PC Security Handbook

2nd Edition

Defensive Computing Techniques to Help You
Avoid Malware and Data Loss

Windows Guides

Rich Robinson — Microsoft MVP — http://mintywhite.com

About the Author

Rich Robinson is the author and creator of Windows Guides, Windows Forums, and MyWindowsPC. Rich is a Microsoft MVP in the Desktop Experience category and authored Windows 7 –The Pocket Guide, Windows Vista – The Pocket Guide, Windows Vista – Customization Manual, and the PC Maintenance Handbook. He also co-authored the Windows 7 Media Center Customization Handbook. His hobbies include spending time with family, road biking, web design, programming, running, soccer, skiing, and swimming.

See more books Rich authored.

Contents

Introduction

This handbook is designed to help you find ways to protect your Windows XP/Vista/7 PC and ensure your data is safe. I get countless emails from site visitors who ask about the best anti-virus software, firewall program, backup utilities etc. and there are often questions like this in the forums.

I set up PCs for companies, friends, and family; the advice I give in this manual is what I use when building any PC. My tips are tried and tested and have left hundreds of people satisfied with the way their computer works. I hope you too can follow these instructions and enjoy an error-free, spyware-free, and speedy PC.

In this second edition of the book, a lot more detail is given on keeping your computer up to date, avoiding malware, and protecting your data. For full details on what's new, go here.

The purpose of this book is not to define the ultimate solution; its purpose is to give you simple, unbiased advice on what I've found to be the best options out there. In this handbook, I only give advice and share programs that I've used for at least a year. Some programs seem good when you first use them, but quickly annoy you or slow down your PC.

If you have any questions about PC security or PCs in general, you can head to Windows Forums where you'll find friendly, knowledgeable members who are happy to assist in your learning. If you disagree with anything in this handbook, please join us also and share your solutions.

Notational Conventions

In this handbook, I have used these notational conventions:

Italic: Text from the current dialogue you are working with.

Bold: the name of a keyboard key.

Italic bold: something you type as shown, e.g., ***regedit***. Unless otherwise specified, you can use uppercase or lowercase letter.

Click: move the cursor to the referenced item and press the left mouse button.

Press: push on a keyboard key.

Select: choose from a list.

Blue Links: Links to external websites.

Teal Links: Links to Windows Guides and Windows Forums.

Green Links: Links to other sections within this book.

Security 101

Many terms in this handbook may be new to you; I make every effort to explain things in a simple manner that is easy to digest. Before we begin with solutions, I present some key terms and phrases that will assist you as you work your way through the rest of this handbook. These phrases are commonly thrown out in conversation and in online discussion forums, but it's hard to know exactly what they mean.

Adware – Like spyware, adware is software that may track visited websites and act as a key logger. Adware tracks this

information to automatically display downloaded or installed adverts to a user. You may wonder why you are being offered "PC Super Anti Spyware 2011" when using your PC; this is adware at work. AIM, FlashGet, Deamon Tools, and RealPlayer are all examples of adware.

Antimalware / Antivirus / Antispyware - Software designed to remove or block malware (e.g. AVG Internet Security and ESET Smart Security.)

Backdoor - A backdoor is a point of access to a computer that does not require authentication. An unlocked house back door gives access to an otherwise secure home; a computer backdoor allows access to your PC without your knowledge or permission.

Crimeware – This is a class of malware used to facilitate cybercrime by using social engineering etc. to aid in identity theft. This type of malware steals private data, which is used to defraud a person of their personal belongings. Examples of crimeware are: key loggers, used to collect sensitive data, password stealers, and browser redirects to pages that look like banking, social networking etc. pages that send login information to identity thieves.

Cybercrime – Also known as *computer crime*, cybercrime refers to any crime that involves a networked (e.g. connected to the internet) computer. An example of cybercrime is the use of crimeware to steal personal information for identity theft.

Defensive Computing – Reducing security risks when using your computer by taking precautions to avoid security attacks and avoid data loss. This book is a tool to help you practice defensive computing.

Firewall – A firewall both permits and blocks access to a network or PC. Firewalls are included with popular security software (e.g. ESET Smart Security) and a basic firewall comes bundled with Windows XP, Vista, and 7. Firewalls limit communication between your PC and devices that are not authorized to communicate with you.

Key logger – Key loggers are used to monitor keyboard activity on a PC. These can be software-based (bundled with Trojan horses, adware, and spyware) or hardware-based (between the keyboard cable and the PC, acoustic etc.) Usually this information is retrieved across a local network, the internet, or from the physical device connected to the keyboard.

Identity Theft – The act of someone pretending to be someone else by using another person's identity. Usually identity theft is used to obtain credit or other benefits in another person's name. Identity theft is a big problem online as so much information is readily available.

Malware – The generic term used for all forms of software designed with malicious intent. Viruses, worms, spyware etc. are all forms of malware. The term *virus* is often used when malware should really be used as it describes all forms of malicious software.

Privacy-invasive software – A formal term used to describe software that invades your privacy. This software comes in different forms including spyware and adware.

Real-time Scanning – Good antimalware programs scan files in real time; as you download, copy, and install files on to your computer, your antimalware program will scan these files for infections and malicious code. You should only have one real-time scanner installed at any time—otherwise they will conflict as they compete to scan the same files.

Rootkit – Can be either hardware or software used to gain administrative (root) control over a computer without detection. Rootkits target the BIOS, hypervisor, kernel, or boot loader. A rootkit is used to provide a hacker will full access, via a backdoor, to a machine. They are also used in legitimate software for emulation and security to add functionality or protect themselves from being closed while running your operating system.

Social Engineering – Do you ever get chain emails asking you things like: what's your favorite color? What's your mother's maiden name? What school did you go to? In what city were you born? Most of us have sent these emails out and, for the most part, they are harmless. However, social engineering is just this: getting people to divulge confidential information. Giving out your town of birth may not seem that confidential, but what if that's the security question on your email account? What if your email account contains a welcome email, with your password, from a social networking site? What if you used the same password for your online bank? Social engineering can also be used on the phone, which is outside the scope of this book. Just remember, never give out personal information unless you initiate the conversation and even then – be careful.

Spam – The use of electronic messaging (e.g. email, instant messaging, spam blogs, forum spam etc.) to send unsolicited messages. Spam is solicitation without prior consent. Spam can lead to fraud, identity theft, and more.

Spyware – Spyware tracks a user's activity by monitoring browsing habits and keyboard activity and can even take screenshots while you use your PC. This information is sent back to the creator or beneficiary of the spyware. Signs of spyware include: modified browser homepages, slow internet, and suspicious looking sites in place of legitimate sites (for example: banking sites.)

Trojan horse (Trojan) - A Trojan horse is a seemingly harmless program that looks to provide value. However, just as in Greek mythology, a Trojan horse has a secret agenda and acts as a backdoor to your computer. This backdoor can be accessed by a hacker to compromise your PC. Trojan horses are not self-replicating and spread due to users installing them manually on their PC.

Virus – A computer virus acts very much like a human virus. Human viruses are spread, via thumb drives, floppy discs, network connections etc., to other PCs. Viruses need a host (like a free screensaver program) to spread. By pure definition: a virus has the ability to spread itself, via a host, to other computers.

Virus Hoax – A virus hoax is a message (e.g. email, forum post) that alerts the reader of a non-existent virus and usually contains outrageous claims like "if you don't send this on, a kitten will cry every time you hear the word 'oblong'" (okay, I made that one up.) Often, these claims are falsely backed up by CNN, Microsoft etc. If CNN really broadcast this message, it wouldn't be in email form. Please don't forward these emails and do encourage others to do the same.

These hoaxes can do great harm and have been known to advise you to search for important system files and delete them.

Windows Firewall – Comes bundled with Windows XP, Vista, and 7. This is a great solution; however, due to a lack of comprehensive definition updates, Windows Firewall is not completely effective in blocking threats and allowing safe connections.

Worm – A worm is much like a virus. The key difference is worms can spread between PCs without a host (free screensaver program, downloaded game etc.) These programs rely on computer networks and usually damage files and slow down networks in their path.

Now you have your jargon set straight, you'll learn how to avoid malware, some specific steps to ensure you are protected, and how to protect your files from data loss.

Defensive Computing

The subtitle of this book is *Defensive Computing Techniques to Help You Avoid Malware and Data Loss*. To reiterate the definition, from security 101, of defensive computing is:

> Reducing security risks when using your computer by taking precautions to avoid security attacks and avoid data loss.

To help you practice defensive computing, this book covers:

- How to avoid malware.
- How to protect your data.

How to Avoid Malware

This book shows you how to do the following to protect your PC from malware:

- Keep your operating system up to date.
- Keep your browser and Flash up to date.
- Keep installed software up to date.
- Use Windows Firewall.
- Install good antimalware.
- Download free software only from sites you know and trust.
- Test suspicious software in a virtual environment.

Other ways you can protect yourself that are not covered in this book:

- Don't forward emails that contain virus hoaxes that make outrageous claims like "this virus will communicate with your car and unlock it when you get near a thief's house" – we've all seen *those* emails. Please don't forward them. If an email asks you to search for and delete a "virus" file, it's probably an important system file that should not be deleted.
- Avoid clicking links inside pop-up windows.
- If you are offered antimalware programs while browsing, don't install them. Stick with the software I outline in this handbook.

By following these rules, you'll protect yourself and decrease the chances of getting malware on your system. The rest of this handbook will show you how to apply the first four tips listed above.

Keep Your Operating System up to Date

To keep Windows up to date, Microsoft uses Windows Update. Windows Update should run automatically on your PC. However, you should check if your PC is up to date. To check for Windows updates:

1. Click *Start*, *Run*, and type:

a. Windows XP: ***wupdmgr***
b. Windows Vista/7: ***wuapp***

2. Press **Enter**.
3. Click *Install Updates*.

You may need to download the Windows Genuine Advantage (WGA) tool, which checks to see if your copy of Windows is genuine.

Windows may need to reboot your machine several times as new updates are installed.

Your computer is now up to date.

If you are having problems with Windows Update, you should resolve the issue as soon as possible; many of the updates are security related and will protect you from vulnerabilities. Windows Guides writer, Angel Luis, has written the following guide to help you troubleshoot Windows Update problems: Windows update troubleshooting.

Keep Your Browser and Flash up to Date

Browsers are a common source of computer vulnerabilities because they use so many plugins and programs that create loop holes that malware can exploit.

You should, above all else, keep Adobe Flash up to date. Flash is notorious for security vulnerabilities and, because it's so widely used, possibly more so than Windows (because it works on other platforms), is a target for malware creators.

Adobe Flash

To update Adobe Flash:

Keeping Adobe Flash up to date can be tedious, but I highly recommend it. There are several ways you can do this. This guide shows you two ways:

1. Download it from the Adobe Flash Player website.
2. Use a tool like FileHippo to keep it updated.

For option 1, you can get the latest version of flash here.

Note: if you use Internet Explorer and another browser, you will need to go to this site in both browsers to get the Adobe Flash Active X update also.

For option 2, see the section on Keep Installed Software up to Date.

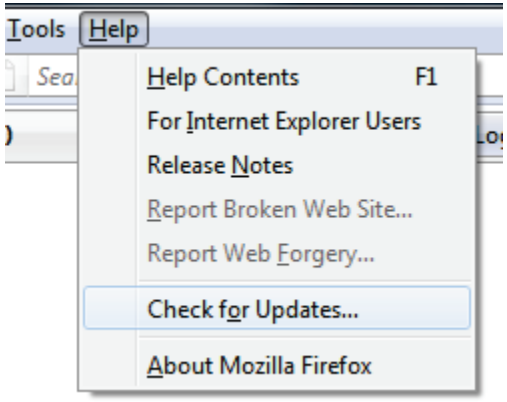
Internet Explorer

If you are using Internet Explorer (IE) as your browser, use Windows Update—explained above—to keep it up to date.

Mozilla Firefox

To check for updates for Mozilla Firefox:

1. Open Firefox.
2. Click *Help > Check for Updates*.



3. If updates are available, follow the on-screen instructions.

Google Chrome

To check for updates for Google Chrome:

1. Open Google Chrome.
2. Click the Tools menu.

3. Click *About Google Chrome*.
4. If an update is available, click the *Update* button.

When you restart Google Chrome, you will have the latest version running.

Safari

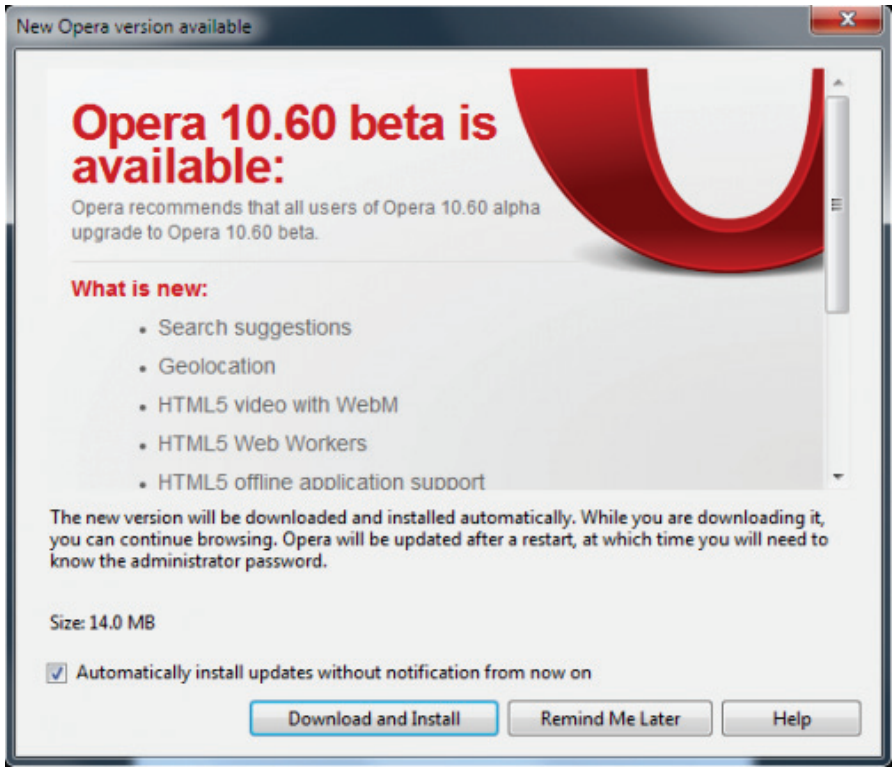
When you install Safari, you are given the option to "Let

1. Click the *Start* button and:
   a. Windows XP: Click *All Programs*, click *Apple Software Update > Apple Software Update*. Windows Vista/7: Type ***apple*** and click *Apple Software Update*.
2. If an update is available for Safari, you can check the button and click *Install 1 Item*.

You can also download the latest version of Safari here.

Opera Web Browser

Opera pushes updates automatically:



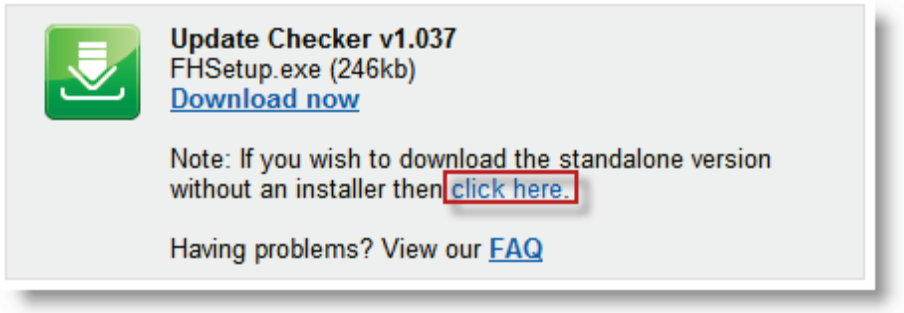
To update Opera manually:

1. Open Opera.
2. Click *Help > Check for Updates*.
3. If a new version is available, you will see an alert and an option to upgrade.

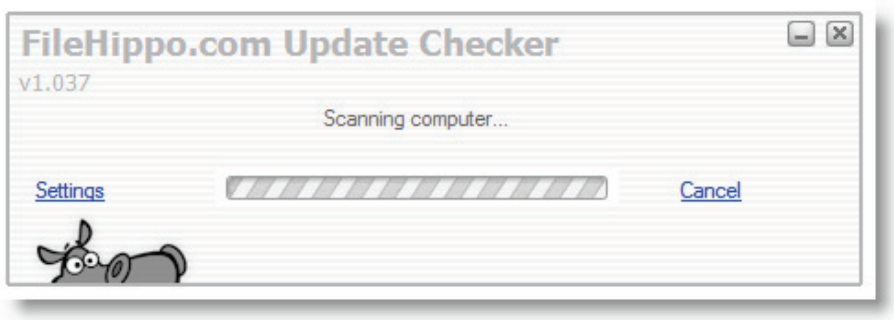
Keep Installed Software up to Date

Now that you're keeping Flash and your browser up to date, you should also consider keeping other software updated. As software ages, more and more security and performance holes are found; these holes leave you vulnerable to all kinds of nastiness like viruses, computer slowdowns, and just looking rather old fashioned. Many programs come with software updaters, but I find these slow your computer down and rear themselves at the most inconvenient times (like at startup) so I tend to disable or opt out of software checking for updates.

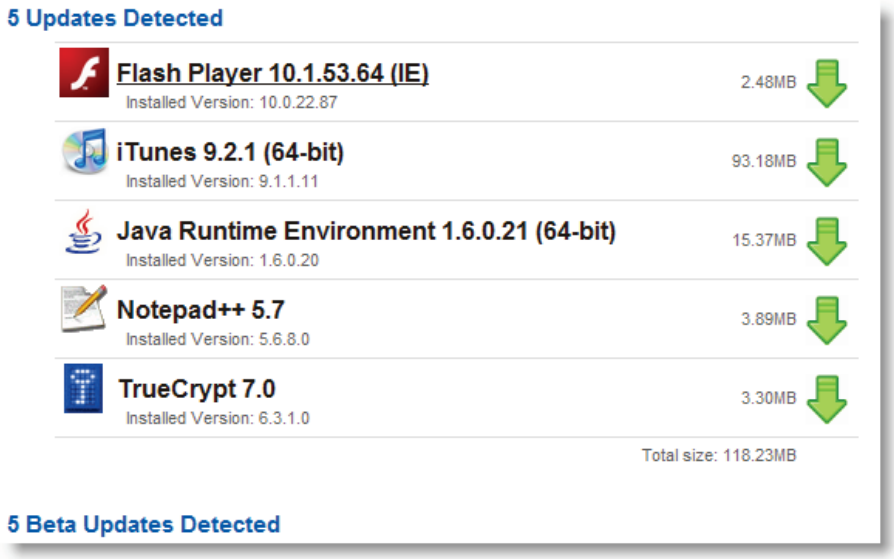
FileHippo Update Checker overcomes this problem by checking to ensure you have the latest version of all installed software on your PC. You can even run the program as a standalone app (download the standalone version from the download page):



The program scans your installed programs and retrieves version numbers to check against the latest updates in their database:



I like to keep my software updated (although I often wait a week or so before upgrading to ensure there are no bugs etc. in the latest version); as you can see, I have five updates available and five beta updates.



I've been using this program to check for updates for over a year now and have never had problems with any of the software downloads they provide. This is a solid piece of software and I highly recommend you download it.

Download FileHippo Update Checker.

Keep Security Software up to Date

If you don't want to keep every program up to date (maybe you have a slow internet connection and don't want to spend too much time downloading every update), I highly recommend you keep your security software up to date.

Windows Guides writer, Taylor Ling, teaches you how to use a simple program, called SSDownloader, to keep your security software up to date: Automatically download the latest security software with SSDownloader.

If you don't have good security software or you don't know which one to pick, you can find suggestions in the next section.

Use Windows Firewall

To reiterate the definition of a Firewall:

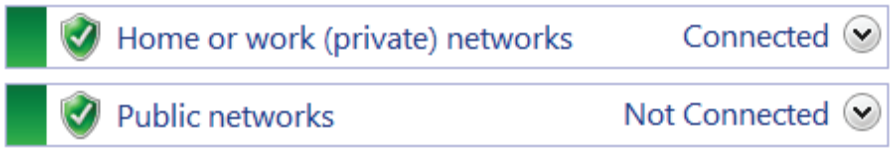
> A firewall both permits and blocks access to a network or PC. Firewalls are included with popular security software (e.g. ESET Smart Security) and a basic firewall comes bundled with Windows XP, Vista, and 7. Firewalls limit communication between your PC and devices that are not authorized to communicate with you.

At the very least, you should have Windows Firewall running—always. If you feel the need to run another firewall, go for it (ESET Smart Security comes with a really good firewall.)

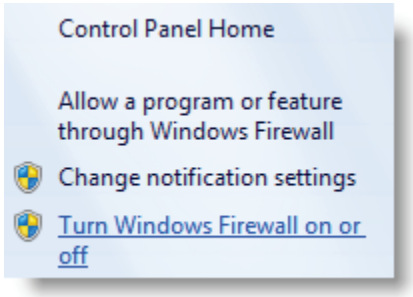
To make sure Windows Firewall is running:

Windows 7:

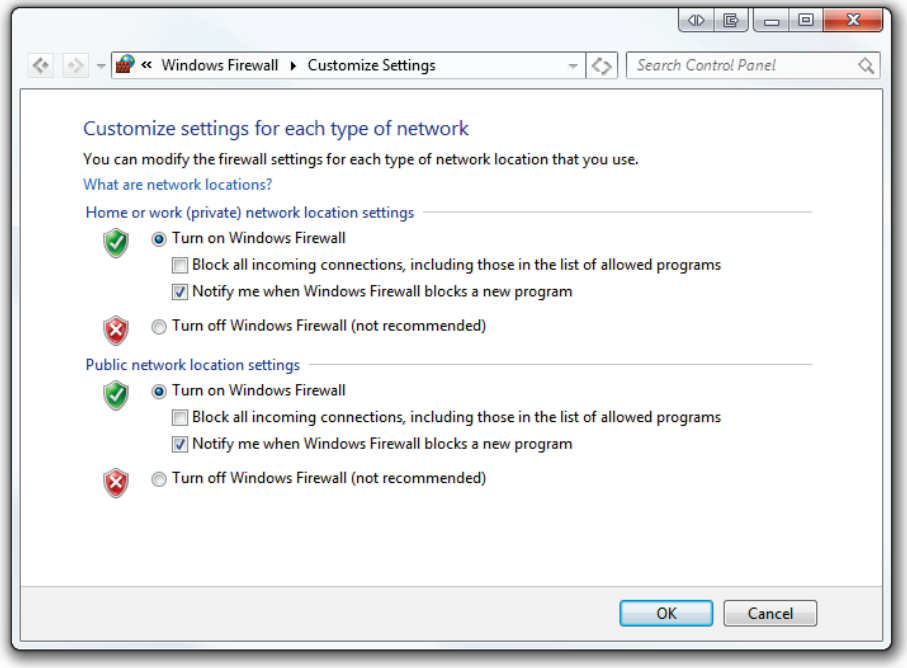
1. Click the *Start* button, type ***firewall*** and click *Check firewall status*.
2. If you see all Green, like in the screenshot below, you are in good shape. If you do not see all green, go to step 3.



3. In the left-hand menu, click *Turn Windows Firewall on or off*.

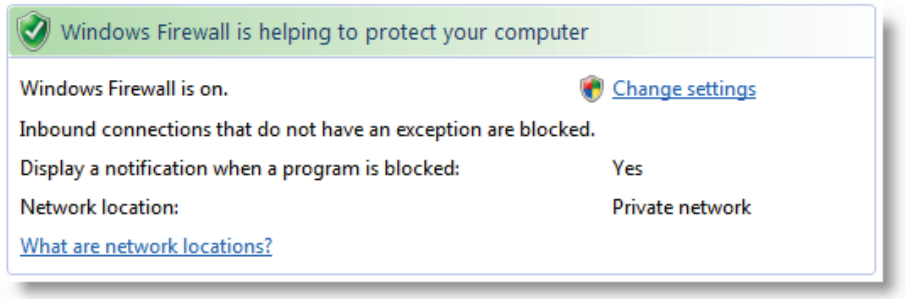


4. Select *Turn on Windows Firewall* for both Home or work (private) and Public networks:

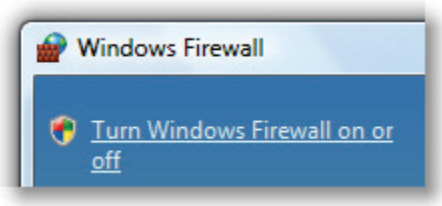


Windows Vista:

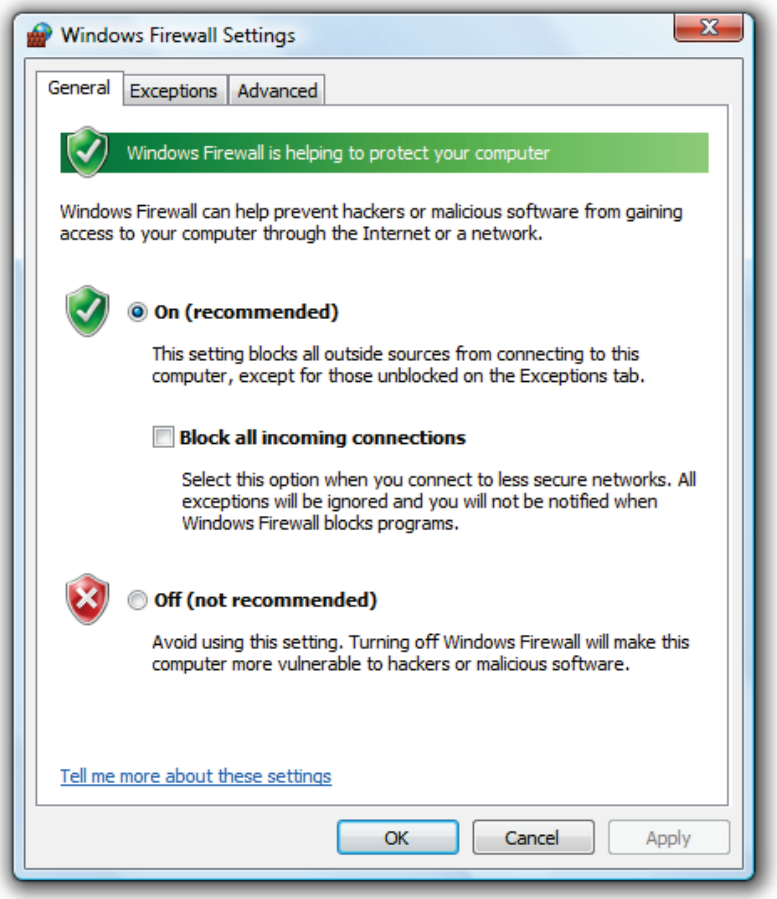
1. Click the *Start* button, type ***firewall***, and click *Windows Firewall*.
2. Ensure you see the following message: *Windows Firewall is helping to protect your computer*. If you don't move to step 3.



3. Click *Turn Windows Firewall on or off*.

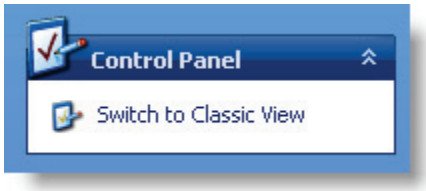


4. If prompted, click *Continue*.
5. Select *On (recommended)* and click *OK*.



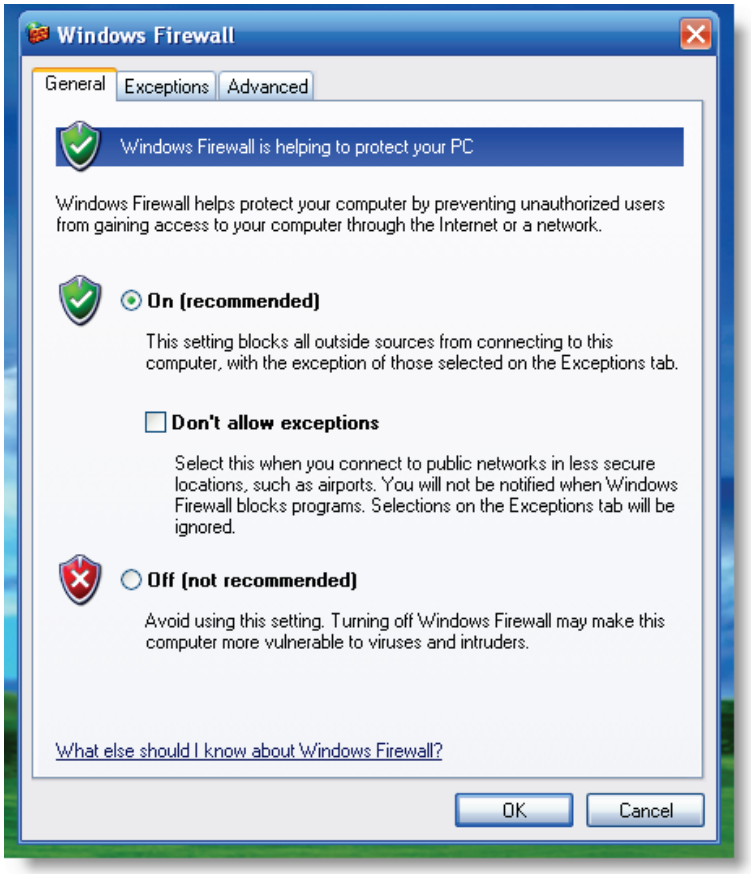
Windows XP:

1. Click the *Start* button and click *Control Panel*.
2. Click *Switch to Classic View*.



3. Double click *Windows Firewall*.

4. Select *On* (if it's not already) and click *OK*.



Install Good Antimalware

In this section, I recommend antimalware software that I've used for years. I highly recommend these programs and am confident they will protect your PC and minimize system slowdowns, which are an all-too-common side effect of security software.

The two programs I recommend are Microsoft Security Essentials and ESET Smart Security. The former program is free to all owners of a genuine copy of Windows; the latter is a paid program. I recommend either of the two different programs because they will both provide the level of protection you need, not bog down your computer, and the latter is reasonably priced. You should give both programs a try if you are unsure which one to use. However, don't install both programs because the real-time scanners on both of these programs will conflict.

If you are currently using different antimalware, you may encounter problems uninstalling it. If you want to completely uninstall antimalware from your computer, you can download the uninstall program for it here. The guide lists uninstall programs for:

- Avast!
- AVG
- Bitdefender
- F-Secure
- Kaspesky
- McAffee
- Norton
- Panda Antivirus

Microsoft Security Essentials

Microsoft Security Essentials (MSE) is a free program from Microsoft that is available to all users of a genuine copy of Windows. This software is great and, in this section, I'll cover the following:

- Where to download MSE.
- How to configure MSE correctly.
- How to run a full scan with MSE.

- Advanced tips for MSE.

Where to Download MSE

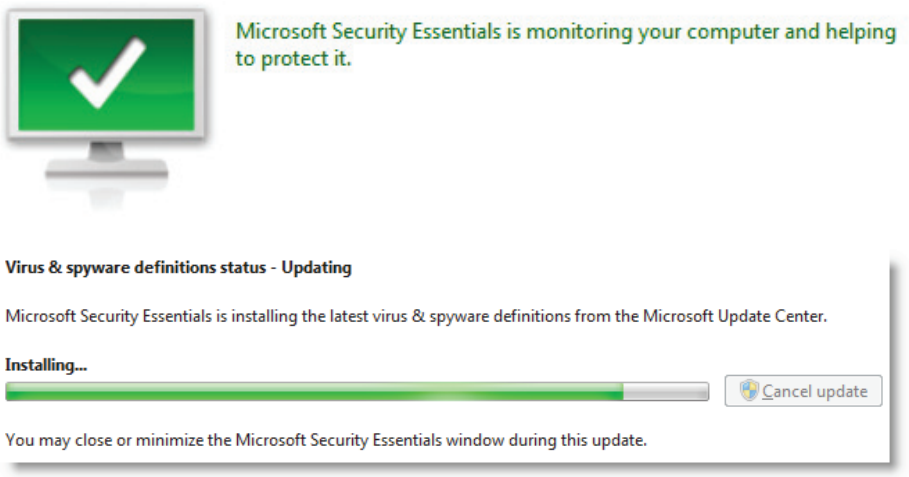
You can download MSE here. If you'd like to try the latest beta, you can download the Beta here.

How to Configure MSE Correctly

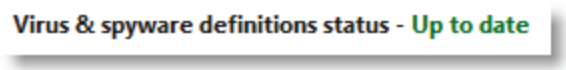
This section covers the basic configuration of MSE and explains what the settings mean and, in some cases, what the optimal settings are.

To get started, open MSE by double clicking on the MSE icon in the system tray.

Under the *Update* tab, click *Update* (if available.) MSE will now get the latest virus definitions so you are up to date with your protection:

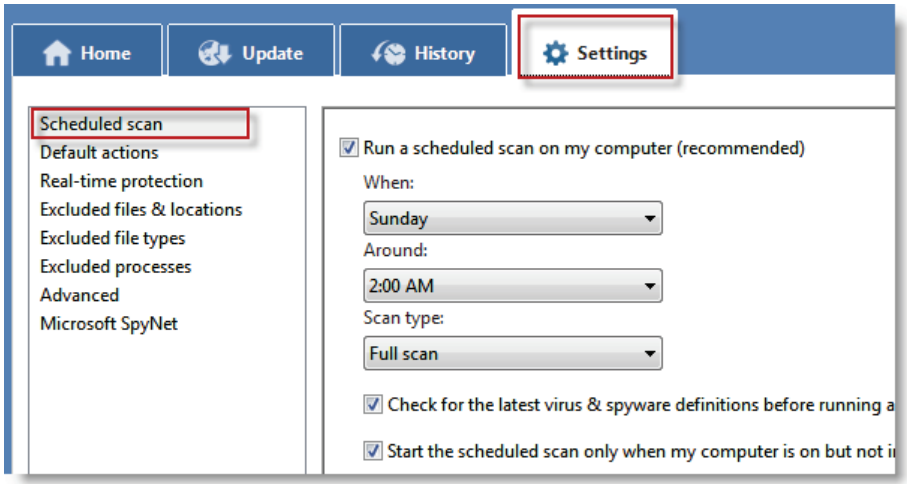


Once downloaded, you should see the following message on the *Home* tab:

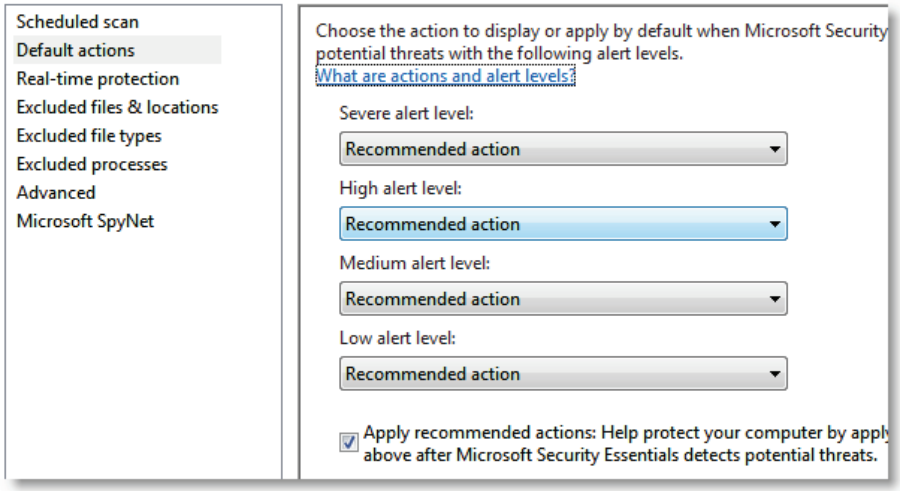


Now click the Settings tab and click *Scheduled scan*. You should run a scheduled scan by *selecting Run a scheduled scan on my computer* and picking a time when your computer is turned on but you are not using it. I have my scan run on my desktop at 2AM every Sunday. I also recommend you run a *Full scan* on this schedule.

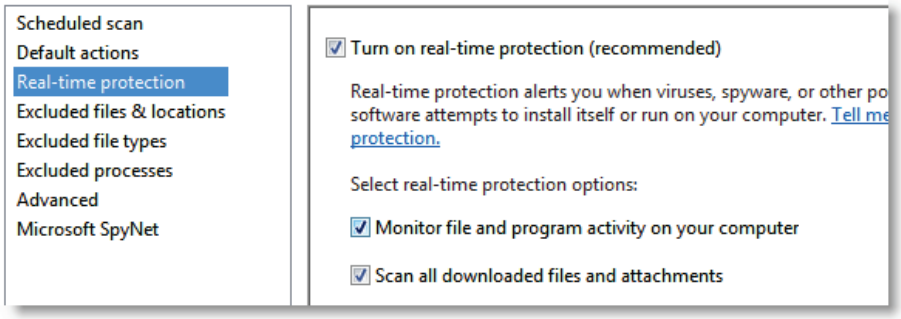
Also, be sure to check *Check for the latest spyware definitions before running a scheduled scan* and *check Start the scheduled scan only when my computer is on but not in use*. The first of the two options will make sure you have the latest definitions and the second option will ensure that if you happen to be on your PC during the scheduled time, MSE won't start the scan (as you will probably notice slowdowns during the scan.)



Now click *Default actions*. I choose *Recommended action* for all four alert levels. If you'd like to learn more about actions and alert levels, go here.



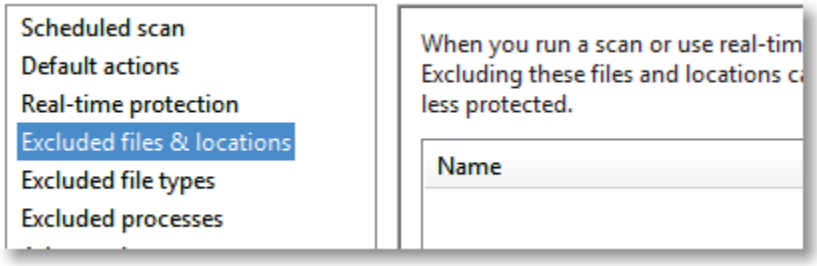
Click *Real-time protection*. I highly recommend you use real-time protection, which monitors files as they appear on your PC (i.e. internet downloads, thumb drives etc.) Learn more about real-time protection here.



Click *Excluded files & locations*. Here you can specify files, folders, or drives where MSE should not scan. Possible exclusions could include:

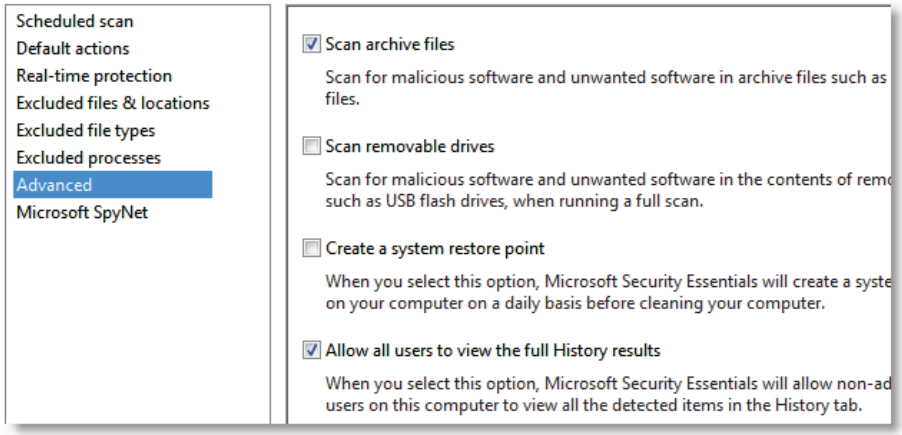
- Network drives monitored by other PC's virus checking utilities.
- Files, folders, and drives that are read-only (thus, they don't change and should not pose a threat.)
- Folders you are absolutely sure are safe and are not modified.

Personally, I recommend you leave this screen blank unless you have a good reason not to.

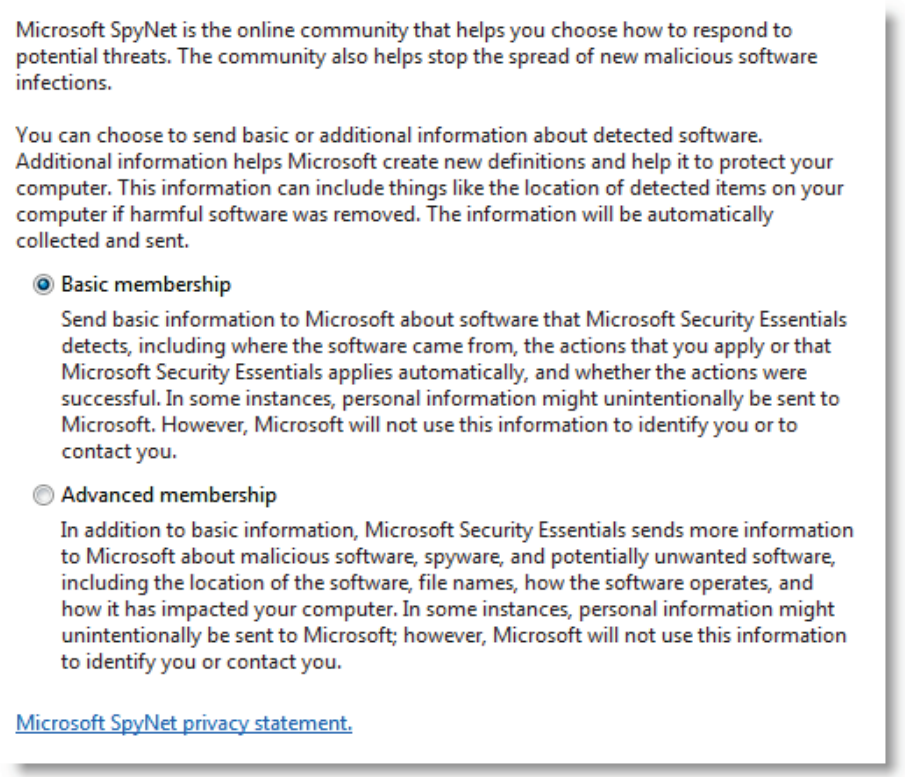


The same goes for *Excluded processes*. If you know processes that should be excluded, you probably don't need to read this part of the guide (and you can definitely teach me a thing or two!)

Click the *Advanced* tab. I recommend you check *Scan archive files* i.e. zip files as they are some of the most common files to contain viruses (in the files that are stored in the archive.) The next three options are up to you and you can see my configuration below. I disable reading of USB thumb drives on my computer so I don't need to scan them but you may want to check this one.



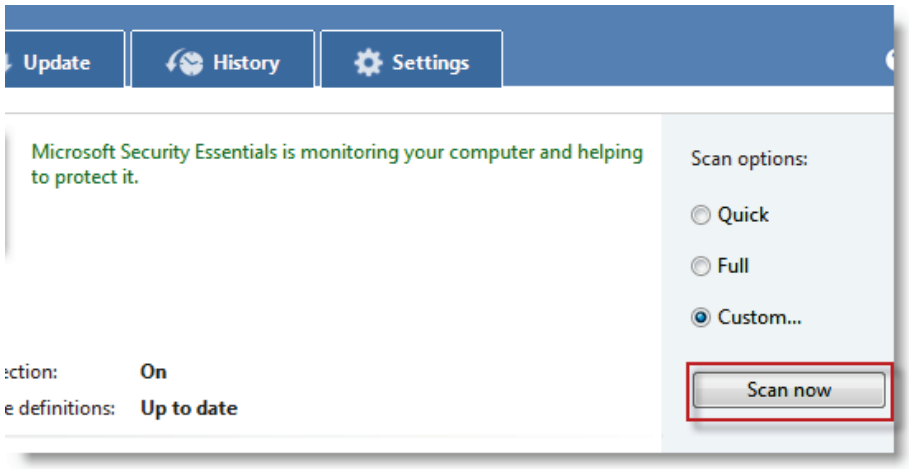
Finally, click *Microsoft SpyNet*. Here, I opt for the *Basic membership*, which sends non-identifying information to Microsoft to help them improve MSE's effectiveness in virus detection and removal. The advanced membership sends more detailed information to Microsoft about the virus and how it operates on your machine. It's up to you which membership you use, but I chose Basic.



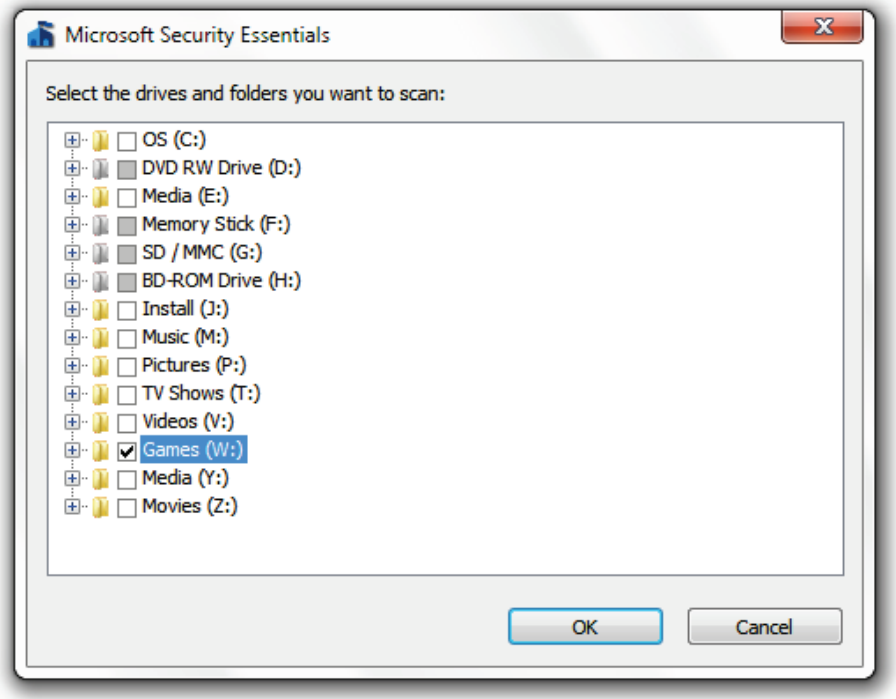
How to Run a Full Scan with MSE

Now you've taken time to set up MSE, why not run a scan to make sure there is no malicious software on your PC?

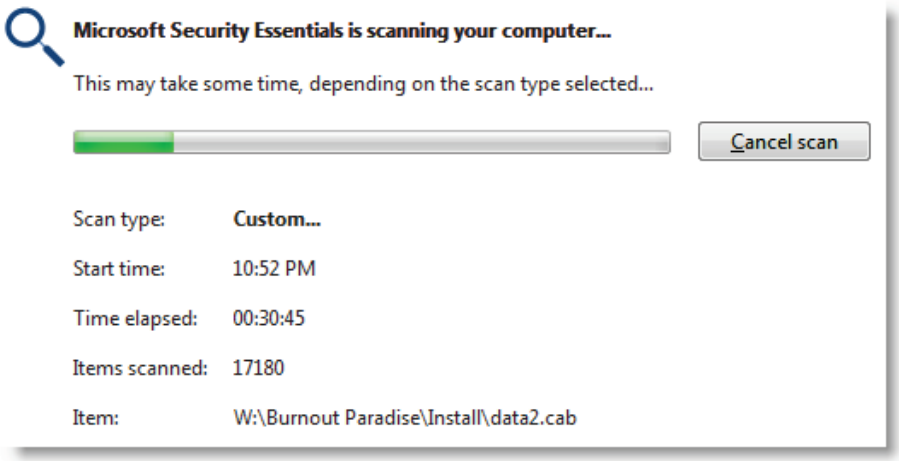
Click the *Home* tab, under *Scan options* select *Custom...* and click *Scan Now*.



Chose the drives or folders you'd like to scan and click OK.



Take a break (or a nap if you have large hard drives) and let MSE do its job:



Advanced Tips for MSE

If you'd like to learn some advanced tips for MSE, you can view them in the complete guide to protecting your PC with Microsoft Security Essentials.

ESET Smart Security

I love ESET Smart Security and have been using it for over two years. If you ask anyone who is computer "savvy", they'll know about (and may already use) ESET.

I know some people live by the motto "you get what you pay for" so, if you don't want to put your trust in Microsoft's free software, then you will get great value from ESET Smart Security.

I've reviewed ESET in more detail here. For sake of brevity, I'll explain the best details in this handbook.

When you first start the program, you will be presented with the simple menu. You can enable the advanced menu by clicking at the bottom of the main menu. The interface for this program is simple and intuitive with a clean dashboard that shows you the most recent statistics from the program. From the main menu, you can see the status of the different modules of ESET Smart Security. If you are going to use this program, I highly recommend running all the modules together. This way, you do not need a separate firewall, anti-spam, or anti-spyware program running in the background.

Note: the screenshots I will show you are from the business edition; however, I will only cover features available in the home edition.

System Scanning

The system scanning is both quick and efficient and in, in my opinion, quicker than any other virus program I've ever used. You are shown a simple interface while the system scans your files, which is an improvement over many programs which show an elaborate display when checking your computer.

Scheduled Protection

I always like my computer to run a schedule so that tasks are taken care of without my intervention. Virus scanning is no exception to this rule and ESET comes with a built in scheduler so you don't have to worry about setting up a schedule tasks via Windows control panel.

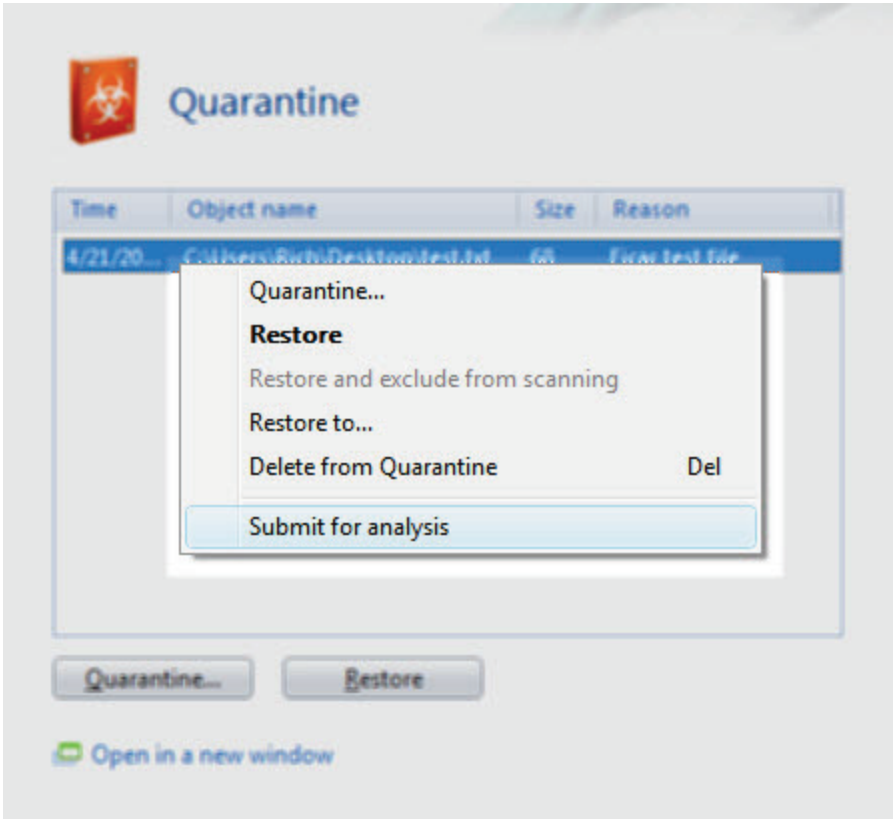
Harm Prevention

Protection against viruses is great but prevention is even better and ESET constantly update their virus definitions to ensure that the even the newest viruses are well protected against. Virus updates do not consume unnecessary system resources and do not fail–other antivirus programs I have used have issues with updating and sometimes need a manual fix.

Harm Protection

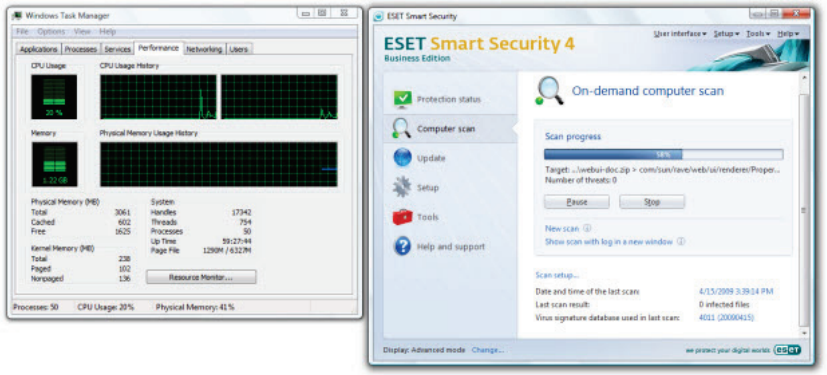
Most viruses should not find their way on to your system, because of real-time protection, and should be caught immediately. However, if a virus is detected during a scan, it will also be quarantined where you can review it and delete it if necessary.

You can even submit the file to ESET for further analysis. This will help you identify if the file is malicious and also help ESET protect other users who may have the same file on their machine.



Resource Usage

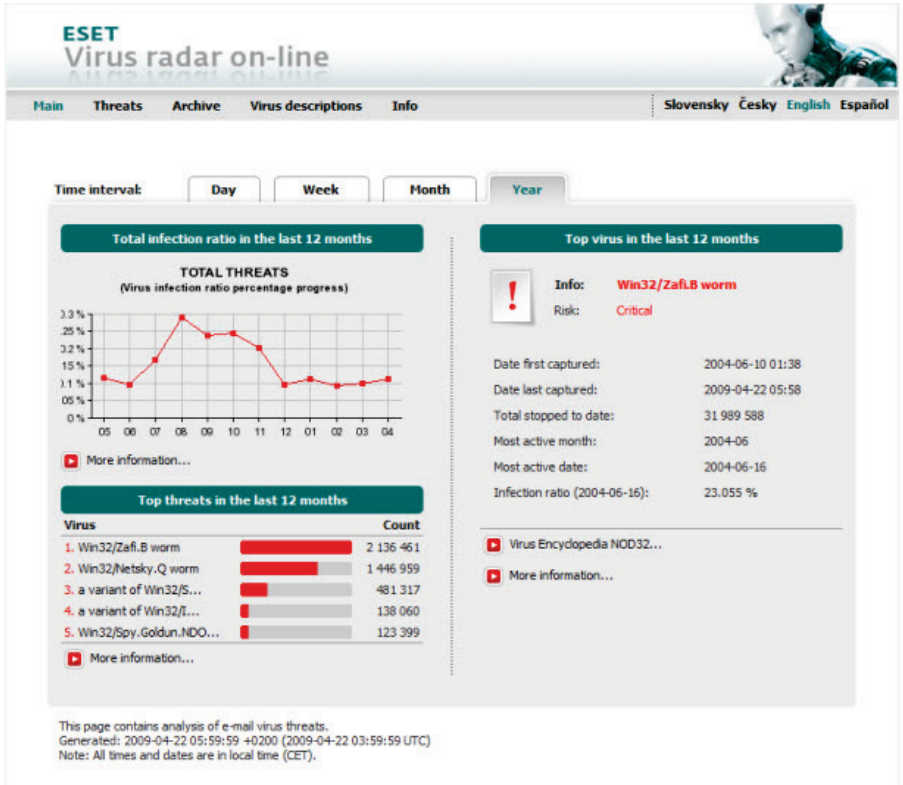
Virus checkers are a notoriously bloated and slow your system down to a halt when I running a scan. Many people who use ESET hold it high because it uses such low system resources. I've never completely tested this rely on the fact my computer still runs just fine when the scans are running. For this review, I decided to run a deep system scan and monitor system resources. The results of this experiment are shown below (click to enlarge):



As you can see from the enlarged screenshot, even with a full system scan running, system resources are at 22% on a 2 GHz dual core processor (T7250.) RAM usage is also very low but this is not usually a problem with most virus scanners.

Real-time Status

The final aspect of ESET I want to cover is the virus radar. While this may not be useful to you, it's nice to see that ESET are monitoring current threats and sharing them with you so you can keep an eye out for any suspicious activity on your PC.



In Conclusion

ESET Smart Security 4.0 is an excellent program and I recommend it to everyone. You can download a 30 day trial from ESET's website here. You can also buy it with a 25% discount here.

Read a full review here.

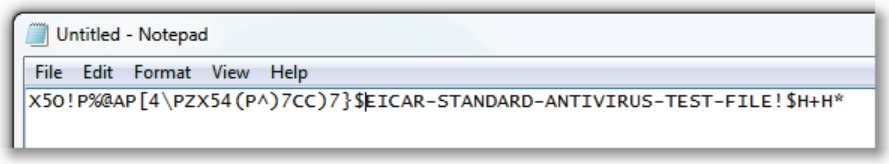
Put Your Antimalware to the Test

This section teaches you a fun "trick". You'll create a test file, which will trigger all good antimalware programs. There is no point in doing this other than for entertainment value and to provide a sanity check.

This file is a dummy virus, which simulates a virus. This string is provided by EICAR for distribution as the EICAR Standard Anti-Virus Test File. The file is a legitimate DOS program and produces sensible results when it runs (it prints the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!")

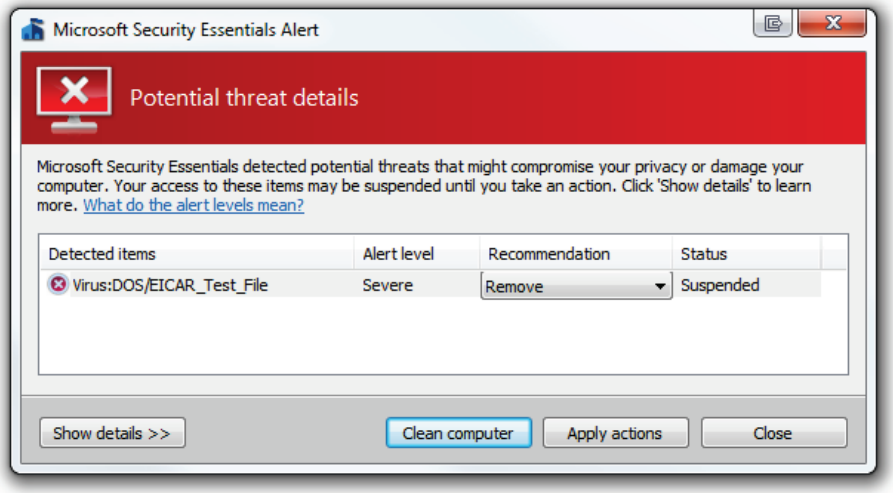
Paste the following text into Notepad and save the text file to your desktop:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

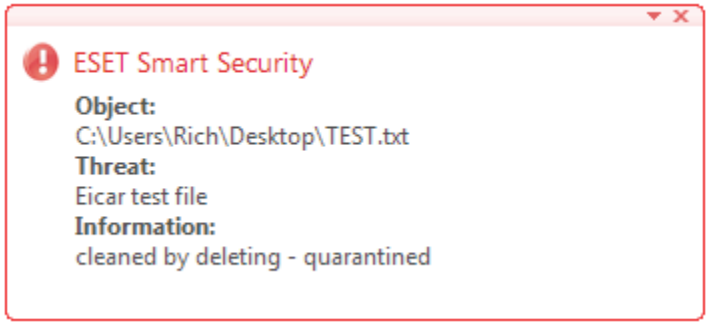


You should see the following:

MSE



ESET



Your virus checker works!

Download free Software Only from Sites You Know and Trust

You should only download software from sites you know and trust; however, this is easier said than done. Don't you wish that the community could get together and rate sites on integrity and trust and give this information to you as you browse? Well, of course, this has been done before and, in this section, I'll show you how to take advantage of this system, called the Web of Trust (WOT), and how to give back to help others.

What is the Web of Trust (WOT)?

From the web of trust site:

> WOT, Web of Trust, warns you about risky websites that try to scam visitors, deliver malware or send spam. Protect your computer against online threats by using WOT as your front-line layer of protection when browsing or searching in unfamiliar territory. WOT's color-coded icons show you ratings for 21 million

websites – green to go, yellow for caution and red to stop – helping you avoid the dangerous sites.

WOT is free and easy-to-use

- Our active community has rated millions of websites
- Ratings are updated every half hour
- Our trusted sources provide extra protection against phishing, spam and other Internet scams

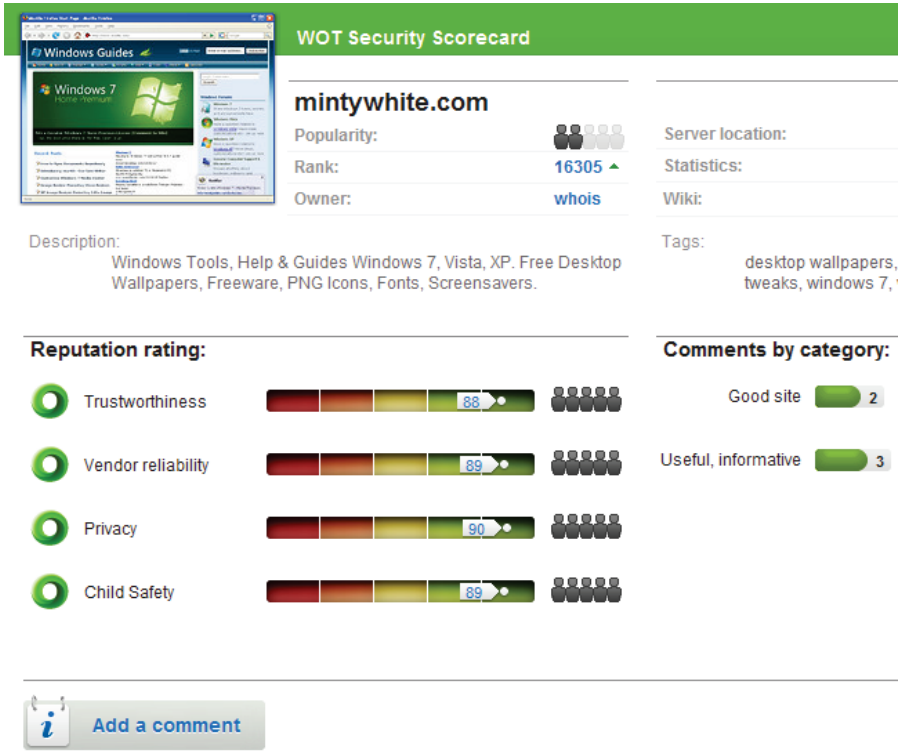
To summarize, the WOT alerts you of dangerous sites so you can get out of there quickly.

Download the WOT add-on

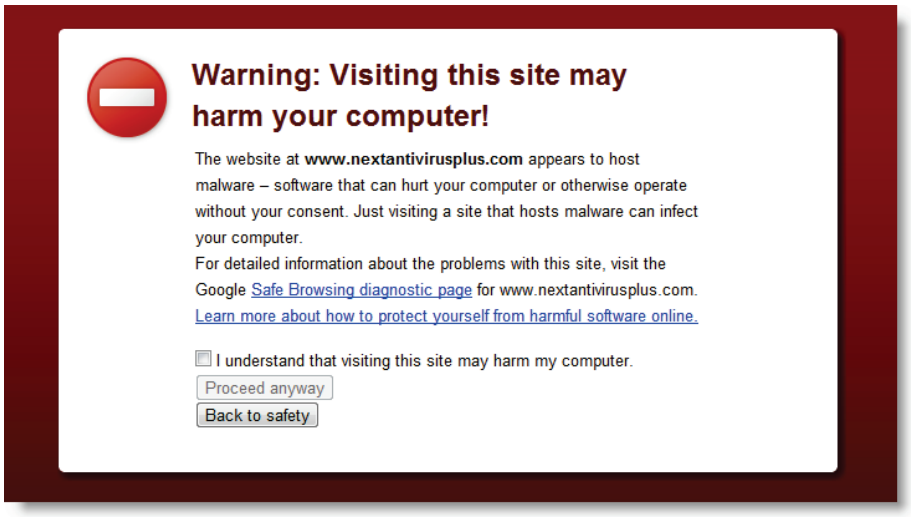
You can download the WOT add-on for your browser here.

View Reports on Sites and Leave Reports Yourself

Once you've installed the add-on, you will get the status of every site and can view reviews and ratings left by others. You can also rate a site and leave a comment to help others (even if the site is good):



If you decide the WOT add-on is not for you, it's okay (I don't use it much.) Modern browsers (notably Mozilla Firefox and Google Chrome) offer some level of protection by warning you of dangerous sites:



Test Suspicious Software in a Virtual Environment

If you want to test a downloaded program but don't want it destroying your data and sending your bank passwords to the other side of the world, you should probably test it in a safe environment that's not connected to the rest of your home network. You can do this a number of ways; here are two suggestions:

1. Download the program on a spare computer that's not connected to the rest of your home network.
2. Download the program in a virtual machine that's isolated from your host machine.

If you don't have a spare computer or want the convenience of testing without using a separate machine, you should use a virtual machine. In this guide, we'll show you how to set up a virtual machine and how to isolate it from your home network so you can test software.

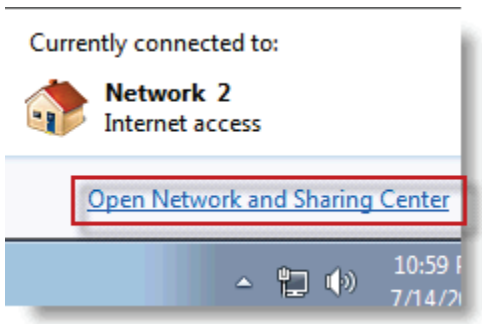
How to Set Up a Virtual Machine (VM)

To create a virtual machine, I recommend using Windows Virtual PC. Here's some basic information on Windows Virtual PC and here are specific instructions for setting up a virtualized copy of Windows Vista (the same steps apply for creating a Virtual copy of Windows 7.)

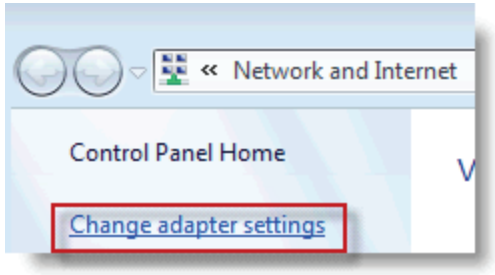
How to Isolate Your VM from Your Home Network

Once your VM is up and running, you should isolate it's connection to your local area network. To this in a Windows 7 VM:

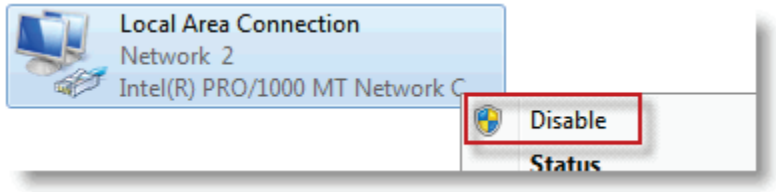
1. Click the network icon in the system tray and click Open Network and Sharing Center.



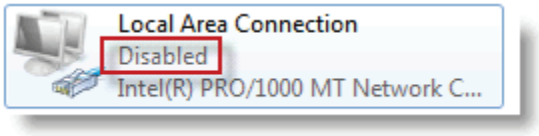
2. In the left-hand menu, click Change adapter settings.



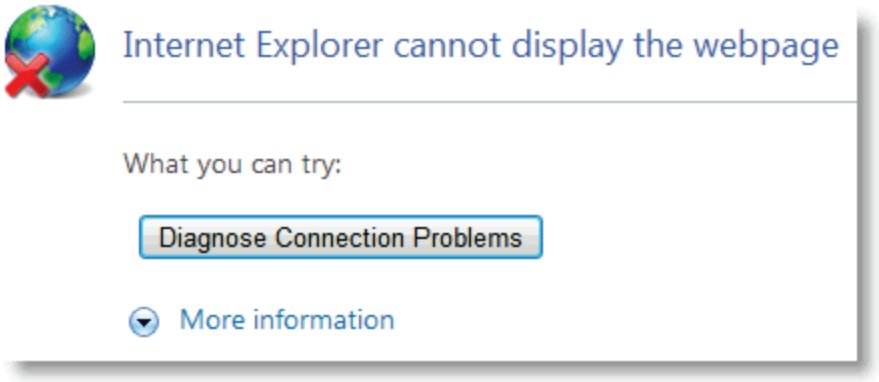
3. Right click each network connection and click Disable.



4. Verify the connection is disabled:



5. Now open Internet Explorer and verify you truly have no internet connection by attempting to browse to any webpage:



Optional: Install Antimalware

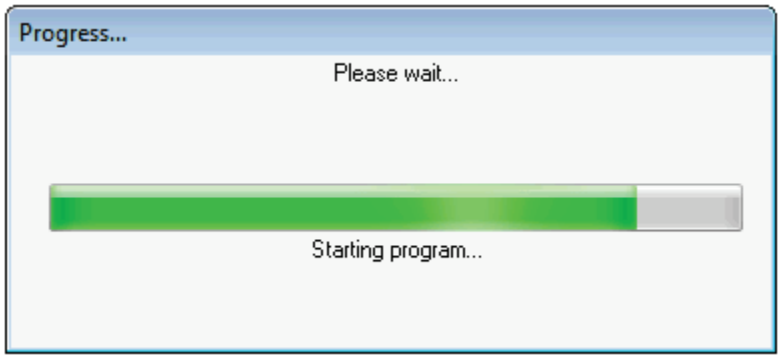
You don't have to do this, but I recommend you install antimalware so you can understand a malicious program if you download one.

Install Programs and Test

Now comes the fun part: testing suspicious software to see what it does to your VM.

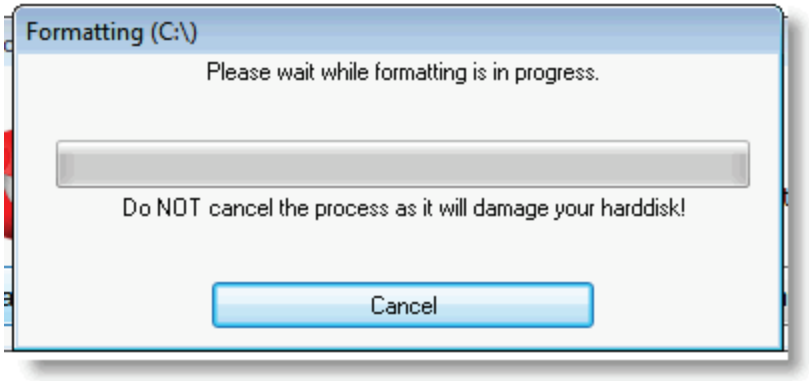
I chose this file: Suspicious Download.exe. How exciting:

Let's see... a progress bar for starting the program... looks pretty legitimate to me:

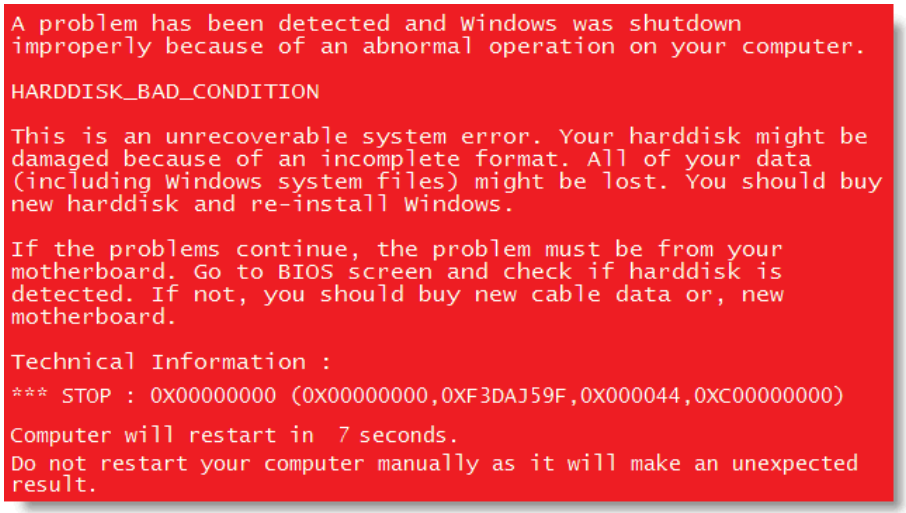


Oh #@!* this doesn't look good. I guess I'll go with *Format Harddisk*. Seems pretty harmless, I mean it could probably do with some cleanup anyway...

While it cleans up my disk I check the definition of "format" with respect to a hard disk... #@!*!! Double #@!*!!! It erases everything?!?



A... RSOD?? Erm.. this really can't be good.



BIOS you say... that seems important and now it's corrupted...

Luckily for me I used a Virtual Machine to test this out and luckily for me this program is a joke.

So, there you have it. A safe(r) way to test suspicious software without losing everything!

How to Protect Your Data

This section of the book details how to protect your data. There are three main threats to your data:

1. Malicious software.
2. Unauthorized access.
3. Hardware failure/data corruption.

The first threat should now be taken care of as you've taken precautions to protect your data.

This section will show you how to protect your computer from unauthorized access and how to back up your data in the event of data loss.

Prevent Unauthorized Access to Your Computer

The best way to keep people from physically accessing your data is to:

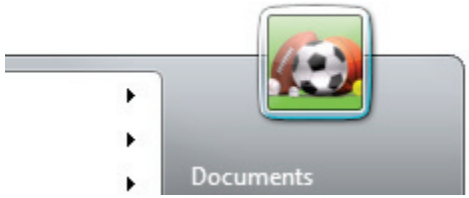
1. Use a password for your account.
2. Lock your PC when you walk away from it (or take your computer with you if you are in public.

Use a Password for Your Account

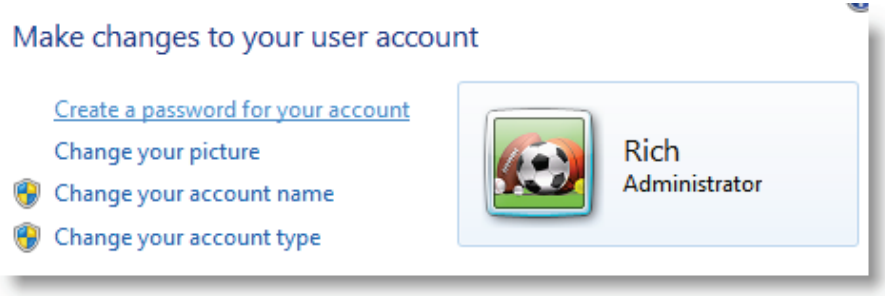
To add a password to your account:

Vista/7:

1. Click the *Start* button and click your account picture.



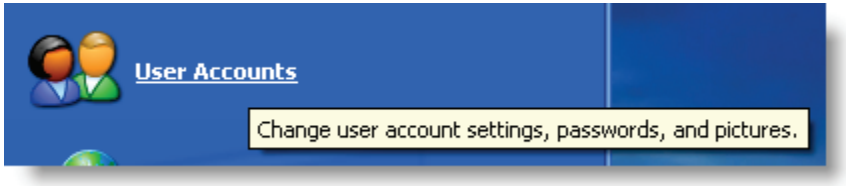
2. Click *Create a password for your account*.



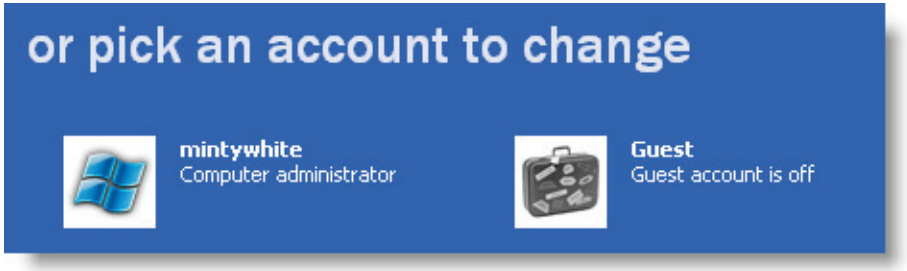
XP:

1. Click the *Start* button and click *Control Panel*.

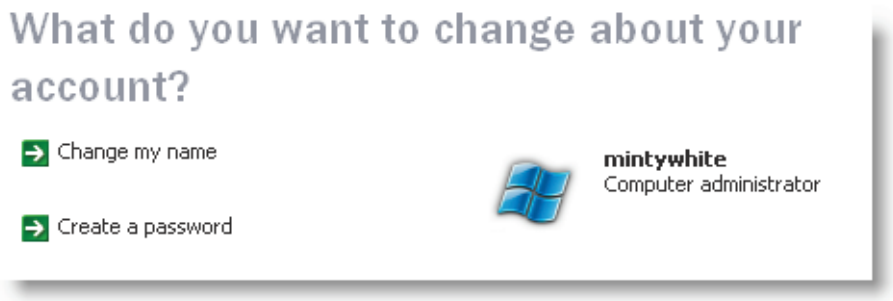
2. Click *User Accounts*.



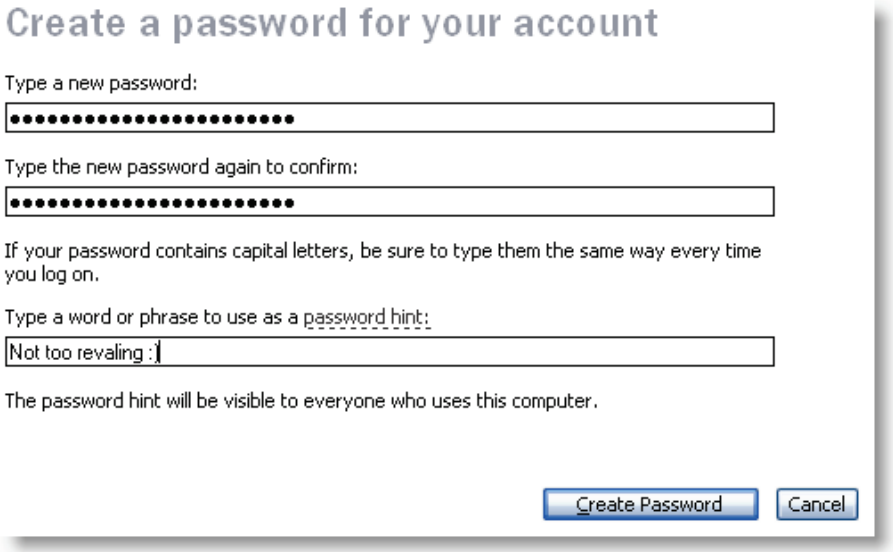
3. Click the account you'd like to change.



4. Click *Create a password*.



5. Type a ***password***, verify, and a hint and click *Create Password*.



6. I recommend you click *Yes, Make Private* when asked if you want to make your files and folders private.

Quickly Lock Your PC When You Walk Away

To quickly lock your PC when you walk away from it, simply press **Winkey+L**. Note: you need a password set to effectively lock your PC.

Protect Your Data from Hardware Failure/Data Corruption

Data backup is essential. There are three main ways you can back up your data and this section will cover them:

1. Local backup.
2. Backup to optical media.
3. Online backup.

Backup Your Data Locally

Backing up your data locally includes making copies of files on your PC, a different internal drive, and an external drive.

Backing up your data to optical media is also another form of local backup, but I hope you will send the backups somewhere safe in preparation of a worst-case scenario.

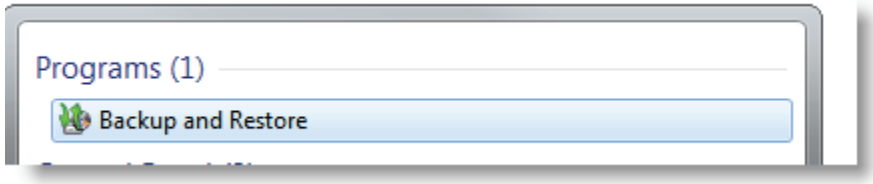
This section will show you how to back your data up locally using Windows backup. In this specific example, I'll show you how to back your data up to a networked PC. The steps to back up to the same PC are almost identical.

Note: Network backup using Windows Backup is not available in the Home editions of Windows XP, Vista, and 7.

Backup Your Data with Windows Backup

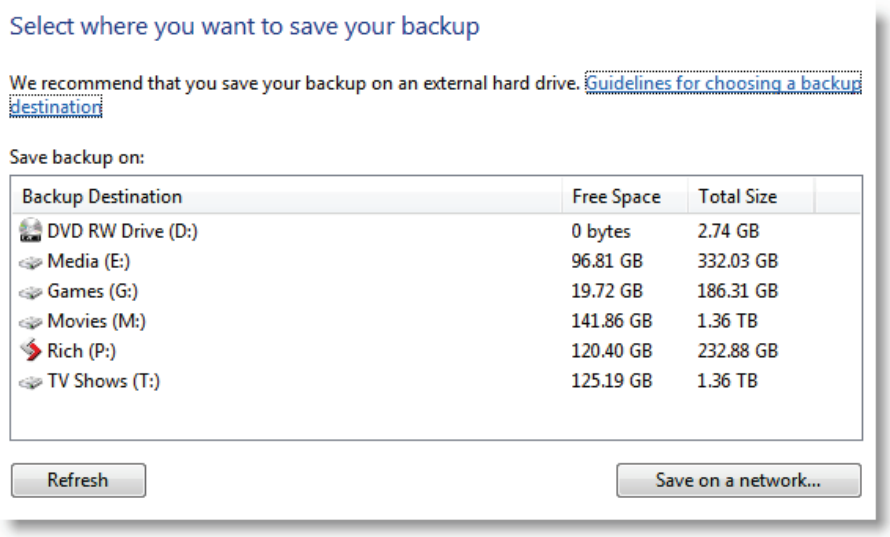
To back up your data across your home network:

1. Click the *Start* button, type ***Backup*** and click *Backup and Restore*.

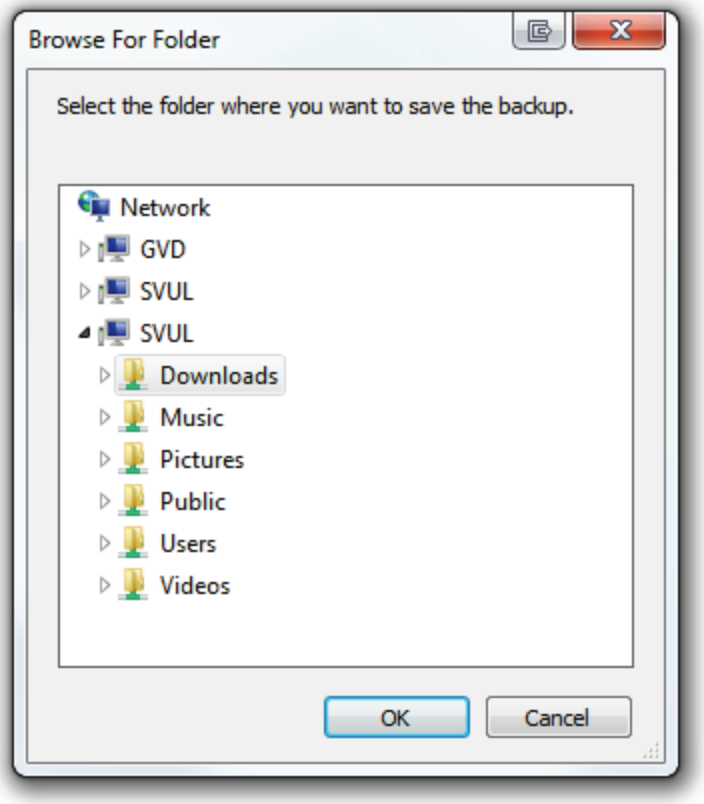


2. Click *Set up backup*.

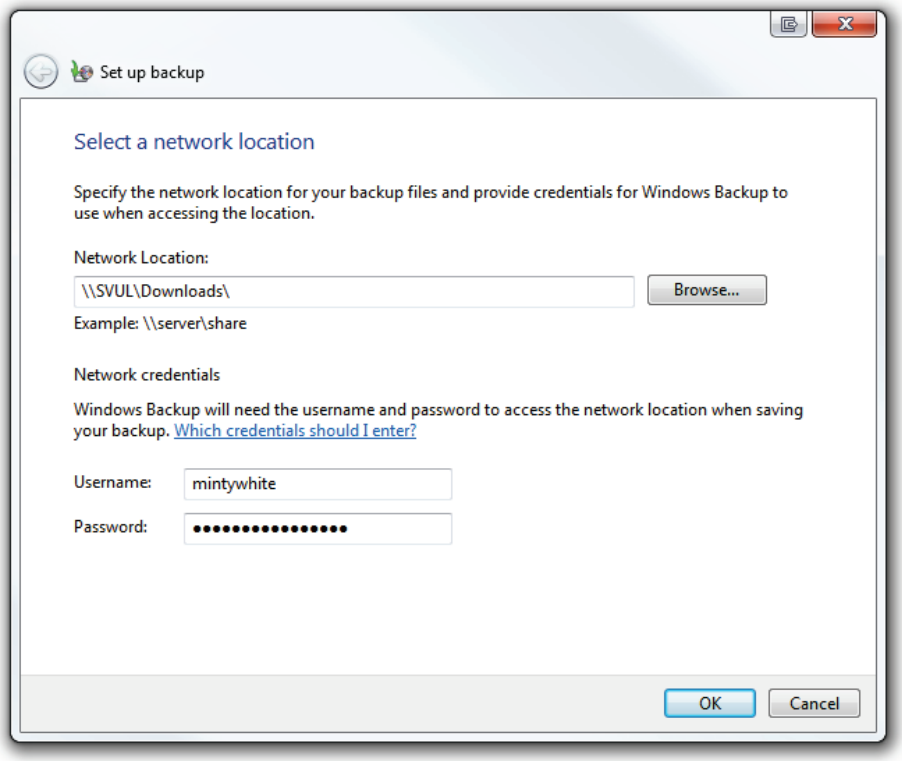
3. Click *Save on a network...*



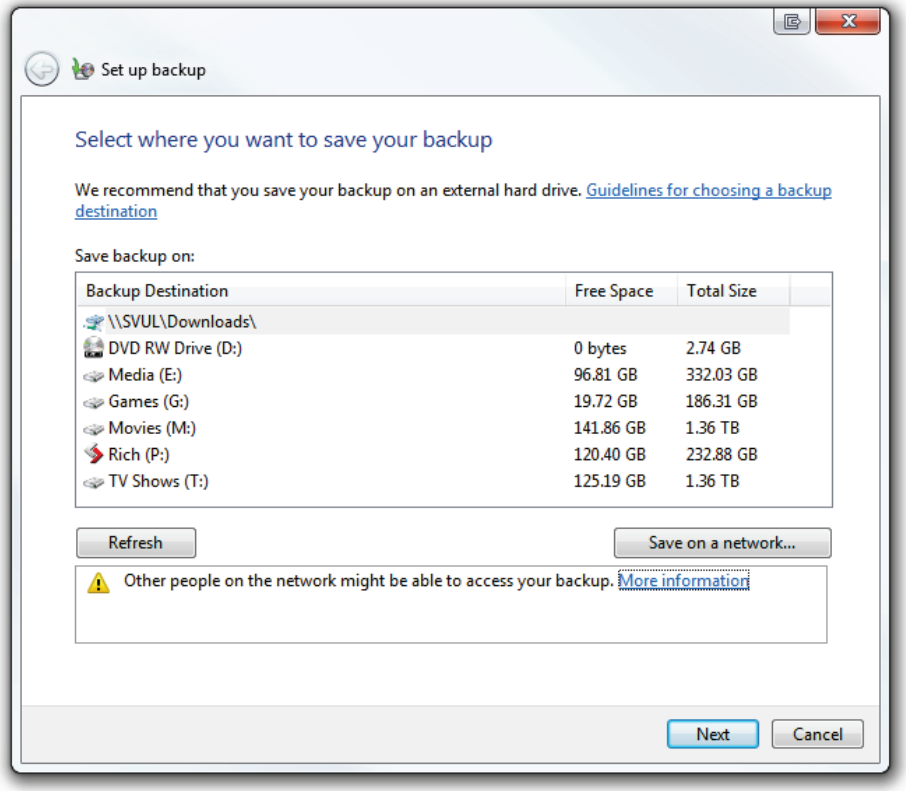
4. Click *Browse* and Choose your networked PC and pick a shared location (how to set up networked PCs and shared locations.)



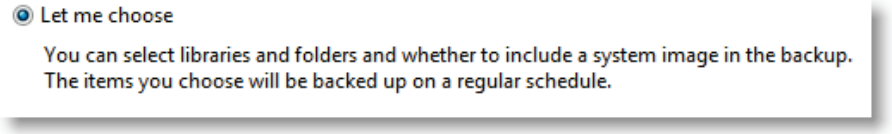
5. Type in the ***username*** and ***password*** of the PC that will store the backup. Click *OK*.



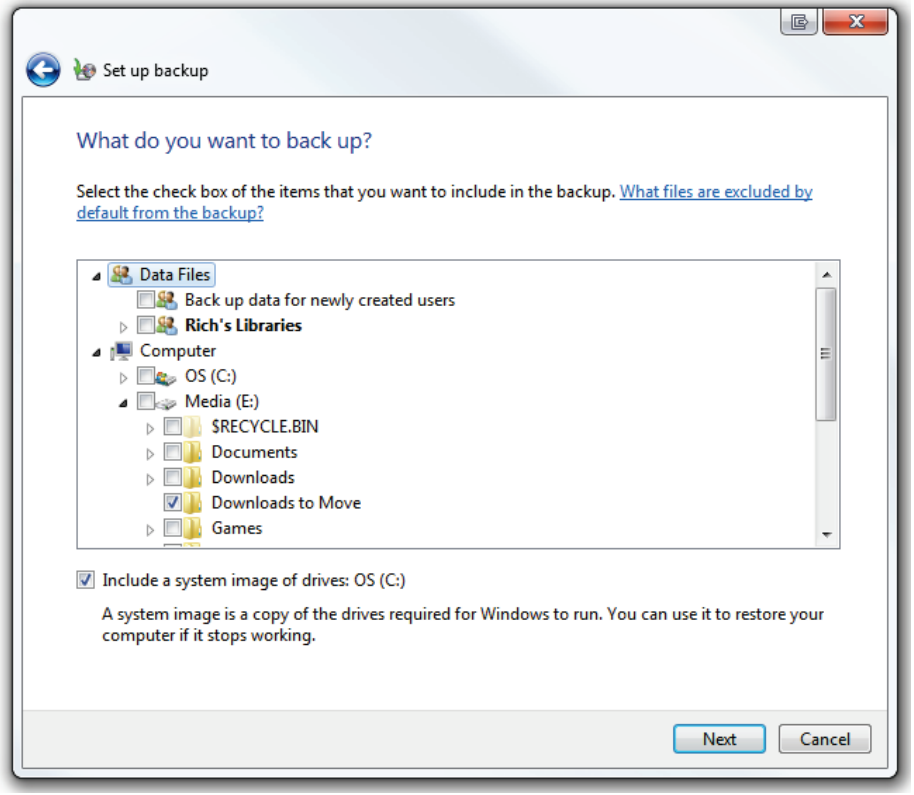
6. Click *Next*.



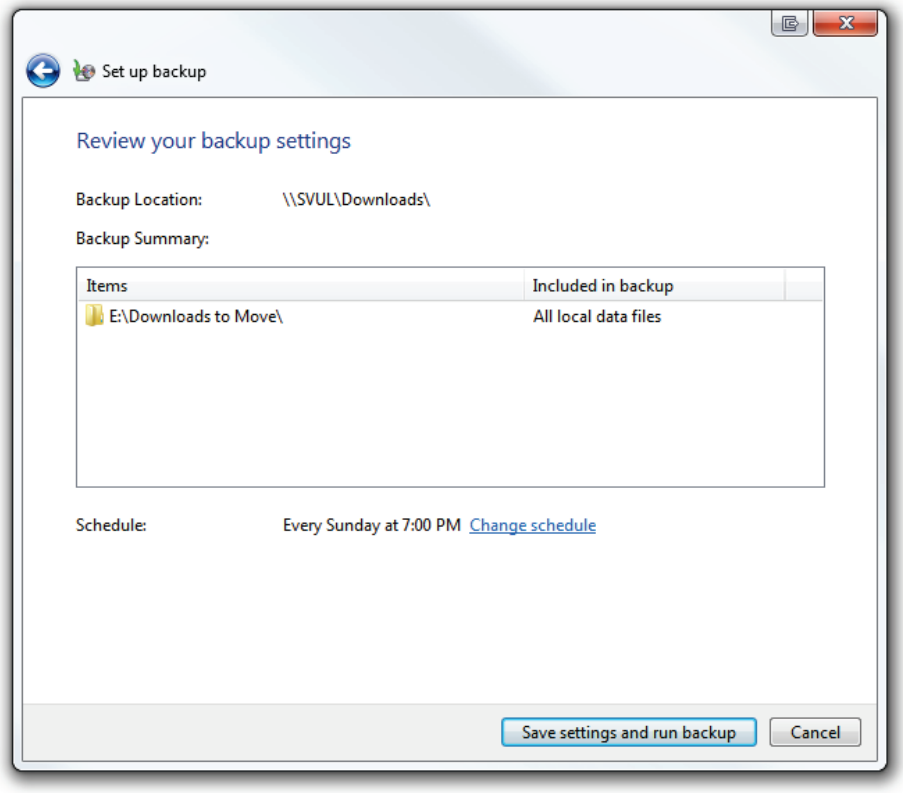
7. I recommend choosing the files you want to back up by selecting *Let me choose* and clicking *Next*.



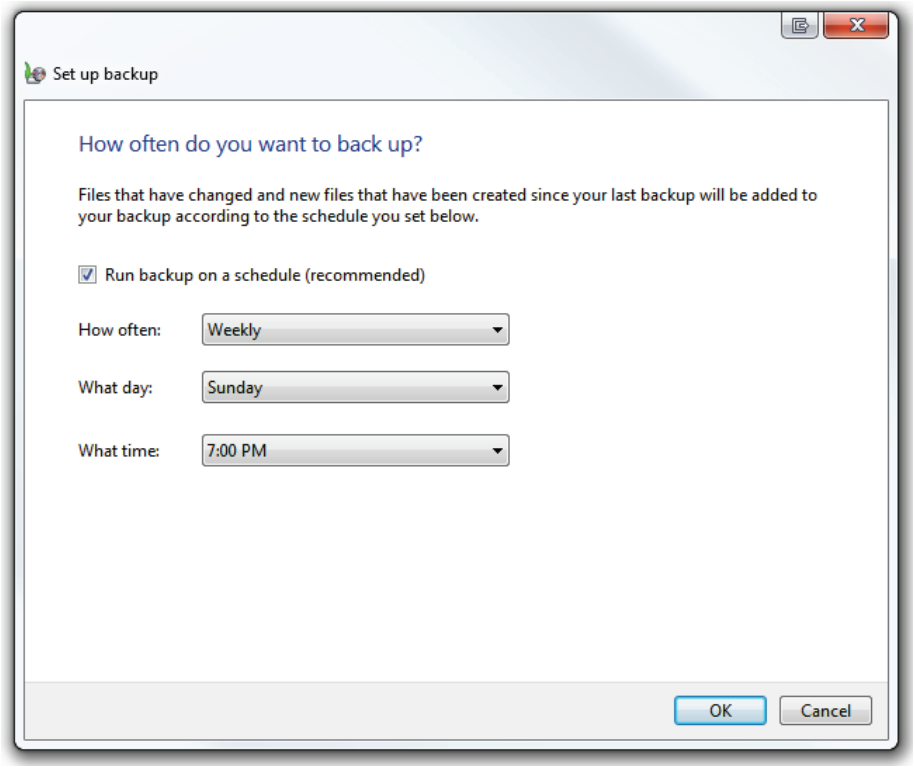
8. Choose the files you'd like to backup (be sure to uncheck Include a system image of drives if you are already making a system image backup or if space is limited on the backup location.)



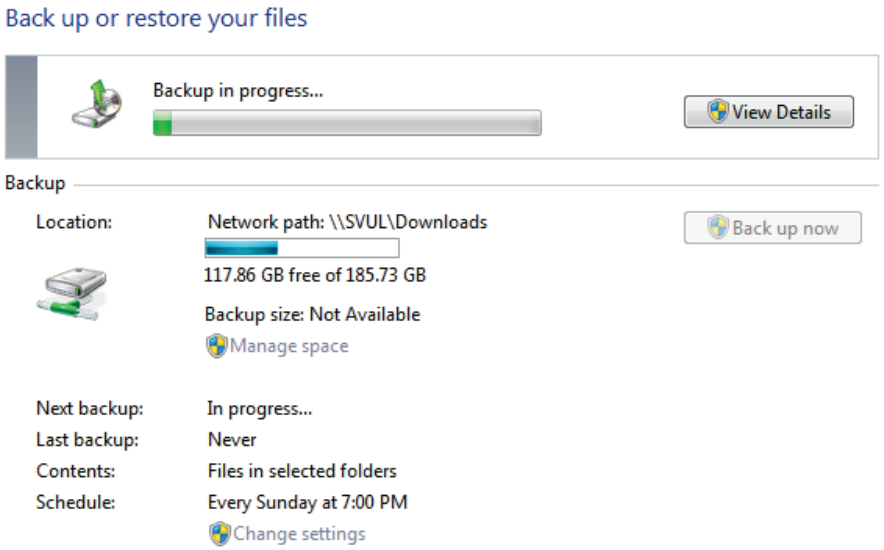
9. Verify your settings and click *Save settings and run backup*.



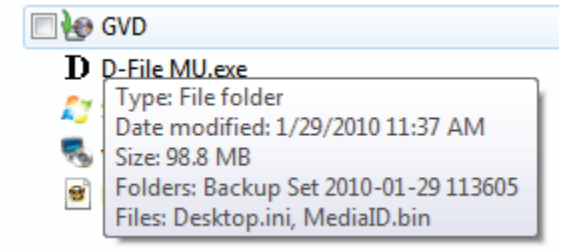
10. Set a schedule so backup is automatic. Click *OK*.



11. Your backup will now take place (be sure to not turn off your PC or the PC the data is being backed up to during the backup.)



12. Now go to the PC where the data was backed up and verify the data is there (it doesn't hurt to look.)



That's it; you're done. Your data is now backed up, automatically according to your schedule.

Backup Your Data to Optical Media

Ashampoo Burning Studio Free pretty much burns any files to any type of optical media. The program is free and simple to use. If you want more information, check out these guides:

- How to Install Ashampoo Burning Studio Free.
- Burn Files Using Ashampoo Burning Studio Free.

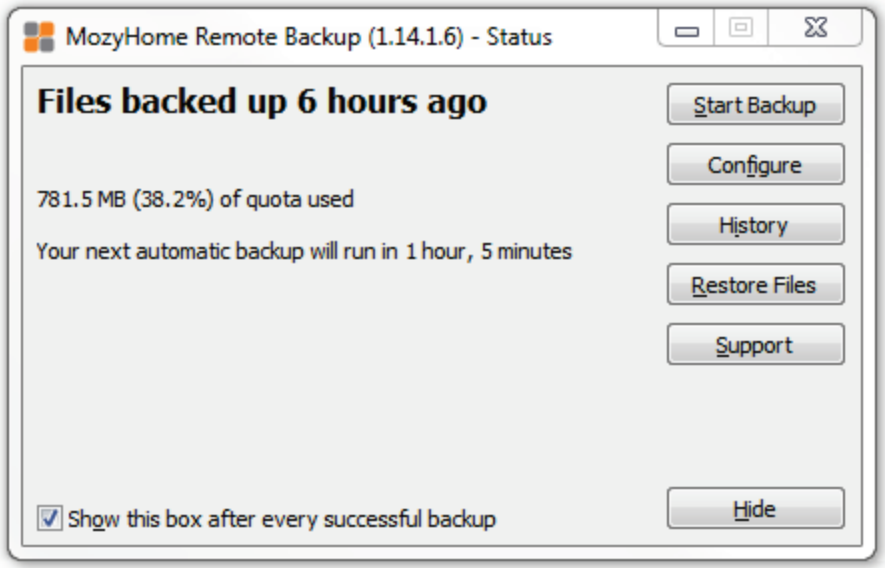
Backup Your Data Online

I strongly recommend using online (off-site) backups. Backing up your data online prevents data loss if your computer is damaged or stolen—or if your data is wiped by malware.

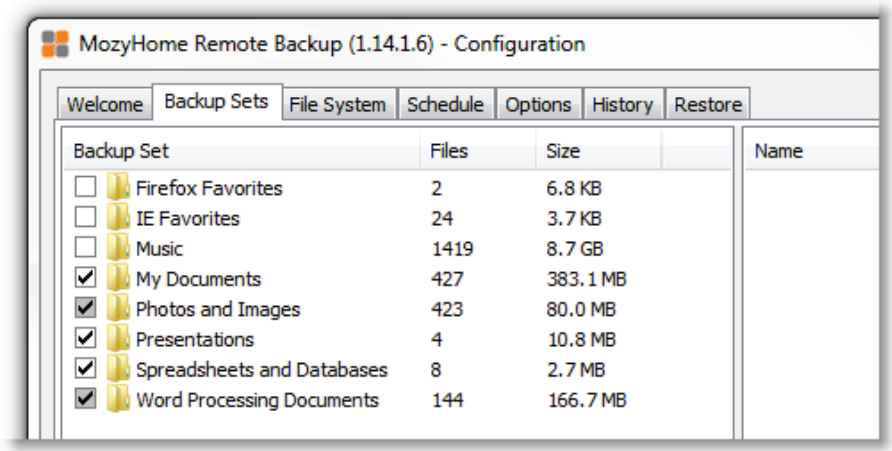
By far my favorite solution for online backup is Mozy. Mozy offers free online storage (up to 2GB for free with paid options too.) I've had Mozy installed on my laptop for over two years and it has saved me on more than a handful of occasions.

Setup is simple and after downloading Mozy, you can specify what you want to backup and when. Mozy will automate your backups and let you decide when it backs up (specific times), what causes it to backup (low CPU usage), and how often (one, two, three etc. times a day.)

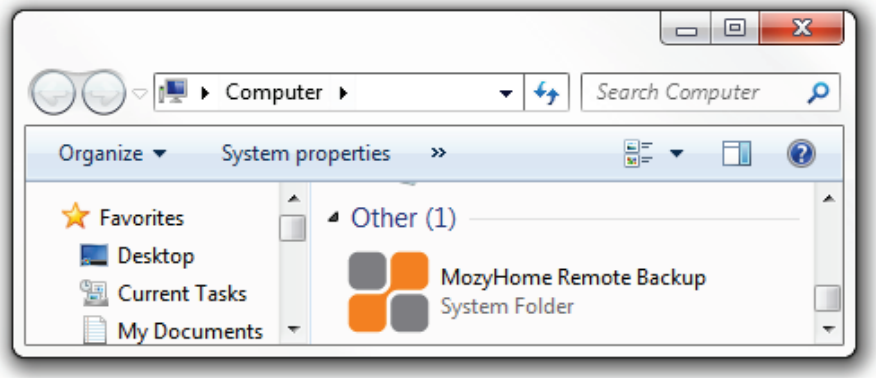
I just let Mozy run and it alerts me after a successful backup:



You can specify what types of files to backup or specify folders— it's up to you:



Mozy even integrates into *My Computer* so you can browse and restore your backed up files (even ones you've deleted from your computer):



MozyHome Features

- Open/locked file support: Mozy will back up your documents whether they're open or closed.
- 128-bit SSL encryption: The same technology used by banks secures your data during the backup process.
- 448-bit Blowfish encryption: Secures your files while in storage, providing peace of mind that your private data is safe from hackers.
- Automatic: Schedule the times to backup and MozyHome does the rest.
- New and changed file detection: MozyHome finds and saves the smallest changes.
- Backs up Outlook files: Disaster-proof email protection.
- Block-level incremental backup: After the initial backup, MozyHome only backs up files that have been added or changed, making subsequent backups lightning fast.

Download Mozy for Free

Download MozyHome free.

What Next?

Now you've read this book, I recommend you ensure you've made changes to ensure your data is protected. After you've done this, I encourage you to visit Windows Guides and learn other ways to improve your PC.

About this Handbook

This handbook is delivered free by Windows Guides.

The author, Rich Robinson, is a Microsoft MVP in the Desktop Experience category; this book is not affiliated with Microsoft. Get more books.