7 steps to make Windows operating system safer

Whenever in a state of insecurity, there will be a warning: the computer is being compromised through services that have not been patched and cannot control these services.

***TipsMake.com* - A computer capable of working independently usually does not require all network services provided by Windows, such as web browsers or file sharing services, printer sharing.** However, these things still happen even if you don't pay attention. Whenever in a state of insecurity, there will be a warning: the computer is being compromised through services that have not been patched and cannot control these services. Important data on your computer (such as a password or credit card number) may leak out through the Internet with previously installed backdoors without your knowledge. So why not turn off these services? This is a good idea, so: make your Windows operating system safer.

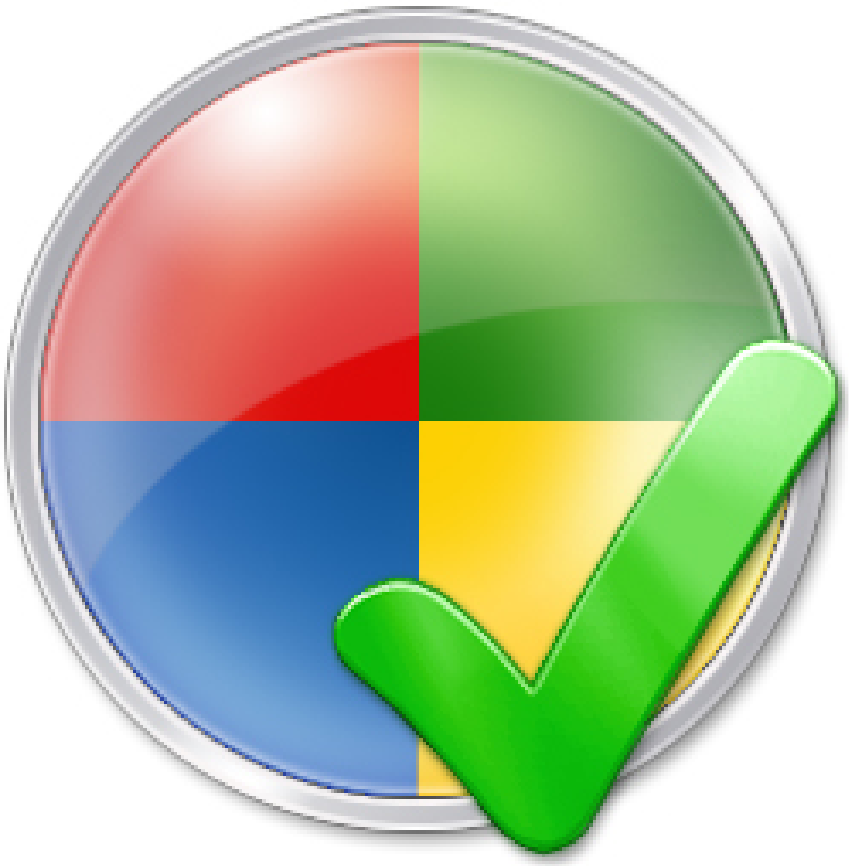
Step 1: Do not work with an administrator account (*Applies to Windows 7, Vista, XP, 2003, 2000, NT*)

With Windows 7, working with standard accounts has become more convenient than ever. There is no reason for not working with restricted rights which has made a big jump in computer security. The way Microsoft uses it to

keep computers secure, balance functionality by integrating User Account Control (UAC), one of the Windows 7 utilities provided. However, created UAC is not to replace the idea of ??account restriction. Basically, the NTFS file system is responsible for protecting files and folders from unauthorized access and changes. This will help the operating system and running programs avoid many viruses, Trojans, spyware, malware, dialers and some other malicious software that could harm your computer in many ways. Your profile may also be compromised, but this does not happen with the basic Windows 7 operating system. Even if your profile is hacked, all photos, MP3 files or data are available. Can be restored easily by logging in with another account, the account has not been hacked.

Start: **Start -> Control Panel -> User Accounts and Family Safety -> User Accounts -> Change your account type**

Step 2: Always update the operating system with Windows Update (*Applies to Windows 7, Vista, XP, 2000*)



Since security issues are discovered daily and monthly, it's important to keep your Windows operating system up to date. Microsoft often provides updates and updates for Windows. These updates are given at least once a month, or even shorter, whenever a serious problem requires immediate action. And really, it's easy to keep safe.

Let Windows automatically check for security updates. With Windows 7, you'll have to install - make sure this feature is turned on:

How to do it: **Start -> Control Panel -> System and Security -> Windows Update -> Change settings**

1. Important update: immediate update settings (recommended)

2. Select a date / time when you want to install these updates

If you prefer to check for yourself and download security updates for Windows. Just follow these steps: **Start -> Control Panel -> System and Security -> Windows Update -> Check for updates.**

1. Wait until Windows finishes checking for updates

2. Next, view and check the updates you want, at least important updates

3. Finally, click " **Install Updates** "

Alternatively, you can select Microsoft Update to receive updates for not only Windows but also MS Office and other products.

How to do it: go to https://www.update.microsoft.com/microsoftupdate/

1. Agree to the terms in the **Terms of Use** for Microsoft updates and then select Next

2. On the next page, select " **Install important updates only** "

3. Finally, click " **Install** " to finish.

Step 3: Install Windows Services and turn off File Sharing (*Applies to Windows 7, Vista, XP, 2003, 2000, NT*)

The standard Windows Services configuration can be a difficult challenge. The more important thing is to pay attention to what is happening on the operating system. Are there services you do not need or these services can harm your computer by paving the way for worms of computers, Trojans and other malware along with untrusted programs? In the past, some services from Microsoft are known for their 'ability' to contain vulnerabilities that could make your computer vulnerable. So, check the details to be able to configure the services properly.

How to do it: **Start -> Control Panel -> System and Security -> Administrative Tools -> Services.**

Step 4: Use Web and Mail with Confidence (*Applies to Windows 7, Vista, XP, 2003, 2000, NT*)

Whenever you access the web, you always risk accidentally "sticking" to malicious software that you really don't want or don't know about it. Choosing a secure web browser can prevent you from becoming a victim of computer, malware or other attacks of malicious software. In the past, Microsoft's Internet Explorer has been affected by a lot of security-targeted attacks, but we can see very few actions taken to fix security holes. Currently, to avoid this problem, we would like to introduce some popular Web browsers and email accounts with greater security.

• Recommended web browser should use:

o Mozilla Firefox

o Opera

Choose which web browser does not matter, it is important to keep up to date!

Step 5: Turn on Windows Firewall (*Applies to Windows 7, Vista, XP*)

With Windows 7, you can get everything you need. Built-in firewall of this operating system is a shield that helps protect against Internet attacks. This utility blocks all internal requests and searches for a target that could easily harm a computer or hijack. These goals could be very vulnerable to exploits by malicious software. Make sure your firewall is turned on. There is no need to run any other firewall software. Because they cannot upgrade the security of your system like Windows 7's built-in firewall. Your remaining task is simple, install this built-in firewall accordingly.

How to check firewall settings: **Start -> Control Panel -> System and Security -> Sidebar: Turn Windows Firewall on / off (turn on / off Windows Firewall).**

• Settings for home or office network (personal):

o Select " **Turn on Windows Firewall"**

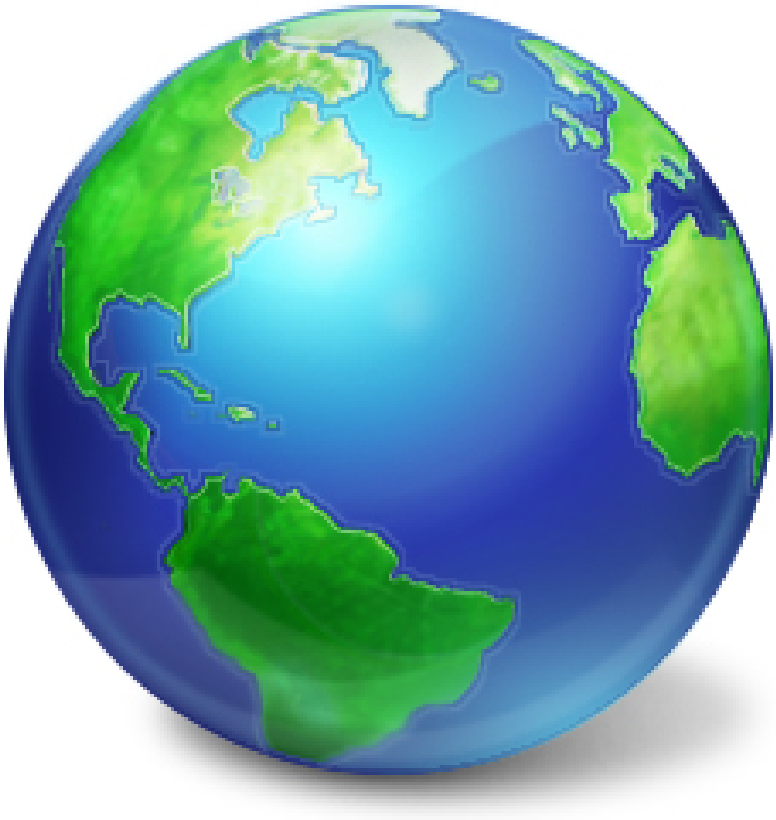
o Remove traces of all other options

• Settings for public networks:

o Select " **Turn on Windows Firewall** "

o Remove traces of all other options.

Step 6: Check Network Locations (*Applied in Windows 7 and Vista*)



Choosing the right location settings for your network connection may help somewhat in upgrading computer security. For example, Windows allows some ports to connect if you notice that you are using the Home Network. When connecting to a public network (library, Internet café or airport), make sure you select Public Network and allow Windows to hide all external ports by filtering them out.

To check your location settings: **Start -> Control Panel -> Network and Internet -> Network and Sharing Center**

Basically, Windows 7 knows three different types of locations:

• **Home Network** : If all computers use the same home network, and you know all these computers and this is called a reliable network.

• **Work Network** : For individual users, this setting is less common. It is similar to the Home Network but there are some additional services that the corporate network requires.

• **Public Network** : If you don't know much about your computer, you are using an unreliable public network and in this case use Public Network and choose one of the following locations. :

o In the restaurant

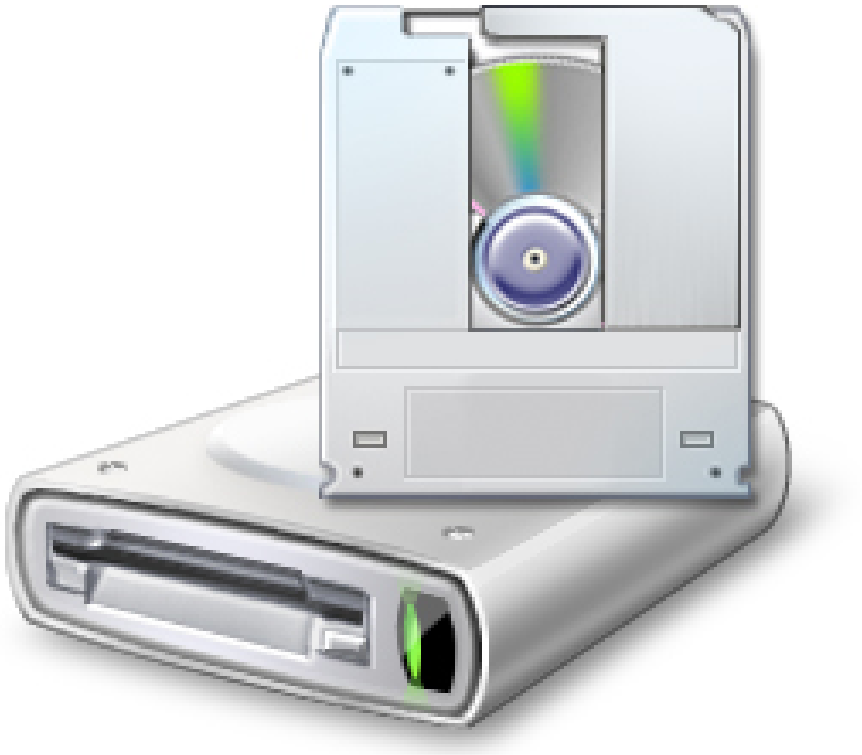
o In the café

o At the airport

o Using the telephone network

Just follow these basic, simple steps and experience surfing the web much faster.

Step 7: Backup data (*Applies to Windows 7, Vista, XP, 2003, 2000, NT*)



Desktop and laptop computers are vulnerable to attack, system files face damage, data loss or hard drive failure - these can happen anytime and anywhere. wherever we don't, we don't want to. Today, people use smartphones more, and the same things can happen with your data. Creating a backup (your data, photos, music files .) at least once a month can significantly reduce the risk of data loss. Along with the right strategy, failure or financial loss is no longer a problem for you.

• Applications that help create backups:

o **Backup and Restore** : Windows 7 provides tools for creating backups of files and folders, as well as creating backups for the entire system.

How to do it: **Start -> Control Panel -> System and Security -> Backup and Restore**

o **Acronis True Image** (paid app): A reliable solution that helps you create a backup copy of your entire hard drive and back up a lot of files and folders. In the event of losing all the data, you can use the application's bootable DVD to recover all lost data.

• Create data backup strategy:

o **Backup what** ? You can save single data (file system level) or create a backup of the entire hard drive system (partition level).

o **Where to backup** ? One place has enough space to store backups of your data such as: hard drive (the fastest and easy to use), online hard drive (difficult to use in emergencies), DVD-RAM (Very reliable but expensive in reducing capacity).

o **When to backup** ? Save your system at real time whenever: daily, once a week or at least once a month.

o **Full, incremental or differential** ? Full backup - full backup - will save all your data but will take up a lot of disk space. Incremental backup - backs up only the changed data from the last backup - saves any new files or new files that have been changed from the last backup. Differential backup - partial backup - helps you save new files or be changed since the last complete backup.

o **How long should a backup be kept** ? There is no general answer to this question. However, we recommend that you keep at least 3 backups or create a new backup at least once a month.

Also, remember to check the backups after creation and later.

The reason why you don't need to use a personal Firewall

1. First, a firewall is known as part of a security concept, applied to computers and networks. This is not a software for you to install, feel secure.

To protect your computer within a network, the first thing you need is a concept that can answer questions like:

o What to protect?

o Which "invaders" need to be on guard?

o What service / user is allowed to connect to the outside?

o How much will these safeguards cost - and is it worth it?

Those are the basics of firewalls. No matter what anyone tells you, just remember: a firewall is a concept, not a software.

2. A firewall running on an operating system needs to be protected, this is not meaningful in most cases.

This is a firewall's task to keep harmful data packets out of the server. Other vulnerable vulnerabilities, which require extra protection, are still surpassed before the firewall can do anything against it. At the same time installing the extra software code (such as a Desktop Firewall) on the server, you should increase their complexity along with increasing vulnerability to vulnerabilities and vulnerabilities.

3. Any additional software can evaluate the vulnerability of a system along with the vulnerability of this system.

No software has no errors and these errors exist with existing software. This means that the total number of

errors of a system is a big security issue. With an extra software installed, the complexity of the system is enhanced and since then, security issues will be less worrisome.

4. Desktop Firewalls make the users feel secure that they are now safe. This fake type of security makes users tend to be less vigilant about the security of the computer they are using. This is known as 'risk compensation'.

Everyone knows that many people often click on attachments without thinking or suspicious. When asked if these software can contain malicious code with computer viruses hidden inside, they often answer: Why bother with that? I have installed Desktop Firewall and antivirus software. They will protect my computer! ' Really, this is not true at least from now on you should be wary of this.

5. The Firewalls desktop can be bypassed or turned off very easily, but users are not aware of this.

Security software often asks users what to do:

o First, many users will respond with Yes or Allow, with the aim of continuing to surf the web or not wanting to be bothered while playing something - no matter what they have done. This is really dangerous!

o Second, these interactive conversation windows appear from Desktop Firewall not only users click on. Malware software can do these things for you when changing rules according to them. This happens so quickly that you cannot notice what is happening. They can do this because most of the time, Desktop Firewall has the same rights as users.

o Finally, Desktop Firewall often comes with bad software. Whenever the Desktop Firewall interacts with the user, there will be a link between high and low levels of privilege and malicious software will take advantage of this to harm the system.