SECURE YOUR COMPUTER

SECURE YOUR COMPUTER

Whether you are setting up a new machine or using using your day-to-day computer, it's a good idea to check your settings. In this section, we lay out some basics of computer security for both Macs and PCs. This section is broken down by operating system. In later editions, we hope to include sections on Linux, ChromeOs, and more, so stay tuned.

SECURE YOUR MAC

1. SETTING UP USERS AND PASSWORDS

It is good practice to set up different user accounts on your computer. For example, if one of your accounts is compromised by malicious software you can delete it so that it does not spread. This process helps to compartmentalise damage, allowing you to sandbox different activities on your machine. In general we recommend having an administrator account and several user accounts.

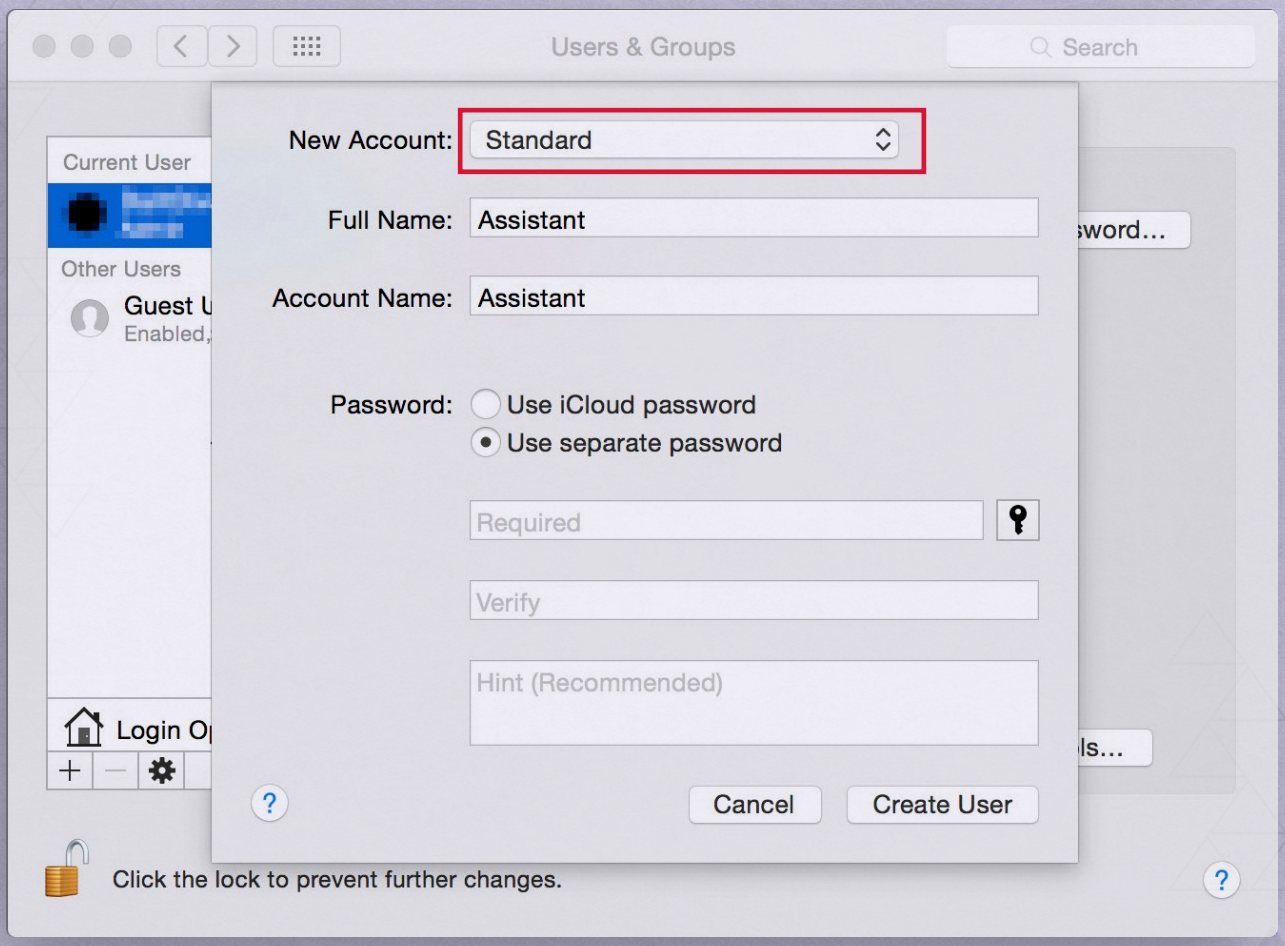
The **Administrator** account should be used to make large-scale changes, such as installing software or changing important settings. Only you or your organization's system administrator should have access. You can use another standard account for other everyday actions.

When using the **Standard** account, your computer will typically request an administrator's password as a permission when a user attempts to download, add software, or make changes. This approach will allow you to assess the resk.

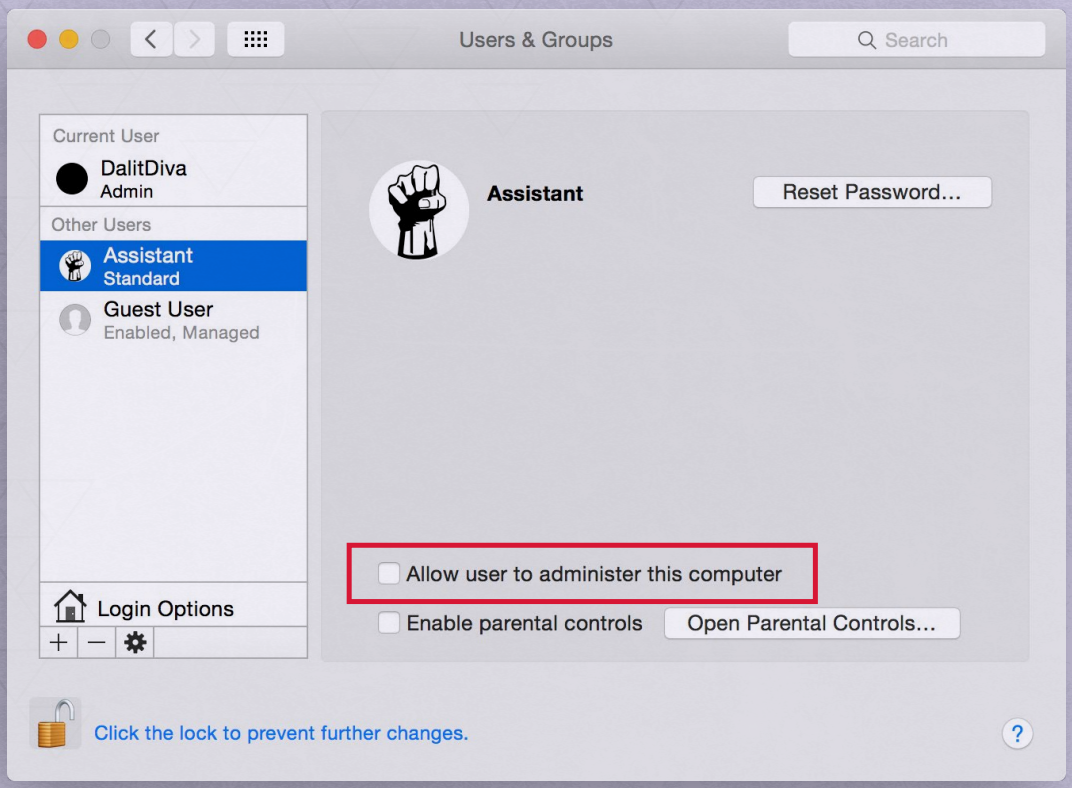
☑ To make this change, go to **Apple Menu → System Preferences → Users and Accounts**.

TIP: Always click the lock after you have selected your settings to make sure further changes require your password.

- [x] Under this section, click on the **"+"** sign to create a new account. Select **Standard** and name the account.



Make sure you keep the **“Allow user to administer this computer”** option **unchecked**.

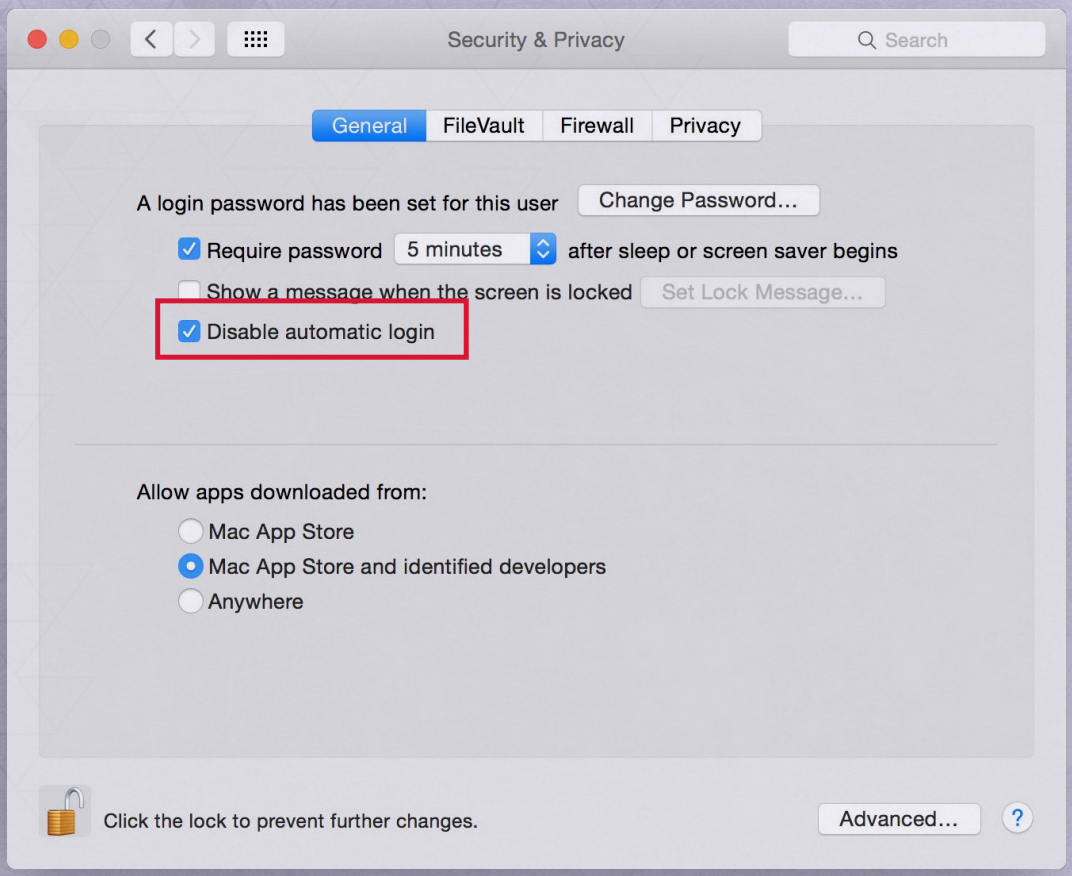


WARNING: If you did not select strong passwords, you will underride all other efforts to secure your computer. See the Secure Your Identity Password section for what makes a good password on page (71).

Also see page 72 and 73 on Rules for best passwords. If you don’t want (or don’t have time) to use a password manager or set a strong password, at least make sure you follow a few simple rules:

- The password should contain around 20 characters.
- Combine upper and lowercase locate, retrieve, and symbols.
- Don’t use the same password for other accounts.
- Change your password at least every three months or more frequently based on your risk assessment.

TIP: Using a standard account ensures that a piece of malware that infects a limited account, won’t do as much damage as one that infects an administrator account.



2. DISABLE AUTOLOGIN

Automatic login is the default setting on your computer. However, we highly recommend that you disable it, because anyone who has access to your computer will then be able to access your files. Don't leave yourself vulnerable, particularly if you work in an open office or in a space where multiple people might access your computer.

You can change this and tell your operating system to display a login screen when you start your computer.

- [x] To do so, go to the **Security & Privacy** preferences under the **System Preferences** panel and click on the **General tab**. There, you will see an option to **Disable Automatic Login**.

3. ENABLE FULL DISK ENCRYPTION

The foundation of protecting your computer is encryption. Encryption scrambles your data so that no one can read its contents unless you have your password. While there are many ways to encrypt your hard drive Apple offers FileVault full disk encryption[17] as an easy option for you to begin encrypting. FileVault can encrypt your entire hard drive using a secure encryption algorithm.

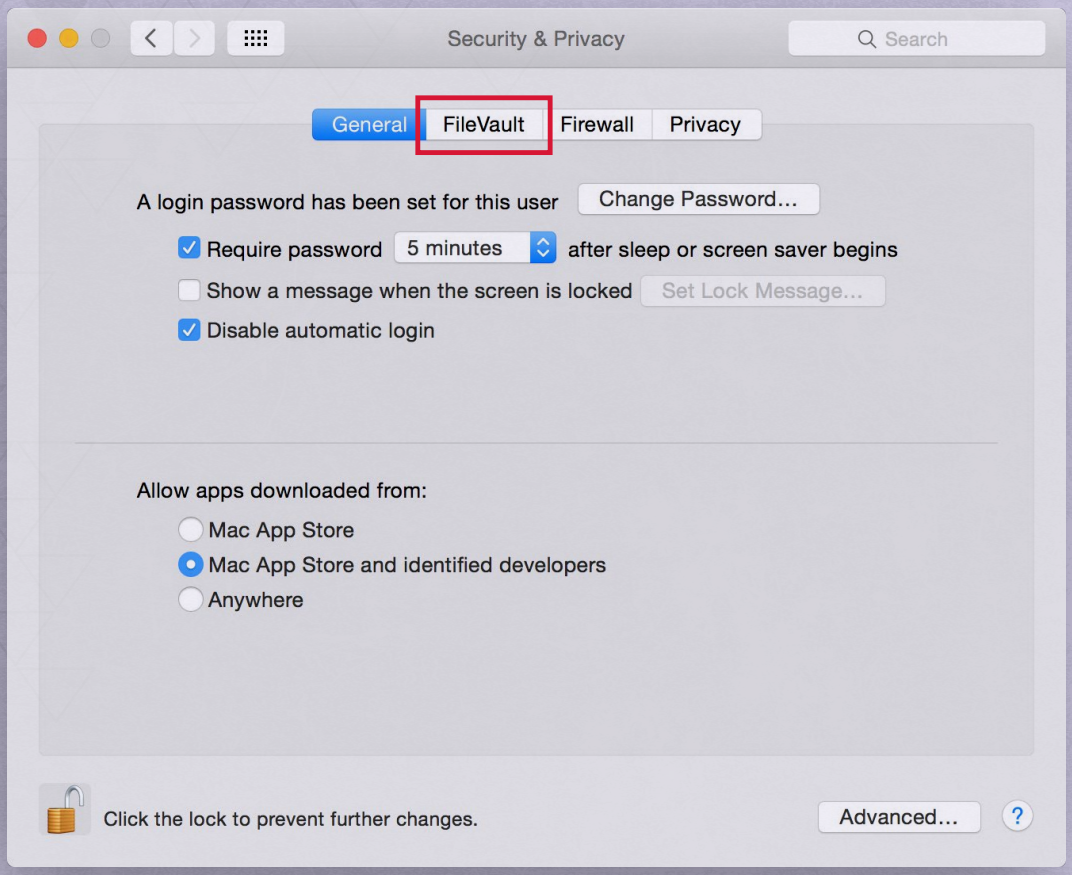
[17] https://www.intego.com/mac-security-blog/15-mac-hardening-security-tips-to-protect-your-privacy/

If you do not enable this feature on your Mac hard drive, anyone who manages to steal your computer can access any data on it.

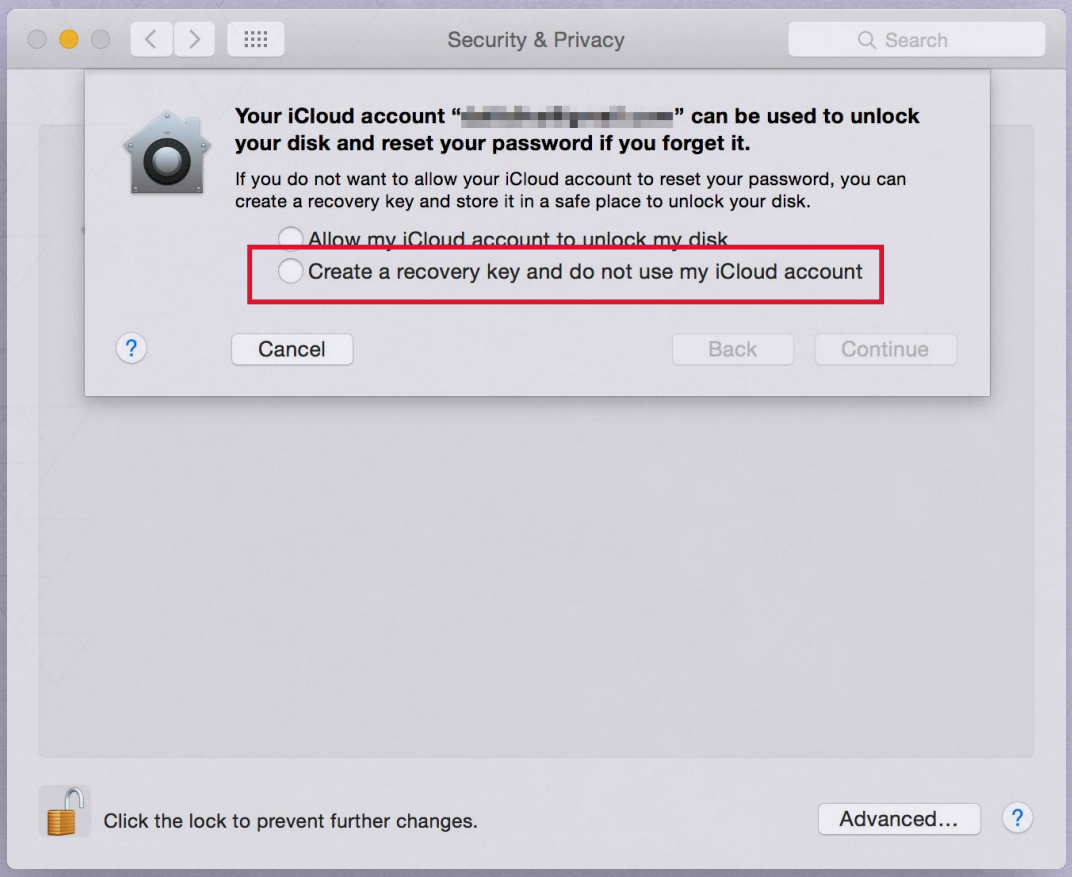
With FileVault enabled, as soon as your Mac shuts down, its entire drive and data are scrambled and rendered inaccessible without your password. The drive's contents only unlock when an authorized user powers up the Mac and logs in. File Vault encryption is an absolutely necessary layer of protection so let's get started in activating it on your computer!

NOTE: Before beginning encryption make sure you have backed up all of your contents of your mac and that you are plugged in. That way if anything goes wrong you can restore your computer from your backup.

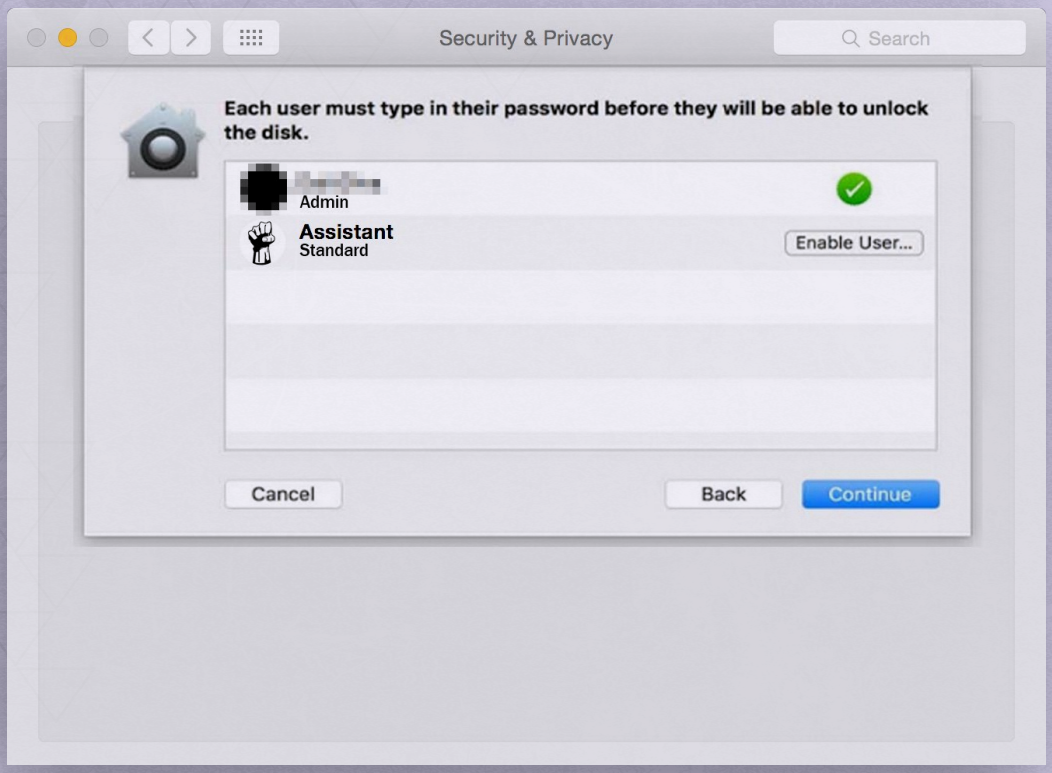
- [x] Make sure you have logged into OS X with an **administrator's account**, then go to **System Preferences → Security & Privacy → FileVault**.



- [x] You now have two options: Allow your iCloud account to unlock your disk, or to create a recovery key. **DO NOT CHOOSE THE ICLOUD OPTION!** This surrenders access to your drive to Apple when you might not want to grant this access.



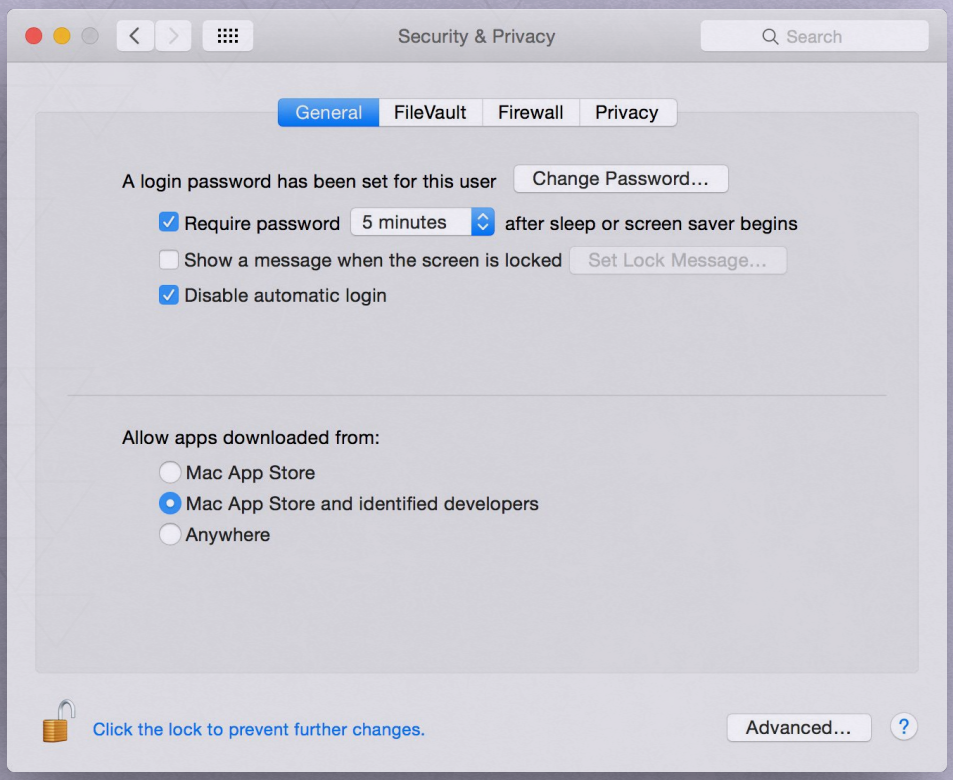
- [x] Once there, press Turn on FileVault. Use the **“Create a recovery key”** option and write down **and save the key in a safe place**. Then click on **Continue**.

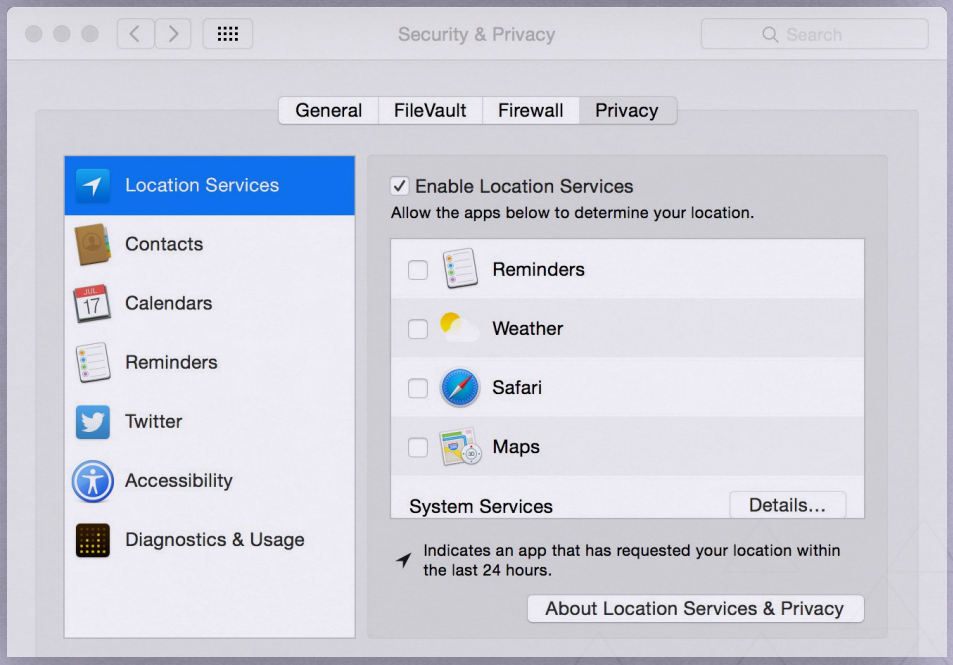


4. AUDIT YOUR SECURITY & PRIVACY SETTINGS

How comfortable are you with sharing your physical location with different apps? Do you even know which apps are receiving the changing details of your locations? A quick visit to System Preferences can reveal all.

- To update these settings, click on **Security & Privacy** and choose the **Privacy tab**. Once there, you can choose **Location Services** and view whether they are enabled, and if so, which apps can access your location. To make changes to these settings, you may need to **unlock the padlock** by entering an administrator password.





5. KEEP YOUR COMPUTER'S SOFTWARE UPDATED

As always, it is important to keep your software up to date to thwart new security threats.

- [x] Going to the **Apple Menu → App Store** will lead you to the software updates section.

SECURE YOUR PC

1. SET UP DIFFERENT USER ACCOUNTS AND PASSWORDS

It is good practice to set up different user accounts on your computer. For example, if one of your accounts is compromised by malicious software you can delete it so that it does not spread. This process helps to compartmentalise damage, allowing you to sandbox different activities on your machine. In general we recommend having an administrator account and several user accounts.

Windows grants a certain level of rights and privileges depending on what kind of user account you have. You may have a standard user account or an administrator user account.

The **Administrator** account should be used to make large-scale changes, such as installing software or changing important settings. Only you or your organization's system administrator should have access. You can use another standard account for other everyday actions.

We recommend using standard accounts for your computer to prevent users from making changes that affect everyone who uses it, such as deleting important Windows files necessary for the operating system.

When using the **Standard** account, your computer will typically request an administrator's password as a permission when a user attempts to download, add software, or make changes. This approach will allow you to assess the resk.

If you want to install an application or make security changes, Windows will ask you to provide the credentials for an administrator account.

TIP: Using a standard account ensures that a piece of malware that infects a limited account, won't do as much damage as one that infects an administrator account.

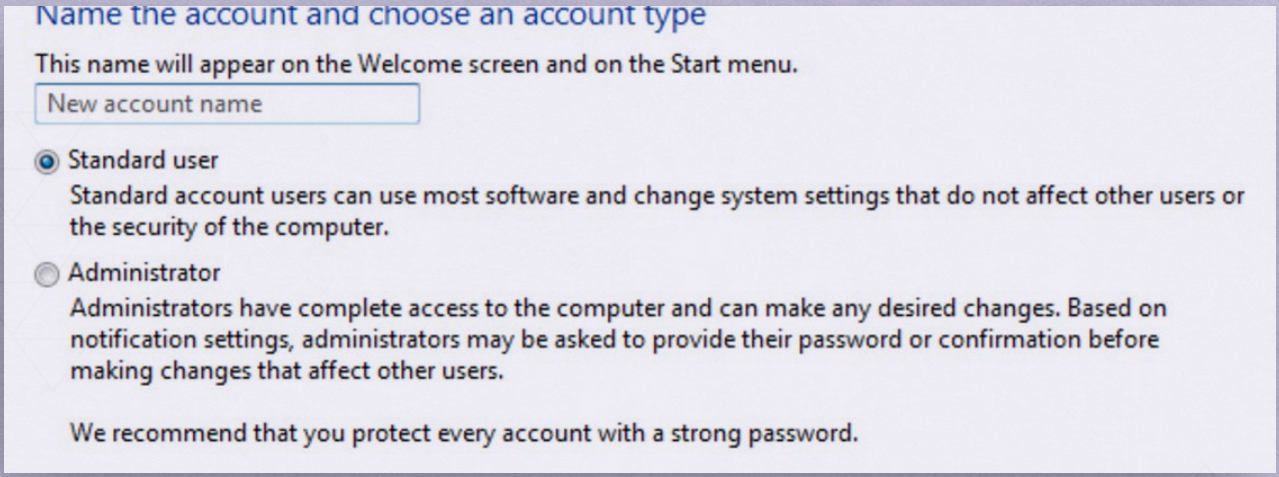
Also see page 71 on Rules for best passwords. If you don't want (or don't have time) to use a password manager or set a strong password, at least make sure you follow a few simple rules:

- The password should contain around 20 characters.

- Combine upper and lowercase locate, retrieve, and symbols.
- Don't use the same password for other accounts.
- Change your password at least every three months or more frequently based on your risk assessment.

☑ To create a new account on Windows 10, select **Start → Settings → Accounts → Family & other people → Add someone else to this PC**

☑ To create a new account on previous versions click **Start → Control Panel → User Accounts and Family Safety → User Accounts → Manage another account → Create a new account**.



2. TURN ON YOUR FIREWALL

One important defense for windows users is a Firewall, it is a piece of software and/or hardware that sits between a computer (or local network) and other networks (such as the Internet), controlling the incoming and outgoing network traffic.

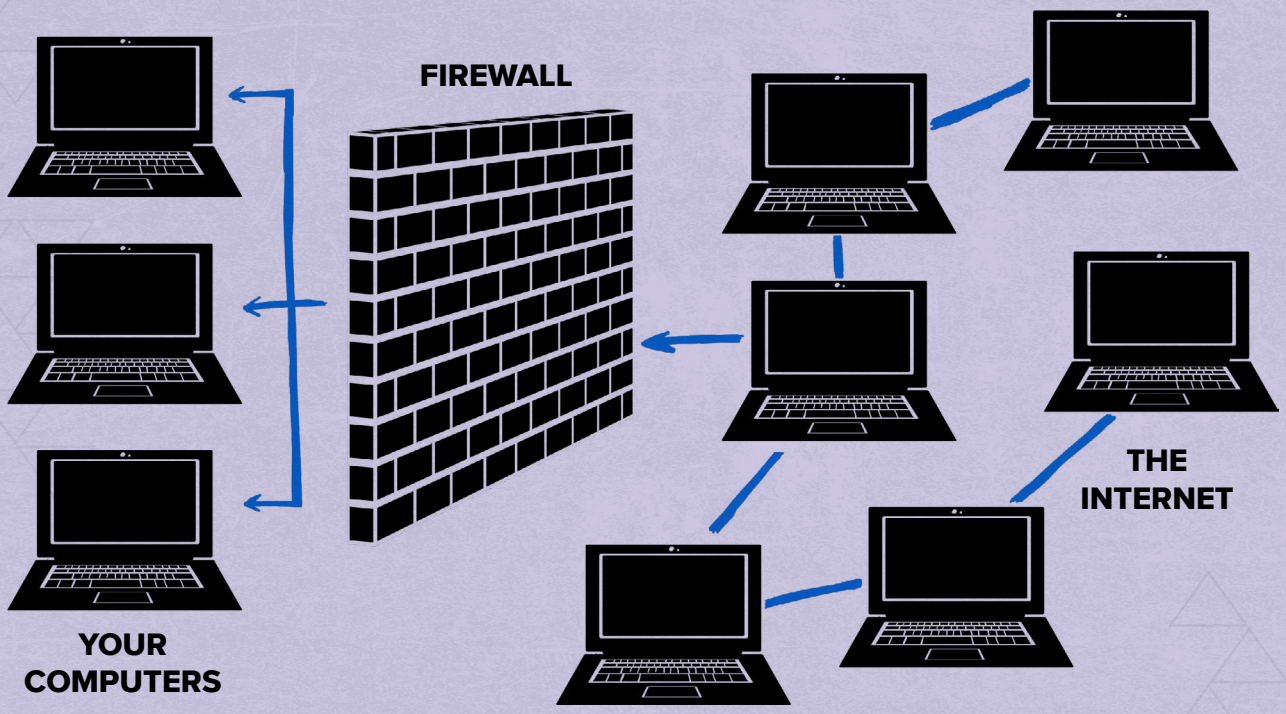
Without a firewall, anything can pass through your network. With a firewall, the firewall's rules determine which traffic is allowed through and which isn't.

This prevents people on the Internet from connecting to local network services on your computer. It also controls access to network services from other computers on your local network. That's why you're asked what type of network it is when you connect to one in Windows. If you connect to a Home network, the firewall will allow access to these services. If you connect to a Public network, the firewall will deny access.

A firewall's main security purpose for home users is blocking unsolicited incoming network traffic, but firewalls can do much more than that. It can analyze all traffic reaching or leaving the network, making decisions on whether to block it or let it pass. For example, a firewall could

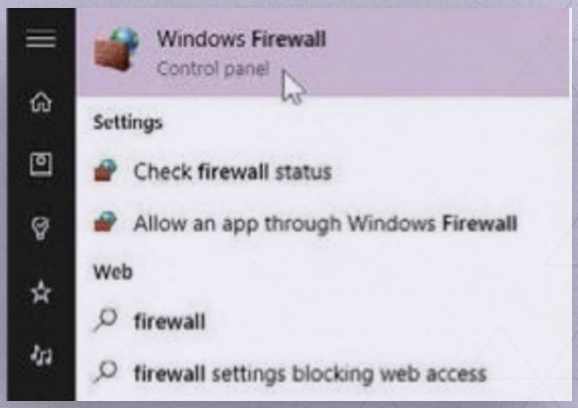
also be configured to block certain types of outgoing traffic, it can also log suspicious traffic or all traffic.

Firewalls can be anything from a piece of software running on your laptop (like the firewall included with Windows) to dedicated hardware in a corporate network. Such corporate firewalls could analyze outgoing traffic to ensure no malware was communicating through the network, monitor employee's Internet use, and filter traffic—for example, a firewall could be configured to only allow web browsing through the firewall, blocking access to other types of applications.

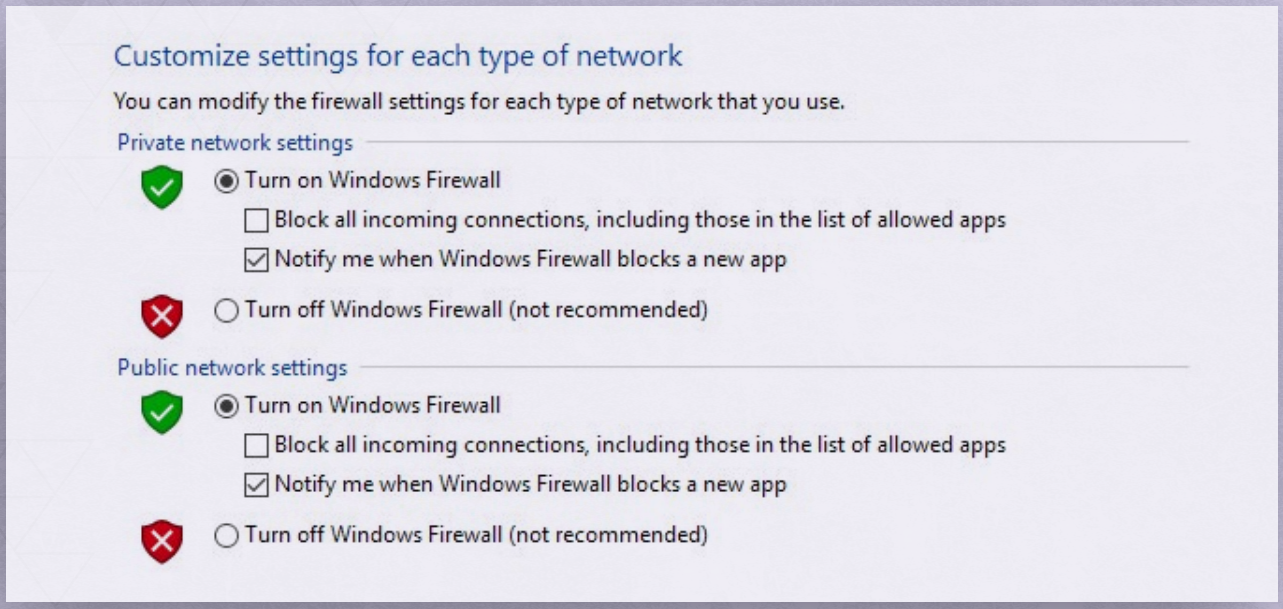


- You can find the Windows firewall in previous versions by going to **Start → Control Panel → System and Security → Windows Firewall**

- For Windows 10 users click on **Start** at the bottom left hand corner of the screen, type "firewall" into the search box, select "**firewall.cpl**"



- [x] Check basic firewall settings, then ensure the firewall is turned on for private and public networks and that notifications are enabled.

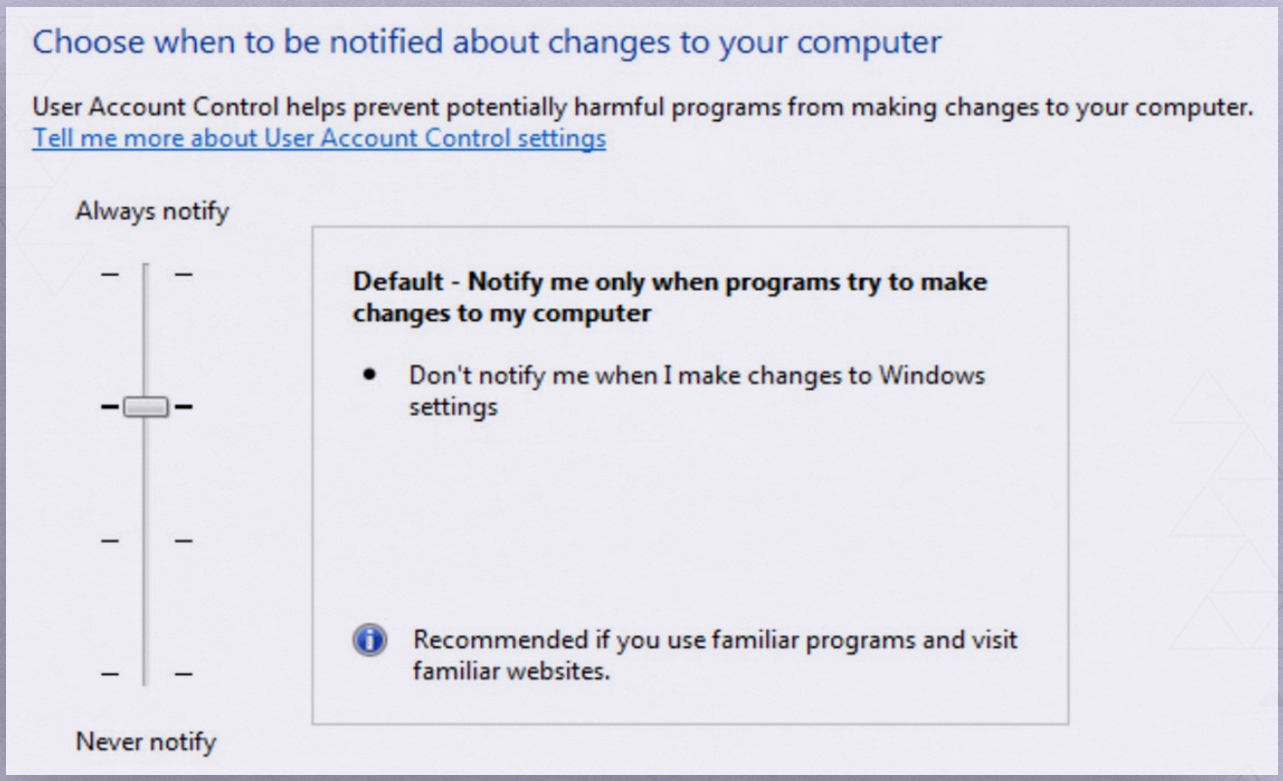


3. KEEP YOUR USER ACCOUNT CONTROL TURNED ON

Many users have the tendency to turn off **User Account Control** (UAC) after installing/reinstalling the Windows operating system. We don't recommend this. Instead of disabling the UAC, you can decrease the intensity level using a slider in the Control Panel.

UAC monitors the changes made to your computer. When important changes appear, such as installing a program or removing an application, the UAC pops up asking for administrator-level permission.

Should your user account be infected with malware, UAC helps you by keeping suspicious programs and activities from making changes in the system.



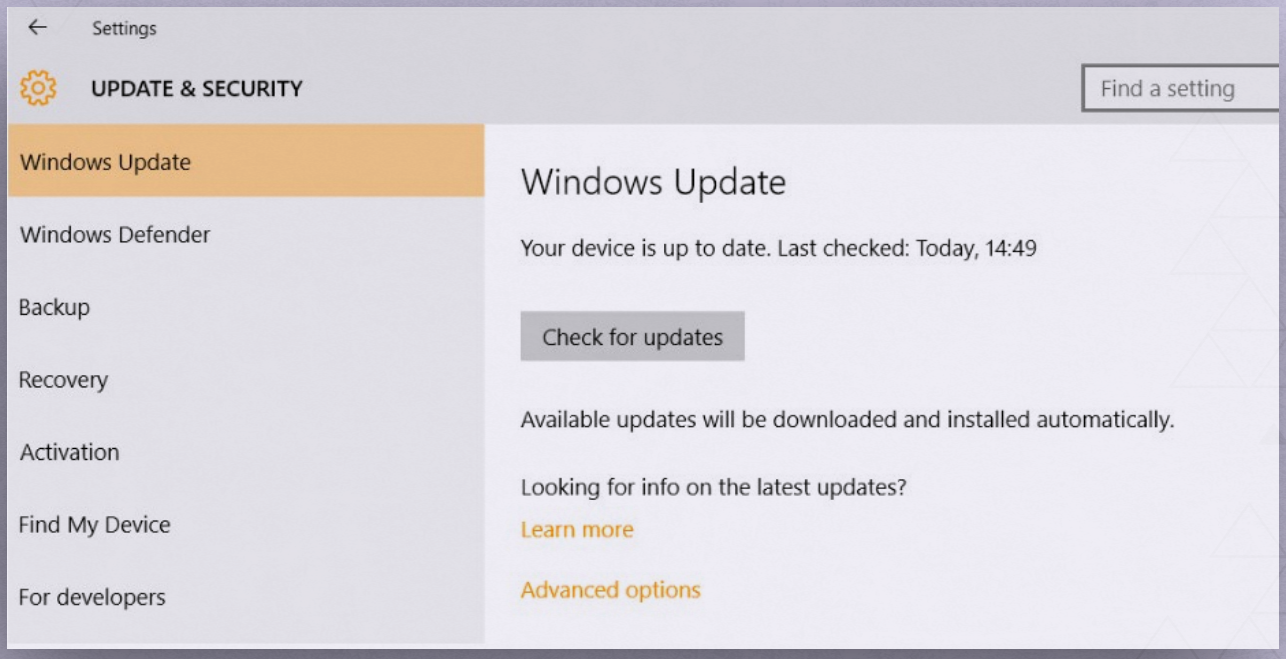
4. KEEP YOUR WINDOWS OPERATING SYSTEM UP TO DATE

The first important step is checking whether you have the latest security updates and patches available for your Windows operating system.

To get these security updates automatically, go to Control Panel and check whether automatic updating is enabled. Or, follow the stepsbelow:

- Access the search box in your Windows operating system, type **"update"**, and then select **Windows Update**.
- Select **"Change settings"**.
- Click **"Install updates automatically (recommended)"**, in case it is not already selected.

After the initial installation of available updates for your Windows operating system, keep the automatic option turned on to download and install important updates that can help protect your computer against new viruses and security threats. It's essential to install the latest security and stability fixes for your operating system, as hackers always try to benefit from these gaps.



5. INSTALL A TRADITIONAL ANTIVIRUS FOR REACTIVE PROTECTION

Use a known antivirus product from a **big security company**. It is important to have a reliable security solution on your system, which should include real-time scanning, automatic update and a firewall.

To find the best solution, check the antivirus test results in AV Comparatives, PC Magazine, AV-TEST, or Virus Bulletin and select the best solution for your system.

In case you choose to install a security product that doesn't include a firewall, make sure you have the **Windows firewall** turned on.

- ☑ To enable it, go to **Control Panel → Firewall → Turn Windows Firewall on or off**. Then, choose **Turn on Windows Firewall** for all options.

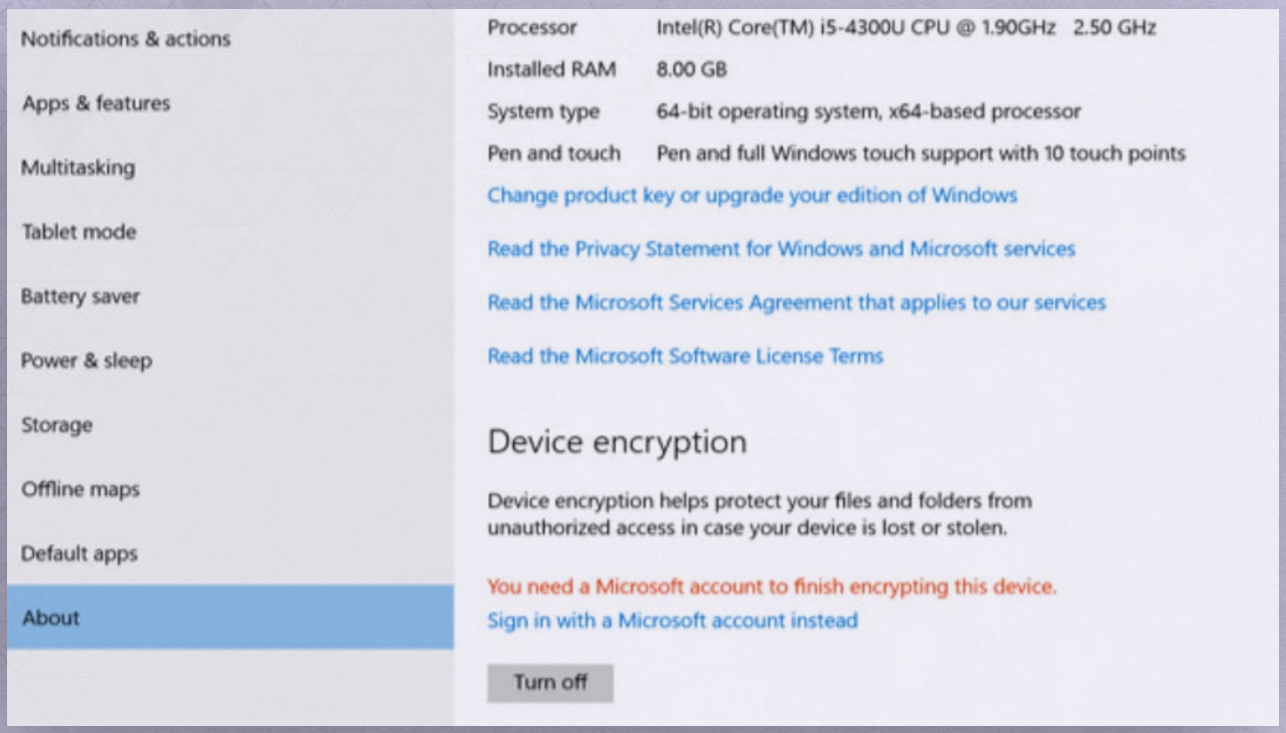
6. DEVICE ENCRYPTION FOR PCS

The foundation of protecting your computer is encryption. Encryption scrambles your data so that no one can read its contents unless you have your password. While there are many ways to encrypt your harddrive many new PCs that ship with Windows 10 will automatically have **Device Encryption** enabled. This feature was first introduced in Windows 8.1 and comes with specific hardware requirements.

With Windows Device encryption enabled, as soon as your PC shuts down, its entire drive and data are scrambled and rendered inaccessible without your password. The drive's contents only unlock when an authorized user powers up the PC and logs in.

This feature also has another limitation—it only encrypts your drive if you sign into Windows with a Microsoft account. Your recovery key is then uploaded to Microsoft's servers. This will help you recover your files if you ever can't log onto your PC but also allows Microsoft to have access to your content as well . (This is also why the FBI likely isn't too worried about Window's Device Encryption, but, for now, we're just recommending encryption as a means to protect your data from laptop thieves If you're worried about the NSA, you may want to use a different encryption solution like **Veracrypt.** We will have a separate unit on Veracrypt in the future so stay tuned.

- ☑ To check if Device Encry http://about.complex.com/ ption is enabled, open the Settings app, navigate to **System → About**, and look for a **"Device Encryption"** setting at the bottom of the **About** panel. If you don't see anything about Device Encryption here, your PC doesn't support it and it's not enabled.



NOTE: In addition to using this option for Windows, we also recommend **VeraCrypt**. It is a free software that allows you to encrypt your files. VeraCrypt is available for Microsoft Windows, Mac OS X, and GNU/Linux.

PC Encryption Using VeraCrypt

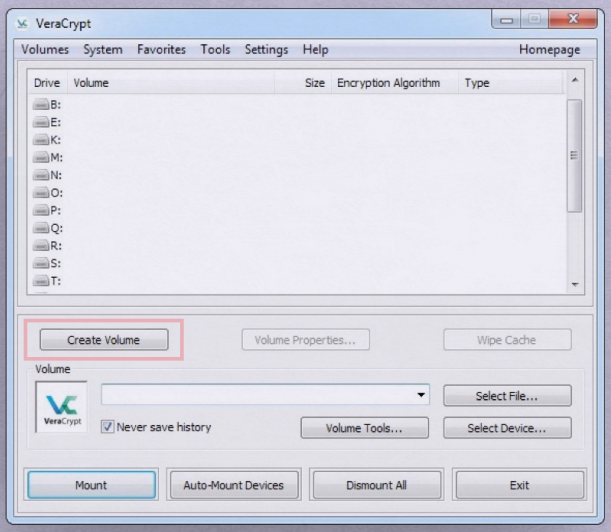
VeraCrypt is free software you can use to encrypt a whole disk, as well as a partition on a disk. You can download VeraCrypt from https://veracrypt.codeplex.com/releases/view/629329

Full disk encryption ensures that your whole computer cannot be turned on or accessed without a password. Read on to start using Veracrypt. As always with encryption processes please back up all your data and plug in to be safe.

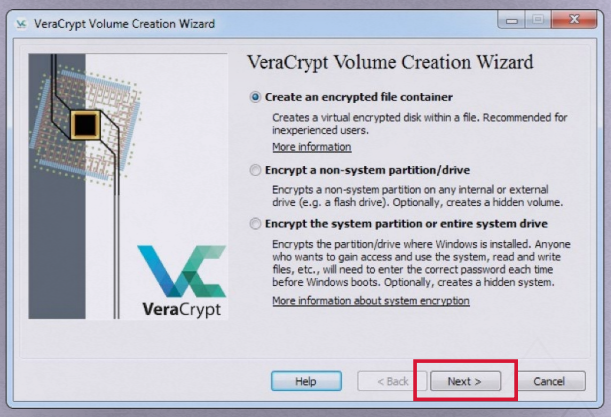
Create a Virtual Partition with Veracrypt (recommended for beginners)

Here, we will create a **Virtual Encrypted Partition**—a file on your hard drive that acts as a completely new, encrypted disk. You can think of this partition as a disk with a password—you can store whatever you like in the disk and the password will give it an additional layer of security.

- To start, open Veracrypt after you have installed it, and click the **“Create Volume"**

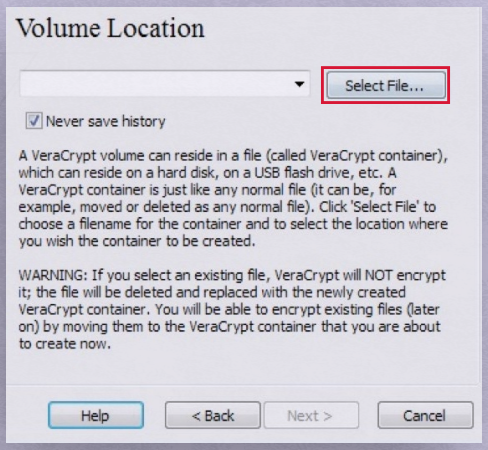


- Then check **“Create an encrypted file container”**

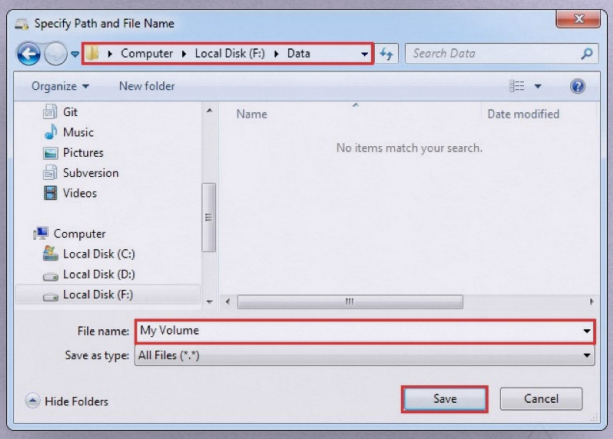


- For right now, we will create a **Standard Veracrypt volume**.

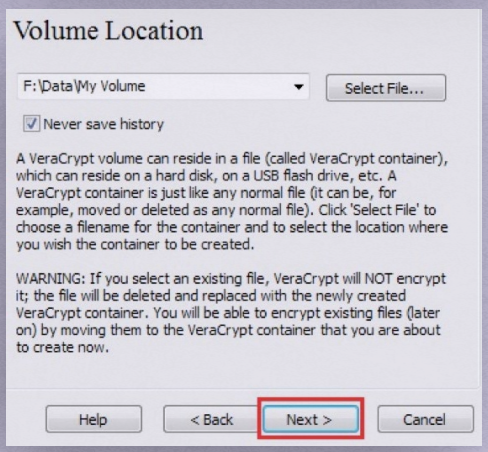
- Now choose **“select file”**. You will be prompted with an file explorer dialogue.



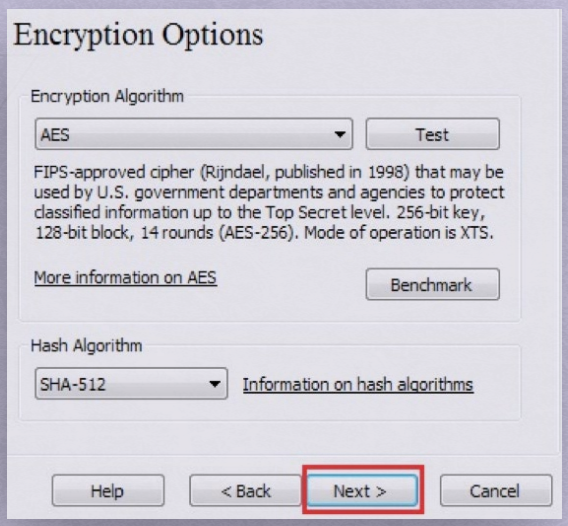
- In this step, we will be Creating a file that will store all your encrypted content. Later in the process, we will “mount” this file, so that it will show up looking like a folder or hard drive. But for now, select a location on your hard disk where this encrypted content will reside.



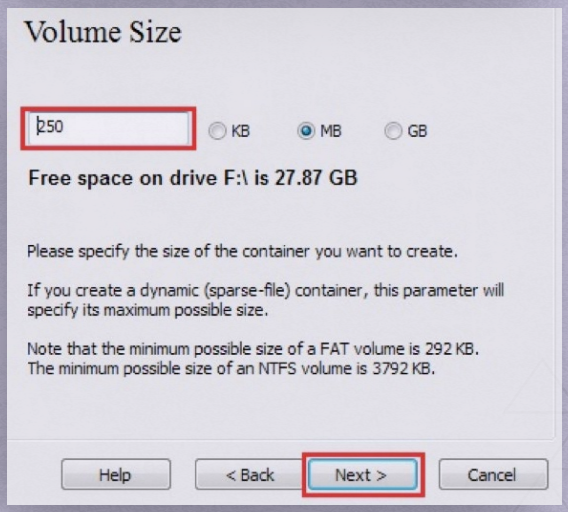
- Go ahead and click **Next** in this next step.



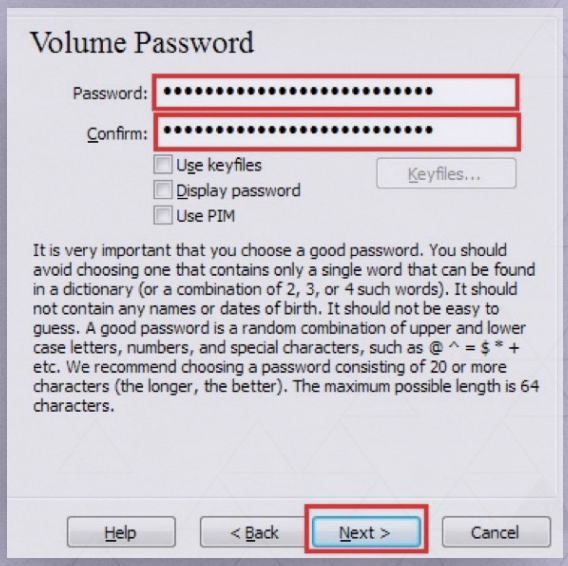
- In this next step, we choose which encryption techniques we should apply. Don't worry if this doesn't make sense, we can click "next" with the default options.



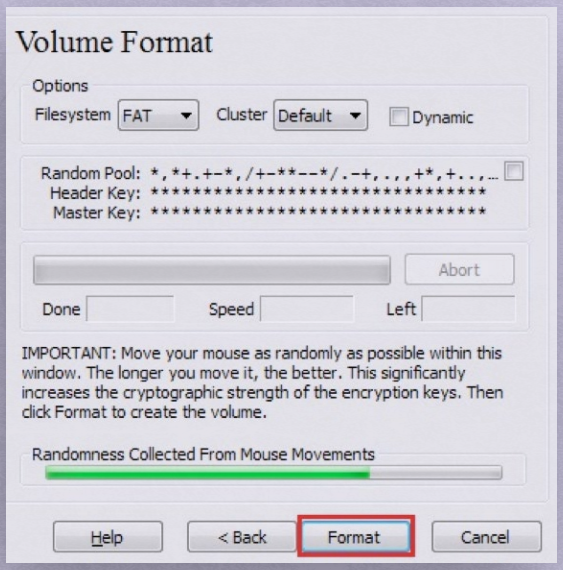
- In this step, you will need to choose how much of your disk space you want to dedicate to this encrypted segment. Make sure that you have that space available on your hard drive. Choose more space if you will be storing movies, video, audio, etc. You can dedicate less space if you are only encrypting text documents or photos.



- Next, you will select a password. **Write this password down. Make sure it is a secure password as per the rules described elsewhere in this document.**

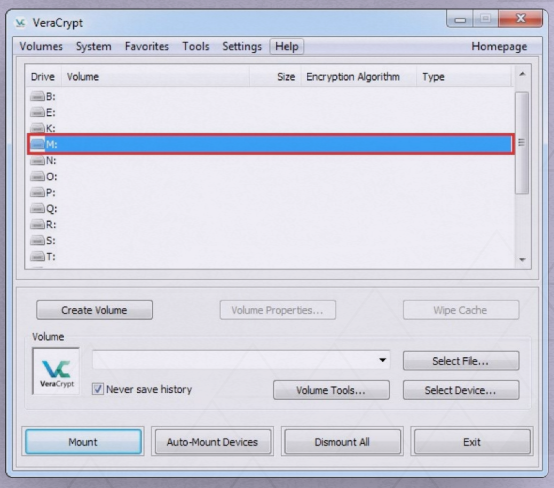


- Next, move your mouse around randomly for about 1 minute. This will generate “random noise” that will then be fed into the encryption in order to make it more un-crackable.



- At this point, you should see a volume successfully being created That is good, but we are not quite yet done.

- Now, we are going to select an available drive letter in order to make the encrypted partition you just made visible as an extra hard drive. Go ahead and select any of the letters in the list and then click on **“Select File”**



FULL DISK ENCRYPTION WITH VERACRYPT

- [x] We do not recommend encrypting your whole disk with Veracrypt if you are a beginner. If you feel confident with your tech skills to troubleshoot, then proceed in this section. **You will need a USB Stick** to finish this process. You will also need to **Boot into your BIOS** and **Disable Secure Boot** in your BIOS.