



Introduction

Malware is malicious software, a program running on your computer that does you harm. Sometimes it's called **spyware**, sometimes it's called a **virus**. Often it's called something unprintable.

This article is a product of eight years cleaning malware off computers. If you think you've got malware and want to get rid of it, contact me at the addresses below. Please feel free to distribute *Computer Security* as long as you keep it intact and include the copyright and contact information.

1. How to Make Money with Your Computer

The first malware I ever saw was amazing. A client brought me up to his young daughter's room and started her computer. As soon as it came up, the desktop was covered with porn site windows opening up as fast as they could. His daughter was terrified. I was too!

Some malware watches you using your computer, what Web sites you go to, who you send e-mail to..., and sends this information to advertisers. That's why it's called "spyware;" it spies on you. Advertisers use this information to profile you so they can send you ads that you will be interested in.

Advertisers are willing to pay big bucks for this kind of information. The problem of malware is growing and growing. **THEY** are making money with your computer.

Most malware is not illegal because you consented to it. When you downloaded that free weather forecasting program, somewhere in the process it presented its terms and conditions to you and you clicked on the "I Agree" button. Somewhere in those terms and conditions was a notation that said you consent to their malware.

The first symptom of malware infection is your computer slows down. That's because it is now the unwilling host to malware programs. It takes forever to boot up, forever for programs to start, forever to shut down.

Another big symptom of a malware invasion is pop-up ads that *just appear* on your screen when you're not doing anything at all. You're thinking about the next sentence in your letter to your sister when *POW!* the University of Phoenix wants you to enroll.

The third big symptom of malware is your Web browser won't go where you want it to go. You try to go to Google and it sends you to *CoolWebSearch*.

One might think the solution is to scan your computer with "anti-malware" programs. *Don't!* There are dozens of "anti-malware" programs out there with very powerful-sounding names like *Windows Antivirus 2009*. Most of them *give* you malware! The money is just too good to resist.

There is even one “malware removal tool” that won’t stop sending you pop-up ads *and* won’t remove itself *until you pay them to remove it!* Cyber-blackmail!

If your computer is not too badly infected, removing malware is fairly easy. Sometimes, however, removing malware can leave the computer in worse shape than before the problem was fixed. Really. Before removal, the computer was running slow but at least you could still get your e-mail. After legitimate removal, sometimes your computer can’t get to the Internet at all. Malware does serious damage to computer system files and removing the bad stuff leaves the good stuff in need of real repair, so watch out. This happens in about 10% of the cases I see.

There are two legitimate and good malware removal tools:

- *Spybot Search & Destroy* (<http://majorgeeks.com/download2471.html>)
- *Windows Defender* (Google “Windows Defender Download”)

There are at least three on-line malware scanners worth trying:

- *Bit Defender* (<http://www.bitdefender.com/scan8/ie.html>)
- *F-Secure* (<http://support.f-secure.com/enu/home/ols.shtml>)
- *Kaspersky* (<http://www.kaspersky.com/kos/eng/partner/default/kavwebscan.html>)

Windows Defender is the best of the bunch because once you’ve installed it you can pretty much forget it. It runs itself, updates itself, and protects you even when you don’t run it manually. Windows Defender is included on Windows Vista. With XP, you’d have to install it yourself.

Assuming your computer is already clean, or clean-able, that is.

None of these programs are 100% effective. When I get a really badly infected machine to clean, I run all of them and even then sometimes there is still malware left that can’t be cleaned.

Stay away from these very popular malware carriers:

- *Comet Cursor*
- *CoolWWWSearch*
- *Gator*
- *Grokster*
- *HotBar*
- *KaZaa*
- *LimeWire*
- *MyWebSearch*
- *Morpheus*
- *Spyware Assassin*
- *Weather Bug*
- *The Weather Channel*
- Those cute *animated icons* you can stick in your e-mail and IM’s.
- There are *lots* of others.

Malware carriers are often very popular and some of them do good things, but they come with hidden trouble. And be especially wary of programs that claim to be removal tools. For every legitimate tool there are twelve bad ones.

2. How Did I Get This Stuff?

Your computer probably became infected by malware in more than one way. Here are the ways your computer can become infected.

1. **You Installed It Yourself.** You installed LimeWire or KaZaa and now you're infected. What were you *thinking*?
2. **In your e-mail.** This is a classic technique. Malware running on one machine mails a copy of itself to everyone in their address book. Despite popular opinion, you're more likely to get infected by people you know than by people you don't know.
3. **Go to the wrong Web site.** Software can be automatically installed on your computer just by browsing a Web site. A recent Google survey said that 10% of Web sites are guilty of this now. This is called a "drive-by infection."
4. **Instant Messaging** users are very prone to malware. Malware on a machine will send a message into a chat room that looks like it came from a person. The message will say, "Joan, this program is *you*." There will be a place to click to download. One click and your computer is toasted.
5. I have seen new computers come delivered with **malware pre-installed**.
6. **Pictures embedded in e-mail** can exploit a flaw in your e-mail program and install malware without asking your permission.
7. **Vulnerabilities** exist in your system all the time. If your computer is not up-to-date the bad guys will come in through the holes. See the next section about updates.
8. **AOL 9.0** comes with two malware programs in it, though AOL claims the information they gather is to help serve their customers better.
9. People who let **Comcast** give them a (black) Linksys cable modem/router box are consenting to have Comcast spy on them. Read your agreement with them. The Comcast-supplied router allows them to gather personal information.

The point is, there are lots of ways to get malware. You can get it through your actions, or through your inaction. Once one malware program is running on your computer, it lowers your computer's defenses and allows others to come on board too. Malware starts out slowing your machine down a little bit, then a little more... Soon your machine can't do a thing. Once your machine is limping along or crashing, it has passed beyond what mortal civilians can do to clean it and it's time to take it to the doctor.

3. How Do I Protect Myself?

The September 2004 issue of *Consumer Reports* had a great cover story, “Protect Yourself Online.” I highly recommend you go to your public library and read the article. Here are the facts about computer security today and lots of things *Consumer Reports* didn’t tell you.

a. Antivirus software

You absolutely *must* have antivirus software, and it *has* to be up-to-date or guaranteed you’ve got a virus. It is only a matter of a week or so before your machine gets infected.

A new copy of antivirus software will cost you \$40 and it will keep your clean machine clean. Removing a virus from a machine that’s infected will cost you \$250. You do the math.

I recommend *AVG Free*. <http://free.grisoft.com/>

I recommend *against* Norton or McAfee. Every nerd I know in the business of fixing computers agrees with me. Norton and McAfee are the big boys in the anti-malware market. Malware writers (“the bad guys”) test their new malware against these programs to make sure they can circumvent their protection. If you’re experiencing a slow computer and it has Norton or McAfee on it, removing it will make your computer run faster. Then install *AVG Free*.

Macintosh? Never mind. Mac viruses are very rare.

b. Firewall

A “firewall” watches your Internet data going in and out and prevents communication from happening if it shouldn’t. Modern PC’s and Mac’s all have built-in firewalls. They are the ones I recommend, and again, you *must* have one.

There are other firewalls available: Zone Alarm, Black Ice, etc. These products are good **if** you know how to use them and that’s the problem. Civilians do not know what to do when the firewall puts up an “alert.” They almost always make the wrong choice, and then they wind up unprotected. Worse, these firewall products slow your computer and Internet connection down so even if they’re working, they get in the way.

If your home or office has a “router” between your machine and the Internet, you can relax a bit on firewalls. The router has a built-in firewall so you’re protected.

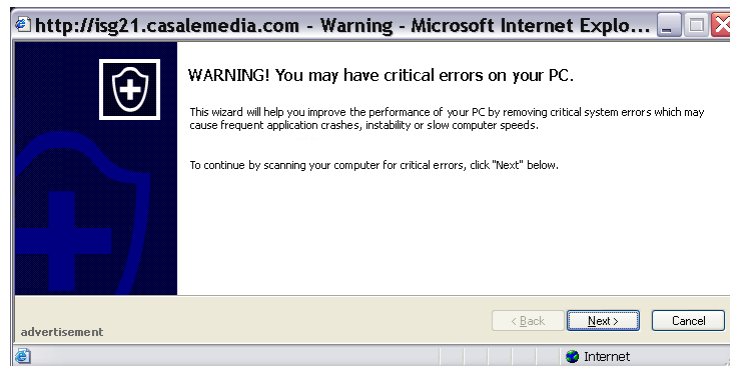
You must have a firewall.

What if you’ve got an older computer? Are you ready for some bad news? Older operating systems were just not written with security in mind. It’s a lot like driving an older car before seat belts and air bags. If your privacy and data are worth anything to you, you’ll move up to XP or Vista, or OS X on your Mac.

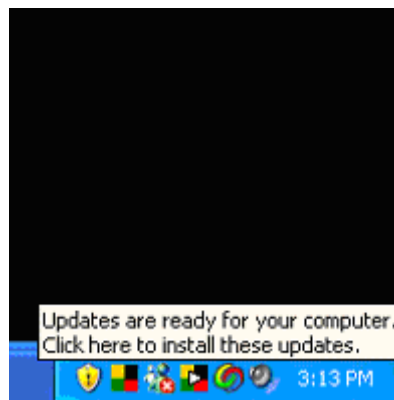
c. And...

Protecting yourself from malware is complicated. But if you're one of the many families or companies that have called me back more than once to remove malware, you'll want to follow these suggestions to protect yourself.

1. **Set your Internet Security.** Do it. This is important. See Part 4, following.
2. **If the window or e-mail says “Malware Alert!” or some-such, close it.** Click the “X” in the corner. When you see a window that says “Your computer may be infected...,” close that window by *only* clicking the “X” in the corner. And, your computer *is* infected, by the way.



3. **Get Windows Defender.**
4. **Get Spybot Search & Destroy.** Spybot is great and free. Download it, install it, run it, get the updates, and if your computer isn't too badly infected, your malware problems are solved for the moment. Run Spybot weekly. You'll be amazed at how much malware you pick up each week.
5. **Get all the updates.** Malware exploits holes in your computer's security. As holes are found and fixed, Apple and Microsoft release “Critical Updates” for your machine to automatically install. Install them all, every time. Set Automatic Updates to run daily. Microsoft releases updates at least monthly (on the 2nd Tuesday of the month) and other times when necessary.



When you see the text, “Updates are ready for your computer...” with the yellow shield icon, you know Microsoft is trying to update your computer. Let them. Every time.

If you *don't* see the "Updates..." prompt at least once a month, your computer needs serious updating, it is years out-of-date.

6. **IM with care.** The people who call me back again and again to remove malware are *all* people whose teenagers do a lot of instant messaging.
7. **If it's free, it's probably bad.** Not to be repetitive, but don't download free clock-setting software, music sharing software, animated icons, weather info, search assistants...

Malware is impossible to completely prevent because *you can infect yourself*. All the home security systems in the world won't protect you if you open the door to a thief. The same applies to a computer. To really protect yourself you have to have *AVG*, run *Spybot* once a week, and have *Windows Defender* too.

If your computer gets too bogged down, even these programs aren't going to help and *may even damage your system* when you run them. If your system is crashing or running too slow to get anything done, don't fix it yourself.

Removing malware is a lot of work.

There is a program out there called *Spy Sweeper*. Though it is a legitimate anti-malware product, I have found it to be largely ineffective. Some Internet Service Providers give away *Spy Sweeper* to people who ask for it. In my humble opinion, don't waste your time unless you want a false sense of security.

I also have a low opinion of *AOL Antispyware* and if you have the option, skip this product. Having it only gives one a false sense of security.

Be very suspicious of anti-malware programs not mentioned here. There are many ad blocker, spy killer, virus cleaner programs that are themselves malware. For example, *Spy Hunter* does indeed protect against some malware, but it pushes its own pop-up ads at you. *Spyware Assassin* is just that, a malware program that assassinates your computer.

4. Set Your Internet Security

Your browser should be set to high security, but it probably isn't. You *need* to do this.

1. Start Internet Explorer (the big blue “E” program on your desktop):



Internet Explorer

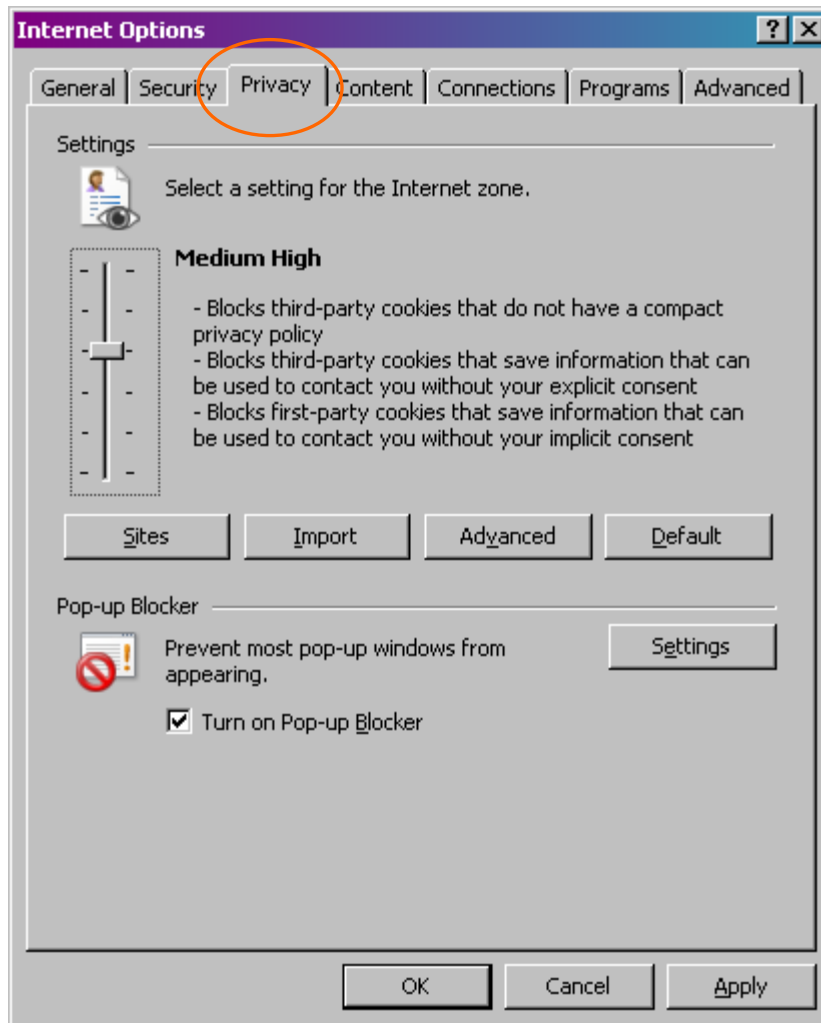
2. Click on “Tools” at the top, then “Internet Options...”

3. Click on the “Security” Tab at the top:



4. Click on the “Reset all zones to default level” button at the bottom. This sets your security for all four kinds of Internet sites. Good job so far.

5. Next, click on the “Privacy” tab at the top of the window:



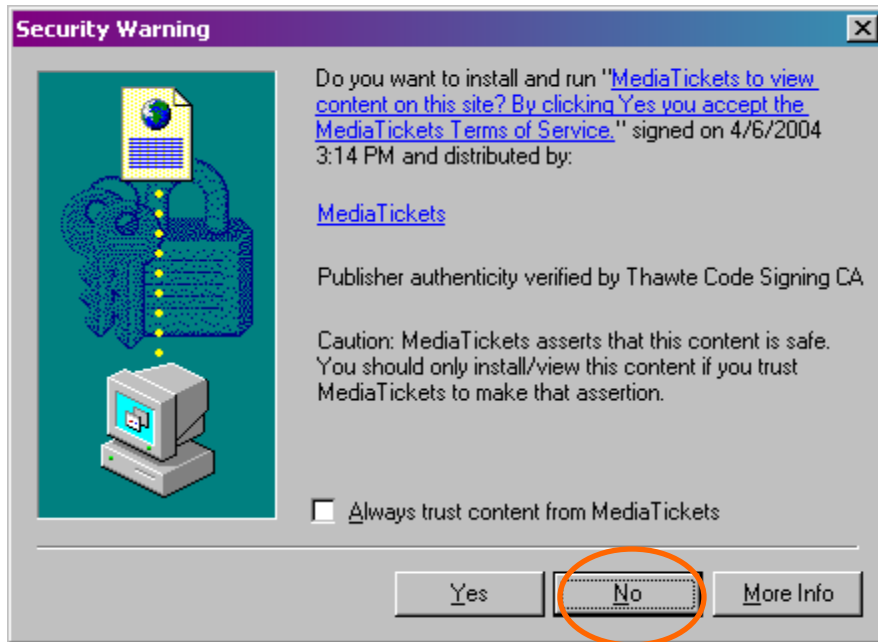
6. Set the slider to “Medium High”. If you don’t see a slider, click the “Default” button first, then set the slider to “Medium High.”

7. If you have a “Pop-up Blocker” choice, make sure it is checked to block pop-ups.

8. Click “OK.” Your Internet Security is set.

You Still Have to Watch Out

Unfortunately that's not all there is to it. With the settings now set in your browser, a drive-by infection can still try to infect your computer, but now it will have to *ask your permission!* This is what one might look like:



Just say "No."

And stay away from that Web site. They have shown themselves for what they truly are.

Some people have switched to the Firefox browser thinking they are getting a more secure browser. They aren't. Firefox has just as big a problem with drive-by infections as IE.

5. Phishing. The First Scam Game of the 21st Century

The bad guys out there looking for your money are not just high school kids, they're pros. Organized crime is into the Internet in a big way. The most egregious method yet of stealing with a computer has come to be called "phishing." In it, you receive an e-mail from a bank or someone you do business with asking you to log on to their Web site and confirm your account information.

You do so. The site thanks you for your cooperation. You go on with your life.

Two weeks later your account is short thousands of dollars.

That e-mail was not really from Bank of America, or eBay, or Schwab, or the IRS. It only *looked* like it came from there.

It is very easy to fake where an e-mail is from. I do it myself every Christmas when my kids receive an e-mail from Santa@NorthPole.np.

It is very easy to set up a fake Web site. Just because a site looks and sounds sincere doesn't mean it *is* sincere. Check the address at the top of your browser. What you see *there* is where you are, *not* what it says on the Web page. Phishing sites will have "similar sounding" names like:

e-bay.com which is not the same as ebay.com

MICROSOFT.com those are *zeroes*, not the letter "o" in "MICROSOFT". See them?

whitehouse.com the *real* White House is at whitehouse.gov

Be suspicious. Call your bank on the phone and verify that they need your account info. Use the telephone number *you* have, *not* the one in the e-mail.

Thieves are very smart. It takes a bit of expertise to spot a fake e-mail or Web site, but if you're interested, [e-mail me](#) and I'll send you some tips.

Poor people can be victims too. Thieves do not only steal thousands from large accounts. They also steal dollars and change from small accounts. This has happened to me twice. If you see an unknown transaction on your credit card, even if it's only for a buck or two, **question it!** Your bank will be happy to help you.

Don't tell your password to anyone, ever. The good guys will never ask for it.

The good guys know your name. The bad guys don't. A good sign of a phish is it is generic: *Dear Account Holder, Dear PayPal User,...* This may change, however, as phishers get better at it.



Make up a “strong” password. The length of the password is not what makes it strong. The *variety* of the characters is. Make up a password that is not going to be in a dictionary. Something with upper and lower-case letters, numbers, and a punctuation mark or two. “23skiDoo!” “GoRedSox2009!” “5000dollars?” Don’t use these, but you get the idea.

-LLiioonneell

Lionel Goulet

Computer Help Company

<http://blog.compHELPCo.com/>

*Personal Attention to Your Personal Computer*sm

(781) 209-0856

Te Deum