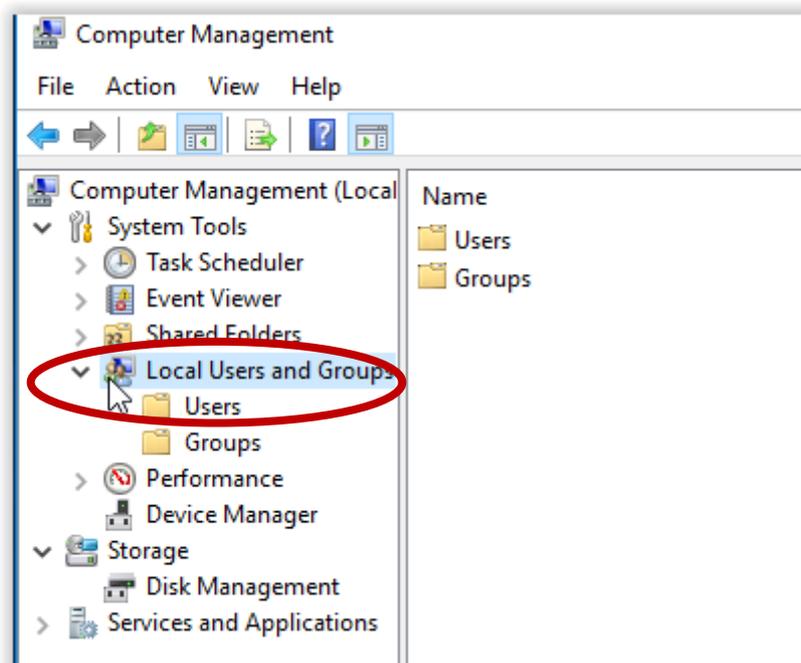
Instead of removing admin rights, the easiest and safest way is to create a new user. By default, these new users will not have any Admin rights. So, the next time you log onto your machine, just use this new user to access your device.

How Do You Create A New User?

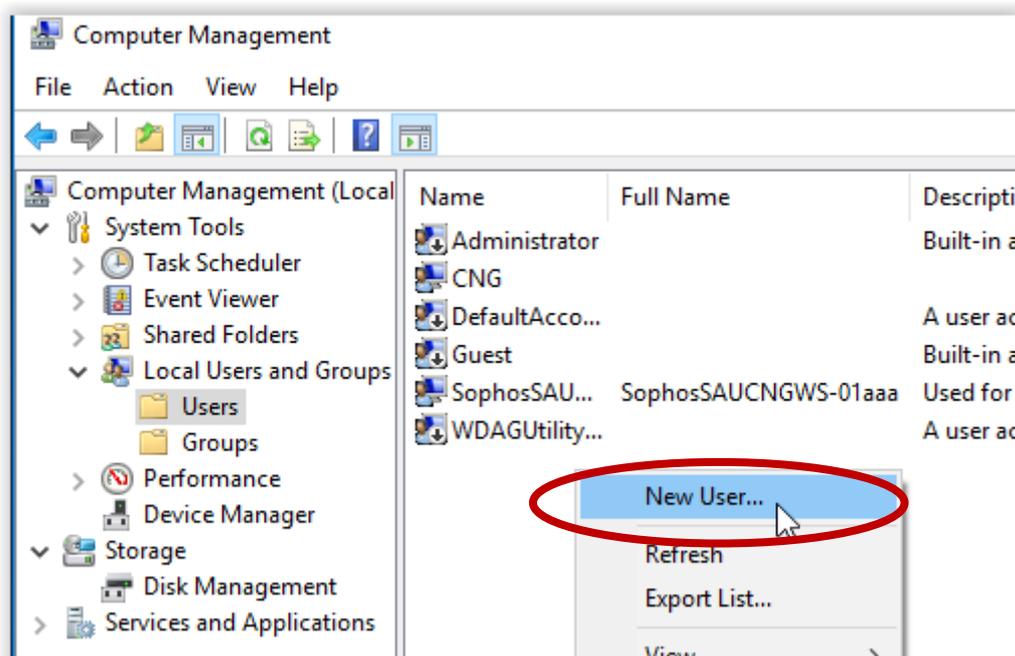
Right-click Start and choose “Computer Management”:



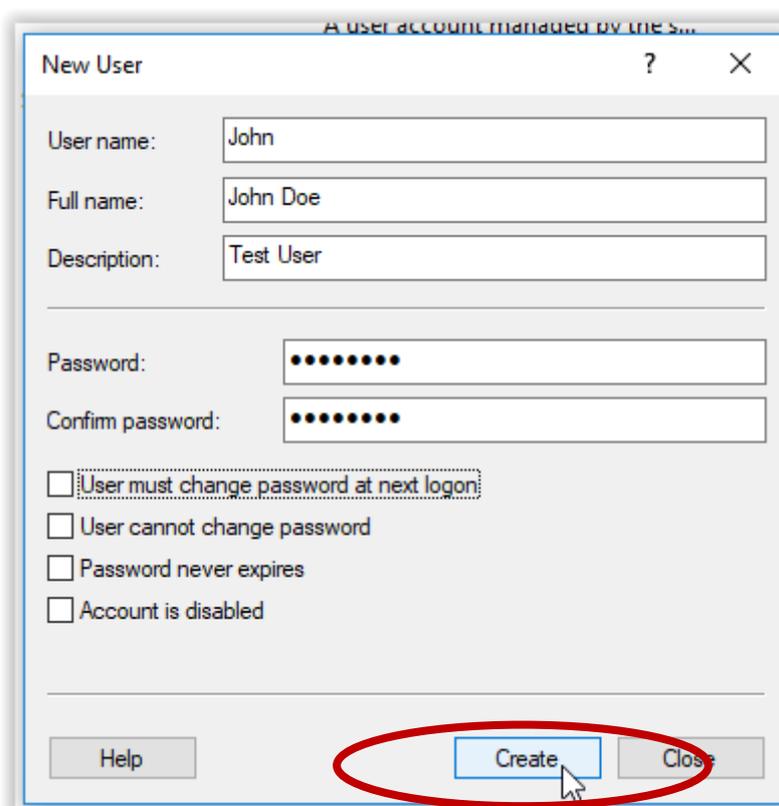
Open “Local Users and Groups”:



Choose “Users”, right-click in the spot without text and choose “New User...”:

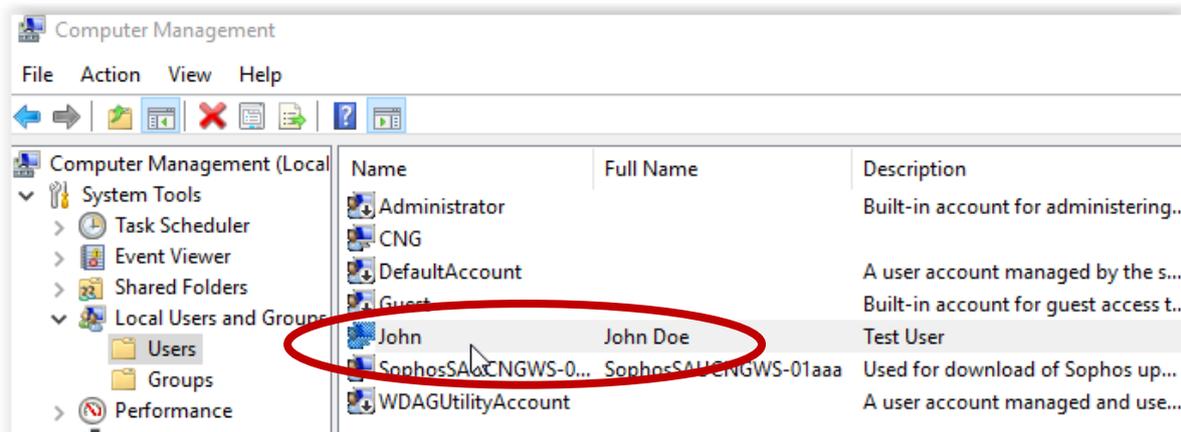


Type the name of the New User and all necessary details. Check next to “User must change password at next logon” and click “Create”:

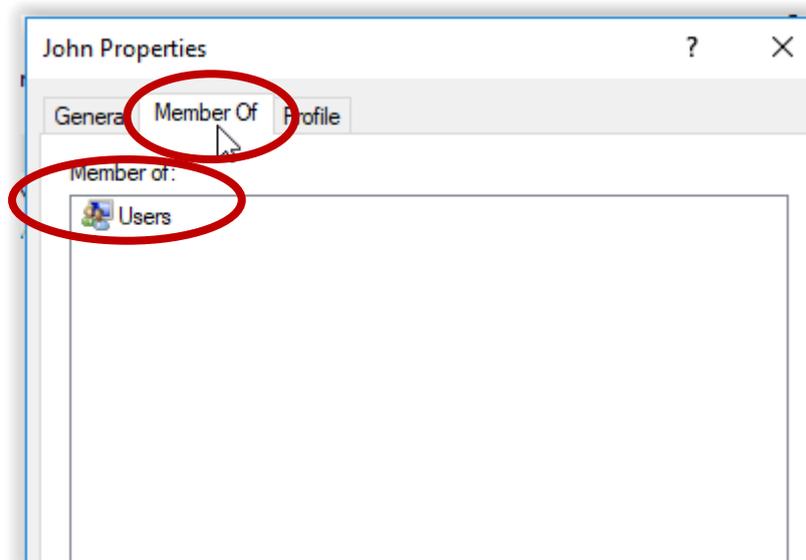


Click on “Close”

This will create a new user John Doe with login name: John



By default, John will have limited permissions on the computer hence minimizing the risk. This can be checked by double-clicking on John and choosing the “Member Of” tab:



As you can see in the screenshot above, John is only a member of the Users group and not the administrators.

Close Computer management again and log off. Use the newly created user for all daily tasks.

Apple macOS



“I want To Put A Ding In The Universe.”
- **Steve Jobs**

The mass appeal of Apple products is undeniable. Every product or software release is often anticipated and greeted with much fanfare. As its desirability gathers momentum, it has become a target like Microsoft for cybercriminals due to its large amassed user base.

While the number of Mac malware isn't as high as those for Windows, this doesn't mean that Mac malware should be taken lightly. Like its Windows counterparts, Mac malware can do severe damage to an infected system.

This Guideline, therefore, provides an overview of some of the recommended features in hardening your macOS. This Guideline can assist you in securing your Apple computer.

macOS system security is designed so that both software and hardware are secure across all core components of every Mac. This architecture is central to security in macOS and never gets in the way of device usability.

The default configuration of macOS remains quite impressive. Any hardening may impact performance and usability across the system. It's highly recommended to try these suggestions out gradually and see how they work for you.

The following four subsections are the fundamentals of hygiene practices that you need to employ within your business.

| Section | Page |
|---|------|
| 1. How To Patch and Update Your Mac Software and Apps | 53 |
| 2. How To Implement Endpoint Protection For Your Mac | 56 |
| 3. How To Employ Email Secure Best Practices For Your Mac | 58 |
| 4. How To Implement Effective Backup / Restore Processes | 61 |
| 5. Miscellaneous - macOS Additional Security Configurations | 71 |

How To Patch and Update Your Mac Software and Apps

Apple macOS includes an automatic software update tool to patch the majority of Apple applications. Software updates often contain important security updates, which should be applied to your machine. The tool automatically checks what updates are available and, with major upgrades, can download patches rather than full installations to minimise the amount downloaded.

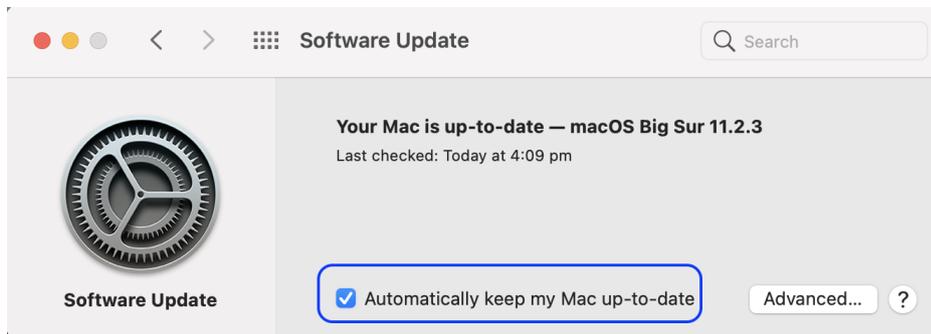
It is best to configure software update to automatically check for updates. The process to check this is correctly configured is as follows:

1. To open Software Update preferences, choose Apple menu  > System

Preferences, then click Software Update.



Tip: You can also choose Apple menu  > About This Mac, then click Software Update.



2. Make sure you check “automatically keep my mac up-to-date.”

3. Options

- Update Now - If your system is not up to date, you will see the “Update Now” button. Click this button to install all the available software and updates



- More Info... - Click “More info” to view information about available updates. Select an update to see information about it. To install updates, select the tick boxes of the updates you want and click Install Now.
- Advanced... - Click “Advanced” to see additional options for installing system software and updates automatically.
- Click “?” to get an understanding of the options and descriptions you have in this window box.

4. Advanced Preferences

1. Make sure all of the following items are checked. This will ensure that all updates are automatically updated.



Updating Third Party Applications Originated From Apple App Store

1. Open the App Store. 
2. In the sidebar, click "Updates".
3. Click "Update next" to an app to update only that app, or click "Update All".

Updating Third Party Applications Not From The App Store

If you have installed a third-party application, then you will have to check for new updates manually.

Most applications work in the same process.

Example 1: VLC media player application

1. Click on the "VLC media player" on the menu bar
2. Click on "Check for Updates..."

Example 2: Slack

1. Click on the "Slack" on the menu bar

2. Click on “Check for Updates...”

Example 3: Google Chrome

1. Click on the “Chrome” on the menu bar
2. Click “About Google Chrome”, and this will take you directly to their Settings page.

How To Implement Endpoint Protection For Your Mac

With the continual burst of new malware, a lot of attention has been brought to potential malicious applications targetting the Mac platform. No longer can Apple users sit idle thinking that it is impervious to such threats. This is just wishful jolly thoughts.

Unfortunately, Apple does not come with its anti-malware software. It relies on a third party.

There are two streams of anti-malware that you can pursue.

1. Free versions
2. Paid versions

What is the difference between the two? Overall, both free and paid antivirus software offer the same general protection against malware infections. The differences are mostly in additional features and how effective the cleanup process is after infection.

Still unsure? Consider your typical computer use. If you take part in more risky behaviour, then you may want to opt for paid antivirus software. If you're very careful about what sites you visit and easily recognise dangerous phishing emails, free antivirus software is good enough.

You should pay for antivirus if...

- You frequent unknown websites
- You download free software off the Internet
- You play online games
- You have your children using your computer
- You are worried about your computer being compromised
- You have sensitive data on your computer

However, if you do not participate in any of those activities, the odds are very good that the free version of antivirus will protect you from threats.

Most well-known brands will have a free and paid version.

Recommendations

- Invest in well-known vendors that provide specialized endpoint protection solutions.
- Ensure that the software has the latest security updates.
- Weekly scan your computer.

- If your computer is clean and free of malware, never assume that you are safe. Be vigilant!

How To Employ Email Secure Best Practices For Your Mac

Your typical email account contains a wealth of information that can be invaluable to all kinds of organisations and individuals – everyone from hackers who might be after your financial information to corporations who are sucking up data in the hopes of targeting potential customers with more relevant online adverts.

Ensuring your private emails remain private is crucial when you're transmitting confidential documents or other sensitive information. However, even if you're just chatting with friends, then chances are you're still not too keen on the thought of other people listening in to these conversations!

Whether you are using Apple's Mail program, Microsoft Outlook, or another third-party program, the approach of ensuring that you practice with security in mind is the same.

To help keep your email account secure, it's essential that you keep the following best practices in mind.

- **Create a strong password for your email account.** You should also make a point of changing your password often and look into any additional security measures your email provider can offer. For example, some email providers can send a text message to your phone if they detect any out-of-character activity, such as someone logging into your account from an unfamiliar geographical location.
- **Check whether you should be scanning email attachments manually.** Email attachments are a huge potential source of viruses and malware. Although many email providers automatically scan attachments for you, if you're unsure whether this applies to your particular account, then don't take the risk. Check your account's 'Settings' or your email provider's documentation to see whether they check email attachments automatically or whether you should be scanning these attachments yourself. And remember that even if your email provider scans all attachments for you, there's no guarantee that it'll catch 100% of dangerous email attachments, so you should never open or download anything that strikes you as unusual or outright suspicious.
- **Establish clear rules about email usage.** Setup an Email Acceptable Use Policy (AUP) that applies to all staff (including temporary staff), visitors, and contractors. This policy should be considered part of the conditions of using your organisation systems.
- **Close and forward accounts for ex-employees.** Closing an account ensures that when employees leave your organisation, they no longer have access to your business operations through their account. Forwarding ensures the business they were handling becomes the responsibility of a current employee capable of completing or delegating the continued communication.
- **Watch out for "phishing" emails.**
 - Don't open attachments. Be wary of any attachment; and
 - Don't click on links. Be wary of any links.
 - Do not respond to requests, as this would suggest that you are a real person behind the email.
- **Do not "unsubscribe" from a spam message.** This tells the hacker that you are a real contact and would also lead to receiving more spam. And some of them may even lead you to a malicious site.
- **Do not send sensitive personal information via email** unless you use specialized tools that can encrypt your message.

- **Whenever you need to email a group of people, use Bcc rather than Cc.** Then, even if this email falls into the hands of potential spammers or hackers, at least they won't immediately have access to the contact details of everyone on that list.
- **Never access your email using public Wi-Fi.** Public Wi-Fi is never secure, and there are many ways hackers can steal all the information that passes through such a network.
- **Don't share passwords either with your colleagues or friends.** You wouldn't share your toothbrush with some else, don't share your password.
- **Be sure to log out when you have finished work.**

Remember

“Do NOT Respond To Any Emails If You Didn't Ask For It In The First Place!”

How To Implement Functional Backup / Restore Process

To safeguard against the more common crypto malware or just accidental data loss, it is essential to have a backup of all files and folders at a location inaccessible to the computer. The best backup is one that you have backups in multiple locations.

You have two options in backing up your valuable information.

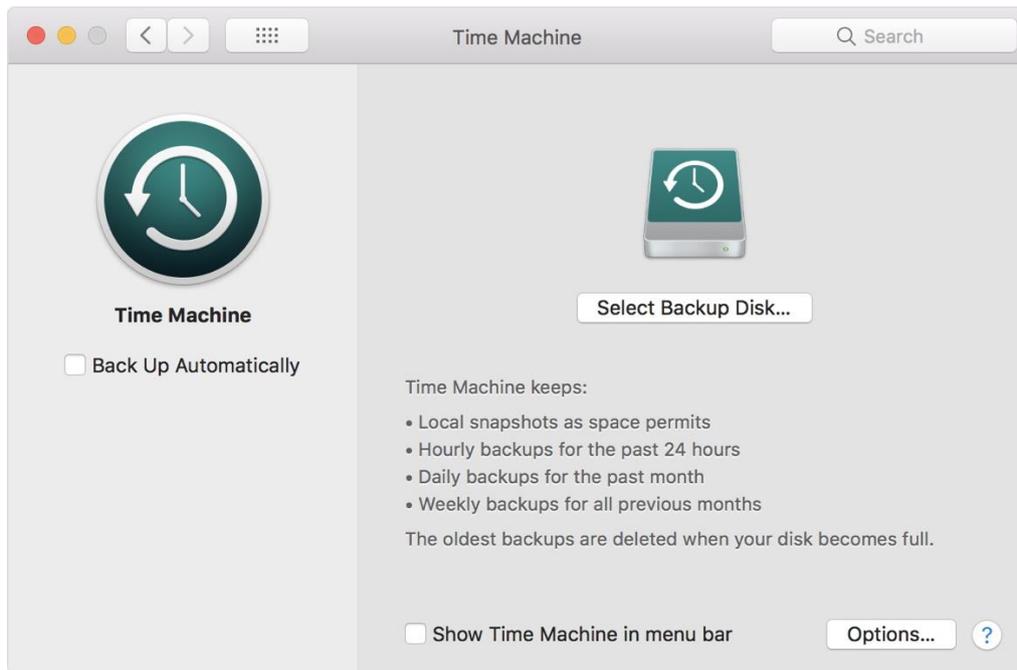
1. Back up with Time Machine
2. Store files in the iCloud

Backup Your Mac with Time Machine

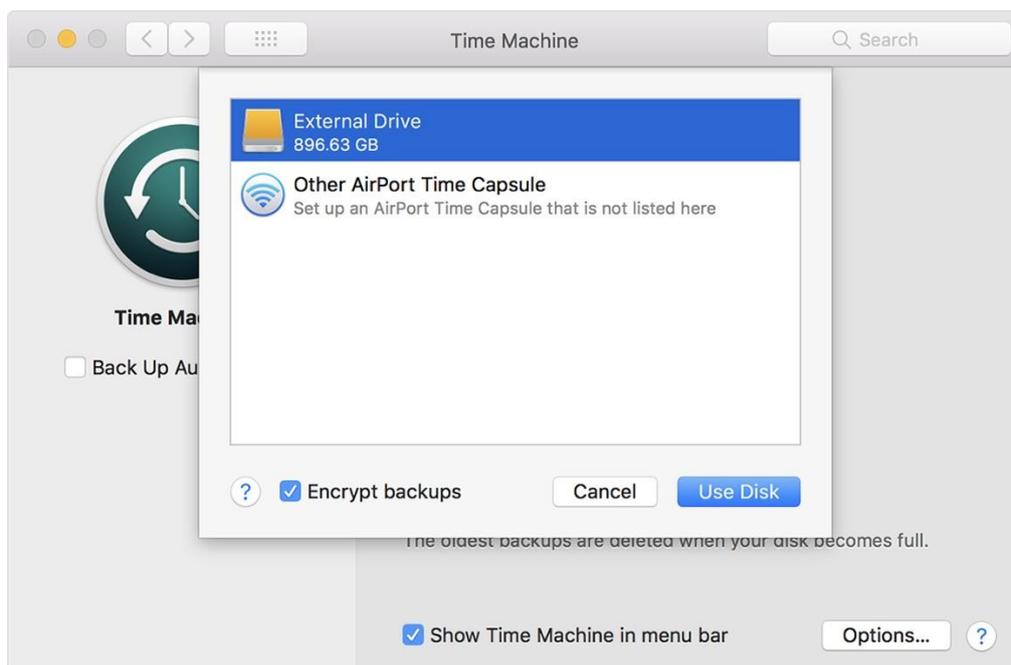
You can use Time Machine, the built-in backup feature of your Mac, to automatically back up all of your files, including apps, music, photos, email, documents, and system files. When you have a backup, you can restore files from your backup if the original files are ever deleted from your Mac, or the hard disk (or SSD) in your Mac is erased or replaced.

Creating a Time Machine Backup

- Connect an external storage device
- Select your storage device - When you connect an external drive directly to your Mac, you might be asked if you want to use the drive to back up with Time Machine. Select Encrypt Backup Disk (recommended), then click Use as Backup Disk. If Time Machine doesn't ask you to use your drive follow the following steps
 1. Open Time Machine preferences from the Time Machine  menu in the menu bar. Or choose Apple menu  > System Preferences, then click Time Machine
 2. Click Select Backup Disk (or Select Disk, or Add or Remove Backup Disk):



3. Select your external drive from the list of available disks. Then select “Encrypt backups” (recommended) and click “Use Disk.”



Automatic Backups

After selecting a backup disk, Time Machine immediately begins making periodic backups - **Automatically** and without further action by you.

If you are unsure, go back to the Time Machine and make sure that the “Back Up Automatically” is selected.

The first backup may take a long time, depending on how many files you have, but you can continue using your Mac while a backup is underway. Time Machine backs up only the files that changed since the previous backup so that future backups will be faster.

- To start a backup manually, choose Back Up Now from the Time Machine  menu in the menu bar. Use the same menu to check the status of a backup or skip a backup in progress.

Backup Your Mac with iCloud Drive

With iCloud Drive, you can safely store all kinds of documents in iCloud and access them from all your computers and iOS devices.

If you like, you can have all the files on your desktop and documents folders stored automatically in iCloud Drive. That way, you can save files right where you usually keep them, and they become available on all your computers and iOS and iPadOS devices.

Setting Up iCloud

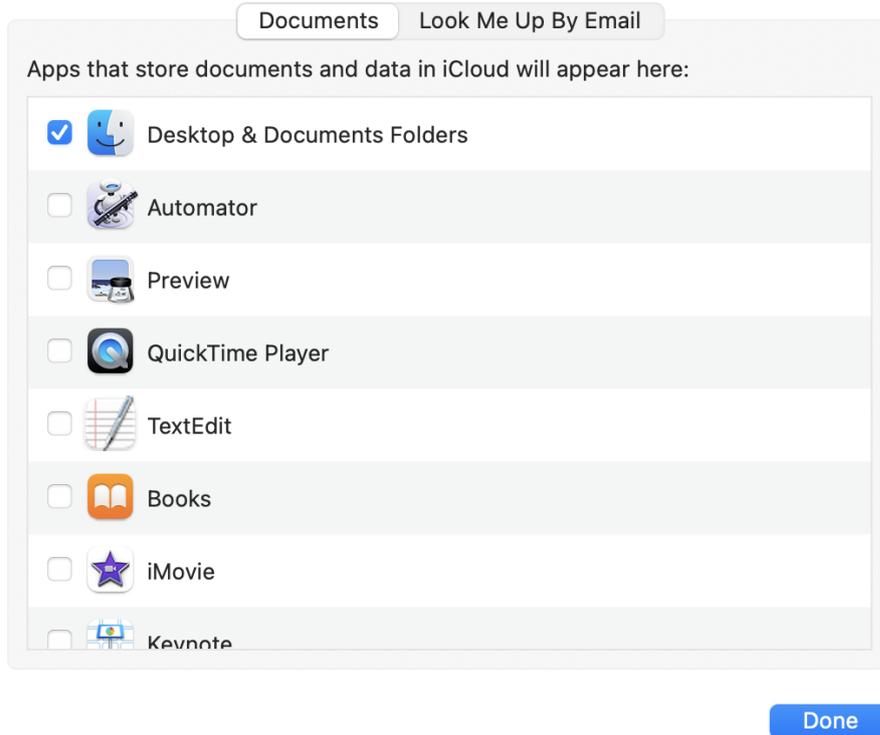
- Go to Apple menu  > System Preferences, then click Apple ID.
- Sign in with your Apple ID.
- Select iCloud Drive

The first time you select the iCloud Drive feature on any of your devices, you’re asked to upgrade. When you upgrade, your documents and data currently stored in iCloud are moved to iCloud Drive. If you’re not asked to upgrade, your account is already upgraded.

Important: After upgrading to iCloud Drive, your documents stored in iCloud Drive is only available on your computers and iOS devices that meet minimum system requirements and have iCloud Drive turned on. Your documents in iCloud Drive are also available on iCloud.com.

Storing Your Desktop And Documents Folders In iCloud Drive

- On your Mac, choose Apple menu  > System Preferences, click Apple ID, select iCloud in the sidebar, then click “Options” next to iCloud Drive
- Select Desktop & Documents Folders
- Click “Done”



Restoring Your Mac From A Backup

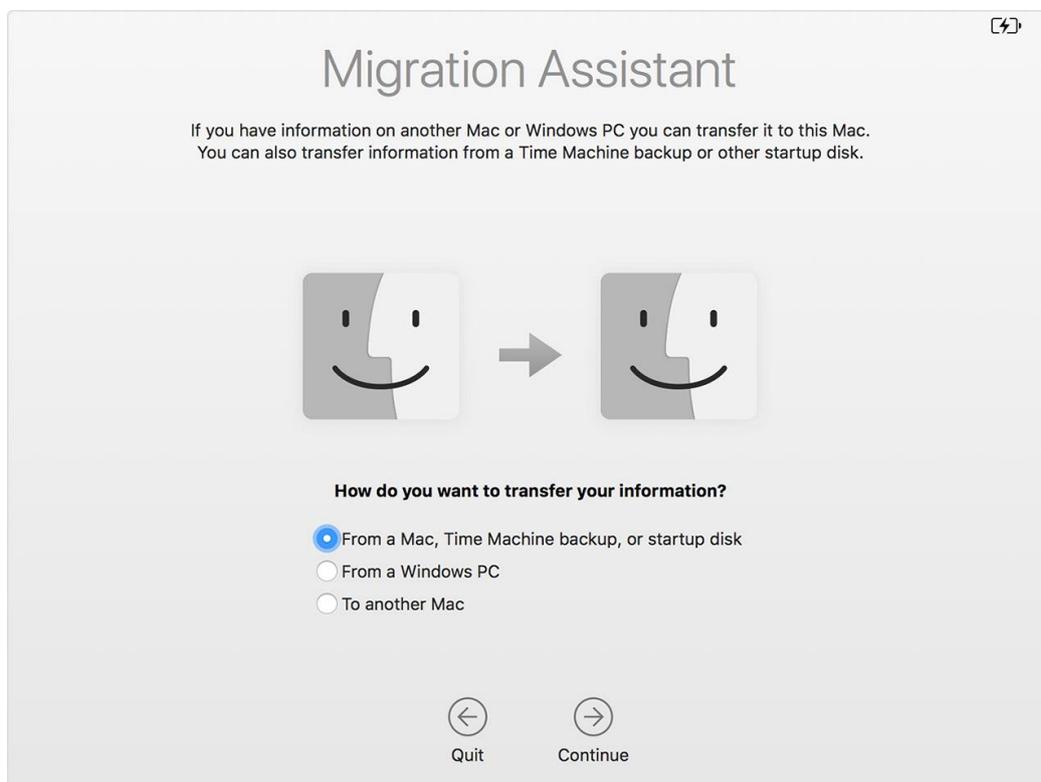
Restoring From A Time Machine Backup

If you used Time Machine to create a backup of your Mac, you can restore your files from that backup.

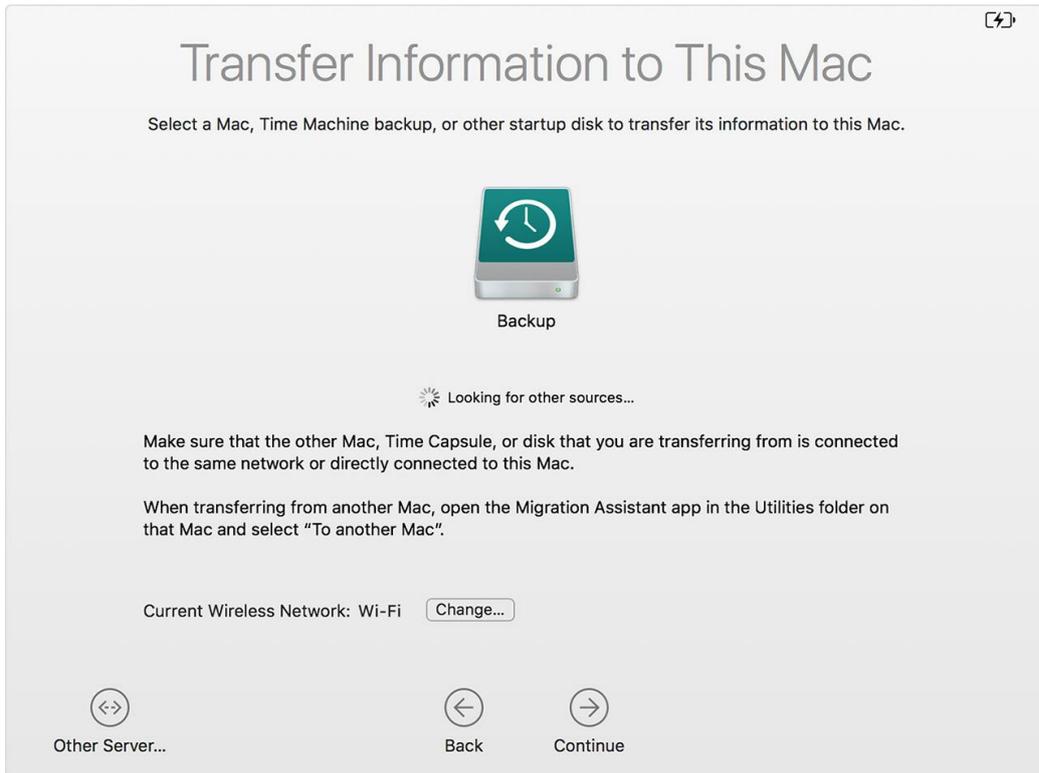
Restore All Files

1. Make sure that your Time Machine disk is connected and turned on, then turn on your Mac.

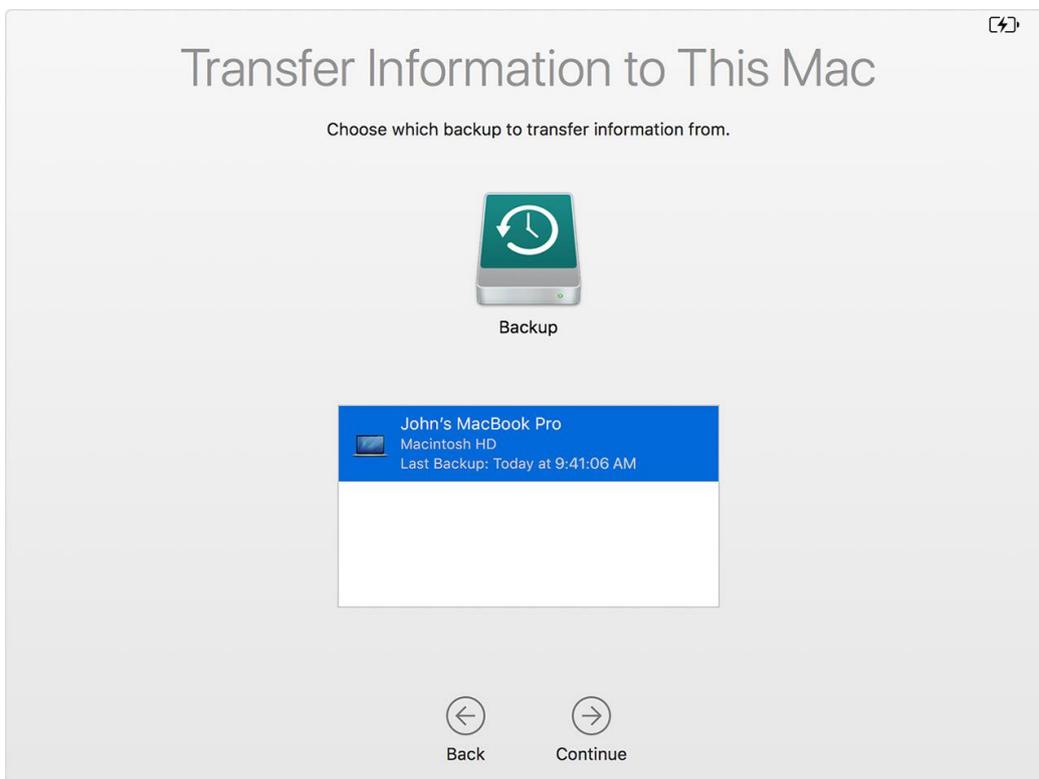
- If your Mac starts up to a setup assistant that asks for details like your country, keyboard, and network, continue to step 2.
 - If your Mac starts up to the Finder, open Migration Assistant, which is in the Utilities folder of your Applications folder. Click Continue in the first Migration Assistant window, then continue to step 2.
 - If your Mac doesn't start up all the way, or you also want to restore the macOS you were using when you created the backup, follow the steps to restore both macOS and your files.
2. When you're asked how you want to transfer your information, select the option to transfer from a Mac, Time Machine backup, or startup disk. Then click "Continue".



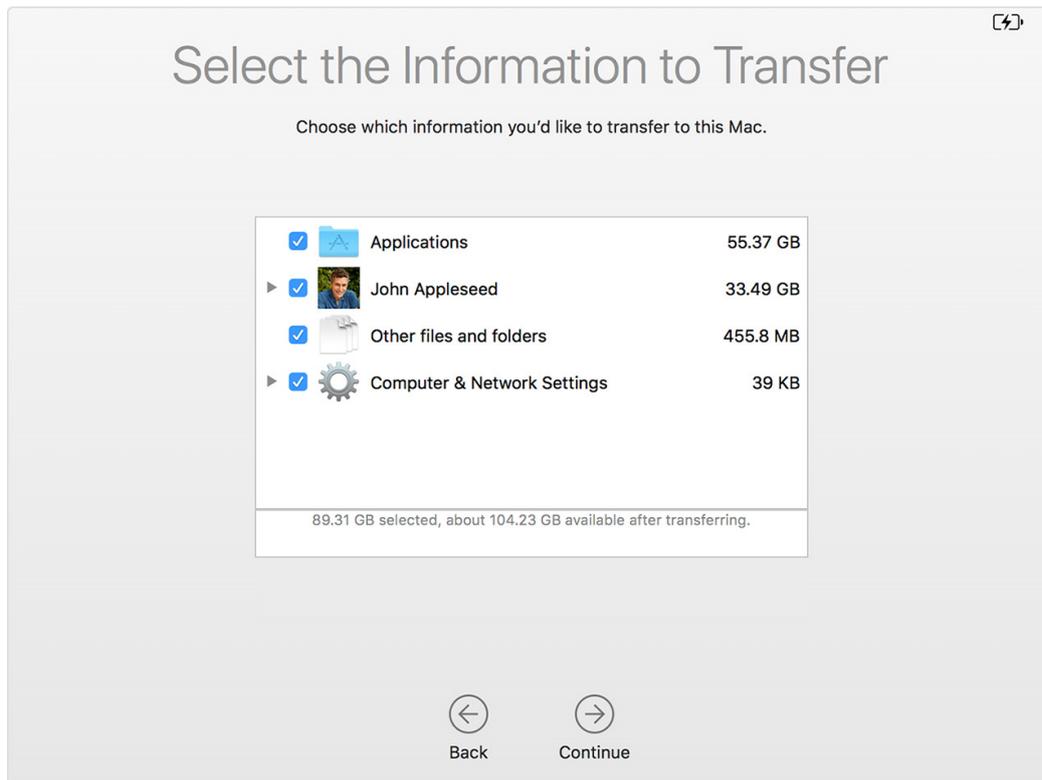
3. Select your Time Machine backup, then click "Continue."



4. If you are asked to choose from a list of backups organised by date and time, choose a backup and click “Continue.”



5. Select the information to transfer, then click “Continue” to start the transfer. This screen might look different on your Mac.



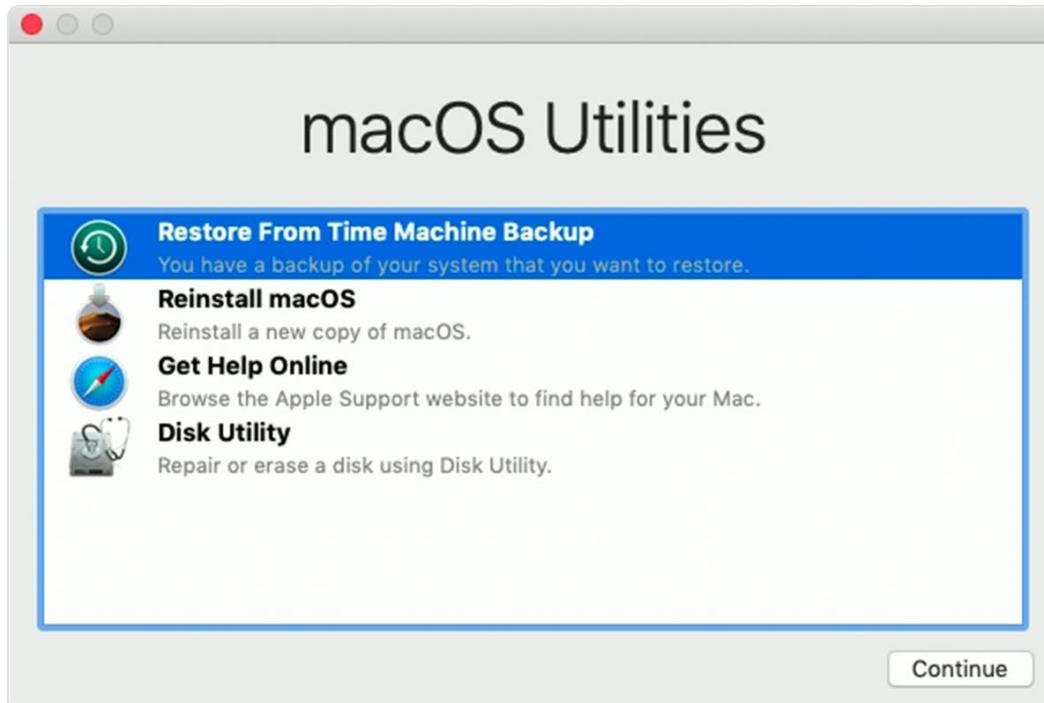
6. If you have a lot of content, the transfer might take several hours to finish. When the transfer is complete, restart your Mac and log in to the migrated account to see its files.

Restoring Both The macOS And Your Files

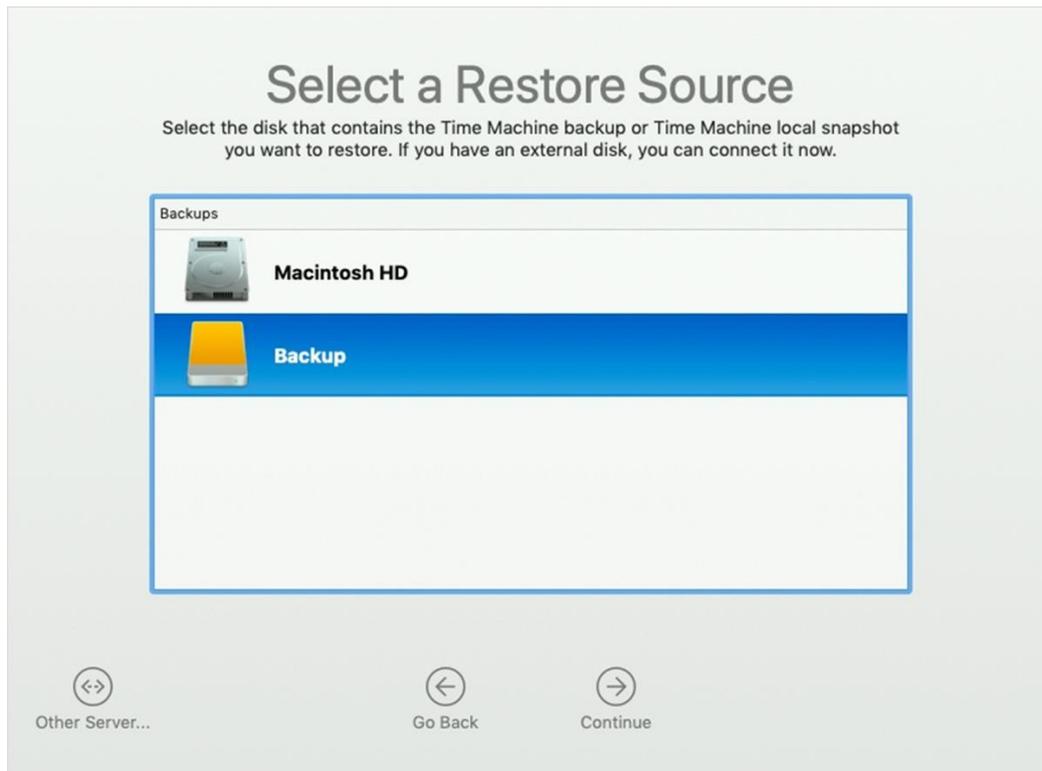
When restoring both the macOS and your files, **this process will erase your hard disk drive.** Then use your backup to restore both your files and the specific version of macOS you were using when you created the backup.

1. Make sure that your Time Machine backup is connected and turned on.

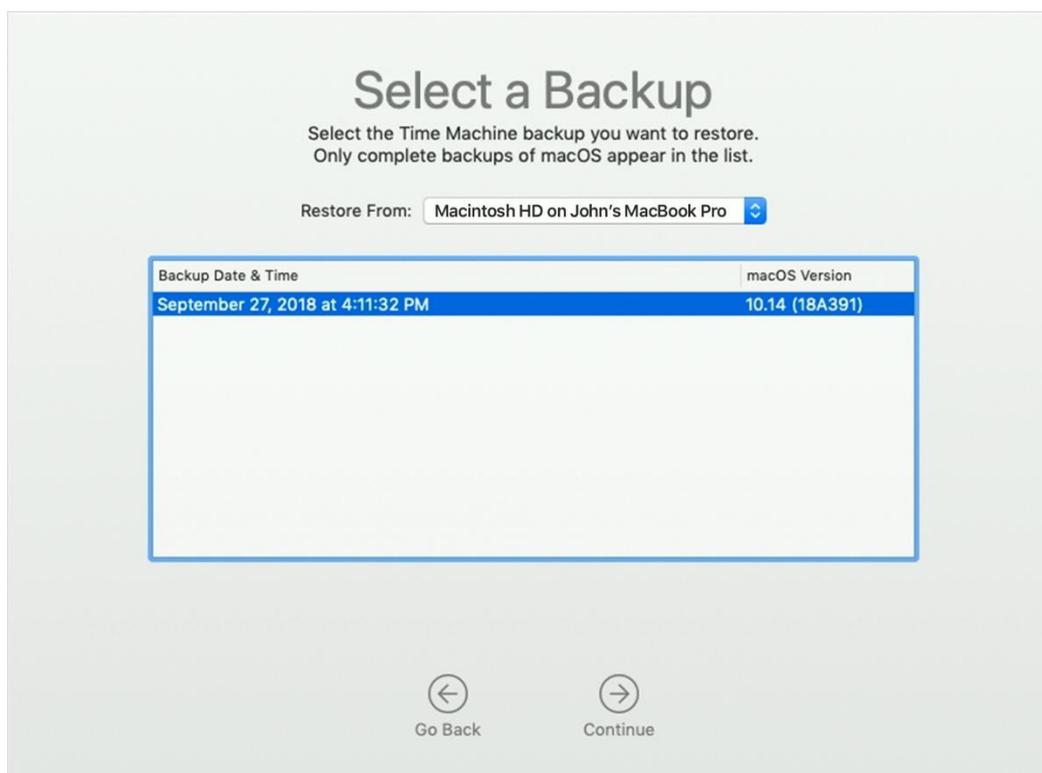
2. Turn on your Mac, then immediately press and hold Command (⌘)-R to start up from macOS Recovery.
3. When you see the macOS Utilities window, choose the option to restore from a Time Machine Backup



4. Click “Continue”, then click “Continue “again on the next screen.
5. Select your Time Machine backup disk as the restore source, then click “Continue” (note: If your backup disk is encrypted, you're asked to unlock the disk. Enter the administrator password you used when setting up Time Machine, then click Continue”)

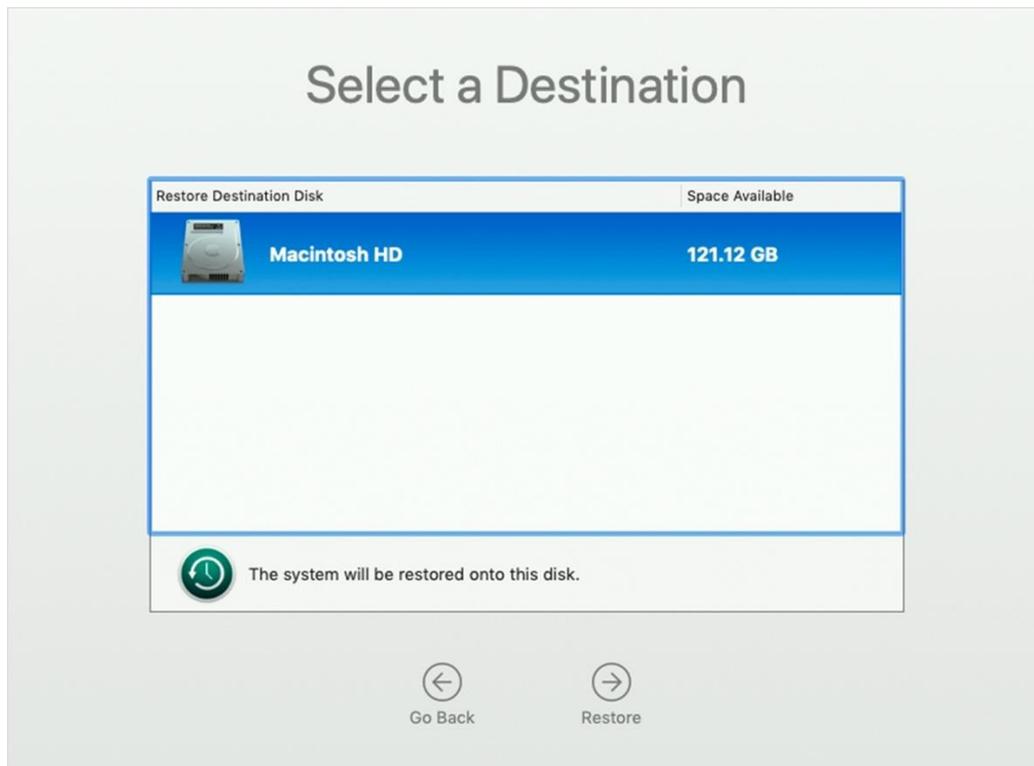


6. Select a back, then click “Continue.”



1. Select the hard disk in your Mac (or other destination disks) that will receive the contents of your backup, then click “Restore” or “Continue” (note: If your Mac has FileVault turned on, you're asked to unlock the disk. Enter the

administrator password for your Mac, then click Restore). When done, restart your Mac

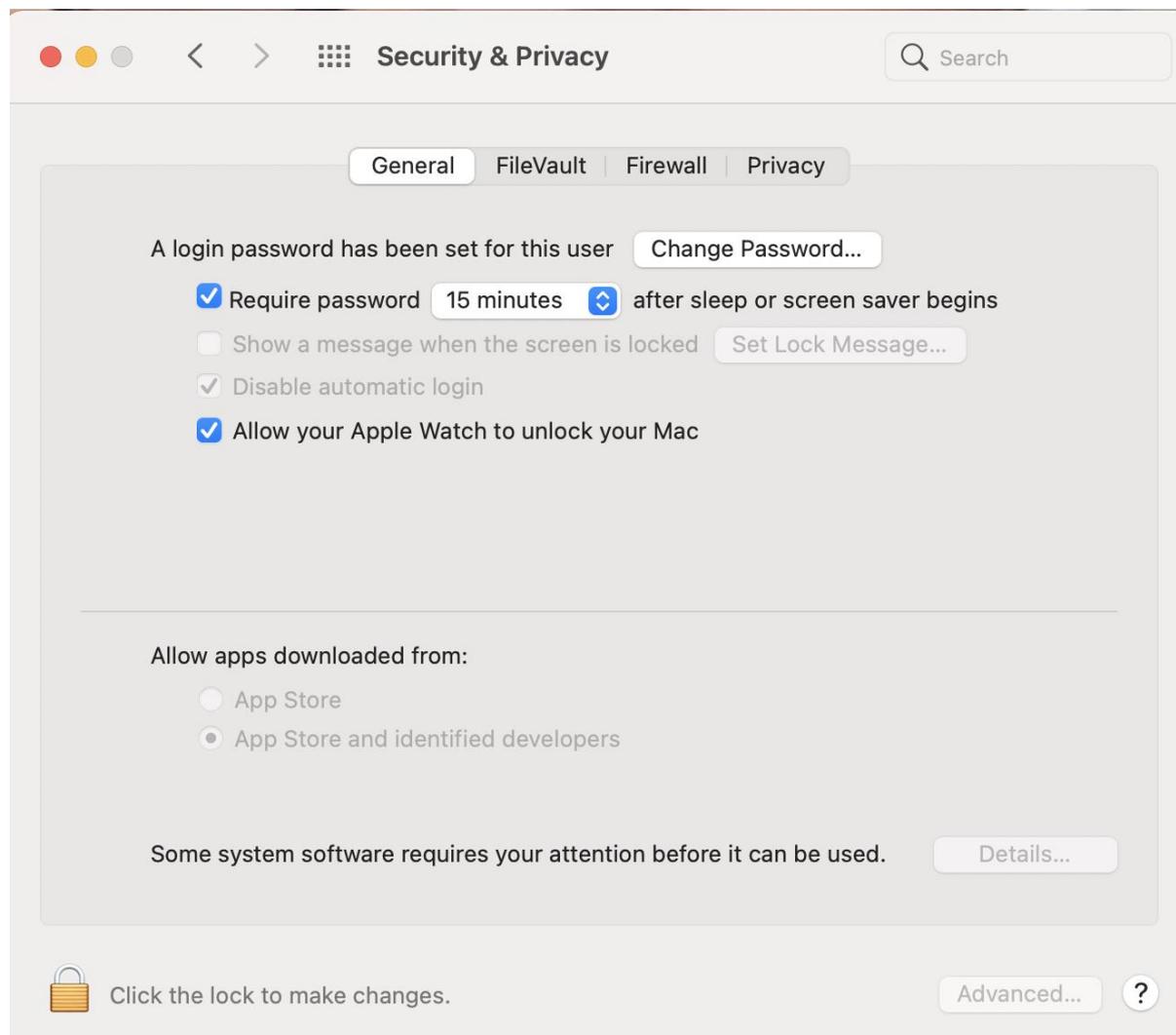


Miscellaneous - macOS Additional Security Configurations

Let's start with the basic Mac settings you should be checking to ensure security is watertight.

To familiarise yourself with the controls, pay a visit to the Security & Privacy pane in **System Preferences**. Here, you'll find four tabs that control various aspects of security.

1. On your Mac, choose Apple menu  > System Preferences > Security & Privacy
2. You'll see tabs for General, FileVault, Firewall and Privacy.



If you have an administrator account, you'll be able to make changes that affect the whole Mac. If not, they'll only apply to your account.

We will look at the various changes you can make here to secure your Mac below.

General Security & Privacy Settings

There are five things you need to pay attention

1. Under “Change Password”, you can set your password for your account if you haven’t done so or change your password if you think it is necessary.
2. The next allows you to specify if a password is needed to unlock your Mac when it goes to sleep, or a screen saver begins. You can choose to do so immediately or at different time increments following the sleep or screen saver starts. If you work in an office with other people, you should consider switching this setting on.

- It is a good idea to have “Disable automatic login” checked. It requires users to log in with a password after restarting the Mac. This feature isn't available if FileVault is turned on.
3. You can also choose to Allow your Apple Watch to unlock your Mac, assuming you have an Apple Watch. With this option selected, all you need to do is be wearing your Apple Watch (and for the Watch to be unlocked), and your Mac will automatically unlock when you are nearby. (You won't be able to use this setting if you have Internet Sharing turned on, though)
 4. Near the bottom of the General screen are two options relating to which apps can run on your Mac.
 - The safest but most limiting option is to only allow apps from the App Store to run. The other option is a good compromise, allowing you to run apps from the App Store and developers known to Apple.
 5. At the bottom of the window --> If you recently installed new software, it may attempt to load system extension - Click Allow to load system extensions from the software developer.

Turning FileVault On

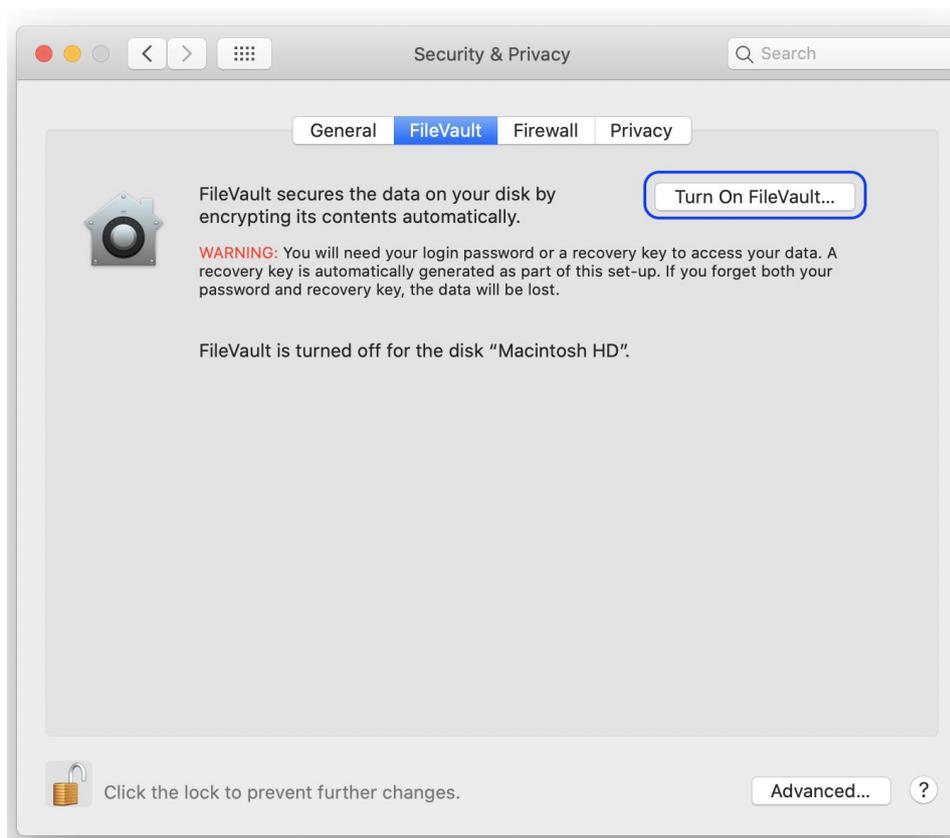
With FileVault turned on, all the files in your user account will be encrypted.

If you store sensitive information on your computer, you should consider using FileVault disk encryption.

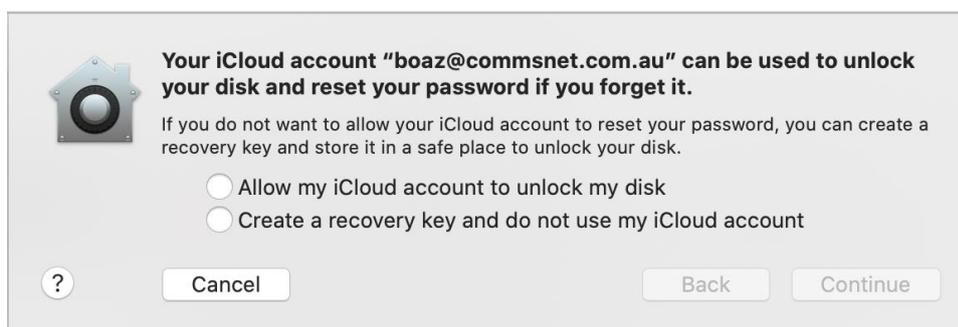
For example, if you carry all your company's financial data on your portable computer, losing it could allow someone to access sensitive data that might hurt your business.

If you are logged out of your account when your computer is lost, but the data is encrypted, your information is protected.

1. On your Mac, choose Apple menu  > System Preferences > Security & Privacy
2. Click “FileVault”



3. Click “Turn On FileVault”, and you will get the following dialogue.



If you encrypted the data on your Mac with FileVault encryption, your information is not accessible unless you first log in with your password.

When you turn on FileVault encryption, you choose a way to unlock your startup disk if you ever forget your login password: either using your iCloud account or using a recovery key that’s created for you.

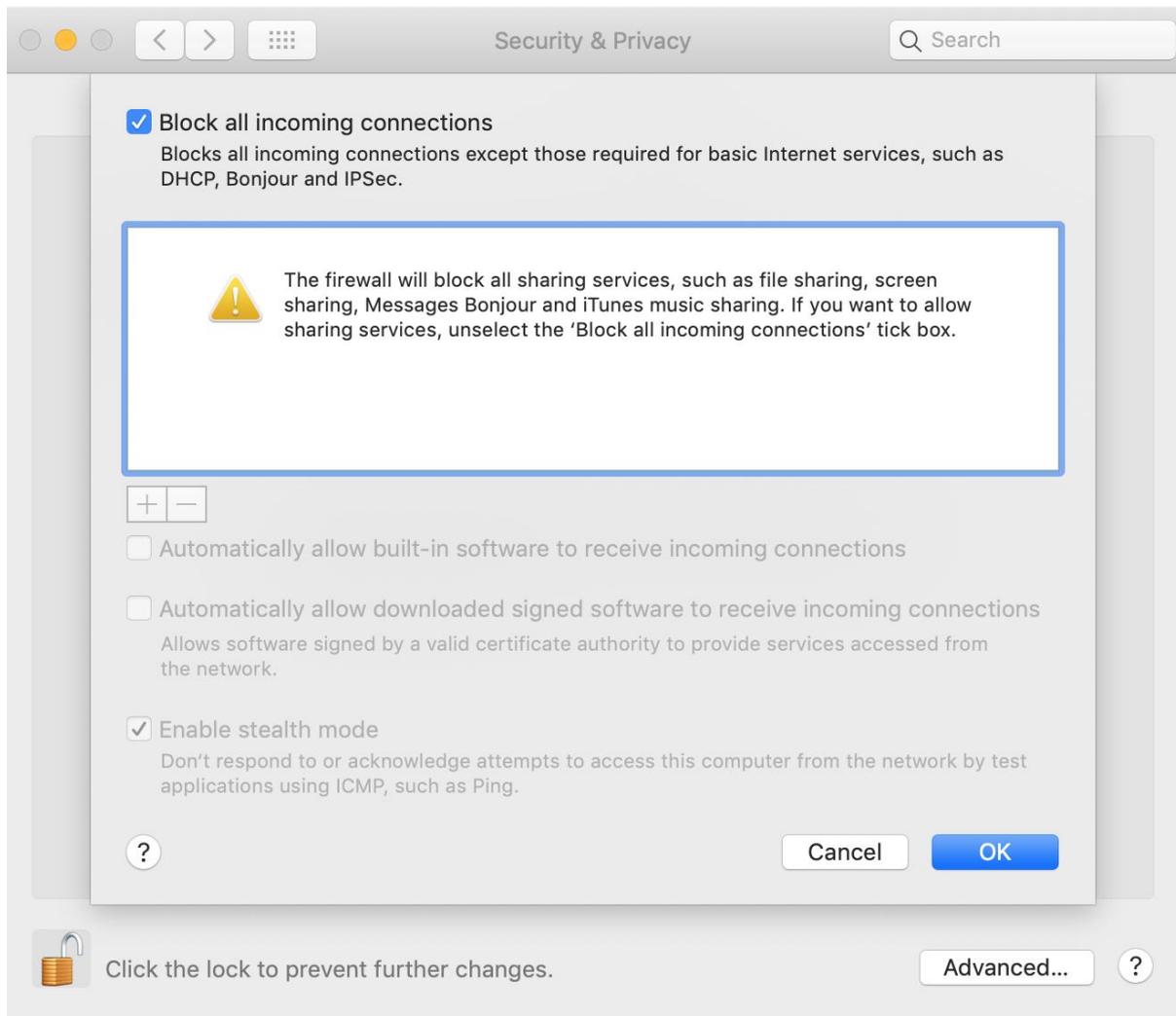
- Click “Allow my iCloud account to unlock my disk” - If you forget your login password in the future, you can reset it by entering your Apple ID and password as you log in
- Click “Create a recovery key and do not use my iCloud account”- A recovery key is a combination of numbers and letters **that you must record and keep track of yourself**. You can use this key to unlock your startup disk or disable FileVault. Keep a copy of this key somewhere other than your encrypted startup disk. If you write the key down, be sure to copy the letters and numbers exactly as they’re shown, and keep it somewhere safe that you’ll remember.

Turning The Firewall On

The first step to securing your Mac is enabling the Firewall, which blocks any unwanted incoming network connections. You might think the Firewall is enabled by default, but it often isn't.

Here's how to turn on the Firewall on a Mac

1. Click the “Firewall” Tab pane we just opened.
2. Click the “padlock icon” at the bottom left to unlock system settings (you'll need to type your login password when prompted)
3. Click the Turn On Firewall button.
4. Then click the Firewall Options button and, in the dialog box that appears, click on “Block all incoming connections”. This option blocks all incoming connections except those that require essential Internet services.

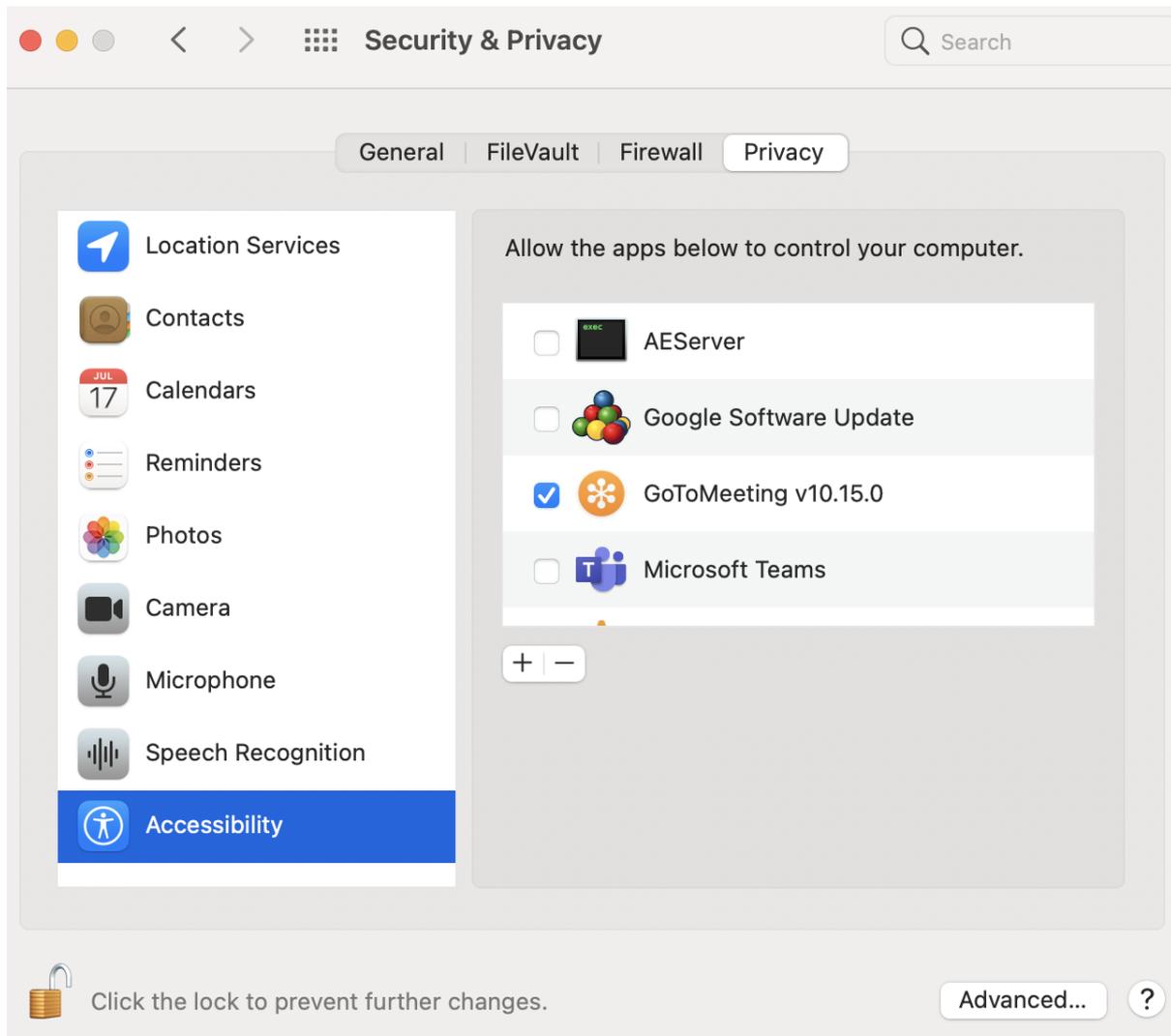


It's important to note that macOS's Firewall, while practical, offer only limited protection from malware. That's because it shields you from inbound traffic only.

Its job is to limit which apps and services can accept incoming connections. It doesn't provide any control over outbound connections, i.e. apps and services which initiate connections. So, for example, if you download a piece of malware, macOS's Firewall won't stop it from connecting to the Internet.

Checking Your Privacy Settings

The last tab, Privacy, covers several different controls and settings. These are listed in the window on the left of the pane.



- **Location Services** - This allows you to control which apps have access to your location data. You can switch Location Services off entirely here or prevent individual apps from accessing data
- **Contacts, Calendars and Reminders** - This shows the Apps that have requested access to your contacts, calendars or reminders. Unselect the App if you want to prevent it from accessing this information.
- **Photos** – You will see which Apps have requested access to your Photos Library.
- **Camera** – You will see which Apps have requested access to your camera. De-select an app if you want to prevent it from accessing this information.
 - *Note:* If you have items that are stored outside the Photos Library, other apps may still have access to them.
- **Microphone** – You will see which Apps have requested access to the Microphone.

- **Speech Recognition** - Shows apps that have requested access to speech recognition on your Mac. De-select an app if you want to prevent it from accessing speech recognition.
- **Accessibility** - Shows Apps that run scripts and system commands to control your Mac. Unselect the App if you want to prevent it from controlling your Mac

Create A Standard Account (non-admin) For Everyday Activities

When setting up a new Mac, the macOS setup assistant asks you for your name, a user name and a password and uses this information to set up your first user account.

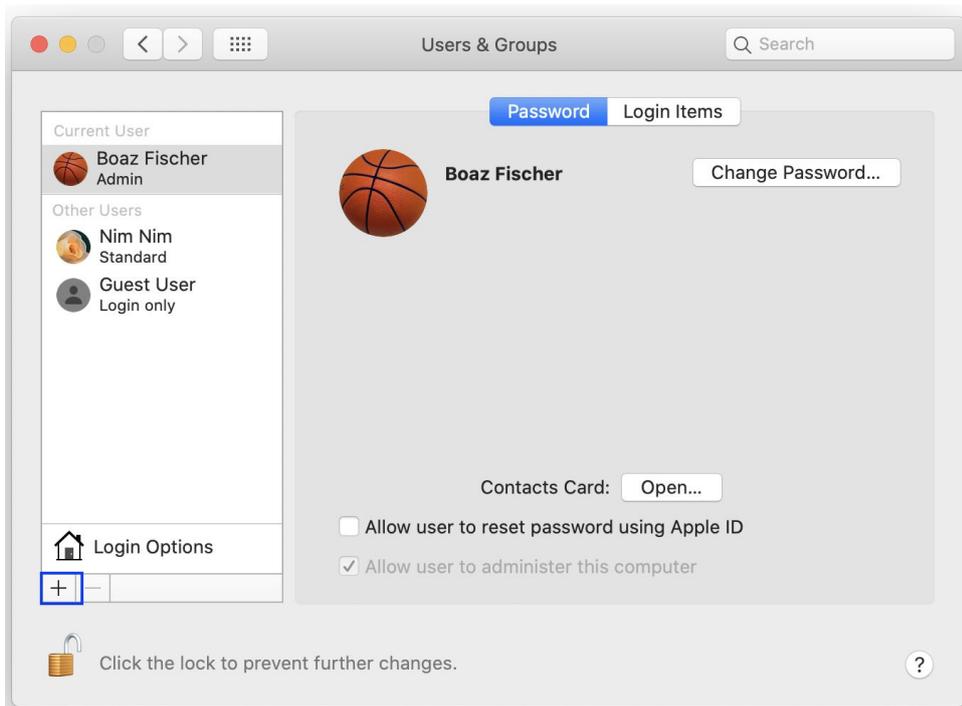
Since there has to be at least one user with administrative privileges on your Mac, that first account is an administrator account. While this is useful, you can install software and perform other actions. After entering your password, it can also be risky.

An administrator may make mistakes, and they can change or delete any file. They can also install any software, which may be a risk if the software is malicious. Standard users, however, have limited access rights on a Mac. They can use, change, and create files in their home folder, access folders on shared volumes if the permissions allow it, change settings to non-secure preferences in System Preferences, and install some software (if it doesn't need to install items in the System or Library folders). While standard accounts are more limited, they can be useful to use for daily work, just to be safe.

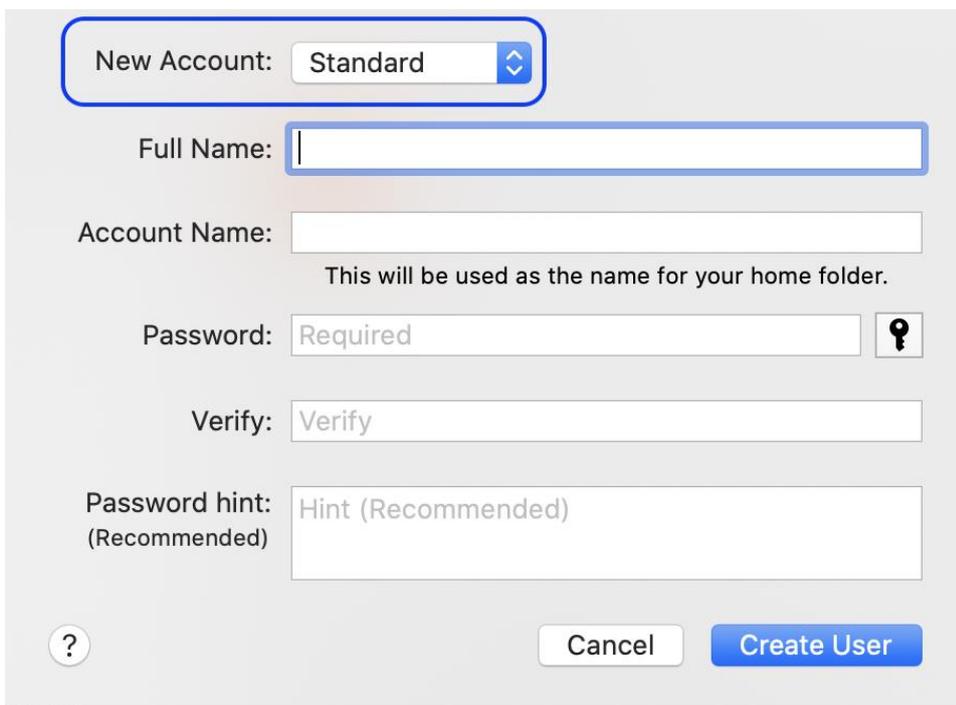
Log into that second account, use it for your everyday activities, and store your personal files. Whenever an administrator's password is required, type the admin user name and the appropriate password. While this will lead to more password requests than working under an admin account, each of these requests should raise a red flag and make you think about whether you should be entering your password.

While using a standard account is not full-blown protection from malware, it protects from some types of malware and can warn that something is going on. It can also prevent you from blundering by deleting files that you didn't mean to erase. Using two accounts is a tiny bit of hassle worth trying out to save you from potential disasters.

1. On your Mac, choose Apple menu  > System Preferences > Users & Groups



2. Click "+", and you will get the following window



3. Select New Account as **Standard**.
4. Enter details of the Standard Account
 - Use "-" to delete a user or Group

- **Guest** account allows users to have temporarily access with limited functionality. Importantly, Guest access works with the **Find My app** to help you find your Mac if you lose it.

You can locate your Mac if someone finds it, logs in as a guest and uses Safari to access the Internet

