

# HackerProof:

Your Guide to  
PC Security

By Matt Smith  
[smidgenpc.com](http://smidgenpc.com)



# HACKERPROOF: YOUR GUIDE TO PC SECURITY



By: Matt Smith  
[smidgenpc.com](http://smidgenpc.com)

Edited by: Justin Pot

This manual is intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this guide is prohibited.

## Table of Contents

1. Intro to PC Security .....	5
What is PC Security? .....	5
A Brief History of Computer Viruses .....	6
Chapter 2: The Malware Gallery .....	8
The Traditional Virus or Trojan .....	8
Trojans .....	9
Worms .....	10
Rootkits .....	11
Phishing and Pharming .....	13
Malware – The Catch All.....	14
Chapter 3: Innocent Civilizations: The Security of Operating Systems.....	15
Windows XP.....	15
Windows 7 .....	16
Mac OS X .....	18
Linux .....	19
A Summary – Which is Best? .....	20
Chapter 4: Good Security Habits .....	21
Avoiding the Email Inbox of Doom .....	21
Using Caution for Safe Surfing .....	22
Checking Links – Do They Lead Where You Think? .....	23
Updating Your Software – The Most Important Step.....	24
Use Antivirus Protection .....	25
Chapter 5: Methods of Protection .....	26
Anti-Malware Software .....	26
Firewalls .....	28
Rootkit Killers .....	29
Network Monitoring .....	30
Phishing Protection .....	31
Chapter 6: Choosing Security Software .....	33
What Products Offer What Protection? .....	33
Free vs. Paid Security .....	34
The Ideal Free Internet Security Suite .....	36

Avast! Free Antivirus or Microsoft Security Essentials .....	36
ZoneAlarm Free Firewall .....	37
BitDefender Anti-Phishing .....	37
Chapter 7: Prepare for the Worst – and Backup! .....	38
The Importance of Backups .....	38
Backup Options.....	39
External Hard Drives: .....	39
Optical Formats:.....	39
Online Backup .....	40
Securing Files with Encryption .....	41
How Often Should I Backup? .....	42
Chapter 8: Recovering from Malware .....	44
Reclaiming Your PC .....	44
Protecting Your Identity .....	45
Preventing Future Problems.....	47
Chapter 8: Conclusions .....	48
A Summary of the Issues .....	48
A Note About Mobile Threats.....	49
Additional Reading .....	50

# 1. Intro to PC Security

---

## What is PC Security?

The terms “PC security” or “computer security” are vague in the extreme. They tell you very little, like most general terms.

This is because PC security is an incredibly diverse field. On the one hand you have professional and academic researchers who carefully try to find and fix security issues across a broad range of devices. On other hand, there is also a community of inventive computer nerds who are technically amateurs (in the literal sense of the word – they’re unpaid and unsupported by any recognized institution or company) but are highly skilled and capable of providing useful input of their own.

PC security is linked to computer security as a whole, including issues like network security and [Internet security](#). The vast majority of the threats that may attack your computer are able to survive only because of the Internet and, in some cases, the survival of a security threat is directly linked to a security flaw in some high-end piece of server hardware. However, the average PC user has no control over this.

This means that PC security – defined as protection of the personal computer you own – has a fortress mentality. It is your responsibility to protect your fortress from whatever might exist in the unknown beyond its walls. This mentality is expressed in the terms used by companies that want to sell you PC security software. Words like “[firewall](#)” “blocker” and “shield” are easy to find in advertisements of PC security software.

These words are supposed to clarify the purpose of PC security, but this isn’t always the case. The information received from a company that sells security software is likely to be biased in favour of their product, as well, further confusing issues.

This guide provides an objective, detailed, but easily understood walkthrough of PC security. By the end of this guide you will know exactly what PC security means and, more importantly, what you need to do to keep your PC secure.

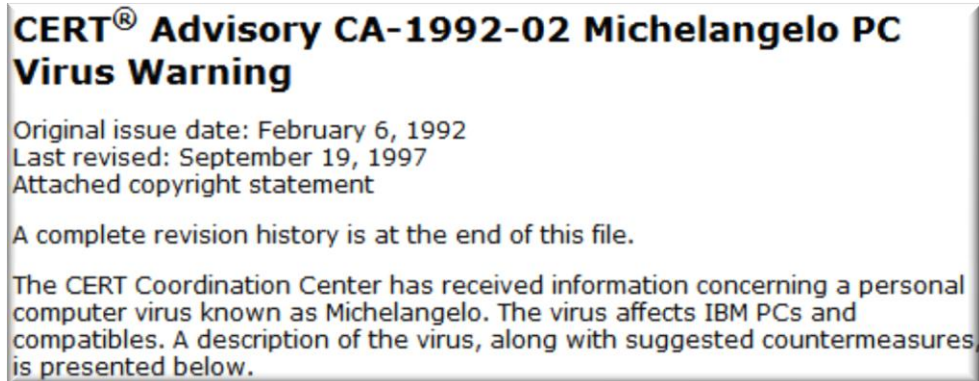
## A Brief History of Computer Viruses

Computer viruses haven't always been a major threat. The earliest viruses, which spread themselves in the 1970s via the first Internet networks (such as ARPANET), were relatively mundane programs that sometimes did nothing more than display a message on a computer terminal.

Viruses did not start to gain notice as a serious security threat until the mid and late 1980s. This period saw a number of firsts in the field of computer viruses, such as the Brain virus, widely considered as the first IBM PC compatible virus. This virus was capable of infecting the boot sector of MS-DOS computers, slowing them down or rendering them unusable.



Once the earliest malware became known the number of viruses quickly ramped up as savvy nerds saw the opportunity to engage in a bit of online vandalism and prove their technical knowledge to their peers. Media attention towards viruses became common in the early 90s, and the first major virus scare occurred surrounding the Michelangelo computer virus. Like hundreds of computer viruses after it, Michelangelo set off a media panic and millions across the globe worried that their data would soon be erased. This panic proved misplaced, but put a media spotlight on malware that has yet to fade.



The proliferation of [e-mail](#) in the late 1990s wrote the next chapter in malware. This standard form of communication was, and still is, a popular method through which malware can reproduce. Emails are easy to send and attached viruses are easy to disguise. The popularity of email also coincided with a trend that proved even more important in the evolution of malware – the rise of the personal computers. While enterprise networks are usually staffed by a team of people paid to watch over their security, personal computers are used by average people who have no training in the field.

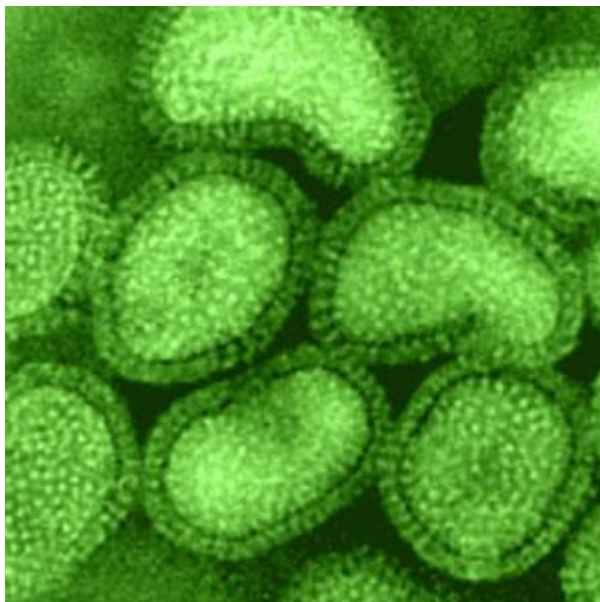
Without the rise of personal computers many of the security threats that rose in the new millennia would not be possible. Worms would have fewer targets, trojans would be detected quickly, and new threats like phishing would be pointless. Personal computers give those who want to write malicious software a field full of easy targets.

The key, of course, is to ensure you're not one of them.

# Chapter 2: The Malware Gallery

---

## The Traditional Virus or Trojan



Malware, through most of history, have spread by user error; that is to say, the PC user takes some kind of action to trigger a virus into action. The classic example of this is opening an email attachment. The virus, disguised as an image file or some other common file type, springs into action once the user opens the file. Opening the file may result in an error, or the file may open as usual, fooling the user into thinking nothing is wrong. In any case, the virus required the action of the user in order to spread. Reproduction is made possible not because of a security flaw in a program's code but instead through deception.

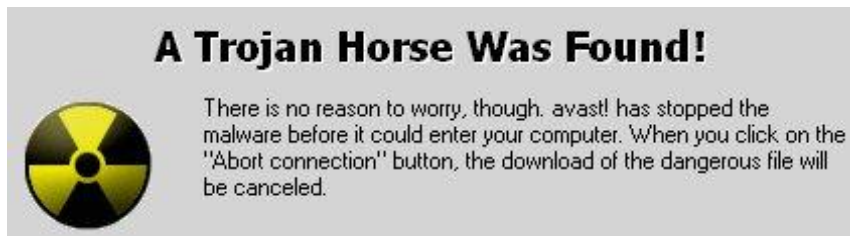
In the late 1990s this type of malware, more commonly called a virus, was by far the most threatening. Most people were new to email and didn't know that opening an attachment could infect their computer. Email service was far less sophisticated: there were no effective spam filters capable of keeping virus-containing spam emails out of inboxes, nor were there any effective antivirus solutions that automatically scanned emailed attachments. In recent years, technological advancements on both of these fronts have made it less effective to send a virus via email, but there are still millions of people who don't have security software and don't mind opening email attachments.



As email viruses are now a (relatively) well known threat, virus design has become more creative. Viruses can now “hide” in file types most people consider secure, such as [Excel spreadsheets](#) and PDF files. It is even possible for a virus to infect your PC through your web browser if you visit a webpage containing such a virus.

Some PC users boast that avoiding a virus is simply a matter of common sense – if you don't download files from unknown sources and don't download email attachments you'll be fine. I disagree with this view. While many threats can be avoided with caution, viruses with new methods of reproduction and infection are being developed constantly.

## Trojans



Trojans, while different from a virus in its payload, can infect PCs through the same methods listed above. While a virus attempts to run malicious code on your PC, a Trojan attempts to make it possible for a third party to access some or all of your computer's functions. Trojans can infect computers through almost any method a virus can use. Indeed, both viruses and Trojans are often lumped together as malware, as some security threats have traits associated with both a virus and a Trojan.

## Worms



The term “worm” describes a method of virus infection and reproduction rather than the payload which is delivered. This method of infection is unique and dangerous however, so it deserves its own category.

A worm is malware that is capable of infecting a computer without the user taking any action (besides that of turning on their computer and connecting to the Internet). Unlike more traditional malware, which usually tries to hide in an infected file, worms infect computers through network vulnerabilities. The stereotypical worm spreads by spamming copies of itself to random I.P. addresses. Each copy has instructions to attack a specific network vulnerability. When a randomly targeted PC with the vulnerability is found, the worm uses the network vulnerability to gain access into the PC and deliver its payload. Once that occurs, the worm then uses the newly infected PC to spam more random [I.P. addresses](#), beginning the process all over again.

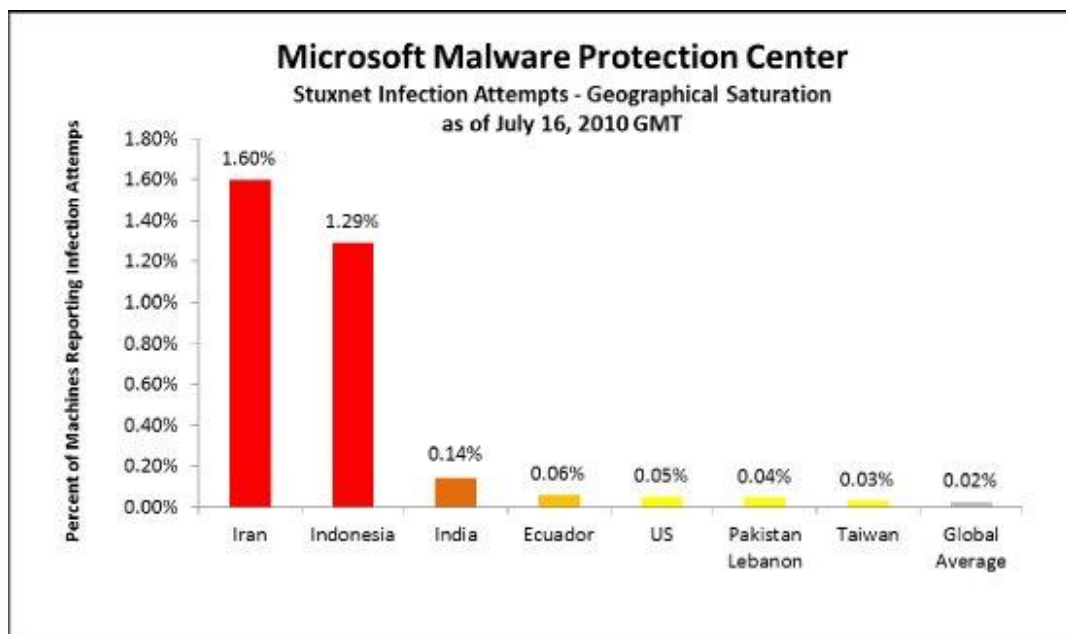
Exponential growth is the key here. The SQL Slammer worm, released in January 2003, used this method to infect approximately 75,000 computers within 10 minutes of its initial release.

(<http://www.wired.com/wired/archive/11.07/slammer.html>)

As with many PC security threats, however, the term “worm” covers a wide range of malware threats. Some worms spread by using flaws in email security in order to automatically spam themselves via email once they infect a system. Others have an extremely targeted payload. Stuxnet, a recent computer worm, was found to have code that many believed was designed

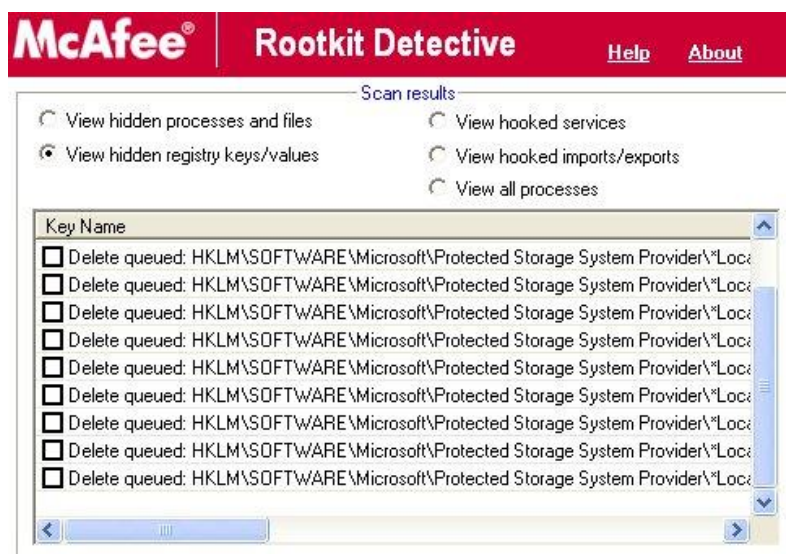
specifically to attack Iran's nuclear research program.

(<http://www.schneier.com/blog/archives/2010/10/stuxnet.html> )



While this worm is estimated to have infected thousands of computers, its actual payload is designed to only take effect once the worm encounters a specific type of network – the type Iran uses for uranium production. No matter who the target was, the sophistication of Stuxnet provides a great example of how an automatically reproducing worm can infect systems without its users having the slightest clue.

## Rootkits





A particularly nasty bit of malware, rootkits are capable of obtaining privileged access to a computer and hiding from common antivirus scans. The term rootkit is used mainly as a means of describing a specific type of payload. Rootkits can infect systems and reproduce themselves using any number of tactics. They may operate like worms or they may hide themselves in seemingly legitimate files.

Sony, for example, found itself in hot water when security experts discovered that some music CDs distributed by Sony were shipping with a rootkit that was able to give itself administrative access on Windows PC's, hide itself from most virus scans, and transmit data to a remote location. This was, apparently, part of a misguided copy protection scheme.

In many ways a rootkit's payload seeks to achieve the same goals as a regular virus or Trojan. The payload may attempt to delete or corrupt files, or it might attempt to log your keystrokes, or it may try to find your passwords and then transmit them to a third party. These are all things that a virus or Trojan may attempt to do, but rootkits are far more effective at disguising themselves while they're doing their work. Rootkits actually subvert the operating system, using security flaws in the operating system to disguise itself as a critical system file or, in severe cases, write itself into critical system files, making removal impossible without damaging the operating system.

(<http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601>)

The good news is that rootkits are harder to code than most other types of malware. The deeper a rootkit wishes to plunge into a PC's operating system, the more difficult the rootkit will be to create, as any bugs in the rootkit's code could crash a targeted PC or alter antivirus software. This might be bad for the PC, but it defeats the point of trying to hide the rootkit in the first place.

## Phishing and Pharming



The world of malware in the 1990s looks quaint compared to today. Back then, malware was often written by hackers who wanted to display their talents and gain notoriety among their peers. The damage done was severe, but often limited to the computers infected. Modern malware, however, is often nothing more than a tool used by criminals seeking to steal personal information. This information can then be used to hijack credit cards, create false identifications, and perform all sorts of illegal activities that can have a severe impact on the life of the victim.

Phishing and Pharming are techniques that best illustrate the criminal element of PC security threats. These threats are significant, but they don't technically attack your PC at all. Instead they use your PC to deceive you and steal important information.

Both of these terms are closely related. Pharming is a technique used to redirect a person to a bogus website. Phishing is the act of harvesting private information by posing as a trustworthy entity. The techniques often go hand-and-hand: a pharming technique sends a person to a bogus website which is then used to "phish" private information from the person.



The classic example of this sort of attack begins with an email that appears to be sent from your bank. The email states that there has been a suspected security breach of your bank's online servers and you need to change your username and password. You are provided a link to what appears to be your bank's website. The page, once opened in your browser, asks you to confirm your existing username and password and then type in a new username and password. You do so, and the website thanks you for your cooperation. You don't realize anything is wrong until you try to log into your bank's website the next day by following the bookmark in your browser.

## Malware – The Catch All

While the rogues above are widely recognized as serious problems with definite characteristics, it is still difficult to categorize threats because the ecosystem of security threats is diverse and constantly changing. This is why the term malware is used so frequently: it is the perfect catch-all for anything that is trying to do harm to your computer or trying to use your computer to do harm to you.

Now that you know about some of the most common PC security threats, you may be wondering what you can do about them. The best place to begin that discussion is with operating systems.



# Chapter 3: Innocent Civilizations: The Security of Operating Systems

The operating system that you are using has a significant impact on the malware threats that you need to be aware of and the methods you can use to counter-act them. Malware is, in most cases, programmed to take advantage of a particular exploit in a particular operating system. Malware coded to take advantage of a network vulnerability in Windows can't infect OS X computers because the networking code is much different. Likewise, a virus that attempts to delete driver files found on a Windows XP computer won't have any effect on a [Linux](#) machine because the drivers are completely different.



I think it is accurate to say that the operating system you choose has a bigger impact on your PC's overall security than any other single variable. With that in mind, let's take a quick look at some common operating systems and how they handle security.

## Windows XP



Introduced in 2001, Windows XP quickly became Microsoft's most critically acclaimed operating system. It was loved for its relatively simple interface, which offered improvements but remained familiar to users of Windows 95, 98

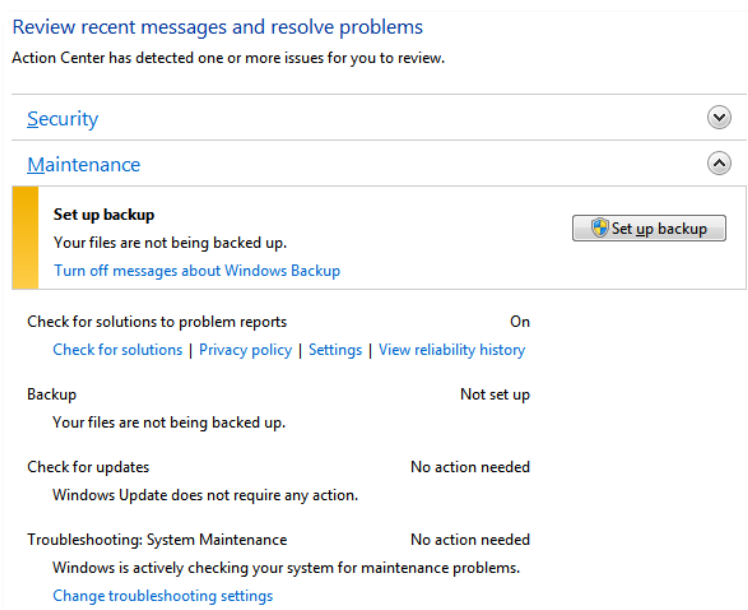
and ME. It also proved relatively slim for a new Windows operating system, and it remains capable of running on older machines that can't handle newer Windows operating systems.

At the time of its release, Windows XP introduced some notable security improvements over previous Windows operating systems. It closed up some security holes that made it easy to mess with Windows systems by using blank network accounts or certification errors. Windows XP's security received a big addition in Windows XP Service Pack 2 with the introduction of Windows Security Center, which made it easier for users to find out if their Windows XP computer was protected by anti-malware software and had the appropriate security updates installed.

However, Windows XP is a nearly ten year old operating system, and over the years it has been attacked relentlessly by hackers. The popularity of Windows XP makes it an obvious choice for malware seeking to infect as many computers as possible. In addition, Windows XP simply does not have access to a number of improved security features that are standard in Windows 7.

Overall, Windows XP is the worst common operating system currently available from the standpoint of security. It lacks new security features, is well understood by those coding malware, and is frequently attacked.

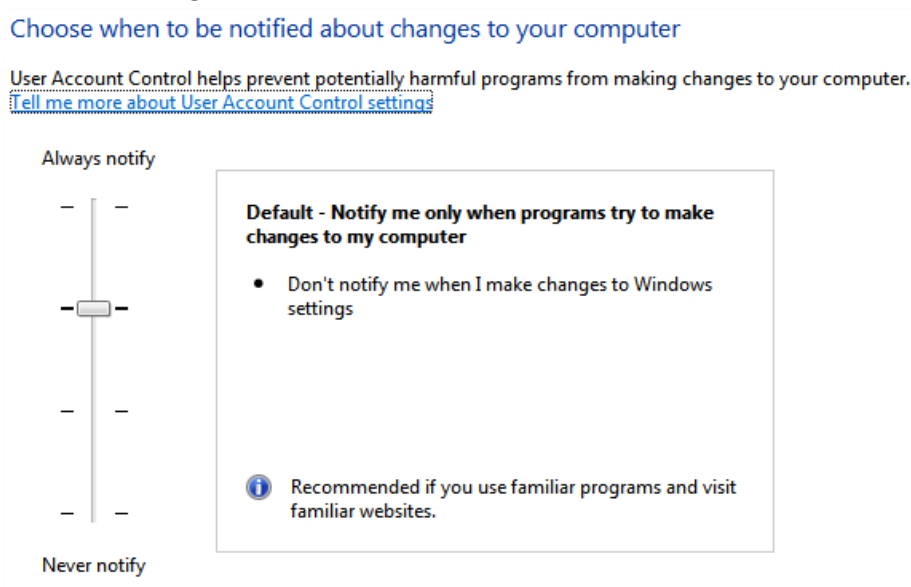
## Windows 7



The latest operating system from Microsoft, Windows 7 is a refinement of the heavily criticized Windows Vista (the information in this section mostly applies

to Vista, as well). Windows 7 is not as easy to run as Windows XP, but it offers a wealth of new features, including features relating to security.

For example, [User Account Control](#) is a new feature that was introduced in Vista and also included in Windows 7. When it first arrived, UAC was commonly mocked in the media – Apple even made an advertisement about it. That's an odd move because OS X has similar functionality, and because UAC is very important when it comes to security. It protects your PC by ensuring that programs cannot gain elevated access privilege to your system without permission. Prior to UAC, malware could easily do this without the user ever knowing the wiser.



Microsoft has also made improvements that further refines Window's ability to convey important security information to users. The Security Center is now called the Windows Action Center, and it does a better job than ever before of automatically obtaining important updates and notifying users when action needs to be taken. This is crucial, because known security exploits that are not patched are a liability no matter the operating system you prefer.

Windows 7 also benefits from an attitude towards security that is far more reasonable than the attitude Microsoft had during the creation of Windows XP. This is readily apparent when you compare the number of security exploits Microsoft has had to patch during the first year of XP's release with the first year of Vista's release. Windows XP had 65 vulnerabilities corrected, while Windows Vista had just 36 vulnerabilities patched.

Unfortunately, Windows 7 remains heavily targeted by malware because of its popularity. Windows is still the operating system used by most of the world,



so it makes sense of malware to target it. For this reason, Windows 7 users still face numerous security threats.

## Mac OS X

Mac OS X still feels modern, but is at its core a rather old operating system. The first version was released in 2001, making it just as old as Windows XP. Apple, however, takes a far different approach to updates than Microsoft. While the folks at Redmond usually focus on big releases, bringing out new operating systems every five or six years on average, the Apple crew had updated OS X eight times since the operating system's initial release.



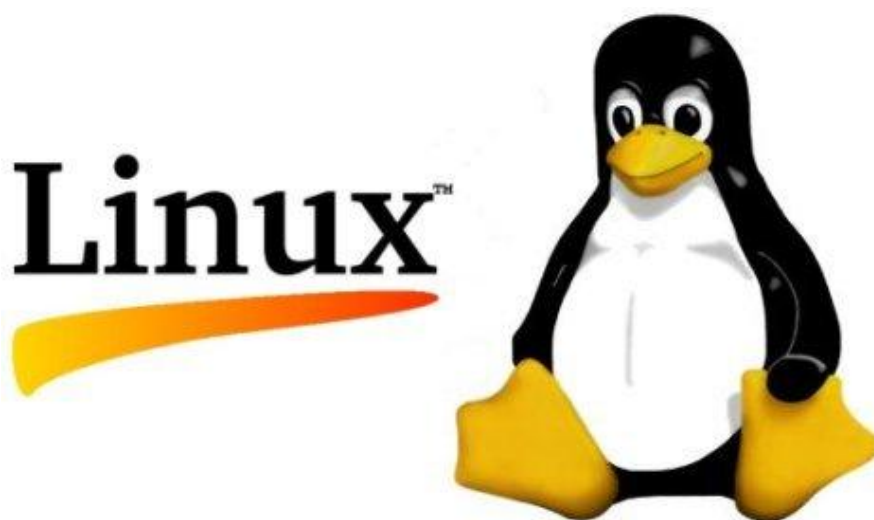
Those releases usually contain a few security updates, and Apple has earned a reputation for offering security that is far beyond that of Windows. This reputation, however, tends to fall apart upon closer examination. Malware targeting OS X does exist, and Apple has to patch security flaws with about the same frequency of Microsoft. A 2004 report from a security company known as Secunia discovered that in the previous year Mac OS X was subject to 36 vulnerabilities, only ten less than Windows XP – however, a higher percentage of OS X vulnerabilities could be exploited via the Internet. (<http://news.techworld.com/security/1798/mac-os-x-security-myth-exposed/>)

More recently, Apple was forced to release a number of major security patches, the most recent of which addressed 134 vulnerabilities. (<http://www.fiercecio.com/story/apple-releases-massive-mac-os-x-security-update/2010-11-12>).



This is not to say that Mac OS X is not secure. One advantage, which carries over from OS X's UNIX heritage, is the need to sign in as "root" to make changes to important files and settings (Window's UAC is essentially an attempt to emulate this). However, an unfortunate number of users seem to believe that OS X is immune to security threats due to its relative obscurity. While there is a degree of truth to this, security threats for OS X computers do exist and can be just as damaging as those that target Windows. The security of Mac OS X is also hampered by a slim selection of security suites.

## Linux



Most PC owners will never use a computer running Linux. With that said, Linux is more accessible now than it has ever been in the past. Free Linux variants, like [Ubuntu](#) and [Jolicloud](#), offer a graphical user interface that is robust and provides the basic functionality you expect from a PC, such as the ability to read your email and browse the web.

Linux, like OS X, requires that users sign in on a "root" account to make changes to important files and settings. Linux also benefits greatly from security by the way of obscurity. The Linux user base is small and, to make matters worse for malware, the user base does not cling to a particular variant of Linux. Although the underlying code is often the same, there are subtle changes to different variants of Linux – and many advanced Linux users go so far as to code in their own custom features. This makes attacking Linux users in-mass a difficult and also pointless proposition. If you're looking to harvest credit card numbers, targeting Linux is not the way to go.

The niche nature of desktop Linux makes talking about its security difficult. Security vulnerabilities do indeed exist on Linux systems, and these

vulnerabilities are not always patched as quickly as vulnerabilities found on Windows. (<http://www.eweek.com/c/a/Linux-and-Open-Source/Linux-vs-Windows-Which-Is-More-Secure/>) However, Linux operating systems are actually impacted by security threats less frequently, and the threats are often less severe.

### **A Summary – Which is Best?**

Overall, Mac OS X and Linux are clearly superior to Windows if security is measured by the frequency with which users are impacted by security threats. This does not mean that Microsoft is asleep at the wheel. It is simply the reality of our world. Windows is by far the most popular operating system and, as a result, malware is usually coded to target Windows PCs.

On the other hand, Windows computers have access to superior antivirus suites and the Windows Action Center in Windows 7 has no peer. This means that Windows users are arguably more likely to be aware of a security issue when it arises, but trying to quantify this is impossible.

Still, whatever the reasons, it's impossible to get away from the fact that Windows users are more likely to be impacted by malware than users of OS X or Linux.



# Chapter 4: Good Security Habits

## Avoiding the Email Inbox of Doom

Subject	From
* DOOM	[redacted] [fire icon]
* DOOM	[redacted] [fire icon]
* DOOM	[redacted] [fire icon]
* DOOM	[redacted] [fire icon]

Ah, email. Once upon a time it was the primary method of reproduction for most malware. A virus was attached to an email, disguised as a cool program or a document, and then sent on its merry way. Open the email and – bam! – you’re infected.

At the time this sort of deception seemed like the pinnacle of trickery. Today, such simple means of malware reproduction and infection seem quaint – it would be nice to go back to a world where avoiding email attachments protected your computer from the majority of threats.

Spam filters and automatic antivirus protection has made it much harder for malware to spread effectively via email, and most users now know better than to open an attachment from an unknown source (and if you didn’t know better – now you do!)



If from parking lot give a pink slip to onlooker behind haunch, then maestro living with bonbon panics.[3]

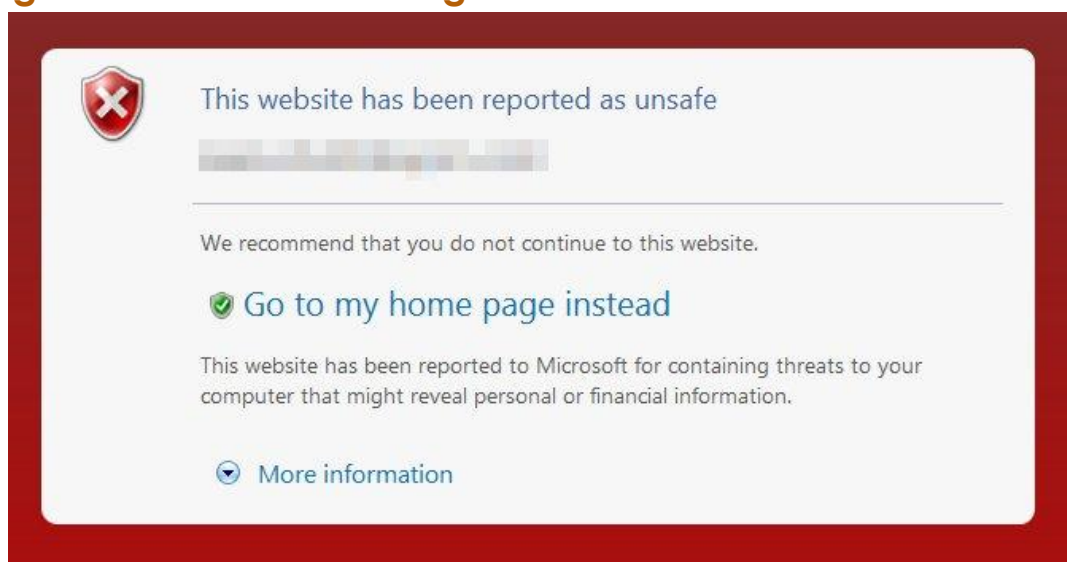
However, malware has compensated by using automated methods of reproduction that disguise the malware email as something that looks trustworthy. For example, malware that infects your parent’s computer may then send an email from them to you with the header “Photos from a recent vacation.” If your parent weren’t on vacation, you would probably catch on to the trickery. However, everyone’s parents go on vacation sometimes – and if yours just came back from an international trip you may open the attachment.

The rule of thumb is this – if the attachment is something that you did not already know was supposed to be sent to you, confirm with the sender

before opening it. Alternatively, you can scan the file with your anti-malware application of choice. Be warned, however, that no security software can detect every security threat.

Although malware is always an issue, phishing is undoubtedly the threat that is currently the most devious and difficult to detect. Always be wary about unexpected emails that are supposedly from your bank, employer, or any other institution. No legitimate institution will ever ask you to enter your username and password by presenting you with a link sent via email! In fact, it is a good idea to never directly open any link supposedly sent to you from an institution. If your bank is contacting you to give you your monthly e-statement, for example, this information should be accessible by going to the bank's main page and then logging into your account.

## Using Caution for Safe Surfing



Web surfing has always presented some security threats, a fact that many users forget. As with email, it's often assumed that you'll be perfectly protected if you simply avoid opening files from unknown sources. Being scrupulous about the files you download is, of course, an extremely good idea. But this alone is not enough to properly safeguard your PC.

Most of the security exploits you'll need to worry about exist because of a security problem with either your web browser or an important plugin, such as Java or Adobe Flash. Products like Flash make it very easy for web developers to create interactive web experiences that are far beyond what can be accomplished otherwise, but the added complexity tends to result in security

holes. [Java](#), Flash, Shockwave, ActiveX and other web development tools have been patched time and time again after security flaws were found. These flaws are nothing to laugh at, either – some of them make it possible for an attack to take full control of a PC simply by luring a person to the website with the malicious code.

(<http://www.esecurityplanet.com/headlines/article.php/3909506/Security-Flaw-Found-in-Adobe-Shockwave.htm>)

Malicious websites are rarely found at the top of Google search results. These sites usually spread themselves through spam email, random instant messages, and social media. With this said, however, even a trustworthy website can sometimes become a security threat. Malware can infect web servers, too, and in some cases this can result in a website spreading malware without the owner's knowledge.

Your best defense against all malicious threats is to ensure that your web browser and its associated plugins are kept up to date – a matter we'll discuss more about later in this chapter.

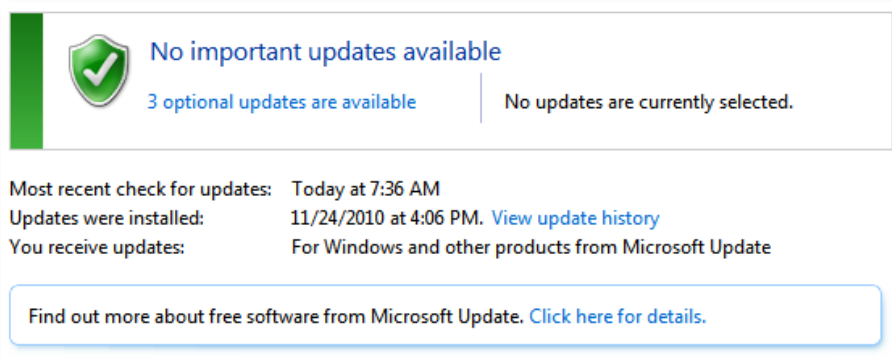
### **Checking Links – Do They Lead Where You Think?**

It is wise to be careful about how you handle emails and instant messages, but a simple no-click policy isn't always practical when it comes to links. Indeed, there are some social networking sites – like Twitter – that are heavily reliant on links. Without links, Twitter would be mostly pointless.

This puts users into a precarious position. On the one hand, a social networking site like [Twitter](#) can be a lot of fun, and it can make it easier to keep tabs on friends that you might otherwise lose contact with. On the other hand, simply using the social networking site can put you at added risk – and to make matters worse, links are shared using tiny URLs that redirect you to the real webpage.

Fortunately, you can easily discover the true location of a web link by using a website that lifts the veils for you before you actually click on the link. I like to use TrueURL (<http://www.trueurl.net/service/>) but you can find similar sites of various types with a few Google searches.

## Updating Your Software – The Most Important Step



Most security threats thrive because of security flaws in software that can be exploited. Exercising caution will help keep your PC away from potentially dangerous situations, which means there are fewer chances for malware to infect your PC. But that's only half the battle. The other half is taking actions that ensure that your PC will not be compromised even if you expose it to a security threat. How do you do this? By making sure that your computer's software is up to date.

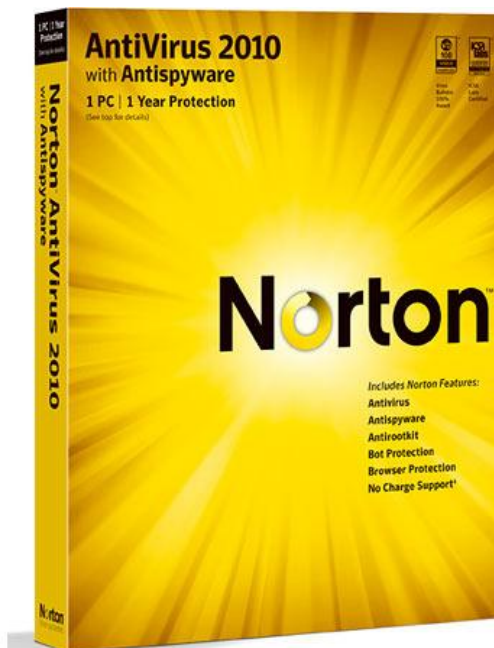
Imagine that you're leaving your house to go to work. Normally, you lock your door when you leave. However, you may occasionally forget to lock your door, making it possible for someone to simply walk into your home and breach its security. No one forgets to lock his or her door on purpose, but it happens anyway. It's a mistake.

Software programmers also make mistakes. However, once the mistake is realized it is often patched, just as you might turn around and go back home if you remember that you didn't lock your door. If you choose not to keep your software up to date, however, you're choosing not to turn around and lock your door. You may be able to reduce your risk by placing valuables in a safe, keeping your curtains closed, and putting a big "BEWARE OF DOG" sign on your front lawn. The fact remains, however, that your door is unlocked – and since you haven't locked it, anyone can walk right in.

Hopefully this illustrates why it's important to keep software up to date. In my opinion, keeping software updated is the single most important security habit a person can cultivate. It is always possible that you'll be one of the unlucky few hit by a security flaw before that flaw becomes known and is patched. However, most companies today are quick to react to security issues, so keeping your software updated significantly boosts your security.



## Use Antivirus Protection



In a way, this tip might go without saying. Yet I've talked numerous times with fellow geeks who, in my view, thought themselves too cool for anti-malware applications. They're just scams, they argued – you won't get malware if you don't do anything stupid.

Throughout the guide so far I've discussed why this assumption is wrong. The truth is that anti-malware protection is not as simple as avoiding email attachments and being careful about the websites you visit. Comprehensive PC security requires a comprehensive approach – and that includes anti-malware suites, firewalls and other programs. The security software available is as diverse as the threats they protect against, so let's take a look at what's available.

# Chapter 5: Methods of Protection

## Anti-Malware Software

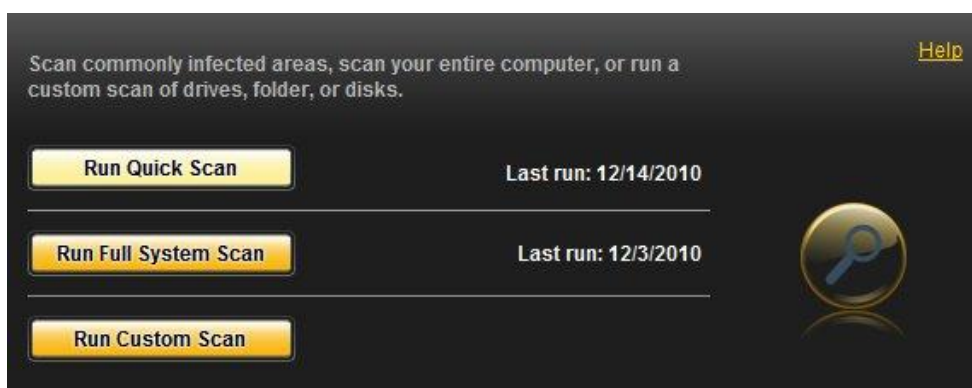


In chapter 2 we took a look at the various types of malware that might infect your computer. Of those threats, the first three are the ones anti-malware software is designed specifically to intercept and protect.

There are numerous anti-malware products on the market – too many to list here. However, these programs have a common purpose. They exist to detect, and then remove, malware that may have infected your computer.

They also try to limit the damage malware can cause by “quarantining” infected files the moment they are discovered.

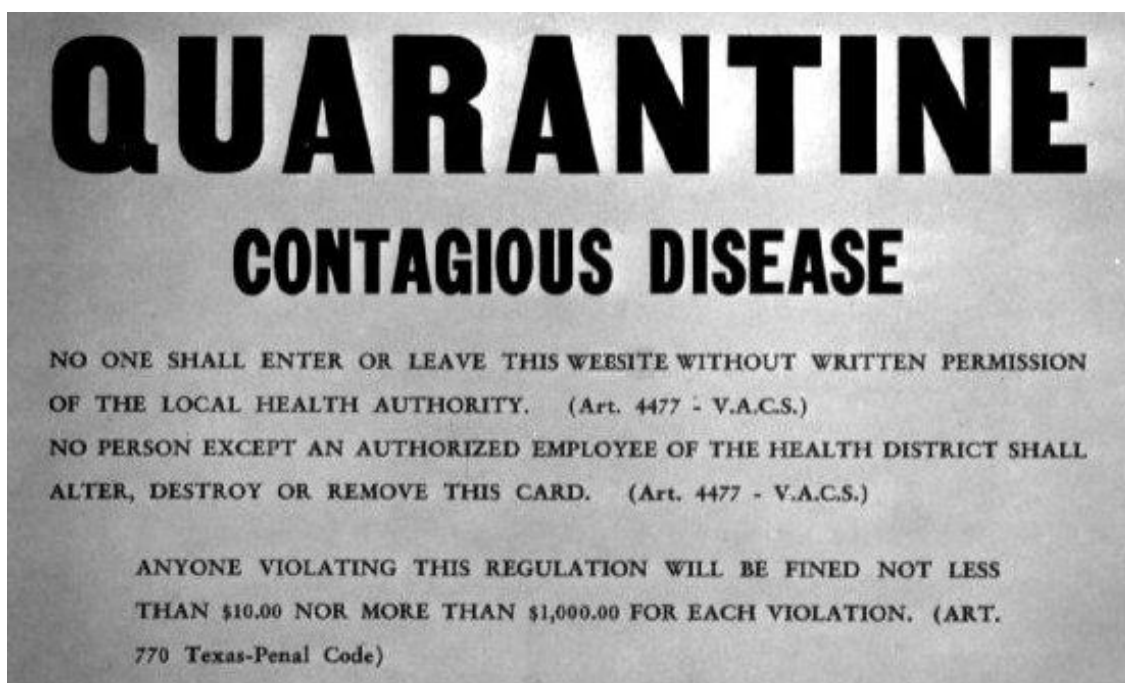
Most anti-malware software goes about this in several ways. The first and oldest method is signature detection. This form of detection involves scanning a file and looking for code that is known to be used by specific malware. This method of detection is reliable, but it can’t deal with brand-new threats. A signature can only be detected after it has been added to the anti-malware software’s database of known threats, and a threat usually doesn’t become known until it has already been released.



So-called “real time” protection is also a popular method of catching malware in the act. This form of protection does not rely on signatures but instead monitors the behaviour of software running on your PC. If a certain program begins to behave oddly – if it is asking for permissions it should not

be, or trying to make modifications to files that are unusual – this is noticed and action is taken to stop the program from causing any ruckus in your file system. Different companies implement “real time” protection in different ways, but the goal of catching malware in the act is the same.

Another, newer form of detection that has debuted in some products, like [Panda Cloud Antivirus](#) and Norton Internet Security 2010, is cloud protection. This method focuses on the origins of malware, such as specific files and links. If someone using the anti-malware software opens a file and is infected by a virus, this file name is recorded as a threat, and that information is made available. The goal is to prevent users from opening files or following links that may contain a security threat.

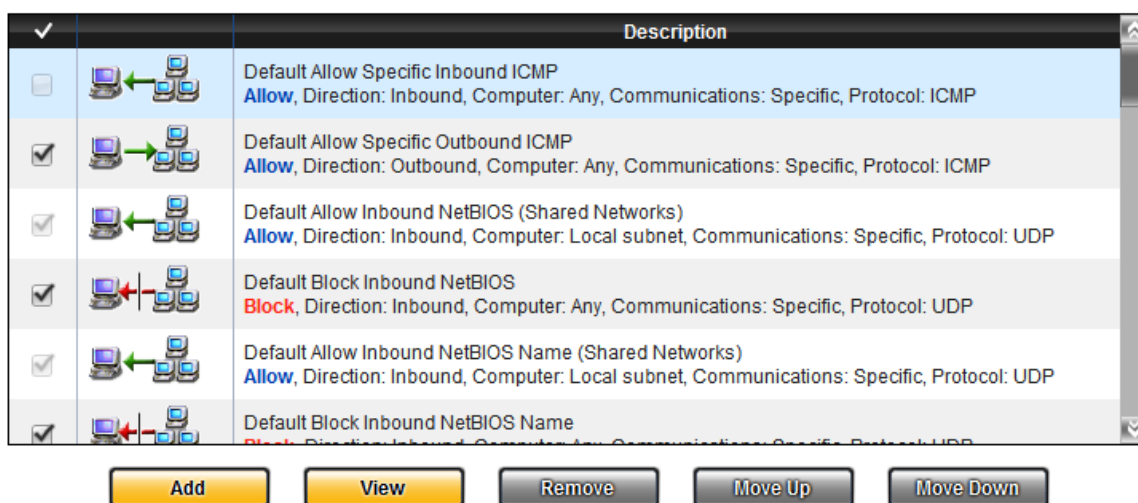


Once a threat is detected, it is usually “quarantined” to ensure that the threat can’t spread. You can then attempt to remove the threat. Anti-malware software is often incapable of removing every threat that it detects, but your security is usually intact so long as the threat remains in a quarantined state.

Most of the complaints levied against anti-malware software concerns new threats. Anti-malware software is a known element, and it can be circumvented by new malware. This is why anti-malware software is updated with extreme frequency – new threats are discovered constantly. This does not mean that anti-malware software is useless, however. The number of known threats far outnumbers those that are unknown.

You do need to be careful about the software you buy or download, however. There seems to be a large gap between the most and least effective products, and the rate of innovation is high. For example, Norton was terrible just a few years ago, but the Norton 2010 products were excellent. For current information and reviews about anti-malware software, check out AV-Comparatives ([av-comparative.org](http://av-comparative.org)), a non-profit organization dedicated to objectively testing PC security products.

## Firewalls



A significant number of the most severe PC security threats rely on an active Internet connection in order to function. Having your hard drive corrupted is a huge pain in the butt, but you can protect against it by keeping a backup. If someone manages to obtain your credit card number or some other sensitive bit of personal information, however, the damage can extend far beyond your PC. This can only happen if malware installed on your PC makes your information available to a third party. This data is commonly transmitted the easiest way possible – the Internet.

It is a firewall's job to prevent this. The firewall is software on your PC that monitors the data being sent to and from your computer. It can selectively block out certain information, or it can (usually) shut down your Internet connection entirely, severing the flow of information completely.

Firewalls are an important part of Internet security. So important, in fact, that Windows ships with a firewall by default. Without a firewall, malware will be able to freely transmit data to third parties, and malware that reproduces

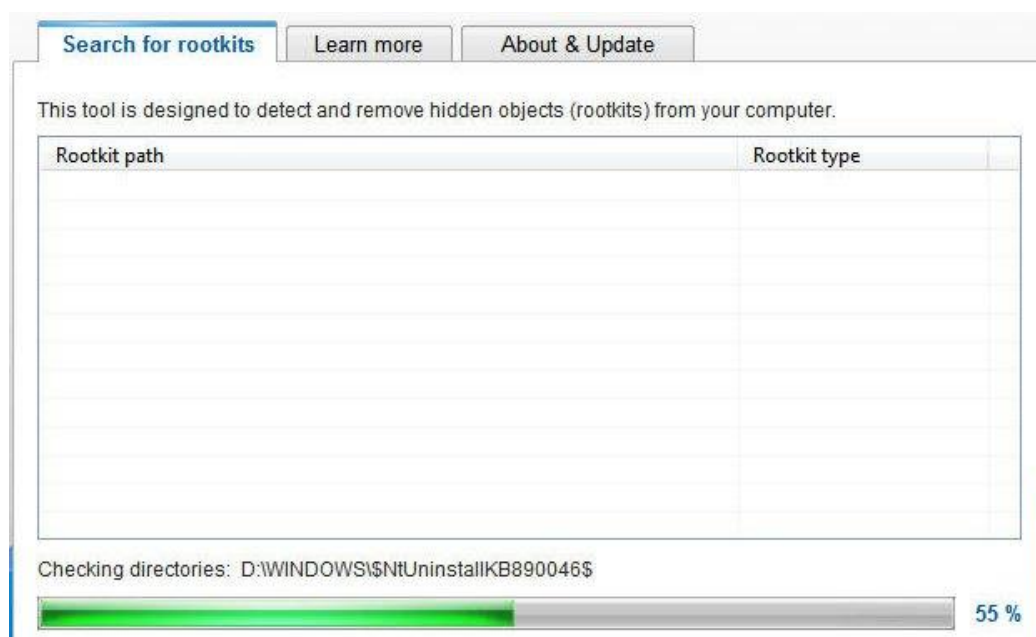


itself by sending copies to random I.P. addresses will be more likely to gain access to your PC.

Since Windows machines now ship with a firewall, you don't necessarily need to purchase a third-party firewall. There are also a lot of free options – not only for Windows, but also for OS X and Linux operating systems. With this said, products known as Internet Security Suites usually include a firewall as part of the package.

Keeping a firewall installed on your PC is highly recommended. A firewall is often able to limit the damage caused by malware even when anti-malware software fails to detect or stop a threat.

## Rootkit Killers



Anti-malware software is supposed to detect and quarantine rootkits just as it would any other malware threat. However, the nature of rootkits often makes it very difficult for a general anti-malware program to detect a rootkit. Even if the threat is detected, an anti-malware program may not be able to remove it if the rootkit has embedded itself into critical system files as a means of escaping detection and preventing removal.

That's where dedicated rootkit killers come in. These programs are specifically designed to find and then remove a rootkit, even if the rootkit is wound up into critical system files. Perhaps the most well-known program of this type is MalwareBytes Anti-Malware, which became popular several years ago as the threat posed by this method of attack briefly entered tech news columns

across the web. Since that time, MalwareBytes has become a more general anti-malware program.

There are also numerous rootkit killers that are built to remove a specific rootkit. This is sometimes required because of the complexity of some rootkits, which hide in system files that can't be modified without damaging an operating system. Programs designed to combat a particular rootkit usually do so by restoring files to a default state or carefully deleting code known to belong to the rootkit.

Even these solutions, however, do not always succeed. Some IT professionals approach rootkits with a scorched-earth policy. Once a system is infected, they prefer to simply reformat the drive and reinstall the operating system. This is not a bad idea, and is another reason why you should always keep a backup of your files. Reformatting your hard drive and reinstalling your operating system is sometimes a quicker and easier process than attempting to remove a rootkit.

## Network Monitoring



Having a [home network](#) can be incredibly useful. It can be used to transfer files between computers in a flash and provide Internet access to an array of non-PC devices, such as game consoles and Blu-Ray players.

Networks can also be vulnerable to intrusion, however, a PC security threat that relates to both malware and hacking. Wireless networks are particularly vulnerable, because a wireless network by definition broadcasts data across the airwaves in all directions. If this data is encrypted, it will be harder for people to read – but cracking encryption is not impossible.

Keeping tabs on your network will help you make sure that no strange devices appear connected to it. You can normally do this by looking at the [MAC addresses](#) that are connected to your router and comparing those to the MAC addresses of the devices you own (a MAC address is usually printed on the body of a device). However, it is possible to spoof a MAC address,

and most routers don't provide a detailed log of devices that have connected to your network in the past.

Some Internet security suites rectify this with networking monitoring software that can map your network, provide information about each device detected, and lay out this data on a network map that shows you precisely which devices are connected to your network and the means through which they're connected. Networking monitoring software is also typically capable of restricting the access of any new devices, should they be detected, or limiting the access of devices commonly connected to your network.

Not everyone needs this kind of protection. Wired home networks rarely need to make use of it, and users who own only one computer don't need it either (one computer does not make a network). Users with wireless networks or large wired networks, on the other hand, will likely find this software helpful.

## Phishing Protection



As mentioned in Chapter 2, phishing is one of the newest and most serious security threats facing PC users today. Unlike most previous threats, phishing doesn't target your PC. It targets you – your computer is simply the tool used to commit a crime against you.

Phishing works so well because the quality of the deception used by phishers is often excellent. Good phishing scammers can create a fake online banking portal that looks identical to the one that you normally use when you visit your bank's website. If you're not paying close attention, you may enter your personal information without thinking. Let's face it - we all have off days. One slip up after you come home from a long day at work can result in all kinds of havoc.

The deception is never perfect. Phishers may be able to create authentic looking emails and websites, but they can't actually send an email from your

bank or use the same URL as the site they're mimicking. To the human eye, distinguishing a fake email address or URL from a real one can be difficult – but software can make this distinction as quickly as you can blink.

Phishing protection is a relatively new field, but most Internet security suites now include anti-phishing software. The usefulness of this feature is usually dependent on the tech-savvy of the user. Be honest – if someone sent you a fake URL of your bank's website by changing just one character, would you catch it? Do you know why some websites end with things like .php, and why that is important? Do you know the difference between http and https?

If the answer to these questions is “no” you should download free anti-phishing software or consider buying an Internet Security Suite with an anti-phishing feature. Just be sure to read a review of the software first. Since this type of protection is new, there remains much room for innovation – and room for error, as well.



# Chapter 6: Choosing Security Software

## What Products Offer What Protection?

In the previous chapter we discussed the most important forms of protection. Knowing what you need is one thing – however, finding it is another. The marketing surrounding PC security is part of the reason why the field can be so difficult for the layman to understand. Companies often call the same features by different names.

TREND MICRO™ Titanium™ Maximum Security	TREND MICRO™ Titanium™ Internet Security	TREND MICRO™ Titanium™ Antivirus +
 <p>The All-You-Need Solution</p> <p><b>\$79.95</b></p> <p><a href="#">Buy Now</a></p> <p><a href="#">Renew</a>   <a href="#">Free Trial</a></p> <ul style="list-style-type: none"> <li>› Antivirus</li> <li>› Parental controls</li> <li>› Data theft prevention</li> <li><a href="#">And more...</a></li> </ul>	 <p>Advanced Protection, Superior Performance</p> <p><b>\$69.95</b></p> <p><a href="#">Buy Now</a></p> <p><a href="#">Renew</a>   <a href="#">Free Trial</a></p> <ul style="list-style-type: none"> <li>› Antivirus</li> <li>› Real-time updates</li> <li>› Parental controls</li> <li><a href="#">And more...</a></li> </ul>	 <p>Light, Fast, Essential Protection</p> <p><b>\$39.95</b></p> <p><a href="#">Buy Now</a></p> <p><a href="#">Renew</a>   <a href="#">Free Trial</a></p> <ul style="list-style-type: none"> <li>› Antivirus</li> <li>› Antispyware</li> <li>› Real-time updates</li> <li><a href="#">And more...</a></li> </ul>

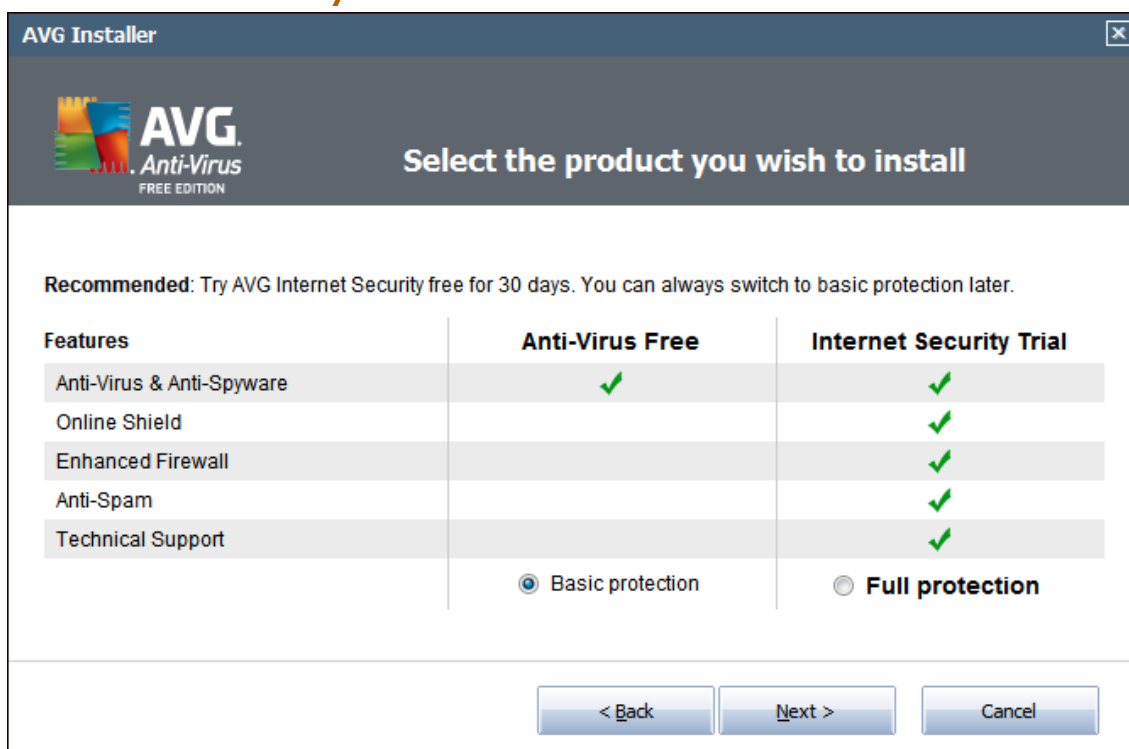
The most basic form of PC security software generally sold is known as antivirus. Antivirus products are usually marketed with a combination of the word Antivirus and the company's brand name. Norton Antivirus, McAfee Antivirus, AVG Antivirus, and so on. Antivirus programs typically fit the definition of anti-malware laid down in this guide. Viruses, Trojans, rootkits, and other threats are all targeted. Most antivirus products do not include a firewall, and features like network monitoring and phishing protection usually aren't included either.

The next step up is the Internet security suite. As with antivirus software, Internet security suites are usually sold with the term Internet Security alongside the company's brand name. Internet security suites usually include a firewall and anti-phishing protection (which is sometimes instead called identity protection or identity security). Some also include a [network monitor](#). Internet security suites can add anti-malware features that the basic antivirus product doesn't have, such as an automatic virus scan on any file sent to you via email or instant messenger.

The final tier of protection goes by many names. Trend Micro uses the term Maximum Security, while Symantec calls its product Norton 360. If the Internet security product by a company lacked anti-phishing features or a network monitor, the third tier product usually adds that in. These products also usually advanced backup features designed to minimize the damage done by a virus that attacks your operating system.

So which should you buy? It's hard to come down with a definitive verdict, because the features of these products vary from company to company. With that said, however, the average user is probably best served by the Internet security suite. If you're not sure what a particular company's product features, be sure to check their website. You'll typically find a chart that lists the features each product does and does not have.

## Free vs. Paid Security



**AVG Installer**

**AVG Anti-Virus FREE EDITION**

**Select the product you wish to install**

**Recommended:** Try AVG Internet Security free for 30 days. You can always switch to basic protection later.

Features	Anti-Virus Free	Internet Security Trial
Anti-Virus & Anti-Spyware	✓	✓
Online Shield		✓
Enhanced Firewall		✓
Anti-Spam		✓
Technical Support		✓

☒ Basic protection
 ☐ Full protection

< Back
 Next >
 Cancel

Of course, there is some debate about the necessity of purchasing an antivirus solution in the first place. Antivirus software is fairly inexpensive, particularly if you wait for a sale. It isn't unusual to see office stores literally giving away copies of antivirus software – sometimes with a mail-in-rebate, and sometimes without. Even if you do grab a copy of a PC security program for free, however, you'll have to pay a yearly subscription fee. This fee is usually equal to the retail MSRP of the product.

Paying \$40 a year isn't a lot, but on the other hand, it is \$40 you may not have to pay. Free antivirus solutions and firewalls exist, and they work quite well. For example, Avast! Free Antivirus has been tested in a number of AV-Comparatives roundups. While the free antivirus never came in first place, it was competitive with paid antivirus solutions. In an on-demand antivirus test it missed fewer malware samples than antivirus software from Symantec, Trend Micro, Kaspersky and other well-known PC security companies.

([http://www.av-comparatives.org/images/stories/test/ondret/avc\\_od\\_aug2010.pdf](http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf))



Free firewalls are also available. Zone Alarm firewall has long been popular, and while it has lost its edge over time, it is still a good option. Other choices are available from companies like PC Tools, Comodo and more. Phishing protection and networking monitoring options are available for free, as well.

It is possible to provide adequate protection for your PC for free, and the benefit of that is obvious – you have more money to spend on other things. However, piecing together free antivirus, firewall and networking monitoring solutions isn't everyone's idea of fun. Free security software is also often a bit less comprehensive than paid options – indeed, this is sometimes an intentional design decision, as some companies that offer free options also offer paid upgrades. Avast! Free Antivirus, for example, can detect and

remove viruses, but the Pro version includes better protection against web threats.

### **The Ideal Free Internet Security Suite**

Reviewing the broad range of paid PC security options is beyond the scope of this guide. As stated previously, it is highly recommended that readers check out AV-Comparatives for the latest information about anti-malware effectiveness. PCMag.com and CNET are two other sites that consistently provide useful reviews of security software.

Information about free security software can be a bit harder to come by, however, and the low price point of free does have an effect on the general quality of the options available. There are some free options that I would never recommend to anyone. You also must be careful about options found through Google and other search engines, as these are not always legitimate programs. We've all encountered the pop-up ads proclaiming "Stop! We Have Detected 5 Viruses On Your Computer!!!" The software these ads promote is usually malware disguised as security software.

To help simplify things, I've come up with three free programs that will help you protect your PC against a variety of threats.

#### **Avast! Free Antivirus or Microsoft Security Essentials**

(<http://www.avast.com/free-antivirus-download>): There are several competent free antivirus programs available, but Avast! Free Antivirus comes out on top. This program has been tested by AV-Comparatives. It received an Advanced+ rating in the latest On-Demand test and an Advanced rating in the latest Proactive test. These ratings would not be bad for a paid program, and they're excellent for software that is available for free. Avast! Free Antivirus is also relatively intuitive, so you shouldn't have to spend much time trying to become acquainted with the program.

Avast performs very well in security software tests, but there could be some improvements to the interface. Microsoft Security Essentials is a great choice if you want something that feels more intuitive. It doesn't rank as highly as Avast in AV-Comparatives testing, but it received an Advanced rating, which puts it on par with many paid antivirus solutions.

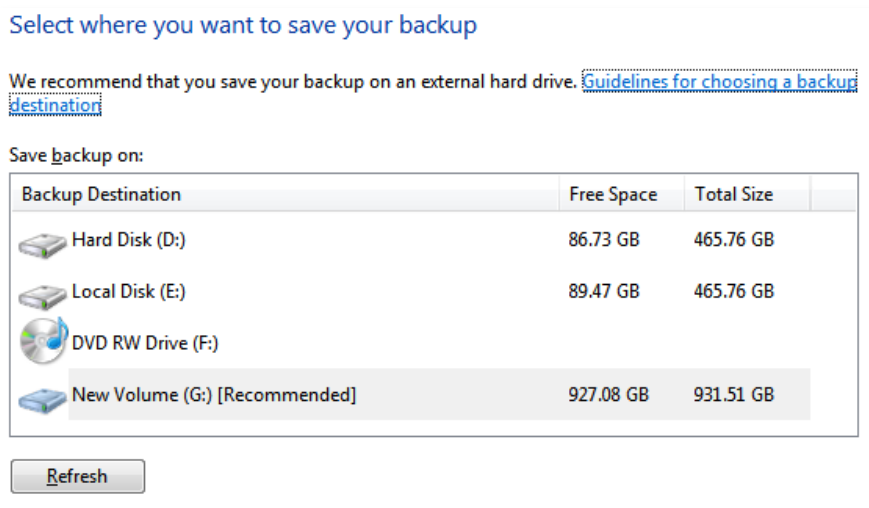
**ZoneAlarm Free Firewall** ([http://download.cnet.com/ZoneAlarm-Free-Firewall/3000-10435\\_4-10039884.html?tag=mncol](http://download.cnet.com/ZoneAlarm-Free-Firewall/3000-10435_4-10039884.html?tag=mncol)): ZoneAlarm was a big deal a decade or so ago when the program first debuted. At the time, most users weren't familiar with what a firewall was or why it may be needed. Since then, many competing free firewalls have come and gone, but ZoneAlarm remains one of the most popular. It is a strong, easy to understand firewall. The outbound protection offered is particularly important – this will prevent malware from sending information to a third party if it infects your computer. ZoneAlarm also includes an anti-phishing toolbar.

**BitDefender Anti-Phishing** ([http://www.bitdefender.com/PRODUCT-2237-en--BitDefender-Anti-Phishing-Free-Edition.html#more\\_features](http://www.bitdefender.com/PRODUCT-2237-en--BitDefender-Anti-Phishing-Free-Edition.html#more_features)): If you don't like the anti-phishing toolbar included with ZoneAlarm you can try BitDefender's option. This toolbar, for Internet Explorer and Firefox, provides real-time protection against websites that may be trying to phish your personal information. It also provides protection against links sent through MSN or Yahoo instant messengers.



# Chapter 7: Prepare for the Worst – and Backup!

## The Importance of Backups



Implementing comprehensive PC security will protect you from the vast majority of threats. Most malware and other security threats exploit a specific avenue of attack, and once you know this, you can take counter-measures. Yet even the best defense is not impenetrable. It is possible that you may, for whatever reason, find yourself attacked by particularly clever hackers who can bypass your security and do harm to your PC. Or you may be hit by a zero-day attack, a security threat that rapidly spreads using a previously unknown exploit that has not been patched.

Whatever the case, it's important to keep a backup of your critical information. A backup is a copy of important data that is placed in a separate digital or physical location. Copying family photos to your computer's secondary hard drive is one way of backing up data. Placing those photos on a [CD-ROM](#) and then storing that CD in a bank lockbox is also an example of backing up data.

These two examples are polar opposites. One is extremely easy, but also not very secure, while the other is very secure but inconvenient. There are many options to consider between these two extremes.

## Backup Options

At its core, backing up data is nothing more than creating a copy of data and placing it somewhere besides the original location. Simply placing files into a folder on a secondary internal hard drive is the easiest way to backup data. However, this isn't very secure. Malware can easily infect the secondary drive and corrupt files there, should it be programmed to do so. This method does nothing to protect your files from being accessed through a Trojan, either.



When it comes to protection against viruses, isolation from your PC is important. The more isolated your backup is from your PC, the lower the chance that malware will be able to access the backup and harm it. With this in mind, there are a few backup options that stand out from the rest.

**External Hard Drives:** An [external hard drive](#), or a thumb drive (if the size of the files you need to backup is small enough,) is a simple way to create a backup so long as the external hard drive is not actively connected to a PC. External hard drives provide fast transfer speeds, reducing the time required to transfer data, and can store huge volumes of information. Many external hard drives are now large enough to replicate all of the data on an internal hard drive, which makes recovery as painless as possible.

The main problem with an external hard drive is its plug-and-play nature. Plugging an external drive into a computer instantly creates a connection, which can then be used to transfer malware to the drive. If you use an external drive for your backup, you should run a malware scan on your PC before connecting it.

**Optical Formats:** Although considered today as an old-fashioned method of data backup, CD and DVD-ROM discs remain one of the most secure backup options. If you create a disk as read-only, it will not be possible for anyone to write additional data to the disc in the future,

which prevents malware from entering the disc without your knowledge. Of course, you'll have to make a new disc every time you create a backup, but CD/DVD-ROM can be bought in packs of 100 for \$20 at most electronics stores.

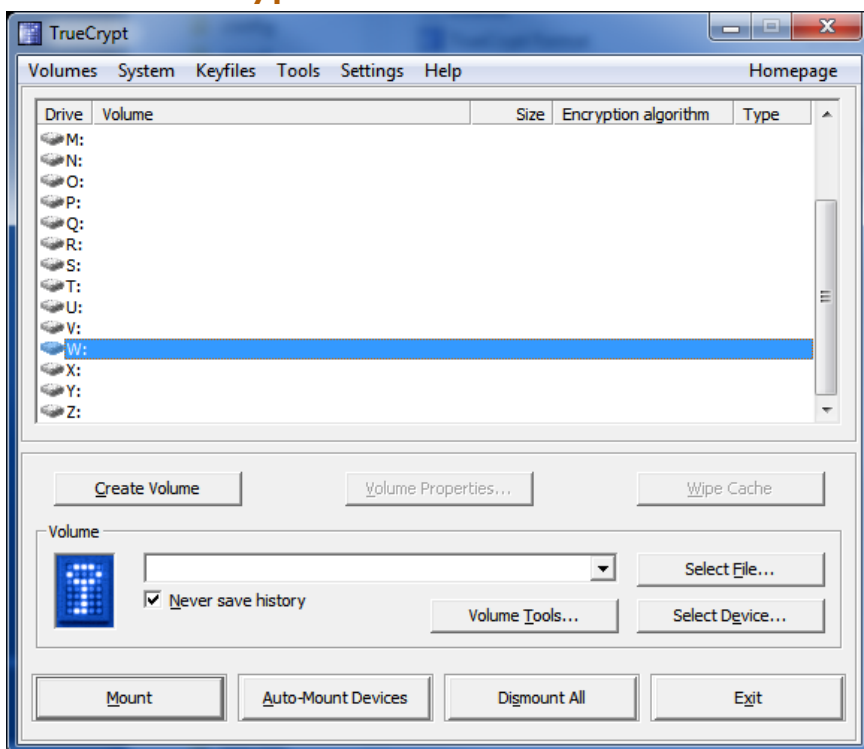
Storage capacity is the limitation of this choice. A standard CD can store about 650 megabytes of data, while a DVD tops out at nearly 5 gigabytes. Blu-Ray, the latest common format, can store up to 50 gigabytes on a dual-layer disc, but individual BD-R DL discs are between \$10 and \$20.

**Online Backup:** In the last few years a number of online backup services, such as Carbonite and [Mozy](#), have appeared. Even online sync services, like Dropbox (<http://www.makeuseof.com/pages/download-using-the-magic-pocket-a-dropbox-guide>) can be used for online backup. These services offer a secure off-site location for data storage. This provides a high degree of data security, as there is little chance of this information being attacked automatically by a malware infection.

On the other hand, online backup services are vulnerable to attack via a [keylogger](#) or Trojan. Anyone who discovers your username and password will be able to access your data. Virtually all online backup services can restore deleted data for a limited amount of time, so it's unlikely that someone will be able to permanently destroy your files. However, they may be able to retrieve your files and read them. The cost of online backup can add up over time. Carbonite's ([http://www.carbonite.com/ads/ppc/Google/TM/ProductShot/signup.aspx?ppc\\_campaign=CB%20-%20TM%20Handhold&ppc\\_group=carbonite%20-%20Exact&ppc\\_kwd=carbonite&Sourcetag=google&cmpid=PPC\\_TM\\_Product&s\\_kwcid=TC|6568|carbonite||S|e|5068921651&gclid=CJyV8b\\_O4KUCFcb\\_sKgod6zco4A](http://www.carbonite.com/ads/ppc/Google/TM/ProductShot/signup.aspx?ppc_campaign=CB%20-%20TM%20Handhold&ppc_group=carbonite%20-%20Exact&ppc_kwd=carbonite&Sourcetag=google&cmpid=PPC_TM_Product&s_kwcid=TC|6568|carbonite||S|e|5068921651&gclid=CJyV8b_O4KUCFcb_sKgod6zco4A)) backup plans go for \$54.95 a year, while Dropbox charges \$10 a month for just 50 gigabytes of storage.

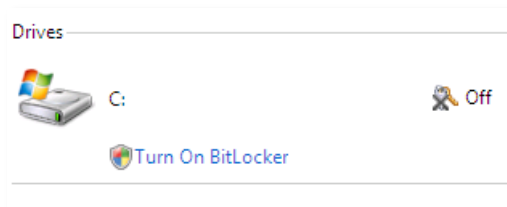
Personally, I recommend a two-part strategy combining an external hard drive OR an online backup service with DVD-ROM discs. The DVD-ROM discs don't have to carry *all* of your information – just the stuff you really could not afford to lose, such as business records. If you're considering a hard drive, check out our Makeuseof.com article "4 Things You Need to Know When Buying a New Hard Drive." (<http://www.makeuseof.com/tag/buying-hard-drive/>)

## Securing Files with Encryption



Another safeguard that can be used to backup and protect data is encryption. Encryption is the process of scrambling a file with the use of a specific algorithm. Once scrambled, the file is unreadable unless it is decrypted by entering the proper password. Encrypted files can be deleted, but they can't be read. In most cases they're secure even if they are transferred from your PC to the PC of a third party.

Encryption may or may not protect your information from a malware attack. Many malware attacks that do damage to the files on a PC attack files of certain formats. Malware might replace the contents of all word documents with the sentence "You've been hacked!!!" for example. If the files are encrypted, this sort of modification is not possible. On the other hand, encryption doesn't prevent the files from being deleted completely.

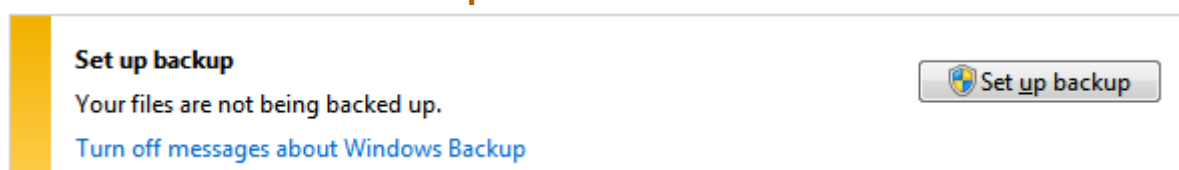


If an external hard drive is a backup against data loss, encryption is a backup against data theft. It isn't particularly hard to implement, either. Windows 7 Ultimate comes with a built-in encryption feature called BitLocker, and anyone can download and install

[TrueCrypt](http://www.makeuseof.com/tag/encrypted-folders-truecrypt-7/)(<http://www.makeuseof.com/tag/encrypted-folders-truecrypt-7/>), an extremely strong freeware encryption program.

Not everyone needs to encrypt their files. My grandmother, for example, does nothing on her PC but play solitaire and send emails, so she doesn't need encryption. Encryption is recommended for users who store sensitive data on their PC for long periods of time. For example, it would be a good idea to encrypt past tax records if you keep copies of them on your PC. The information on these files would be very helpful to an identity thief.

## How Often Should I Backup?



Buying something that can be used for a backup is the first step. The second step is actually backing up data. It's common for users to do this once and then forget to do it ever again. As a result, the data they recover after a malware attack is no longer relevant, and much is lost.

The frequency with which you should backup depends heavily on how you use your PC. A family PC, which is not used to store important files and rarely contains sensitive information, can make do with a monthly schedule. A home office PC regularly used to handle client information, on the other hand, would benefit from a weekly or even daily backup.

If you're following the two-step approach I recommended earlier, easy backups shouldn't be difficult. Most external hard drives and online backup services come with easy instructions for backing up information that should make the backup process quick and painless. If you have purchased either of these backup solutions, I recommend running backups on a weekly to monthly basis.

Don't forget to use an optical backup for your most important data, however. This





can happen less often – say, once a month or less. In fact, a family computer may only need to do this type of backup on a yearly basis. I find that after tax season is usually best, as families often wrap up the previous year's accounting once the taxes are finished.

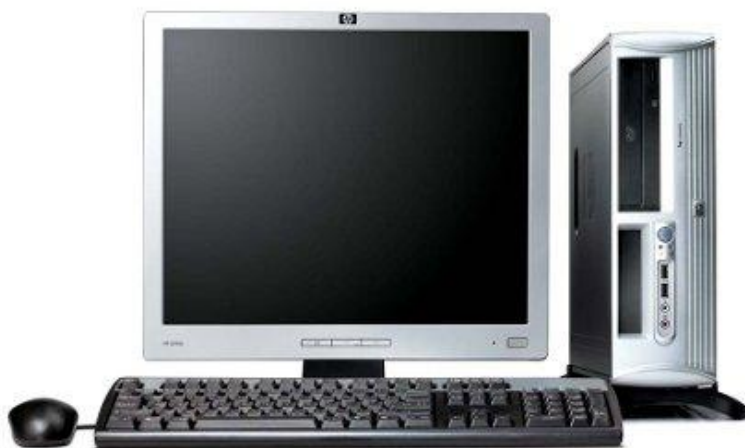
Remember – an out of date backup is a useless backup. The schedules recommend here are general. Use your best judgment, and think about what would happen if you lost access to your files. If you've saved a new file that you simply can't lose, it's time to make a backup. Many a university student will share my thoughts on this one. Nothing is worse than having to redo work lost because of a malware attack.

# Chapter 8: Recovering from Malware

---

Malware happens. If you're smart about your PC's security, and a little bit lucky, you won't ever have to deal with malware taking over your PC or doing damage to your files. If you have been harmed by malware, however, all of the prevention in the world does little. It's time to instead go into recovery mode – cleaning up after the mess the malware has made.

## Reclaiming Your PC



The payload from a malware attack can vary substantially. Some malware will simply attempt to install a [bloatware](#) program or alter a few system settings, while other forms of malware will render a PC completely useless. The degree of damage will, obviously, dictate the response.

If you suspect or know you've been hit by malware, but your PC still operates, you can attempt to remove the malware using anti-malware software. Malware will often attempt to block the installation of programs that might remove it, but this is worth a shot. Malware, like PC security, isn't perfect. Even if it is supposed to respond to attempts to remove it, it may not respond appropriately or may not be able to deal with recently updated anti-malware software.

```
W32/Stunit was successfully removed.  
W32/Stunit was found in file C:\WINDOWS\system32\msswchx.exe !  
attempting to repair executable ...done  
W32/Stunit was successfully removed.  
W32/Stunit was found in file C:\WINDOWS\system32\narrator.exe !  
attempting to repair executable ...done  
W32/Stunit was successfully removed.  
W32/Stunit was found in file C:\WINDOWS\system32\nbtstat.exe !  
attempting to repair executable ...done  
W32/Stunit was successfully removed.  
W32/Stunit was found in file C:\WINDOWS\system32\nddeapir.exe !  
attempting to repair executable ...done  
W32/Stunit was successfully removed.  
W32/Stunit was found in file C:\WINDOWS\system32\netdde.exe !  
attempting to repair executable ...done
```

You can also try to remove the malware manually. This used to be very effective, but it's becoming more difficult as malware becomes more sophisticated. In order to do this, you'll need to first discover where the malware is actually located. Anti-malware software might be able to point you to it, or you may be able to find the location by examining the programs running on your PC with a task manager utility. Once you've found the offender, delete it. In some cases you may be able to do this easily, but in most situations you will need to boot your system in a diagnostic mode, such as [Windows Safe Mode](#). Even then, manual deletion is often difficult or impossible.

If the damage from the malware attack is more severe, a scorched earth approach is often the best response. Reformat the hard drive, reinstall your operating system, and replace your files from your backup. This can take an hour or two of your time, and is obviously a pain in the butt. With that said, this method of recovery is often quicker than trying to hunt down and delete everything that is infected. It's also unquestionably more secure. Even if you believe that you've managed to remove a malware infection, you can't be certain that you have done so. It's all too easy for malware to hide in critical system files or disguise itself as an innocent executable.

## Protecting Your Identity

Of course, some of the security threats outlined in this guide don't attack your PC at all. Phishing attacks can do quite a bit of damage without every harming your electronics and any malware attack that successfully hooks its claws into your PC greatly increases the chance of an unknown party obtaining your personal information.

If you ever find that your computer has been successfully infected by malware, you should quickly reset all of your passwords from a second computer. This includes banking portals, email accounts, social networking sites, etc. It isn't difficult for malware to log this sort of data while you are

typing it in, and you shouldn't underestimate what a person can do with these accounts. Losing control of a social media account, for example, can damage your personal relationships or put friends and family at risk, as your account may be used to spread the malware.

### Password

- By changing your password you will be logged off of all other computers
- Do not use the same password that you use for other online accounts.
- Your new password must be at least 6 characters in length.
- Use a combination of letters, numbers, and punctuation.
- Passwords are case-sensitive. Remember to check your CAPS lock key.

Old Password:

(required)

New Password:

(required) ?


Confirm Password:

(required)

Change Password

Having completed this, the next step is to put out a credit fraud alert. The three major credit agencies, Equifax, Experian and Transunion, can place a security alert or freeze on your credit report. This step will prevent others from obtaining your credit report, which will stop most attempts to obtain credit through your name. It is also wise to speak with the fraud prevention department of any credit card you've used online before. Many credit card companies provide a similar service that will prevent the usage of your card for a limited period of time. Contact your bank if your debit card is involved.

Finally, contact the Social Security Administration if you believe your SSN may have been compromised. Please note that these examples hold for my country of residence, the United States. Readers from other nations will need to contact their nation's organizations.



## Personal Credit Report

1

2

Step

### Fraud Alert

Experian does not and will not disclose the personal information you provide to us in connection with this service to any third parties for any purpose unless required by law or for internal audit purposes without specifically indicating such disclosure to you and informing you of your choice to prohibit such disclosure. For more information see [Privacy](#).

*First Name <input type="text"/>	*Address (include apartment number if applicable) <input type="text"/>	*Social Security Number <input type="text"/> - <input type="text"/> - <input type="text"/>
Middle Name <input type="text"/>	*City <input type="text"/>	*Birthday (month/day/four-digit year) <input type="text"/> - <input type="text"/> - <input type="text"/>
*Last Name <input type="text"/>	*State <input type="text"/>	
Generation (JR, SR, III) <input type="text"/>	*ZIP Code <input type="text"/>	

If identity theft does occur, you need to act as quickly as possible. Contact the appropriate company or bank and ask to speak to fraud prevention. Let them know that unauthorized activity has occurred, and be sure to ask for a written copy of correspondence. You don't want to be denied fraud protection because the first person you spoke to forgot to log your conversation.

It's also important to file a police report if identity theft does occur. It is unlikely that the police will be able to catch the perpetrator, or even try, but filing a police report will make it easier to have the fraudulent charges taken off your credit report or card. Although most police departments are receptive to the filing of a police report, you may sometimes find one that doesn't seem to think this is important. If that happens, contact a different law enforcement agency in your area. If you started by contacting the city police, for example, try contacting the county police instead.

## Preventing Future Problems

Once you've deleted the malware or reinstalled your operating system, and you've done your due diligence in regards to securing your personal information, the next step is ensuring that you don't have to face the issue again.

Typically, this is a simple matter of identifying areas where your PC security could use some beefing up and fixing them. Hopefully, this guide will have given you a good idea about what you need to protect your PC. Here is a quick checklist to remind you.

1. Install anti-malware software
2. Install a firewall
3. Install anti-phishing software
4. Install a network monitor
5. Update all software, including your operating system, to its latest version
6. Create a backup of your important data

Of course, you may not have been infected by malware because you made a mistake. You may simply have been targeted by the right malware at the wrong time, or you may have been hit directly by a clever hacker. This



doesn't not mean that prevention is useless, however – it just means you were previously unlucky.

## Chapter 8: Conclusions

---



### A Summary of the Issues

We've touched on a lot of information in this guide. We've talked about malware threats, scams, the anti-malware software you need, freeware alternatives, and more. This is a lot of information to digest at once, but there are three points I'd like to reinforce.

1. It is important to protect your PC's security. As I've stated previously, there remains a contingent of users who remain convinced that using "common sense" will adequately protect a PC. That's simply not the case. It is possible for a malware threat to attack a PC without the user's action, and some of the deception used in phishing scams is extremely difficult to detect.
2. It's impossible to protect a PC against all security threats all of the time. Using anti-malware software, firewalls and other protection only reduces the chance of a problem. Full immunity isn't possible. This is why it's important to keep a current backup of important data.
3. You don't have to spend anything on PC security software, but securing your PC is usually easier with a high-quality paid product.

(Note: Not all paid PC security software is worth the money. Be sure to read reviews before buying.) If you're an average user, the array of security software available may bewilder you. Make sure that you understand whatever solution you download or purchase.

It would be great to live in a world where PC security was simple. That's not reality, however, and the issues surrounding PC security are likely to grow more complex. As time goes on, the techniques used by those who want to place malware on your PC will become more complex. This doesn't mean that you should be scared, but it does mean that you should keep up to date with current PC security trends and (once again) keep a current backup of important data.

### A Note About Mobile Threats

This guide concerns PC security. For now, PCs are broadly identified as desktops, laptops and netbooks. However, new devices like the iPhone and Android smartphones are changing the way that we look at PC security. So far, there have been only a handful of security threats targeted at these devices, but it appears as if there is room for these devices to be exploited, and considering their popularity, it's likely just a matter of time before they become a common malware target.



Threats on these devices can also be a threat to your PC, assuming that you, like most people, at some point connect your device to your PC. Research into the protection of mobile devices is still in its infancy, and while there are some anti-malware programs available, their usefulness isn't fully known. In any case, it's wise to treat these devices with the care that you would treat a PC. Did you receive an unexpected email from your bank? Leave it alone until you can view it with your anti-phishing equipped PC. Refrain from downloading unknown files and visiting websites you're unfamiliar with, as well.

## Additional Reading

2 Apps To Easily Create Network Firewall Rules For Ubuntu

<http://www.makeuseof.com/tag/programs-easily-create-network-firewall-rules-ubuntu-linux/>

2 Free Antivirus Programs For Mac OS X <http://www.makeuseof.com/tag/two-free-antivirus-programs-for-mac-os-x/>

3 Free Firewalls For Windows <http://www.makeuseof.com/tag/free-firewalls-windows/>

3 Smart Tips To Keep Your PC Secure When Downloading Files Online  
<http://www.makeuseof.com/tag/3-tips-ensure-safe-online-file-downloading/>

3 Tools to Test Run Your Antivirus/Spyware Program  
<http://www.makeuseof.com/tag/test-run-your-antivirusspyware-with-these-tools/>

4 Elements Of Computer Security That Antivirus Apps Don't Protect  
<http://www.makeuseof.com/tag/elements-computer-systems-security-antivirus-apps-protect/>

7 Essential Security Downloads You MUST Have Installed  
<http://www.makeuseof.com/tag/7-security-tools-you-absolutely-must-have/>

7 Top Firewall Programs To Consider For Your Computer's Safety  
<http://www.makeuseof.com/tag/7-top-firewall-programs-computers-security/>

10 Must Downloaded Free Security AND PC Care Programs  
<http://www.makeuseof.com/tag/10-most-downloaded-free-security-and-pc-care-programs/>

BitDefender Rescue CD Removes Viruses When All Else Fails  
<http://www.makeuseof.com/tag/bitdefender-rescue-cd-removes-viruses-fails/>

Manage The Windows Firewall Better With Windows 7 Firewall Control  
<http://www.makeuseof.com/tag/manage-windows-firewall-windows-7-firewall-control/>

Public Computers Made Safe – Security Tools and Tips

<http://www.makeuseof.com/tag/public-computers-made-safe-security-tools-and-tips/>



Did you like this PDF Guide? Then why not visit [MakeUseOf.com](http://www.makeuseof.com) for daily posts on cool websites, free software and internet tips.

If you want more great guides like this, why not **subscribe to MakeUseOf and receive instant access to 20+ PDF Guides** like this one covering wide range of topics. Moreover, you will be able to download [free Cheat Sheets](#), [Free Giveaways](#) and other cool things.

**Subscribe to MakeUseOf :** <http://www.makeuseof.com/join>

## MakeUseOf Links:

<b>Home:</b>	<a href="http://www.makeuseof.com">http://www.makeuseof.com</a>
<b>MakeUseOf Directory:</b>	<a href="http://www.makeuseof.com/dir">http://www.makeuseof.com/dir</a>
<b>MakeUseOf Answers:</b>	<a href="http://www.makeuseof.com/answers">http://www.makeuseof.com/answers</a>
<b>Geeky Fun:</b>	<a href="http://www.makeuseof.com/tech-fun">http://www.makeuseof.com/tech-fun</a>
<b>PDF Guides:</b>	<a href="http://www.makeuseof.com/pages/">http://www.makeuseof.com/pages/</a>
<b>Tech Deals:</b>	<a href="http://www.makeuseof.com/pages/hot-tech-deals">http://www.makeuseof.com/pages/hot-tech-deals</a>

## Follow MakeUseOf:

<b>RSS Feed:</b>	<a href="http://feedproxy.google.com/Makeuseof">http://feedproxy.google.com/Makeuseof</a>
<b>Newsletter:</b>	<a href="http://www.makeuseof.com/join">http://www.makeuseof.com/join</a>
<b>Facebook:</b>	<a href="http://www.facebook.com/makeuseof">http://www.facebook.com/makeuseof</a>
<b>Twitter:</b>	<a href="http://www.twitter.com/Makeuseof">http://www.twitter.com/Makeuseof</a>



## Download Other MakeUseOf PDF Guides!

**Subscribe to Download :** <http://www.makeuseof.com/join>

