

# Basic security steps to keep your computer safe

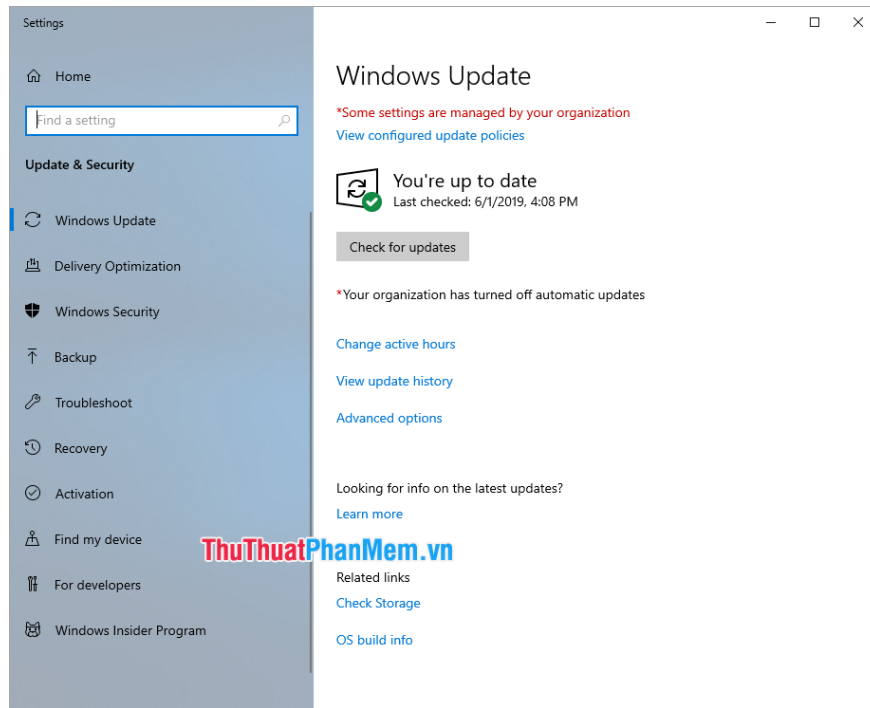
Basic security steps to keep your computer safe. Because every personal computer device contains important data and personal documents, security is a top priority. But not everyone knows the steps to protect your computer in the best and most effective way.

Because every personal computer device contains important data and personal documents, security is a top priority. But not everyone knows the steps to protect your computer in the best and most effective way. Sometimes the subjective not protecting the computer makes users encounter many troubles about data being stolen or hacked. In this article, Software Tips will guide you through the basic security steps to keep your computer safe.



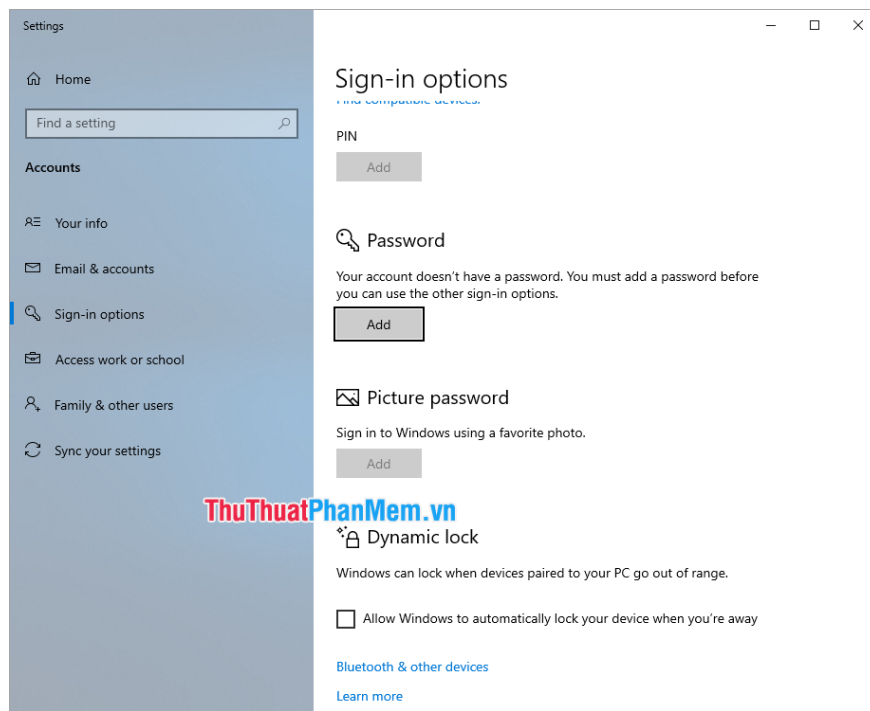
## 1. Update Windows

With each version of Windows released after the release, the manufacturer will release the patch to support patching of the previous version of Windows. Therefore, updating new Windows versions is one of the first essential issues to secure your computer. Normally, the patched Windows version will be carefully checked and fixed by the previous team for users' peace of mind. But nothing is 100% sure that your computer will not encounter errors or security problems, but at least we are much more secure. Currently Windows 10 will automatically update new versions for users after you shutdown.



## 2. Set a password for the computer

This is one of the most basic ways to protect users' personal data from the curiosity of others. Windows 10 now supports users to set passwords, numbers, or drawings. With password security, your data will be safer when your computer is in the hands of strangers. If the security with password does not help you feel secure, you can refer to using Bitlocker to encrypt your data.



### 3. Using anti-virus software

With the current 4.0 technology era, the Internet is both beneficial and harmful. If you are not alert enough when using the Internet, it is very likely that Hacker will trick you into downloading Virus files to your computer. With these Virus files will conduct encryption of data on your computer and demand a ransom. The anti-virus software has the ability to alert and prevent you from continuing to access malicious files. Currently each antivirus software focuses on developing certain viruses, so installing two or more anti-virus software will bring good results and be resistant to more malicious types.

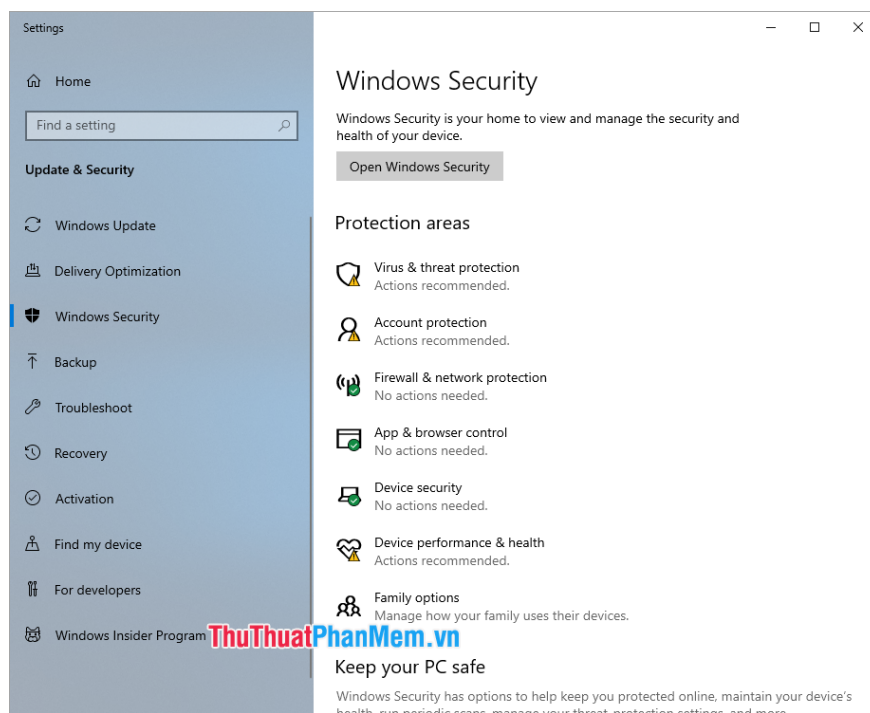


### 4. Turn on the Windows firewall

Imagine Fire (Fire Wall) on Windows 10 has a lot of functions which can not be mentioned is to control and shorten communication between unsafe networks. The firewall will automatically exploit information related to the security and safety of other networks before you want to connect to them. Firewall is one of the important and useful security features so you should not turn them off in any case.

### 5: Windows Defender Protection

With the release of Windows 10, Microsoft has provided Windows Defender for free, which is a highly regarded anti-virus software. Unlike other software to pay to be able to experience the advanced features, Windows Defender is completely free. But the performance of Windows Defender is highly appreciated when it has quickly reached the third rank of the best antivirus software.



## 6. Download the software at home page

Currently, there are many Web sites that re-upload software from different manufacturers and when they post back, we cannot know what they have added. If at unofficial download sources, it is not safe to download the Virus to your computer. Because of that, before you want to download something, check that it is from the manufacturer's source.

## 7. Limiting the use of non-copyrighted software

Non-copyrighted software comes from programmers and they intervene in the manufacturer's system to crack and control copyright so that users can use it for free. As long as they add any malicious file inside, your computer can be exploited data or encrypted.



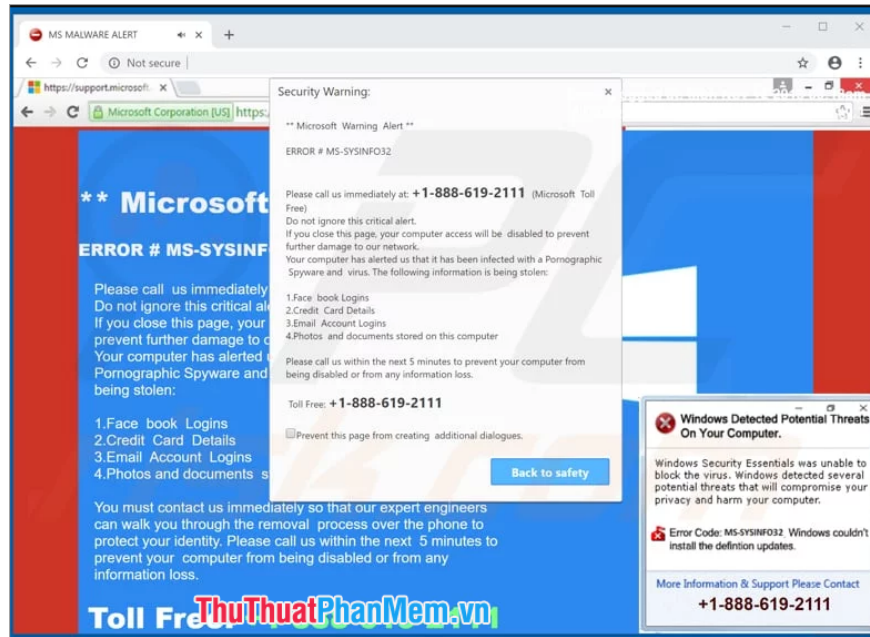
## 8. Control of peripheral devices

Today, the use of USB or portable hard drive storage is too familiar. But such connection problems also make our computers more likely to be infected with viruses. When you connect strange USB of other people to your computer, you will not know whether there are viruses or malicious files that should not be for the most peace of mind, please scan USB Virus before connecting to the computer. .



## 9. Beware of online advertisements

How to make money by clicking now very familiar with Internet users constantly. Just click on any location on some Web sites, you will immediately see the following window: "Your device has been infected with the virus", "Your system is corrupted" . You guys Don't trust them, they are just pop-up ads to entice users to install miscellaneous applications on their computers.



## 10. Use skills, master

This is one of the most important components for securing your computer. You need to be alert to your computer operations to avoid security problems. There is no software or tool that can give you 100% security, you need to use your experience to master them and protect your own devices.

In this article, the Software Tips have given you 10 most basic ways to secure your computer, with these ways, you can be somewhat more secure when using your computer. Have a nice day!

You finished reading the article "**Basic security steps to keep your computer safe**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.