If you don't want to be a victim of Ransomware, read this article

No matter what platform you are using, your computer, tablet or smartphone, remember to always update the updates available to upgrade your device version to ensure safety.

No matter what platform you are using, your computer, tablet or smartphone (smartphone), be sure to update the available updates to upgrade your device version. Updates (updates) will be patched and ensure a more secure level of security.

If you do not want to be a victim of Ransomware, or do not want your important data "wingless", follow the basic steps below. To find out more details and what is Ransomware, you can refer here.

Measures to prevent Ransomware

1. 1. Perform regular data backup
2. 2. Always update updates
3. 3. Stay away from suspicious files, activate file extensions
4. 4. Use email filters
5. 5. Use Internet security software
6. 6. Check the safety of the system regularly
7. 7. Use modern firewall utility
8. 8. Do not use the administrator account daily
9. 9. Turn off Macros in Microsoft Office
10. 10. Set browser security, check for updates and remove unsafe extensions
11. 11. Avoid malicious ads

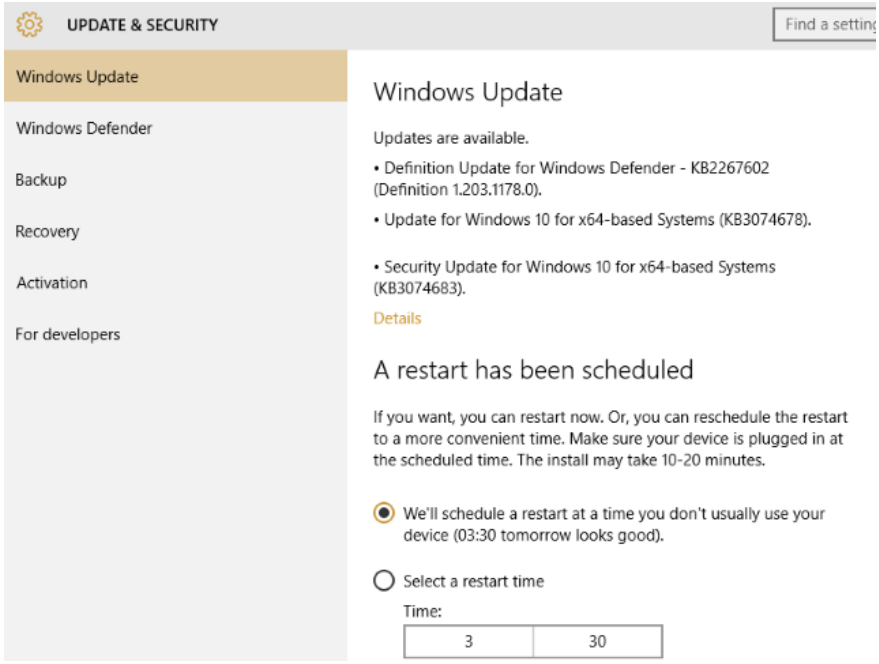
1. Perform regular data backup

This is Ransomware Defense 101. Scammers want to 'narrow' access to your data, and once your data is hacked it is certain that the data will be lost. Therefore you should proceed to backup and synchronize important data on your system.

Arrange and manage your important data in a single location, and regularly back up all of this data in case if there is an attack, your data is still available and can be restored easily.

For backup frequency, it is recommended to back up data regularly.

1. Things to keep in mind when backing up data on your computer



2. Always update updates

No matter what platform you are using, your computer, tablet or smartphone (smartphone) remember to keep the updates available to upgrade to the latest version on your device. Updates (updates) will be updated by developers, correcting patches and ensuring a higher level of security.

3. Stay away from suspicious files, activate file extensions

One of the easiest and effective ways to combat Ransomware (and other malware) is to use your own eyes. Many malicious tools have file extensions such as .PDF.EXE, you can immediately confirm these are malicious files.

So to determine which files are dangerous that you need to stay away from or should delete, the only way is to enable file extensions on Windows. You can refer to the article 8 ways to identify strange format files.

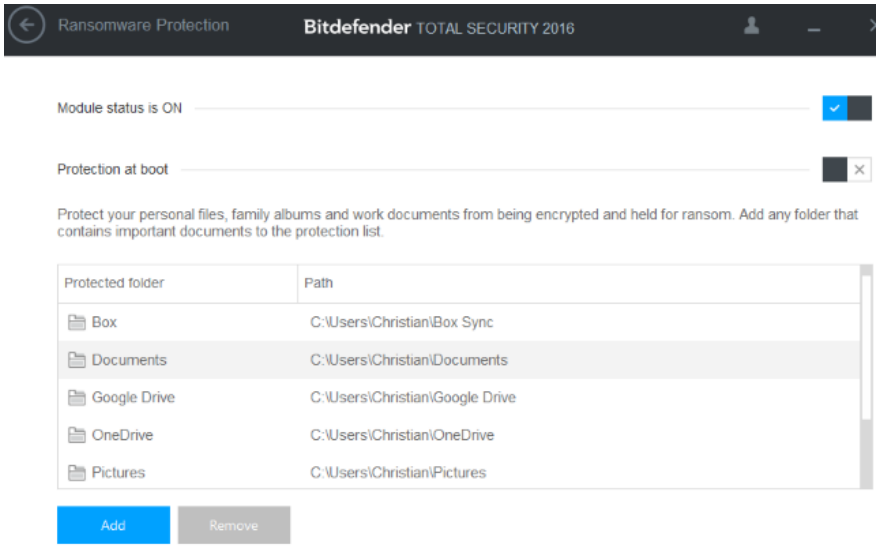
4. Use email filters

Until now, there is no way to prevent the attacks of malware and phishing, so to limit you should use email client to scan malicious messages sent on my email. If not, you should at least set up an email filtering rule, and delete EXE email files.

Also an immutable rule is never to open or send emails that you feel 'suspect'. Those are the tricks that hackers are always using and the simplest part is to trick others into launching executable files that hackers send with icons and 'fake' formats like DOC or PDF to spread malicious code. and thereby invade and control the computer.

5. Use Internet security software

The solution to protect your data from Ransomware attacks is to use security software. While free Internet security tools are also quite good, enough to scan directly and like a firewall, however, when using the paid version, the security level will be higher.



6. Check the safety of the system regularly

In the simplest and most understandable way, you should regularly check your system using antivirus software and programs. Some effective antivirus software and programs that you can use such as Kaspersky Virus Removal Tool, AVG Anti-Virus, Microsoft Security Essentials, MalwareBytes, etc.

Also you can refer to some of the most effective antivirus software for Windows computers here.

During the scanning process, if a threat is detected, the software, this antivirus program will conduct "quarantine" and remove it for you.

7. Use modern firewall utility

Firewalls play an important role in limiting the spread of all malware, including Ransomware. Although Ransomware often infects via email attachments, malicious ads or infected media such as USB, it can also move on networks (networks) with amazing speed. To avoid Ransomware infection, you need to be sure to block port 445, which is an internal port that prevents all devices on the Ransomware transmission network and other malicious software.

Although this port is usually blocked by default, to be safe you should check carefully. In addition, you should note that most ramsomware communicate with a remote server, so regularly update the firewall to restrict this access.

1. 10 free firewall software is most worthwhile

8. Do not use the administrator account daily

Users often use the main account on the computer with administrative rights to facilitate the operation, but this job can be exploited by Ransomware to damage the computer. Therefore, when used daily, you should use a guest account to restrict administrative rights, prevent software installation, etc.

With this 'preventative' approach, you can prevent all types of malware and Ransomware from being installed on your system. When you want to install the software or update the operating system, you should log out, switch to the administrator account and install or update.

9. Turn off Macros in Microsoft Office

There is another way malware used to attack Windows users is through Microsoft Office. Although this office suite is quite secure, macros (especially in Microsoft Excel) do not.

Although this macro feature is disabled by default, you should still check to make sure it is safe. To turn off the macro feature, go to **File> Options> Trust Center> Trust Center Settings** . In the **Macro Settings** , select **Disable all macros except digitally signed macros** .

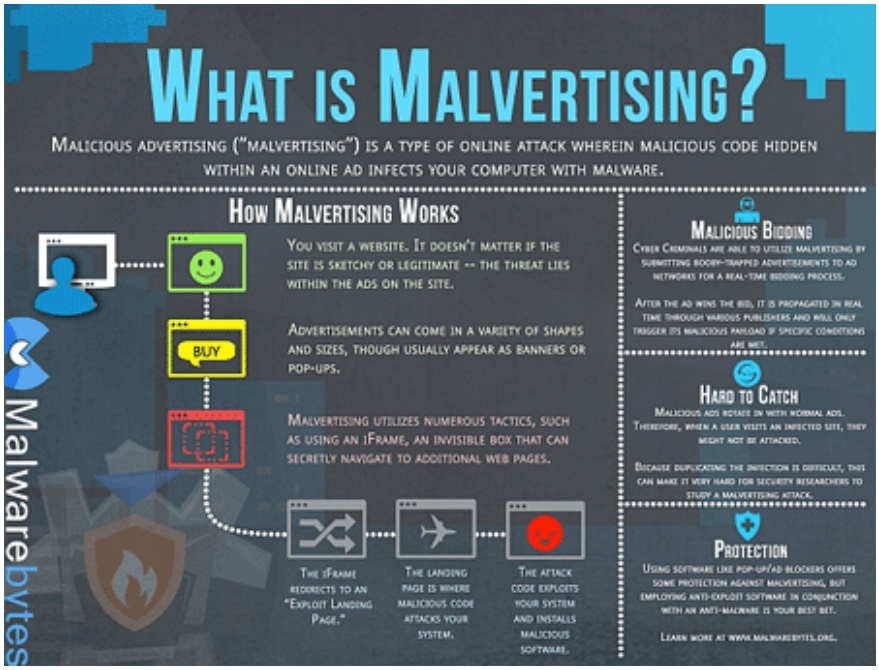
1. How to turn on / off Macro in Word

10. Set browser security, check for updates and remove unsafe extensions

If you don't regularly update your browser or extension, the risk of computer infection with Ransomware is quite high. This is not a problem for browsers such as Google Chrome, Mozilla Firefox and Microsoft Edge because they are updated automatically, but on other browsers you should keep up-to-date.

For plugins or extensions, you should also update them regularly or uninstall unnecessary utilities. In addition, you should disable Adobe Flash and reactivate if requested.

11. Avoid malicious ads



Ransomware is hidden in malicious ads, so you need to stay away from certain websites. These websites often provide download files or download links to illegal documents containing malicious ads.

Therefore, you need to be careful when accessing these websites. Although you can use ad blocking tools, there are sites that offer free content depending on your ads to maintain your site so you should look for other options to control how ads show up. Marketing.

Refer to some of the following articles:

1. 7 kinds of ransomware you didn't expect
2. Summary of effective Anti-Ransomware software
3. How many types of malware do you know and how to prevent them?

Good luck!

You finished reading the article "**If you don't want to be a victim of Ransomware, read this article**" 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.

© 2019 TipsMake.com