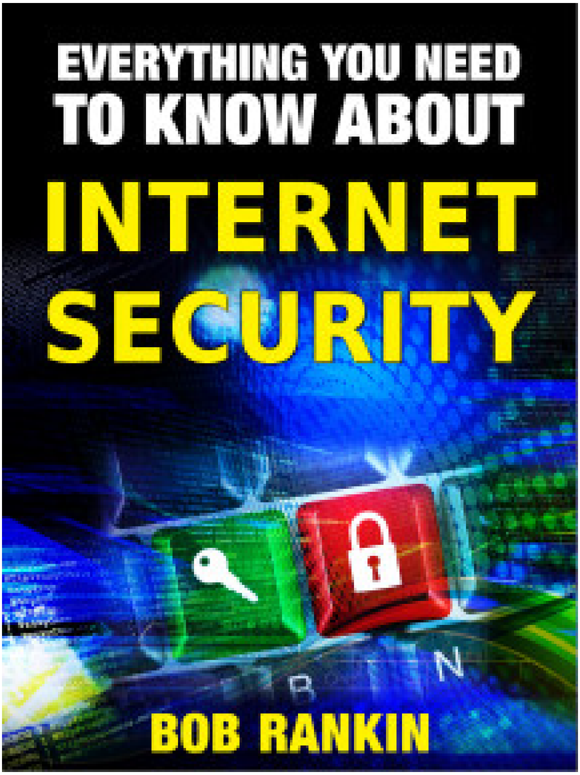
EVERYTHING YOU NEED TO KNOW ABOUT INTERNET SECURITY

– Preview Edition --



Copyright © 2013, **Bob Rankin**
All Rights Reserved

Introduction

The Internet is filled with wonders and dangers. This book will show you how to stay safe while enjoying everything the online world has to offer. You'll get the scoop on viruses, spyware, spam, scams, and other online threats. You'll learn techniques to keep yourself safe online, and find software to protect your computer from all of those threats.

This free 81-page Preview Edition will acquaint you with the most common online security threats, where they come from, and why they exist. You've undoubtedly heard about computer viruses and spyware. But what about botnets, rootkits, and keyloggers? Are you vulnerable to zero-day exploits, browser hijacking, or wifi sidejacking? Are hackers using your webcam to spy on you? And is your smartphone or tablet safe from mobile malware attacks?

In the **full edition** of **"Everything You Need to Know About Internet Security and Privacy"** (256 pages) there's much more to learn and explore...

SPAM: You'll learn how spammers get your email address, how to report them to the appropriate authorities, filters to help you manage your email inbox, and other techniques to stop spam from ever reaching you.

SCAMS: Online scams are a huge problem. The next section will educate you on phishing, and how to avoid falling prey to this and other online scams that can affect not just your computer, but your bank account as well.

SECURITY TOOLS: After learning about all these potential pitfalls, you'll discover the tools and techniques you need to protect and defend yourself online. You'll learn how to secure your operating system, your software and your passwords. You'll know if you should buy a commercial anti-virus program, or download a free one. You'll know more than your friends about firewalls, encryption, and wifi security. You'll find out where to download free tools to take your internet security to the next level, and how to find out if there are any holes in your defenses.

PRIVACY: Finally, you'll learn how to protect your privacy, defend against identity theft, what information you do (and do not) reveal while online, and who might be watching while you surf the Web. You'll find out how to lock down your privacy with anonymous surfing, and techniques to clear your tracks if desired. If you're afraid of cookies, or using your credit card online, you'll find peace of mind and practical solutions. You'll also be equipped to protect your privacy while using search engines, Facebook, or surfing the Web at work. Finally, you'll learn how to manage your online reputation, and remove your personal information from public databases.

I love to explain technology in plain English. Since 1994, I've been helping people learn about the online world, and have been called a "translator for the technology impaired." I hope you'll find this book informative and enjoyable. -- Bob Rankin

For FREE daily tips on computers and the Internet,
sign up for my **AskBob Updates** newsletter!

CLICK HERE to save $10 on your
purchase of the full edition of this book.

CONTENTS

Viruses, Spyware and Other Bad Stuff

You've undoubtedly been told to be wary of computer viruses, spyware and other online threats. The chapters in this section will introduce you to the most common online hazards, along with practical defenses and solutions.

But before we begin, lots of technical terms get tossed around when people start talking about the dark side of the Internet. So let's start by defining a few terms, and then move on from there.

Virus - A computer virus is a malicious self-replicating computer program that spreads by inserting copies of itself into other programs or documents, similar to the way a real virus operates. When the infected program or document is opened, the destructive action (payload) is repeated, resulting in the infection, destruction or deletion of other files. Sometimes the infected programs continue to function normally, albeit with the side effects of the virus; in other cases the original program is crippled or destroyed.

Spyware - A type of malicious software designed to take action on a computer without the informed consent of the user. Spyware may surreptitiously monitor the user, reporting personal information to a remote site, or subvert the computer's operation for the benefit of a third party. Some spyware tracks what types of websites a user visits and send this information to an advertisement agency. Others may launch annoying popup advertisements. More malicious versions try to intercept passwords or credit card numbers.

Adware - A piece of software that displays advertisements on a computer after the software is installed. Adware can be benign, as in the case of a free program that displays ads in a manner that is agreed upon in advance. Or adware can be a nuisance, displaying unwanted ads with no apparent way to remove the program. The nuisance variety is often silently downloaded along with some other desired software, such as a game or toolbar.

Malware - Any form of malicious software. This can include computer viruses, spyware, trojan horses, rootkits and other software that is deliberately harmful, destructive, or invasive.

Botnet - A collection of ordinary home or office computers that have been compromised by malware. Computers that have been caught up in a botnet have been effectively taken over, and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals whose motives include spewing spam, operating financial scams and crippling websites through coordinated attacks.

Phishing - The act of stealing information using lies or deception as bait. Online scammers try to trick people into voluntarily providing passwords, account numbers and other personal information by pretending to be someone they trust. Commonly, a phishing email asks recipients to login to a rogue site that looks exactly like the real one. When the victim logs in, the operators of the fake site then have that person's login credentials.

Rootkit - A rootkit is a software tool designed to conceal files, data or active processes from the operating system. Because of their ability to hide deep in the operating system, rootkits are hard to detect and remove. Although rootkits may not cause damage when installed, they are often piggybacked with additional code written for the purpose of taking control of a computer, disabling certain functions, or spying on the user.

Scareware - Software that is created for the purpose of tricking people into downloading or purchasing it, when in reality it's either unnecessary, marginally useful, or outright dangerous. Online ads that display fake warnings such as "Your computer may be infected -- click here to scan for viruses" or "ERROR! Registry Damage Detected -- click to download Registry Cleaner" would qualify as scareware. Scareware programs often run a fake or cursory scan, and then present the user with a list of hazards that must be corrected. Fixing these "problems" then requires the user to pay a fee for a "full" or "registered" version of the software.

Keylogger - A program that records everything a user types on the keyboard. The data collected can be read by a third party that is typically unknown, remote and malicious. Keyloggers do have legitimate uses, such as troubleshooting, training, analyzing employee productivity, and law enforcement surveillance. But keyloggers are most often used illegally to spy on people.

Where Do Viruses And Spyware Come From?

Several thousand new viruses and spyware programs are detected every day by security analysts. Have you ever wondered who creates these plagues, and why?

Who Creates Computer Viruses, and Why?

If I may quote Burt Reynolds, who said in justifying his illegal beer run in "Smokey and the Bandit," the usual reasons for creating malware are "For the money, for the glory, and for the fun... mostly for the money."

In the 1990s, when the Internet was still relatively small and non-commercial, most malware writers did it just to prove that they could. Self-taught programmers considered it a challenge to write software that could replicate itself, penetrate the rudimentary security defenses of that time, and not much more. Many of these viruses did no real harm after penetrating their targets. They displayed braggadocio messages like, "You've been had by the Dark Knight!" The authors of such malware sought to bolster their reputations among other hacker types.

Revenge is another reason why programmers write malware. A disgruntled employee might plant a virus on a company's network as a "going away present" after being laid off, passed over for promotion, or otherwise "disrespected" in his twisted mind. Sometimes an unhappy customer of a corporation would unleash a virus designed to damage or humiliate the company.

Twenty years ago, it might have been the nerdy kid that everyone made fun of in high school, looking to get even. But nowadays, most malware is written and distributed to make money for its authors. And those people are increasingly found to be highly organized cyber-crime gangs, hiding in the shadows of the online world.

What Motivates the Virus Creators?

Viruses may be written to extort money from corporations. "Your network is infected. Pay us or we will shut you down." On a smaller scale, this same blackmail technique is used by fake anti-malware program authors to terrorize consumers into buying (equally fake) cures for non-existent virus infections.

Viruses may be the means to spread botnet software to millions of computers. A botnet, or network of computers secretly controlled by a centralized criminal command, can be used to launch denial-of-service attacks against Web servers, or to distribute millions of spam emails from many enslaved computers at once. See Warning, Danger: Botnets! for more details.

Spyware is sometimes written to capture identity and security information that can be put to profitable use. Spyware may capture financial account login information, credit card and bank account numbers, and information that can be used to steal someone's identity. There are underground trading sites where lists of stolen credit card records sell for up to $30 per record. The buyers then use the stolen info to buy goods and services in the victims' names.

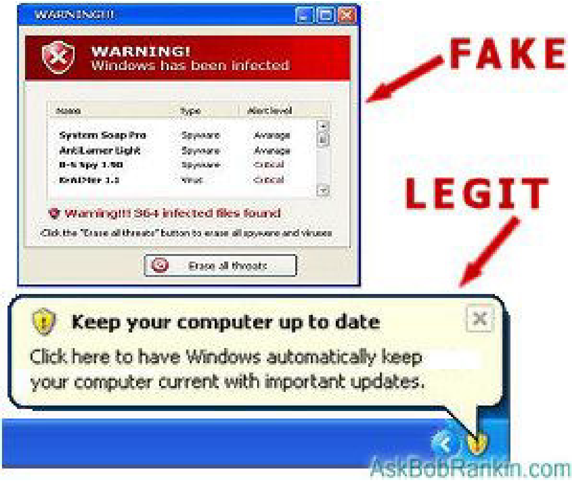
Some cyber-crime gangs operate for both profit and socio-political reasons. A group called Anonymous has taken credit for denial of service attacks against PayPal and Visa, to protest their refusal to aid the WikiLeaks project, and they have also attacked or threatened the IMF and the US Federal Reserve over policy issues.

Eastern European and Asian nations such as Russia, Romania and China are hotbeds of malware authorship. Brazil is another leading source of malware. These nations have in common a concentration of educated, talented programmers and few legitimate employment opportunities. Cyber-crime is perceived as the best use of their skills. Some of the world's most notorious spammers and cyber-crime gang leaders are listed in a **Spamhaus report** that is updated regularly.

Malware is big business, and it will continue to grow as the Internet and e-commerce grow. So will the security business. Think of it as an arms race in the digital world.

Securing Your Operating System

Is your operating system as secure as you can make it? A lot of people fail to take the simplest step to ensure that they have the best protection against malware and hackers that their Windows operating system can provide. Can you guess what they're missing...?



WARNING!!

WARNING!
Windows has been infected

Name	Type	Alert level
System Soap Pro	Spyware	Average
AntiLamer Light	Spyware	Average
B-S Spy 1.90	Spyware	Critical
BrAiDter 1.2	Virus	Critical

Warning!!! 364 infected files found

Click the "Erase all threats" button to erase all spyware and viruses

Keep your computer up to date

Click here to have Windows automatically keep your computer current with important updates.

Securing Your Windows Operating System

So what's the one simple step that many people neglect? They don't keep their systems updated with the latest security patches and Windows Service Packs. It doesn't matter if the root cause is fear, ignorance or laziness. The end result will be a system that is wide open to viruses attacks and privacy invasions.

Microsoft calls these things "critical updates" for a good reason. Security patches plug holes in the Windows operating system that hackers can exploit to plant viruses, steal personal information, and enslave your computer in a botnet used to spread malware and attack other computers via the Internet. Service Packs are major overhauls of Windows that include prior security patches.

It really is critical to download and install security patches and Service Packs as soon as they become available. Windows Update is a tool built in to Windows 7, Vista and XP, to provide you with these updates. I strongly recommend that you run Windows Update in automatic mode. See **this link** to learn more about Windows Update, and how to make sure it runs automatically.

So why don't many people do it? Here are some of the reasons I hear for not updating Windows, and rebuttals to all of them:

“I can never tell if a popup on my screen, warning me to install or modify something, is really legitimate. I'm afraid I'll accidentally download something malicious.”

Yes, you should avoid clicking on unsolicited popups that appear in a browser window (Internet Explorer, Firefox, etc.). Many of these popups present dire warnings that your computer has a virus, and encourage you to run a free scan. It will help to remember that there is a difference between a popup and a balloon. Popups will appear in a web browser window, floating in the middle of your screen, and are generally to be avoided. Balloon notifications are attached to the little yellow shield on the taskbar at the bottom of your screen, and should be heeded -- especially if they direct you to apply critical security fixes. (See the graphic above for examples of each.)

“I still use Windows XP and Microsoft no longer supports XP. So I don't check for updates.”

True, Microsoft is no longer releasing improvements to the aging Windows XP. The last Service Pack for Windows XP was SP3, released in 2008. But millions of copies of XP are still in use worldwide, and Microsoft will continue to issue critical security updates for XP, up through April 2014. You need them.

“It takes too long to download and install updates and Service Packs.”

You don't have to sit in front the computer waiting for updates to be installed! Windows Update can be configured to automatically check for, download, and install critical security updates (including Service Packs) at any time, like when you are asleep or at work. Optional updates that do not affect security will not be installed automatically. If you want to live without the latest mouse driver, go right ahead. But don't leave your system open to invaders.

“I've heard that some updates 'break' Windows installations.”

It is extremely rare for an update to corrupt a Windows installation. Even if that happens, you can do a repair re-installation from your Windows CD. You won't lose any user data or applications, but you will lose all of the security updates and Service Packs that are not included with your CD copy of Windows. So you will have to re-install all of those updates and Service Packs via Windows Update. I've run Windows Update on autopilot (automatically installing all recommended fixes) for years and have never run into a problem.

“Windows Update said my copy of Windows is not 'genuine' so I could not continue with updates.”

In all likelihood, you are running a pirated copy of Windows. Maybe it came with the used computer your bought, or a new one that you purchased from a dishonest seller. Maybe, just maybe, your copy of Windows is legit but for some reason Windows Update doesn't think so.

First, it doesn't matter whether your copy of Windows is legit or not. Microsoft will still provide critical security updates through the Automatic Update utility described above. You just can't use the Windows Update service manually. If you know that you are running a pirated copy of Windows, do the right thing and purchase a legitimate license. Then you will be able to get all of the service packs and optional updates, as well as critical security patches.

Securing Your Software

Is your computer really secure? If you have antivirus software, malware scanners and a firewall, you might think you're safe from hackers, crackers and identity thieves. But chances are, you're missing one critical piece of the security puzzle. Read on to learn how to secure your software and truly lock down your computer...

What's the Missing Link in Computer Security?

You may feel safe behind a firewall and anti-virus software. But you're not. Bad guys can still get to your personal information stored on your computer, and even take over your computer and run it as if it was their own. The gap in your armor? It's the application software you use every day. Let's look at just one recent example.

Do you ever read Adobe PDF files, in your browser or with Adobe Reader after downloading? Tens of millions of people do; PDF is one of the most widely used file formats. But unfortunately, hackers have found ways to embed malware in PDF files. New vulnerabilities are discovered in application software every hour, it seems.

Software developers issue patches and updates that close these doors to hackers in a never-ending game of Whack-A-Mole. A vulnerability pops up here, hit it with a patch. Another pops up over there, hit it with another patch. Developers provide the patches, but it's up to you, the end user, to whack the moles by applying these patches.

Staying on Top of Application Security

It's vital to keep all your software up to date with the latest patches and upgrades. But the average computer holds about 80 application programs! How can you keep up with it all?

First, concentrate on the programs that are most often targeted by bad guys. They are the most commonly used programs: Microsoft Office, Adobe Reader, Internet Explorer, etc. The more people there are using a program, the more targets there are for a hacker's arrows. Naturally, the hacker goes after the biggest potential "market" for his malware.

Second, activate automatic update features when they are available. Then your software will check its home site for patches and upgrades every day, or week, or whatever. It can download and install updates without bothering you at all, or tell you when updates are available and give you the choice of when to install them.

Some security experts tell you to turn off automatic updates because a connection to a server is an open line through which hackers can invade your computer. But turning off auto-update closes one door while leaving untold numbers of others wide open. Who are you kidding? You're not going to remember to check for updates manually on a regular basis. You'll let it slide until your software is so outdated it contains dozens of vulnerabilities. Leave auto-update on and let the software remember for you.

Third, you can check all the software on your computer for vulnerabilities using something like the Secunia **Personal Software Inspector** (PSI). This free program comes from a trusted security site, and scans your software for known vulnerabilities. It will tell you which programs need updating and provide links to sites where you can download patches.

I ran PSI while researching the issue of software security, and I was very surprised by the results. I have security software in place, and I thought I was keeping up with all my patches. I felt pretty confident about the security of my computer. But PSI flagged Adobe Reader, Flash, Skype, iTunes, QuickTime, Java and a few others as needing updates.

At least SIX of these vulnerabilities were marked Critical, meaning that under certain circumstances, an Evil Hacker could have exploited them to gain complete control over my computer. Yikes.

Bottom line... the software you use every day is the biggest source of danger to your personal information. Keeping your software up to date is your best defense. You cannot afford to let vulnerabilities go unpatched.

Paid Anti-Virus Programs

"My computer came with a free trial of the anti-virus software, and now it's nagging me to pay $49 to renew. Should I pay the ransom, or go with a free anti-virus program?"

Should I Pay For Anti-Virus Protection?

There are dozens of free anti-virus programs available. Most of them do a decent job of protecting your computer and network against common malware threats (viruses, spyware, rootkits, etc.) But the paid versions of these and other programs can provide added protection, easier administration in business settings, and other benefits over their free counterparts.

When should you pay for security software? Many vendors offer their programs free for personal, academic, and other non-commercial use. If you use anti-malware for business, you are expected to pay for it. Also, some features such as real-time protection and email scanning may not be available in free versions.

The commercial security tools typically include a suite of programs that includes anti-virus, anti-spyware, firewall, spam filtering, and download scanner. A common friendly interface lets you interact with all of them, when you need to change settings, run reports, or get help. And all of the components will have been tested to work well will together.

But with the freebies, you have to cobble together your own set of tools to get the equivalent. You might end up picking 3, 4, or 5 of those tools, all from different vendors. The downside is that each program will have a different user interface, and the learning curve will be steeper. And there's always a chance that one of them might not play nice with the others.

Keep in mind that technical support is not included with the free anti-virus programs. That's a big plus for the commercial alternatives, especially for less technical users who might run into trouble while installing the program, or be confused by warnings that pop up while surfing the web or downloading.

Commercial Internet Security Software

Here are some of the best paid anti-virus programs and internet security software currently available. I've given the vendor's list price for each (as of March 2012), but if you search online for the titles, you can usually find them at discount prices.

BitDefender Internet Security ($49.95) does an excellent job of detecting and eliminating malware infections on hard drives. In a recent test by AV-TEST labs, BitDefender scored better than any of the other tested programs, based on protection, ability to repair infections, and usability.

McAfee Total Protection ($59.99) or similar is often pre-installed on new computers, as a trial version with a nagware component. McAfee gets average ratings from users, but scores well in malware blocking, spam filtering, intrusion detection, and warning when malicious websites are encountered. The software installs easily, and has a minimal impact on system performance.

Norton Internet Security ($79.99) gets top marks for detecting and eliminating many kinds of malware. It's also easy to install - only two screens must be navigated before the program begins installing itself. The user interface is also intuitive. On the downside, Norton scans relatively slowly.

Avast! Internet Security ($39.99) is only middling-fair at detecting infections, finding about 94 percent of test malware installed on a hard drive. It was able to remove only 70 percent of the infections that it did find, about average for anti-malware programs. Consistent with these results, Avast is one of the fastest anti-malware programs when it comes to scanning a hard drive. Its boot-scan feature will scan your hard drive for malware before Windows loads, a key feature in defeating some infections.

G-Data Internet Security ($34.95) is above-average in malware detection and elimination, and has a "Silent Firewall" that operates invisibly without constantly nagging the user. Its setup and setting screens are more complex than consumers may like. G-Data yields very few false positives - safe files wrongly identified as malware.

Kasperky Internet Security 2011 ($69.95) does a great job of blocking malware attacks before they can infect a computer. In tests, it detected over 95 percent of known malware based on signature files. It also removed 80 percent of infections, tying with the best competitor. However, Kaspersky is one of the most resource-intensive anti-malware programs. Running it on a low-end computer will significantly impact performance.

Bottom line: Plenty of free anti-virus and anti-spyware software is available. If you're willing to assemble and trouble-shoot all the pieces yourself, you should be well protected. But if you want the simplicity of an all-in-one solution, the most comprehensive protection, and expert technical support, you should pay for it. At four or five dollars a month, the price tag is modest, and for many home users, the additional peace of mind is worth it.

Free Anti-Virus Programs

"I've been using the free Norton anti-virus package that came with my computer, but the subscription will expire in a few days. Are the free anti-virus programs any good? What do you recommend?"

Protect Your Computer With Free Anti-Virus Software

Your computer is running slow... your high-speed internet connection feels like dial up, and popups are everywhere. What's wrong? It could be a computer virus, or perhaps a bunch of viruses, infecting your hard drive. Viruses not only take up valuable memory and slow down your computer, they can also expose your personal information to Evil Hackers.

The good news is, there are plenty of anti-virus programs that can clean up the mess and keep you safe going forward. Some of them are even free! Here's a rundown of the most popular free anti-virus packages. I'll also share my take on free versus paid anti-virus software. Find out which option is right for you.

Free Anti-Virus Programs

AVG - is one of the most often-recommended freeware anti-virus packages. While Grisoft offers a paid version, there is a freeware version of the virus protection on the website. It only offers anti-virus and anti-spyware protection (no anti-spam, anti-rootkit or firewall) but provides very effective protection from the most common threats. The Pro version has Web Shield to screen your downloads, rootkit protection, and free support.

Avast! - another freebie anti-virus program with basic features, and ease of use. It is updated regularly, also highly recommended.
The Free Home Edition includes anti-spyware and anti-rootkit detection.

Avira Anti-Vir - claims over 30 million users worldwide, and the free Personal Edition gets good reviews. There is a paid version with anti-spyware and firewall protection as well.

BitDefender - is another highly rated freeware anti-virus tool. It offers just basic anti-virus protection, so I recommended that you add anti-spyware protection as well.

Comodo AntiVirus uses a unique approach to detecting and defending against viruses. Comodo claims their Default Deny Protection and Auto Sandbox Technology will completely prevent infections. Comodo also eliminates the guesswork regarding blocking or allowing untrusted software, an issue that trips up many users.

Microsoft Security Essentials is a free security tool from Microsoft. It's meant to provide protection not just from viruses, but also spyware, rootkits, and trojans as well.

Sure, there are other free anti-virus programs I could have listed, but these are the most popular and provide excellent protection, according to my research. And since I noted that some of the programs above do not include spyware protection, let me mention that I recommend the free **MalwareBytes AntiMalware** (MBAM). MBAM protects you from spyware and security threats that are sometimes missed by other anti-malware tools. The free version works great, but lacks the real-time protection feature found in the paid version.

Some people swear by **Spybot Search & Destroy**, **Super Anti-Spyware** or some other anti-spyware utility. These are very good free anti-spyware programs as well, but in my experience MBAM has done the job for me every time when a spyware "search and destroy" mission was called for.

What You Should Know About Anti-Virus Software

Look for virus protection that comes with frequent, automatic updates and covers all viruses, not just the major threats. If you aren't getting regular updates, at least once every two weeks, you should consider another program. New viruses are created every day, so you need constant, up-to-date protection.

You should also not rely on a single anti-malware program if you are going to use the freeware solutions. Standalone anti-virus programs are not a replacement for anti-spyware or a firewall. I recommend that you also read Do I Need Anti-Spyware Protection? and Do I Really Need a Firewall?

I do have one caution about using free anti-virus packages. Some people assume that because the software is free, then more is better. I've gotten reports from people who are using TEN or TWELVE "anti" programs at the same time. The truth is that anti-virus programs like to be left alone, or they can end up in a "death spiral", each thinking that the other is trying to do something bad.

Multiple anti-virus programs can interfere with each other, causing system slowdowns or lockups. And running multiple anti-spyware tools at once can have the same result. That's why I recommend that you pick ONE of each.

Paid Versus Free Anti-Virus

Do you really need paid anti-virus software? That depends on you. If you or others in your household are prone to visit the dark corners of the Internet (peer-to-peer music/movie downloads, adult sites or warez), or if you have children that will click and download almost ANYTHING, then you will probably want the best protection possible.

Generally, the commercial anti-virus packages with monthly subscriptions offer very high levels of protection, fast updates when new viruses are found, and good customer support. You should also consider a paid anti-virus package if you run a business, or if you have sensitive information on your computer. It's a small price to pay to ensure that your data is secure.

For more details, see the chapter Paid Anti-Virus Programs or check out these commercial anti-virus packages, all of which are rated "Advanced" in the latest **AV Comparatives** report, which is an independent, unbiased testing group.

BitDefender Internet Security

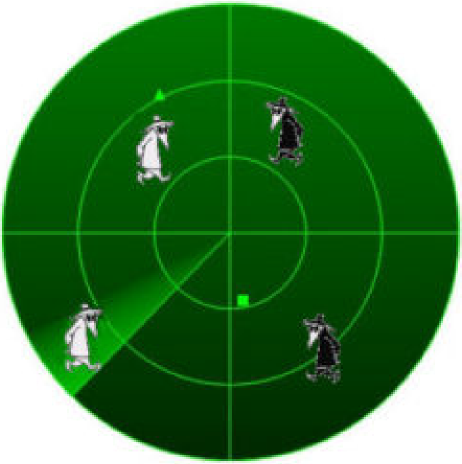
McAfee VirusScan

Norton Anti-Virus

In summary, don't take your Internet security lightly. For most casual home users, I believe the free internet security software options listed in this chapter will do an excellent job. Just be sure to supplement it with an anti-spyware component if yours doesn’t include it.

Do I Need Anti-Spyware Protection?

"Do we still need both anti-virus and anti-spyware protection? I've always been told that, but I use Norton AntiVirus 2012, which claims to handle viruses, spyware and other threats. Is this sufficient, or should I still download a dedicated anti-spyware tool?"



Is Anti-Spyware Software Obsolete?

For many years, it was essential to use both anti-virus and anti-spyware software. That's because viruses and spyware are distinctly different types of security threats, and different technologies were required to detect and remove them. But today, we have the more generic "anti-malware" programs which attempt to protect against all types of threats, including spyware. So do you still need a dedicated anti-spyware program? There are two schools of thought.

On one hand are those who say dedicated anti-spyware is a waste of time, computer resources, and money if you already run a good all-around anti-malware package that scans for spyware. The anti-spyware functions of Norton, McAfee, Avast, and many other internet security suites are just as effective as dedicated anti-spyware programs such as Spybot. So why pay twice for the same protection? Even if you use free anti-spyware alternatives, you're still running two programs, and likely impacting the overall performance of your computer.

On the other hand are those who can never be too careful. They probably have chain bolts on their front doors as well as locks. No security program detects all threats, they say, so it pays to have more than one line of defense against spyware.

I tend to agree with the first group. Anti-malware software has evolved to the point where it provides adequate protection against spyware for most users under most circumstances. If you are worried that some spyware may have slipped through your defenses, or you use a free anti-virus program that does NOT include a spyware component, download a free program such as **MalwareBytes AntiMalware**, **Super Anti-spyware**, or **Spybot Search & Destroy**.

A Word of Caution...

If you decide to use a dedicated anti-spyware program, use this secondary security tool to do a one-time scan, but don't run it in "always on" or "real time" mode. Here's why...

I've always advised that it's not a good idea to run multiple anti-virus programs at the same time. Because these programs contain the virus signatures that are used to detect viruses, one anti-virus program may detect the other as evil, and attack it. In some cases, BOTH programs will go on the offensive against each other, and a "death spiral" ensues. This can cause your computer to slow to a crawl or lock up entirely. If you MUST have more than one real-time anti-virus program installed, use the program's control panel to temporarily disable one of them.

Some people swear by MBAM, and claim that it can find nasty viruses, spyware and rootkits that other programs do not detect. I've had some success using MBAM on badly infected machines, and found that it runs just fine alongside an active anti-virus program. I have not tried the "Real-Time Active Malware Prevention" feature in the paid version of MBAM, because I've never had a case where the on-demand scanner in free version didn't get the job done.

Here's an even better idea, if you think your anti-virus may have missed something, or you can't even start Windows due to a virus infection. Scan your system with a standalone tool that runs from a boot disk. You can load **Microsoft System Sweeper** to a CD or USB flash drive, then restart your computer. This allows System Sweeper to scan and remove any infections without loading Windows, or tripping over your anti-virus software.

So YES, you do need anti-spyware protection. But if your internet security software handles spyware, I no longer recommend a dedicated real-time anti-spyware program in addition. I spend a lot of time online, and in the course of my research I visit a diverse range of websites to which most people are not exposed. My personal strategy is to use AVG or another of the free anti-virus programs, and keep MBAM handy for occasional "peace of mind" scans.

Do I Really Need a Firewall?

Perhaps you’ve heard conflicting reports on whether or not you should be using a firewall. Some people say they are only needed for dialup users. Others say you MUST have a firewall if you have a high-speed DSL or cable connection. Here’s the straight story on firewalls…

What Happens When You Yell "MOVIE!" in a Crowded Firehouse?

Well all the firemen go running out into the streets, of course. Okay, it's a bad joke. But it illustrates the point that even people who are claim to be knowledgeable on computer safety are often confused about firewalls. Here's the scoop on WHO needs a firewall, WHAT they do, and WHY you might be wasting your money on firewall software.

First, let's look at what a firewall is supposed to do. A firewall is hardware or software that limits access to a computer from an outside source. If your computer will ever be connected to the Internet, a firewall is an essential tool needed to prevent malware and hackers from accessing or damaging your computer.

So YES... you do need a firewall. Without a firewall, your computer can be compromised within SECONDS after connecting to the Internet. If you're a dialup user, it might take a little longer, but it will happen. The reason for this is the automated hacking drones that are constantly scanning Internet-connected computers, looking for any vulnerability.

What Kind of Firewall Do I Need?

The real question is "Do I need a software-based firewall or a hardware-based firewall?" If you have a high-speed Internet connection such as DSL, cable or fiber optic, then you should have a little black box inside your home, that was installed by the phone/cable company. This is sometimes called a modem, but in most cases it's actually a network router, or a combination modem/router. If you have a router with the NAT feature (Network Address Translation), you already have a hardware firewall which effectively makes your PC invisible to the attacking hordes. However, there are some cable internet providers that still install cable modems WITHOUT routers.

If you're not sure that you have a NAT router with built-in firewall, ask your internet service provider. You can also do a web search for your modem or router to find the manufacturer's specs or a review that answers the question. Most routers allow you to login and customize the firewall settings, and also offer content filtering and parental controls. Contact your Internet provider if you’re not sure how to login to your router.

If you have a dialup connection, where the telephone line connects directly from the wall socket to your computer, you definitely don't have a hardware firewall. So in the absence of a hardware firewall, you absolutely need a software-based firewall.

What About the Built-In Windows Firewall?

If you have Windows 7, Vista, or Windows XP with the latest service pack, then you already have a software firewall. Windows Firewall has been part of the operating system since 2004, and the default setting is ON. To check or change the firewall setting, click on Start / Control Panel / Security, then click on the Firewall link.

My position is this: If you have a hardware firewall, there is no need to run a software firewall in addition. It doesn't matter if you have a wired or wireless connection to your router.

If you do turn off the Windows firewall, you should tell Windows that you have your own firewall solution, or it will nag you about the firewall every time you start up your computer. For XP, click Start / Control Panel / Security Center. Then under Firewall, click the Recommendations box. On the next screen, check the box labeled "I have a firewall solution that I'll monitor myself."

On Vista, click the Start button, open Control Panel, click Security, then Security Center. Under Firewall, click “Show me my available options.” Then click “I have a firewall solution that I'll monitor myself.” On Windows 7 systems, click the Start button, then open Control Panel. Under System and Security, click “Review your computer's status. “ In the left pane, click “Change Action Center settings.” Uncheck the box next to Network firewall, then click OK.

Other Software Firewalls

I know there is heated debated on this topic. Some people claim that you MUST have a software firewall to protect you from malware that might be trying to make an OUTBOUND connection for nefarious purposes. My position is that anti-virus and anti-spyware programs should be installed to remove and prevent the malware in the first place.

Sure, you can use the Windows Firewall, or install ZoneAlarm, Black Ice, etc., but my experience shows that many users are confused and unnecessarily alarmed by the constant stream of "warnings" that these programs present.

Lots of good programs DO need to make outbound connections to the Internet. Your browser, email program, FTP client, media player, and any software that checks for available security updates will need access. So if you're not very careful you'll end up blocking them, and then they don't work correctly. I've also seen cases where software firewalls malfunction and either interfere with certain programs or end up blocking ALL connections. And don't get me going about all the times when a software firewall prevented access to a shared folder or a networked printer... arrgh!

But I will grant you this. Installing a software-based firewall as an extra layer of protection is not a bad thing. If you have kids in the house that are likely to click on or download almost anything, it could be helpful. See **Free Firewall Protection** for some excellent free software options.

A Word About Laptops

If you have a laptop that's connected to the Internet through your home network, there’s no difference in terms of the firewall setup. But if you take that laptop on the road and make a wired connection (as in a hotel room with a network cable) or go wireless (in the airport or a coffee shop), you are no longer protected, so it's a very good idea to turn ON your software firewall. See the instructions above for details on how to do this with the Windows Firewall.

To summarize, YES you need a firewall. My personal opinion is that if you have a hardware firewall, don't bother with a software firewall. Can you run both? Yes, but the "benefits" may be outweighed by the problems.

Warning, Danger: Botnets!

Maybe you've read warnings about your computer getting caught up in a botnet, but don't really understand the danger. This chapter will explain in simple terms what a botnet is, how it can affect your computer, and how to avoid them.

AskBobRankin.com

What is a Botnet?

Okay, here's the scoop... a botnet is a collection of ordinary home and office computers that have been compromised by rogue software. The term "botnet" is short for "robot network" and describes the situation rather well. Computers that have been caught up in a botnet have been effectively taken over, and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals and other miscreants whose motives include selling products, operating financial scams and crippling websites through coordinated attacks.

Should you be concerned about botnets? Yes, because botnets operate silently, and your computer may be affected without you ever suspecting it. Botnets are everywhere. It is estimated that over 30 million "zombie" computers are unknowingly caught up in these networks that distribute spam, steal personal information and participate in denial of service attacks. Botnets are carefully planned to spread via viral infections and other malicious software. They use email, social engineering and P2P (peer to peer) technology to spread to other computers. Once your PC is infected, it may attempt to spread the botnet code to others on a local network in a home or office setting.

Botnets are most often used to spew massive quantities of spam, which is where most of the "enhance your body part," offers and phishing scams come from. But since the botnet code runs with full privileges on the infected computer, it can be used to gather sensitive information from businesses, political groups or governments. Sometimes, the attacks are used to damage or take down a competitor's website by flooding it with emails or web connections. These attacks can be hard to defend against, because the attacking computers are spread all over the Internet. And when the "attacker" is identified, it's just some guy in Podunk who let his anti-virus protection expire, and had no idea his computer was involved in a global crime spree.

Bots can also be used as agents for mass identity theft. This happens through phishing emails that appear to be from a legitimate company in order to convince the user to submit personal information and passwords. Be especially wary of emails claiming to be from eBay, Paypal, banks or the government. Never click on email links to access these sites -- always use your bookmark or key it in directly.

How to Avoid Botnets

You are most likely to get sucked into a botnet if you do these things:

- Fail to use a good **spam filter**.
- Fail to use **anti-virus** and firewall protection
- Click on **dubious links** in spam emails or shady websites

Use good security practices outlined in the links above, and avoid suspicious emails, especially unexpected messages with subject tags related to holidays, celebrities or current events. Watch out for phishing scams, never click on (or buy!) anything advertised in a spam email, and when in doubt, just don't click.

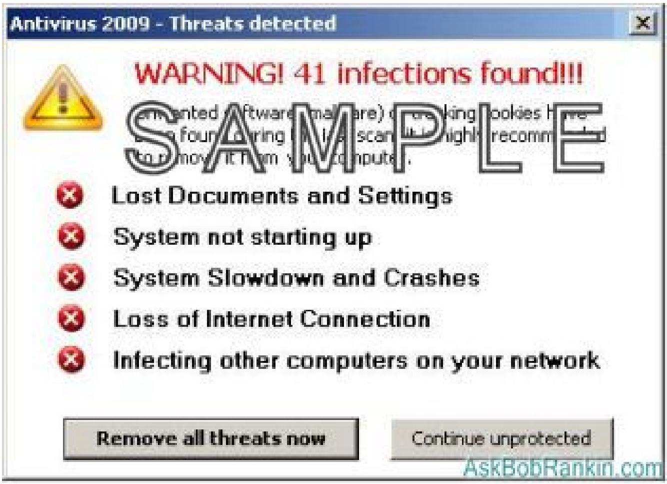
Fortunately, in the past two years, law enforcement and computer security companies have had some success in tracking down and neutralizing some of the most notorious botnets. In March 2010, the FBI and authorities in Spain busted the Mariposa botnet (over 12 million computers) and arrested the people behind it. In 2011, Microsoft and Kaspersky combined to neutralize the Rustock and Kelihos botnets, but were unable to identify the overlords. Most recently police in the US and Estonia arrested the people running the Esthost botnet.

How to Detect and Remove Botnet Infections

It's difficult to detect if your computer has been caught up in a botnet. If you notice that your computer is sluggish, that *may* be a sign that you are affected. But in general, if you have been affected by a botnet, you've got some sort of malware infection. Install good anti-virus and anti-spyware software (refer to the links above), and it should detect, take care of, or prevent the problem.

What is Scareware?

So you’ve heard of software, shareware, freeware and malware, and you have a pretty good idea what all those things are. But what exactly is scareware?



Antivirus 2009 - Threats detected

WARNING! 41 infections found!!!

Unwanted software (malware) or tracking cookies Have been found during the last scan. It is highly recommended to remove it from your computer.

- ☒ Lost Documents and Settings
- ☒ System not starting up
- ☒ System Slowdown and Crashes
- ☒ Loss of Internet Connection
- ☒ Infecting other computers on your network

SAMPLE

Don't Fall Victim to Scareware

You're surfing the Net and all of a sudden a screen pops up warning you there is a problem on your computer. You're not sure if it's real or not, so what do you do? Be careful, it could be scareware. I define this type of rogue software like this:

SCAREWARE: Software that is created for the purpose of tricking people into downloading or purchasing it, when in reality it's either unnecessary, marginally useful, or outright dangerous. Scareware programs often run a fake or cursory scan, then present the user with a list of hazards that must be corrected.

Fixing these "problems" then requires the user to pay a fee for a "full" or "registered" version of the software.

If you see a popup messages like "CRITICAL ERROR! - REGISTRY CORRUPTED" or "WARNING - PRIVACY VIOLATIONS FOUND" ...then your scareware spider-sense should be kicking in. Scareware popups often warn about problems with the Windows registry, tracking cookies, spyware or viruses. The names sound innocent enough... Scan & Repair, MalwareCore, AntiVirus Pro 2012, XPDefender and WinSpywareProtect. Sometimes the message will have flashing elements, and that should be the first indication that something is wrong. You may be instructed to visit a web site to download a registry cleaner, or to click on something in the message that will diagnose or correct your supposed "errors" for free.

Some people are tricked into downloading free diagnostic tools that run a scan (or pretend to) and then present you with warnings about spyware or evil cookies that were detected. Typically, you must "register" the software to activate or download the code that will fix your problems. You may be charged you $39, $49, or another amount, but you may also be giving your credit card and/or bank information to identity thieves.

Some scareware programs are marginally useful, and will actually diagnose and fix certain problems. But there are plenty of free and reliable tools to do these things for free. In other cases, the scareware is actually infecting your computer and requiring that you buy their product to get rid of it. The scareware problem has become so widespread that Microsoft and Washington State's Attorney General have filed lawsuits against some of the perpetrators.

BOTTOM LINE: Do not click, do not pass go, do not fall for the scam. If you have ANY doubts, ask a computer savvy friend or your tech support person at work. If you have no friends and no job, just close the popup using the little X in the upper right hand corner.

What About the REAL Error Messages?

Of course you may occasionally see a warning or error message appear on your screen that's legitimate. Windows may ask for permission to install some new software, warn you that some other program is trying to modify your system settings. If you are in fact installing new software, you can be pretty sure that it's safe to proceed.

Windows may also alert you that some critical patches are available to download or install. When this message appears in a balloon attached to the taskbar at the bottom of the screen, you can trust it. This is the Windows Update mechanism, and you should use it to keep your Windows system software updated.

Your anti-virus or anti-spyware program may find something, and ask you if it should be deleted or quarantined. If you recognize the warning as definitely coming from a security tool you have installed, then it should be safe to heed the warning. Again, when in doubt, just close the message without clicking on anything inside the popup window.

What Is a Rootkit?

Rootkit... the name sounds innocent enough. Kinda like something your Grandma would use in her garden. Actually, rootkits are a particularly nasty form of malware, created to wreak havoc on computers.

```
ssdpapi .dll  WINDOWS\system32   34816
ssdpsrv .dll  WINDOWS\system32   71680
ssflwbox.scr  WINDOWS\system32  393216
ssmarque.scr  WINDOWS\system32   20992
ssmypics.scr  WINDOWS\system32   47104
ssmyst  .scr  WINDOWS\system32   18944
sspipes .scr  WINDOWS\system32  610304
sssplt30.ocx  WINDOWS\system32  177608
ssstars .scr  WINDOWS\system32   14336
sstext3d.scr  WINDOWS\system32  679936
Status  .MPF  WINDOWS\system32   63296
stclient.dll  WINDOWS\system32   59392
stdole32.tlb  WINDOWS\system32    7168
sti     .dll  WINDOWS\system32   68096
sti_ci  .dll  WINDOWS\system32  136704
stimon  .exe  WINDOWS\system32   14848
stobject.dll  WINDOWS\system32  121856
storage .dll  WINDOWS\system32    4208
storprop.dll  WINDOWS\system32   74752
streamci.dll  WINDOWS\system32    8192
strmdll .dll  WINDOWS\sy
```

Rootkits: A Silent Enemy

Most computers users today are aware of viruses sent in deceptive emails or spyware creeps in while web browsing. Rootkits however, are more sinister. Because of their ability to hide deep in the operating system, rootkits are hard to detect and remove. Although rootkits may not cause damage when installed, they are often piggy-backed with additional code written for the purpose of taking control of a computer, or spying on the user and reporting activities back to the rootkit creator. In short, a rootkit is a software tool (or a set of programs) designed to conceal files, data or active processes from the operating system.

One very widely publicized example of a rootkit was Sony's Extended Copy Protection (XCP) software that was included on 50 music CDs. This XCP software was automatically installed when customers played the CD on a computer, and although it was intended as a copyright protection measure, it had flaws that affected the way Windows plays CDs, and opened up security holes that could allow viruses or spyware to enter a system. It was described by many people as a rootkit because it was installed in a surreptitious manner, it modified Windows operating system files, and was designed to hide itself so as to avoid detection.

No Longer Just a Unix Problem

In the Unix world, the term rootkit (or "root kit") has been used to refer to a set (or kit) of common Unix commands that have been modified to do something sneaky or malicious in addition to their normal function. They display the correct output or perform the intended function, while operating in a "root" (administrator) capacity, so they are difficult to detect. Although most rootkits are malicious or surreptitious in nature, not all are hostile. One example of a rootkit used for a good purpose is the Alcohol 120% software, which emulates disk drives.

Once limited to the Unix world, writers of rootkits are increasingly targeting Windows-based computers for attacks. These hackers often take advantage of unsecured ports on a computer. A port is essentially a door that allows specific types of network traffic to flow in or out of a computer. Businesses have firewalls in place to secure unauthorized entry to certain ports. But many home users do not have firewalls, so are especially susceptible to rootkit ravages.

How Do I Know I've been "Rootkit-ed"?

This is the tricky part. It's often hard to detect a rootkit attack, even for the pros, because of their ability to hide themselves on a system. Even anti-virus software may not be able to detect some clever rootkit components, because they have the same name and file size as Windows operating system files. Rootkits can be delivered via e-mail attachments, through unsafe web sites (often sites that allow file sharing), or they can sneak in with music or software being copied from a CDROM.

Usually diagnosis is made by symptoms, rather than by the presence or specific files. Some signs that a computer has been infected by a rootkit include: extremely slow performance, hard drive space rapidly decreasing, unexplained high CPU activity, programs opening on their own without user input, the crashing of anti-virus software and system freezes.

Protect Yourself from Rootkits and Other Threats

The time-tested advice for protecting yourself against rootkits applies to any other type of computer threat. Do not open suspicious email, even from an address you recognize. Don't download software from file-sharing sites or other bad neighborhoods. Don't ignore Windows update warnings, and keep your anti-virus and anti-spyware software updated.

It's not a bad idea either to use a firewall on your home PC. Windows XP service pack level 2, Windows Vista and Windows 7 come bundled with firewall protection. A firewall will help to secure your machine against viruses, spyware and rootkits, but a third-party firewall solution will offer more robust protection. For more information on what kind of firewall you should use, see Do I Really Need a Firewall?

If You Think You've Already Got a Rootkit...

There are several tools available that are designed to ferret out and rid your system of rootkits. One such tool is **Rootkit Revealer**, Microsoft's utility to discover rootkits on a PC. This tool helps to discover them, but you'll need to investigate the specific rootkit to find out how to get rid of it. Sophos, a respected software security firm, also has a **rootkit detection and remover program** available as a free download. And there's **Blacklight**, another popular free rootkit detection and removal tool.

These utilities are not guaranteed 100%. Because of the stealth-like nature of rootkit programs it is possible that even rootkit removal programs will not detect the most well-hidden rootkits. But, they're a good starting point if you feel that your computer has been compromised. The more aware you are as an end user the less vulnerable you will be against computer threats.

What is a Keylogger?

It's a fact that many malware infections result in a vulnerability to keystroke logging, which can compromise your privacy and lead to identity theft. Learn more about keyloggers, how they work, and how to defend yourself from this growing threat...

AskBobRankin.com

Keyloggers: What they Are and How to Defend Yourself

A keylogger is a program that records everything that you type on a keyboard. All of your keystrokes are stored, in order, in a log file. Hence the name, "key logger." The log file is intended to be read by a third party that is typically unknown, remote and malicious. Keyloggers do have legitimate uses, such as troubleshooting, training, analyzing employee productivity, and law enforcement surveillance. But keyloggers are most often used illegally to spy on people.

Keyloggers are especially useful for stealing usernames and passwords, bank and credit card numbers, and other sorts of personal information that people type every day. Even data transmitted over an encrypted Internet connection is vulnerable to keylogging, because a keylogger records keystrokes before they are encrypted for transmission.

Contrary to what you may have read elsewhere, keyloggers are not limited to spying on your web browsing activity. Anything you type, in any program, online or offline, can be captured by a keylogger. So if you've been told to type your password into Notepad, then copy & paste it to a web form, that's bad advice.

Software keyloggers are often distributed in Trojan, virus, and other malware packages. These keyloggers can operate at the kernel level, making them virtually invisible to the operating system. Others use "hooks" into the operating system's keyboard API to monitor and record keystrokes. Keyloggers generally attempt to transmit their log files secretly back to their masters, either via email or FTP.

Detect, Defeat and Defend Against Keyloggers

A number of techniques can be used to defeat keyloggers, but no one technique is effective against all types of keyloggers.

A keylogger can be housed in a hardware device that plugs into the keyboard port on your computer. Some hardware keyloggers are hidden inside of keyboards themselves. Hardware keyloggers cannot be detected by software, but they have the drawback of requiring physical access to a computer. If you suspect a hardware keylogger is present on your system, inspecting the keyboard's connection to the computer, or replacing the keyboard will solve the problem.

Form-filling software such as **Roboform** stores passwords, credit card info, and other information in a database, then enters it into Web forms as needed. This eliminates the user's need to type such data on the keyboard, and can prevent keyloggers from recording it. However, there are other forms of spyware which can intercept data posted to forms by form-fillers.

Speech-to-text software or **virtual keyboards** can eliminate the keyboard connection, too. However, the text has to get to its destination somehow, and that path may be vulnerable to clever keystroke loggers.

An antikeylogger program attempts to detect and disable keylogging programs. Antikeyloggers scan your hard drive for the digital signatures of known keyloggers. Antikeyloggers are more effective against keyloggers than general antivirus programs because the latter often don't identify keyloggers as malware; keyloggers do have legitimate purposes, as noted above. But antikeyloggers block all keyloggers they find. **KL-Detector** is an example of this breed.

KeyScrambler is an anti-keylogger that works a bit differently. As the name implies, KeyScrambler scrambles your keystrokes with encryption at the driver level (the first layer between the keyboard and the operating system), then feeds them in decrypted form to the software application. The result is that keyloggers see only the scrambled keystrokes.

Some antispyware programs detect keyloggers by signature or by behavior; for example, programs which hook into keyboard APIs may be flagged as potential keyloggers. Ad-Aware, Malwarebytes Anti-malware, SUPERAntiSpyware, Spybot-Search & Destroy and Windows Defender are examples of general purpose anti-malware apps that also have keylogger detection ability.

A final defense against keyloggers is a firewall that detects outbound traffic. A firewall can alert the user to unauthorized attempts to transmit data to the Internet, which could indicate a keylogger is trying to "phone home" with its log file.

Can I Use a Keylogger?

On a related note, someone once asked me how he might hack into the email account of the woman he's thinking about marrying, ostensibly to see if she's gold or a gold-digger. He was considering a keylogger.

It should be obvious that there are some thorny issues here involving privacy, ethics and the law. As for the relationship issue, if you don't trust someone now, you won't trust him or her in the future. You'll keep "checking up on them" again and again, and eventually you'll get caught. That could mean the end of a relationship or marriage, and possibly a few years in jail for you.

Federal law prohibits gaining unauthorized access to another party's data stored on a computer system. It doesn't matter what your relationship is; who owns the computer; or how carelessly the other party stored her password. The password was obviously created to protect the user's privacy, and by accessing the data without permission (with a keylogger or other means) you violate that privacy right.

The law recognizes a few exceptions to this rule. Prison inmates' communications are subject to unilateral search. Parents can access their children's data without permission. Employers can monitor employees' use of company computers. But you cannot invade a spouse's privacy, let alone your fiancée's. Also, a number of parental control and employee monitoring software packages include keylogger utilities.

Generally you need unsupervised access to the target computer in order to install the keylogger software. Some keyloggers have a sneaky feature that will email the logging software to an unsuspecting user, in the hopes that they will be naïve enough to open the attachment and run a program that installs the keylogger. A keylogger may also require access to the target computer to retrieve the log files, but some programs will automatically email their log files at specified intervals.

If you're thinking about installing a keylogger for the purpose of spying on someone else's activities, I would strongly advise against it. The chances of doing so without getting caught seem vanishingly small to me. And the potential downsides - breach of trust, broken relationships, even jail - far outweigh the benefits.

Malicious PDF Files

Not long ago, I got this interesting question about PDF files. A reader asked “I got a warning from a co-worker about viruses in PDF files. I always thought that you could only get a virus from a program file, and PDFs are just for viewing. Am I right, or can you really get infected by a malicious PDF file?”

Can PDF Files Contain Viruses?

It's a widely-believed myth that you can only catch viruses and other malware from executable files - files ending in .com, .exe, .bat, and a few other extensions. Many people are surprised to learn they can also be infected by .pdf files - the ubiquitous Portable Document Format, made popular by Adobe. In fact, PDF files were implicated in more than 65 per cent of malware attacks during 2010, according to researchers at security software developer Symantec. PDF files are becoming the "vector of choice for delivering malware," it seems.

It makes sense, from a hacker's standpoint. Most people don't think a PDF file can do any harm, so they let their guards down and open PDF files without knowing the sender. People tend to trust the familiar, and virtually everyone is familiar with PDF files and the Adobe Reader software for viewing them.

Unfortunately, the PDF format has been enhanced to include capabilities that (unwittingly) made insertion of malware much easier than it used to be. Objects can be inserted into PDF files that may include executable code such as Javascript applets. Such code is allowed to enable advanced forms-editing and other features of PDFs, but it also opens the door to malicious code inserted by hackers. Malicious code may instigate stack overflows which give the hacker access to all of your computer's resources, or it may automatically download another payload from a hacker's site without your knowledge.

How Do Malicious PDFs Attack?

Just today I got an email with the dubious subject line “Your email has won you the Microsoft email lottery!” I was instructed to “view the attached letter” (a PDF document) for details. Of course clicking on that link would not have made me a millionaire. Another example is the "ransomware" installed by a malicious PDF file that encrypted all of the personal documents on a user's hard drive, and then displayed a demand for $120 to unlock the files. Security researchers at Sophos urge users not to give in to ransom demand; if you do, it's possible the hacker will simply demand more money. But the only way to get your files back is from a backup copy which you hopefully have.

PDFs are often sent to consumers by sources they trust, and so people don't think twice about opening them. In one instance, hackers gained control of the email server of pet supplies vendor VioVet and sent bogus discount coupons to all of the companies customers. When recipients followed the instructions to claim their rewards, they actually downloaded malware that infected their computers.

Banks, insurers, and even the IRS commonly use the PDF format for downloadable forms and reports, or to email statements to customers. If one of these sensitive institutions was breached, it could spell financial disaster for millions.

To counter malicious PDFs, Adobe Systems, developer of the PDF format, updated its Adobe Reader program to include a "Protected Mode" which implements sandboxing technology. Enabled by default in Adobe Reader X and later versions, Protected Mode limits access to Windows system resources by executable code embedded in PDFs. It won't allow such code to make changes to your system.

There are some further steps you can take to tweak Adobe Reader, which will minimize your exposure to malicious code. This article from About.com details the **Adobe Reader settings** you need to change. Alternatives to Adobe Reader, such as the free Foxit Reader, also have security settings that can be tweaked to minimize malware risks.

Regardless of which PDF reader you use, it's a good idea to keep the software updated. If the program notifies you that a newer version or a security patch is available, download and install it promptly. You can also visit the developer's website to see if you have the latest version of the software, and follow any steps they recommend to protect yourself from malicious PDF files.

Help, My Browser Has Been Hijacked!

Has this ever happened to you? Every time you open your web browser, it goes to an unfamiliar search engine page, and when you search from the toolbar, it no longer uses Google. It's possible your browser was hijacked. Here's how to detect a browser hijacking and get your settings back to normal.

Web Browser Hijacking

If your Internet Explorer or Firefox browser suddenly behaves in unexpected or undesirable ways, it may have been hijacked. Browser hijacking is an attack by malicious software that changes your Web browser's settings. Some users who have been hijacked report popups or having searches redirected to pages for online casinos, weight loss products and even porn sites.

Here are some other symptoms that indicate you've been hijacked, and how to fix it.

1. Browser home/start page changed to an unwanted site

2. New favorites, bookmarks, toolbars, or desktop shortcuts that you did not add

3. Typing a URL into the address bar and being taken to some other URL instead

4. You default search engine has been changed

5. Inability to access certain sites, particularly anti-malware sites that might help you

6. Your Internet security settings have been lowered without your knowledge

7. Endless pop-up ads for things you don't want to see

8. Sluggish computer response; malware often slows your whole system down

How does hijacking happen? In many cases, the hijacking software is something you downloaded and installed, thinking it was something beneficial. Many hijack programs are written in ActiveX for Internet Explorer, so be very leery of requests to install ActiveX components. Other hijackers are buried in toolbars, add-ons, and even fake anti-malware programs. A hijack is not necessarily malevolent -- some are just annoying -- but you're still better off getting rid of these unwanted browser parasites.

Getting Back to Good

If you believe your browser has been hijacked, shut down your browser immediately. If you cannot close the browser in the usual way, press Ctrl-Shift-Esc to access Windows Task Manager, highlight your browser's file name in the Processes column (i.e., IEXPLORER.EXE, FIREFOX.EXE) and click "end process" to close the browser.

Hijackers are one reason it is vital to have real-time anti-malware defenses in place at all times. If you're already running internet security software, obviously it didn't protect you from this particular menace. If the problem happened recently, System Restore may "undo" the problem and get you back to normal. (Type "system restore" in the Start menu search box and click the "system restore" link.)

If that doesn't do the trick, reboot your system in Safe mode "with networking." This will load Windows with the minimum of startup options, hopefully omitting the hijacking software. You will need the network connectivity to download some anti-malware utilities. Then open your browser again.

Download **MalwareBytes Anti-Malware** or another free anti-malware utility. Install the software and run a full scan on your system. Delete any suspected malware that it finds. Empty the Recycle Bin and reboot in normal mode.

Open your browser and put things back in order. Review and reset your home page, security settings, privacy settings, etc. Delete any unwanted favorites/bookmarks. Review the list of add-ons and uninstall any that look unfamiliar.

But Wait... There's More!

You're not done yet. Hijacking malware also likes to mess with registry settings. Use a registry cleaner such as **Advanced System Care Free** to remove bad registry entries and close security holes in the registry.

The HOSTS file is another favorite target of hijacking software. The HOSTS file contains pairs of host names and their associated IP addresses. When your browser requests a host name listed in the HOSTS file, Windows directs the request to the associated IP address instead of looking up the host name in the DNS system. Hijack software may add entries to the HOSTS file so that certain sites are blocked or redirected to unwanted sites. The HOSTS file is located at **C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS** and can be opened with Notepad or your favorite text editor.

On Vista or Windows 7 you may need to open your text editor by right-clicking, then select "Run as Administrator".

Make sure the HOSTS file includes ONLY the line "127.0.0.1 localhost" and any other pairs that you know you added yourself. Delete unwanted entries and save the HOSTS file.

To avoid browser hijacking, use real-time anti-malware defenses; don't give unknown websites permission to install software, toolbars, or ActiveX controls; and keep your browser's security settings on medium or high level.

Is Public Wifi Dangerous?

If you use wireless Internet access in public places like Starbucks or the airport, you might be unwittingly revealing your passwords and even personal information to others in the vicinity. Here are some simple precautions you can take to make sure you're not broadcasting your business to snoops and hackers...

Safe Surfing in Starbucks and Beyond

I recently met with a group of Internet professionals, all of us sporting laptops with wireless connections to the hotel's access point. On the second day of the conference, one of the attendees put up a slide on the overhead showing logins and passwords from a dozen of the attendees. Needless to say, many jaws dropped open!

He was running a "wifi sniffer" program that anyone can download to spy on the internet traffic floating around in the air. Fortunately, he was a trusted colleague, and was nice enough to tell us that we were caught with our virtual pants down.

Wifi Safety Tips

First, be aware that almost ANYTHING that you type or any info that appears on your screen while you're using a wireless Internet connection can be intercepted by others nearby.

If you are accessing a page that requires a login and password, or if you are entering ANY personal data (credit card, SSN, etc) make sure that you are on a secure site. That's easy enough -- just check that the web address begins with HTTPS instead of the usual http -- and your information will be safely encrypted before transmission. As long as you're on a page with an address that begins with https, the data you send and receive is protected from sniffers and snoopers.

This is almost always true when using online banking, or making a purchase on the web. But other venues, such as Facebook and your web-based email typically do NOT use an encrypted connection. Gmail is fully encrypted, but Yahoo Mail is not. Hotmail has a secure login page, but after you're logged in, it reverts to non-encrypted mode! Hotmail does provide a way to turn on encryption, but it's hard to find. To enable this feature, go to **https://account.live.com/ManageSSL** after logging in.

Let me repeat – if the web address does not start with https, anything you read or post on Facebook, as well as any email you send or receive while using a public wifi connection is exposed. If you enter a username and password on a website that doesn't offer encryption, that account can be compromised. That may sound alarming, but it gets worse. Wifi sidejacking is a technique whereby someone can literally take over a web session from another user. You could be logged into Facebook and suddenly someone else is posting on your wall and impersonating you. Read more about Wifi Sidejacking.

Oh, and there are the "shoulder surfers" to watch out for. Just like when you're entering your PIN code at an ATM, you need to keep an eye open for anyone who might be glancing over your shoulder while you hunt and peck. I always use two fingers when entering my pin or password... one presses the correct key and other is a decoy. So even if someone was watching from across the street with binoculars, it's almost impossible to steal my pin or password.

The bottom line is this: If you must use public wifi in an airport, coffee shop, or hotel room, awareness and encryption are paramount. If the web address displayed by your browser starts with HTTPS, you're safe. If not, everything is potentially exposed to hackers or snoops in the vicinity.

Mobile Malware: Are You Exposed?

A reader asks: “I'm hearing more about viruses and malware on mobile phones. My wife has an iPhone and I have a Droid. Should we be concerned enough to look into anti-virus or other security software for our smartphones? Or is it all hype at this point?”

Do You Need Anti-Malware Protection for Your Smartphone?

Malware targeting mobile operating systems is on the rise. Security firm McAfee Labs says its count of mobile malware programs rose from about 600 in 2009 to 1,200 in 2011. Mobile malware is just as sophisticated as its desktop brethren, too. "Mobile threats already take advantage of exploits, employ botnet functionality, and even use rootkit features for stealth and permanence," according to McAfee's most recent threat report.

Google’s Android platform was the target of 76 per cent of new mobile malware apps detected in the second quarter of 2011 (44 new malware apps, in raw numbers). Clearly, the fastest growing mobile operating system is also the fastest growing target for mobile malware authors. Java Micro Edition placed second with 14 new malware apps. Symbian was third, followed by Blackberry.

The surging popularity of Android smartphones and tablets has made these devices a new target for the bad guys, and there has been a huge increase in Android malware since Fall 2011. Google's Android Market (recently rebranded as Google Play) is the official source for downloading Android apps, and for the most part, these apps are safe. Amazon app store is another source I consider trustworthy.

Notably, no iPhone or iPad malware has been detected yet. McAfee says, "It is probably a matter of 'when' rather than 'if.'" But the fact that Apple closely vets and controls the apps that make it into the Apple App Store undoubtedly makes it difficult for malware authors to sneak their wares in. Google's App Market, in contrast, does not pre-screen apps before they become available to users, but they seem to do a good job of zapping apps that get reported as malicious.

Who Benefits From Mobile Malware?

Mobile malware aims to make money, of course. One straightforward scheme is malware that secretly subscribes the infected device to premium SMS services; every text message sent or received costs the user money. This type of malware may be concealed in another app such as a calendar or game. Each time you add an appointment or kill a robot, a text message is added to your monthly bill. Other forms of mobile malware may log passwords, steal financial data, and so on.

As you might expect from the foregoing, there's a booming market for Android anti-malware solutions.

Lookout Mobile Security offers one called the Mobile Threat Network. App stores and download sites submit their apps to Lookout, which scans and tests them for suspicious behavior. When an app is identified as probable malware, all of the participating stores are notified and the app is pulled. Lookout also offers a free anti-malware app through the **Android App Market** .

All of the major security vendors are rolling out mobile anti-malware apps. **Norton**, **McAfee** and **Avast** are just a few well-known names. As mobile computing grows, so will mobile malware and mobile anti-malware.

But Do You Really Need It?

So do you need mobile anti-malware protection? If you have an iPhone, I'd say definitely not. One caveat to that would be "jailbroken" iPhones. If you hack your phone in order to enable downloading apps from sources outside of Apple's App Store, then all bets are off.

But what about those with Android or Blackberry phones? To the best of my knowledge, there are no mobile threats similar to the "drive-by viruses" that affect desktop users. So if your smartphone activity is centered on web browsing, and not apps, I don't see a risk that warrants anti-malware protection.

Both Google and Amazon make an effort to remove bad actors from their marketplace, but you shouldn't blindly trust any app. If you stick with apps that have lots of downloads and good reviews, you should be fine. Well-known apps such as

Facebook, Gmail, Yelp, Angry Birds, Kindle, Weather Channel and others with good reputations are safe to use. And I have not heard any reports about malware in any paid apps.

Android malware is a much bigger problem in third-party app-stores, such as GetJar, Handmark and Handango. My advice is to steer clear of those alternative Android app markets. If you download from these sources, or you are the type who can't resist the latest game or productivity tool, then I'd say you run a significant risk.

To summarize, the danger zone for mobile users right now is free apps with unknown or sketchy reputations. Stay away from those and you should be safe. For now.

Wifi Sidejacking

A Firefox add-on named Firesheep ignited a firestorm of controversy when it was released in October 2010. Firesheep demonstrates a hacking technique known as sidejacking, or wifi session hijacking. Learn how to protect yourself from sidejacking when using a wifi connection...

AskBobRankin.com

What is Sidejacking?

Firesheep demonstrates how easy it is to "sidejack" a fellow Web surfer's identity over an unsecured WiFi network. Sidejacking is slang for "session hijacking," a technique that lets one user literally steal the current Web session of another. That means, for example, that you could be surfing your Facebook page when, suddenly, someone else is changing your status, posting messages on your friends' pages, and simply impersonating you right under your nose! The same goes for Twitter, MySpace, and most other social media sites.

Your password has not been stolen; passwords are encrypted when you enter them on login pages. But nothing else is encrypted on most Web sites, and that's why sidejacking is so easy. After your password is authenticated, a Web site sends a cookie or session key to your browser that keeps you logged in for the current session - that is, until you log off. That session key is not encrypted, in most cases, and by "borrowing" it, another user can "be you" for that session. This is sidejacking.

Firesheep snoops on unencrypted WiFi sessions, eavesdropping on others connected to the same wifi access point. It can enable you to sidejack someone's session. One Starbuck's patron (just for laughs) noted what another patron just bought on Amazon.com and posted a message about it to the victim's Facebook page. It's that easy, and that scary.

I should note that if you're using a wifi connection that's secured with WPA2 encryption and a password, this is pretty much a moot point. The WPA2 protocol scrambles ALL the data on your wireless connection, making it practically impossible for snoopers to interfere. Also, the snooper is cut off as soon as you log out of your session.

Who Is to Blame For Sidejacking?

Don't blame the people that created Firesheep. They didn't make it possible, they just made it easier. And there are other wifi hacking tools that have been around for years. The truth is that website operators have long known how to protect all users from sidejacking. But this new attention focused on sidejacking may just may embarrass them into protecting their customers as they should have done long ago.

The solution is to encrypt all of every Web session, not just its log-in process. The means to encrypt a session is built into all modern browsers and web servers. It's called the Secure Sockets Layer (SSL) protocol. It's easy to tell if you are protected by SSL -- in the address bar of your browser, you will see "HTTPS" instead of just "HTTP" when the connection is secured with SSL.

Most ecommerce sites, including banks and Paypal, enable SSL for all sessions. But that leaves a lot of reputational damage that can be done on social media sites and via email. Go check your webmail now and see if SSL is enabled. It isn't? Then every time you check webmail from a WiFi hot spot, you run a real risk that the guy sitting next to you can also read it - and possibly send mail in your name.

GMail was the first major email provider to enable SSL on all users' sessions. Google software engineer Adam Langsley noted that Google needed no additional hardware or software, and that SSL encryption adds less than one per cent to Google's computational load. So it really isn't costly to implement SSL.

Hotmail got the memo and added a feature to enable secure HTTPS sessions. But it's not easy to find. I poked around in the Profile > Privacy settings and couldn't find it on my account. But you can go to **https://account.live.com/ManageSSL** and enable this feature after logging in to Hotmail. Yahoo is still exposed, as far as I can tell. You can login securely, but the connection reverts to unsecured as soon as you're in. So is Facebook, unless you change this obscure **Secure Browsing setting**.

Protection From Sidejacking - What YOU Can Do

So far we've dealt with the responsibility that website operators have in offering secure services. Here's what you can do on your end to protect against sidejacking:

First, verify that your WiFi connection is encrypted with WPA2 or stronger encryption. If the wifi router belongs to you, see Is **Your Wireless Router REALLY Secure?** for help on that. If you're using a public wifi connection, you may not have much choice. But you can always ask the library or coffee shop owner to secure their router with WPA2 and a password, so their patrons can surf safely.

Avoid logging into non-secured sites from public WiFi networks. If the login page URL (web address) does not begin with HTTPS, and there's no option to login with a secured page, your password is at risk of being compromised. Also, pay attention to the URL after you login. If it flips back to HTTP, your session may be exposed.

If you MUST login to a non-secured site on a wifi connection, use a VPN (virtual private network), which creates a secure "tunnel" back to your home or office computer. That's really not as geeky as it sounds. See **Personal VPNs for Anonymous Web Surfing** for help with using a VPN.

One other note: Technically, this is not just a wifi issue. Sidejacking can happen on ANY local network, wireless or wired. This could include the office, hotel rooms and other places where you plug in an Ethernet cable to get online. Bottom line, if a website requires a password, or you might be sharing personal info, make sure you have a secure HTTPS connection.

There are some Firefox addons that will try to force websites to always serve pages with HTTPS encryption. **HTTPS Everywhere** is one example, but these tools have limitations, so read the fine print before you use them.

What is Crimeware?

Imagine if, for only $3000, you could buy the role of a crime lord whose millions of minions obediently and constantly funnel money to you. Now imagine that anyone can. Finally, understand this is not fantasy, and you might become very scared. Learn more about crimeware, and how to protect yourself...

Zeus, Botnets and Crimeware

The Zeus botnet is a worldwide network of computers over which hackers have established control, often without the owners' knowledge. A Trojan horse program they picked up by opening an infected email attachment or visiting a phishing Web site controls these robot or “zombie” computers.

The Zeus Trojan is a versatile devil. It's a keylogger that records logon credentials as you type them. It alters your bank's Web page HTML to facilitate identity theft. It redirects your browser to a look-alike Web site where you can be fooled into giving up more critical information. It searches your hard drive for bank account and other financial data it can upload to its masters; and much more. For an exhaustive report on Zeus, its components, and its nefarious capabilities visit **SecureWorks**.

In October 2010, the FBI announced that it arrested more than 90 Americans in "one of the largest cyber criminal cases we have ever investigated". The arrestees were "money mules" who received stolen funds in their bank accounts and forwarded it to their criminal masters in exchange for a commission. The mules received the money - over $70 million total - by fraudulent transfers of money enabled by the Zeus botnet. The thieves originally targeted $220 million, says the FBI.

Now it gets really scary. The criminal creators of the Zeus botnet are now selling a bundle of software called "Zeus crimeware" which enables just about anyone to be a cybercrime kingpin. Zeus crimeware is as user-friendly as any commercial legitimate program. Wizards guide you step-by-step through the process of configuring which keystrokes to capture under what circumstances; where to transmit the stolen logon credentials; and the creation of a seemingly innocent and alluring "free download" to turn loose on unsuspecting victims.

Plus, you too can use the existing Zeus botnet to start robbing strangers. You might possibly also get arrested by federal agents and thrown into prison with some Russian guys. But you know, life is filled with risks and rewards.

Are You an Ignorant Zombie?

You may have no interest in running a global criminal cyber-enterprise. But you COULD be an unwitting participant. Nearly 4 million PCs in the U.S. alone are part of the Zeus botnet, with estimates of worldwide infections running much higher. Using Zeus, cybercriminals have pulled off some spectacular crimes.

A good anti-virus program should protect you, but if you want to double check if your computer is infected with the Zeus Trojan, start by looking for these file paths and files on your system. If you are logged on with Administrator privileges:

%systemroot%\system32\sdra64.exe (malware)

%systemroot%\system32\lowsec

%systemroot%\system32\lowsec\user.ds (encrypted stolen data file)

If you are not logged on with Administrator privileges:

%appdata%\sdra64.exe

%appdata%\lowsec

%appdata%\lowsec\user.ds

Note that Zeus files are "hidden" by default, so you will have to set Windows Search to show hidden files or you will detect nothing.

Protecting yourself from a Zeus infection requires extreme caution. Experts recommend logging on to online banking and other password protected accounts using an "isolated" computer that is not used for general Internet work (email and Web browsing). But that's not very practical for most consumers and small businesses.

Alternatively, you might consider a different operating system. Zeus is most often found on Windows XP systems. An optional Zeus crimeware kit makes Zeus Trojan compatible with Vista and Windows 7; not every crook spends the money for this option so these OSes are safer than XP. But to escape Zeus altogether you would have to switch to a non-Windows operating system, i.e., Mac OS or Linux.

At the very least, keep your anti-malware software up to date and constantly activated. Avoid clicking on email attachments from unknown senders. Enable the anti-phishing features of your Web browser and if it says, "don't go there," don't go there.

Zero Day Exploits

Adobe Corporation, the Mozilla Foundation, and other large enterprises have been hit by zero-day exploits launched by organized groups of hackers. The term zero-day sounds sinister and dramatic, but what does it mean?

AskBobRankin.com

What is a Zero-Day Exploit?

Very simply, a zero-day exploit is a hacker attack that takes advantage of a security vulnerability in a piece of software on the same day the software developer becomes aware of the vulnerability. In other words, the developer literally has zero days in which to come up with a fix. Let's look at these two recent examples to see why zero-day exploits make headlines.

In Mozilla's case, hackers discovered a Javascript programming flaw that allowed them to redirect visitors trying to access the

Nobel Prize Web site to another site, which downloaded a Trojan program to the redirected visitors. The Trojan installed itself on infected computers and attempted to connect to two servers in Taiwan. If the connection succeeded, the owners of those servers would gain complete control over the infected computers. That's pretty scary!

Adobe was luckier. A "white hat" hacker discovered the flaw in Adobe's popular Shockwave animation software and simply demonstrated what he could do if he was a bad guy or "black hat". Visitors to a Shockwave animated Web page unexpectedly found their Windows Calculator accessory popping open. But the vulnerability could have been used to infect a computer with something like the Firefox Trojan.

What's really interesting is the difference between the responses of Mozilla and Adobe. The Mozilla team released a patch that was automatically installed on affected versions of Firefox within 24 hours of learning about its zero-day vulnerability. Adobe simply advised everyone to "exercise caution" with Shockwave Web pages, and said it is "currently working on determining the schedule for an update to address this vulnerability."

Should I Panic?

A zero-day exploit seldom results in widespread mass infections of computers with malware. Security researchers - "white hats" like the Firefox trickster - detect many vulnerabilities before hackers do, and responsible companies patch vulnerabilities quickly. But some zero-day exploits go unpatched much longer, and that can be a problem as more and more malware is released to exploit the vulnerabilities.

Don't panic when you read that a "new zero-day exploit has been detected" in any program you use. Just learn how the exploit works and avoid it. That may mean not using a particular program, not clicking on email attachments; avoiding unknown Web sites and those known to be compromised by the exploit.

Check for patches at software developers' Web sites as soon as you learn about zero-day exploits. Not every developer pro-actively distributes patches as Mozilla did to Firefox users. You may have to find, download, and install a patch yourself.

Subscribe to automatic installation of at least "critical security updates" for your operating system and application software, if they're available. Use anti-malware software to constantly monitor your computer and its incoming Internet traffic for suspicious activity or software code.

Another good idea is to scan your software for vulnerabilities using the **Secunia Personal Software Inspector** (PSI). This free program will tell you which programs need updating and provide links to sites where you can download patches.

A zero-day exploit is simply a newly discovered threat, a possible avenue of attack. It is not an actual attack. As the ancient Romans said, "Our fears always outnumber our dangers."

Is Your Webcam Spying On You?

Someone may be spying on you via your computer's Web camera. It's an old hacker trick, dating back to the late 1990s. But don't worry, such attacks are relatively rare. Here's how to tell if your webcam is being used by someone else, and security steps to minimize this risk...

I Always Feel Like Somebody's Watching Me

It might be paranoia, but then again... Police in Fullerton, California recently arrested a computer tech who was surreptitiously installing webcam spyware on laptops that he repaired. Trevor Harwell used the Camcapture software to remotely photograph women who were duped into taking their Mac laptops into the bathroom while showering.

Most webcams have an activity indicator that alerts you when the camera is turned on. It may be a small LED light on the camera itself, or an icon in the system tray. Pay attention to the webcam activity indicator. If it comes on when you have not activated the camera, someone may be spying on you.

A sudden drop in your Internet speed may indicate that your webcam is streaming video to a remote location without your knowledge. But there are many other reasons why the Internet "slows down" frequently.

Poor security practices are responsible for almost all webcam hacks. Forgetting to turn your webcam off when you are finished using it is an obvious and common mistake. If you do not have a firewall installed on your network, it's possible for hackers to see your web cam and access it remotely. But most webcam hacks rely on remote access software installed on the victim's computer without his or her knowledge.

How Does It Happen?

Remote Access Trojan (RAT) malware is distributed in the usual ways. It can arrive as an attachment to an email, or in file you download from a questionable site. A RAT not only lets the bad guy control your webcam, but also just about anything else on your computer. Anti-malware software can detect and disable RATs. You should also disable remote access services on your computer; most people, most of the time, do not need to have remote access enabled.

It's possible for an unscrupulous repair tech or IT employee to install remote access software on a user's computer. This is rare, but as I mentioned earlier, not unheard of. Whenever you let someone else repair or troubleshoot your machine, you should check to see if any new services or programs have been added when you get it back.

Unplugging your web cam when you are not using it is another precaution you can take. For webcam that are built into laptops, you can disable the device through the Device Manager utility of Windows.

Some webcams come with a "modesty shield," a plastic cover that can be flipped down over the lens. Some people put tape over their webcams as a sort of makeshift lens cover, and remove it when they want to use the camera.

If you are using a wireless router or wireless webcam, be sure to enable WEP or WAP security. Webcam hacks are not very common, but it can be very distressing to have your privacy invaded. Following the basic rules of Internet security and disabling your webcam when you're not using it can spare you such violations.

* * *

You've reached the end of the free Preview Edition of this book. Want to learn more?

CLICK HERE to save $10 on your purchase of the 256-page Full Edition. See the Introduction for details about what’s in the Full Edition.

About the Author

Bob Rankin is a translator for the technology impaired -- a writer and computer programmer who enjoys exploring the Internet and explaining technology in plain English. His goal is to help you solve your computer problems by yourself, for free!

Bob was one of the first Internet publishers, having started the Internet Tourbus project in 1995. The New York Times has featured him in stories, and his work has appeared in *Computer World*, *NY Newsday*, and other publications. He has appeared on numerous radio and television programs.

Bob is the author of several computer books, and offers free tech support at his website **AskBobRankin.com**. Read Bob's **extended bio** to find out why he still remembers his first password, and the computer crime he committed, 35 years ago.

OTHER BOOKS BY BOB RANKIN

Use the links below to save $10 on other titles in this series:

* **Everything You Need to Know About INTERNET SECURITY and PRIVACY (Full Edition)**

* **Everything You Need to Know About BACKUPS**

* **Everything You Need to Know About WINDOWS**

For FREE daily tips on computers
and the Internet, sign up for my
AskBob Updates newsletter!