



Malware - The Silent Killer
by
Cost Effective Computers

Malware

Introduction

by Brian Flynn

Malware is malicious software that is loaded on your computer. This help guide was designed to give you an overview of what Malware is, how you get it, and how to get rid of it.

Though every effort has been made to ensure the accuracy of the information contained in this document, the information is in no way warranted, neither explicitly or implicitly. As with all computer related information, make a point to stay current with what is happening. That is the only way to protect your hardware and your data.

Table of Contents

Part I Introduction	2
Part II Liability	2
Part III Desktop Malware	3
1 Desktop Malware	3
2 File Sharing Apps	4
3 Utilities	4
4 Games	5
5 Miscellaneous	5
6 Task Bar Icons	6
Part IV Internet Malware	6
1 Browser Toolbars	6
2 E-mail Warnings	7
Part V Removing Malware	7
1 Overview	7
2 Uninstall	8
3 Removal Tools	9
Index	11

1 Introduction

The internet is a wonderful tool. We use it everyday for sending prescriptions, doing research, news, and entertainment. But with the internet comes Viruses, Spyware, Pop-up Ads, and a host of other "things" that somehow get on your computer and slow it to a crawl, or, worse yet, shut it down altogether. We call this stuff MALWARE!

Malware is just another name for intrusive or destructive software. We use the term broadly to describe viruses, worms, ad-ware, spyware, and any other program that infects your computer. You get the stuff by browsing the internet, downloading some programs, or opening infected e-mails. Sometimes you never know you get it, until it shuts your system down. So we decided to put together a little document that explains what some of these things are and how you get them. We also will try to iterate how malware effects your computer and can potentially render it useless. Last of all, we tell you how you can remove most of this junk and avoid getting it in the future.

Before we go any further, let's define what the different categories of malware are.

Viruses

Viruses are programs that have been written for malicious purposes. It infects your computer through a download either via the internet or e-mail. Once it is on your computer it is designed to execute instructions. It may send personal data back to its creator or try to harm data on your computer. It typically attacks Microsoft Windows, since most virus writers have a distinct disdain for Microsoft. You must use a virus detection program and keep the virus definitions up-to-date to stop viruses.

Worms

Worms are much like viruses, except worms find their own way into your computer instead of you having to download them. When they get in they execute malicious code and typically hose your computer. To protect against worms you need a firewall and a virus protection program.

Spyware

These are programs that get downloaded, usually from websites, either with or without your knowledge. The intent of these programs is to track personal information and send it to its creator to use in whatever way they desire. Sometimes this collects personal or computer data and sends it out for malicious use. Sometimes it is used for customizing websites for you, i.e. cookies, and displaying advertising specific to your tastes. Amazon.com is an example of a site that uses cookies to customize their pages for the user. Not all spyware is malicious, but sometimes it is hard to know the difference.

Ad-ware

These are typically programs that get loaded to display all the pop-up ads you get. Though these are not necessarily malicious in and of themselves, they certainly are annoying. And if you are not careful, clicking on one of the links from these pop-ups can take you to a site, or download, that is malicious.

2 Liability

The purpose of this document is to provide you with some information on what is out there that can harm your computer, and some tips and tools to remove any junk you have on your machine. It is not all inclusive as there is more junk out there than we can list, but we at Cost Effective hope that you will use this information to protect your computer from harmful infestations. After all, you are in business to fill prescriptions; and if your computers are slow are disabled it will be hard to do that.

In the event that your computers experience slow-downs or quit altogether, malware may be the

problem. If you call us to help clean this stuff off, ***please remember that clean-up services for malware are not covered under our hardware maintenance agreement. We may charge you, at our discretion, our current billing rates for the time to clean up the mess.***

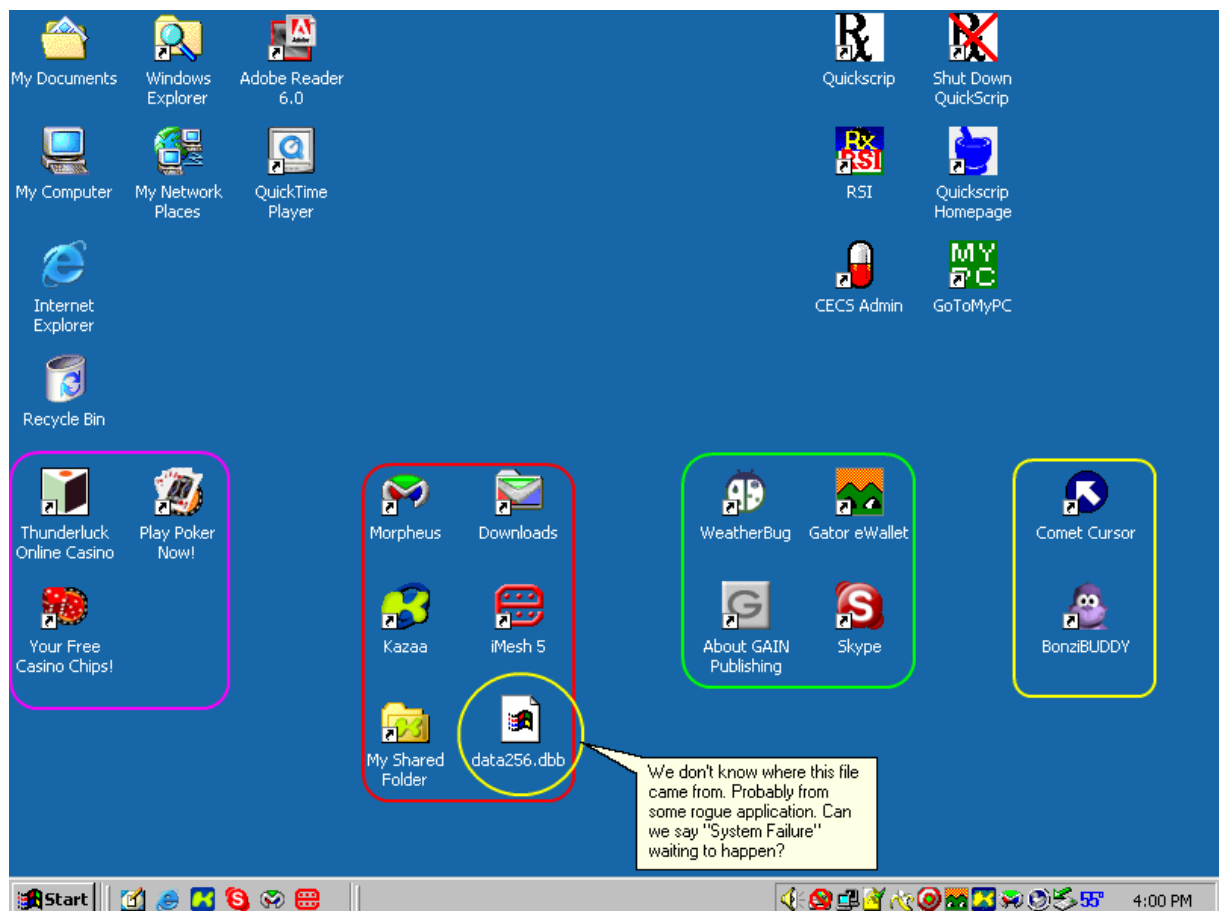
3 Desktop Malware

3.1 Desktop Malware

Desktop malware are programs that you download. They usually place an icon on your desktop "for quick access" and sometimes serve a useful purpose in and of themselves. The problem with many of these programs is that they invite a host of pop-up ads and open the door for viruses and worms. Not only are these annoying, but they can wreak havoc on a computer and sometimes spread to other computers, causing your system to shutdown.

Below is a picture of a computer desktop loaded with malware. At the top are icons for legitimate applications that you might see on one of our computers. At the bottom are icons for different types of malware. Each type of malware is circled with a colored line. We really had fun loading this machine up like this, but please, don't try this at home!

Click on the circled item to go to a description of that particular group of malware. Click on [Task Bar Icons](#) to see a description of the little icons that appear at the bottom of the desktop.



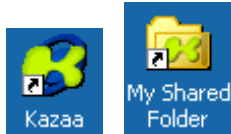
3.2 File Sharing Apps

File sharing applications are programs that allow people anywhere in the world to share files on their computer with anyone else in the world that uses the same software. The most common uses of this type of software is music and video clips.

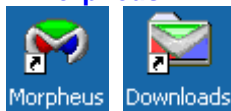
Since you don't know where these files are coming from, you run the risk of infecting your computer with viruses, worms, or any other type of infection. Not to mention that many files load spyware that tracks your usage and possibly personal information. Not only is this type of file sharing dangerous, in many cases it is also illegal (particularly with music). So don't run the risk of data or financial ruin. Get rid of this stuff.

Several of the more popular file sharing programs include:

- **Kazaa**



- **Morpheus**



- **iMesh**



See [Removing Malware](#) for ideas on how to get rid of file sharing applications on your system.

3.3 Utilities

Utilities include programs that actually serve a useful purpose, but may infect your computer just the same. Several popular programs out there include:

- **Weatherbug**



A useful utility for tracking current weather conditions. The program itself is not necessarily bad, but a lot of ad-ware and possibly other spyware piggy-backs on this program. We recommend you don't use it, especially on your main pharmacy computer.

- **Gator**



This is software used for storing your personal information to be used when logging into websites or filling out forms on websites (like order forms). The fact that it stores personal information and is linked

to the internet makes us nervous! Get rid of it!

Gain



Gain is a utility that allows you to receive free software in exchange for letting them send you advertising. This is just opening yourself up for some kind of problem. We suggest you don't participate in this and remove it.

Skype

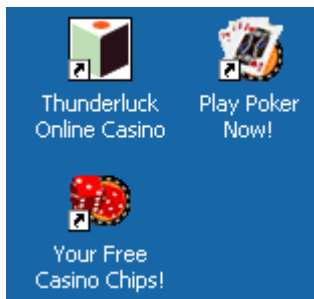


Skype is an internet based telephony product. It allows you to make virtually free phone calls to other Skype users over the internet. But like all utilities, you never know what baggage it brings with it. Be careful with this one.

See [Removing Malware](#) for ideas on how to get rid of utilities on your system.

3.4 Games

Games fall into several categories. The examples here show casino oriented games (very popular right now!). The games in themselves may not expose you to any harm, but they attract ad-ware and spyware. Many times you will be inundated with popups and other garbage as a result of downloading games or playing on-line games. In any case they reduce the productivity of your employees, and provide ways to harm your computer, so get rid of it.



See [Removing Malware](#) for ideas on how to get rid of games on your system.

3.5 Miscellaneous

Miscellaneous comes in a variety of flavors. Two that we highlight here are BonziBuddy and Comet Cursor.

BonziBuddy



BonziBuddy puts a talking monkey on your desktop. I don't know who thought of that, but who needs a talking monkey on their computer?! Get rid of it.

Comet Cursor



This is a program that changes your mouse pointer to different characters. Very useful if you don't like the arrow or the standard cursor options that come with Windows. For us, the pointer works just fine. Get rid of it.

See [Removing Malware](#) for ideas on how to get rid of miscellaneous junk on your system.

3.6 Task Bar Icons

A lot of these programs put icons on the desktop and in the task bar at the bottom of the screen. Here is a shot of the task bar with the icons labeled for identification.



4 Internet Malware

4.1 Browser Toolbars

Browsers are programs that interpret HTML code (the basic language of web pages) and display the information on the screen for you. Browsers in themselves do not hurt your computer (usually!), but malicious programmers have found ways to exploit security holes in browsers for "evil" purposes. Using these security holes, viruses and worms can be downloaded to your computer causing numerous problems.

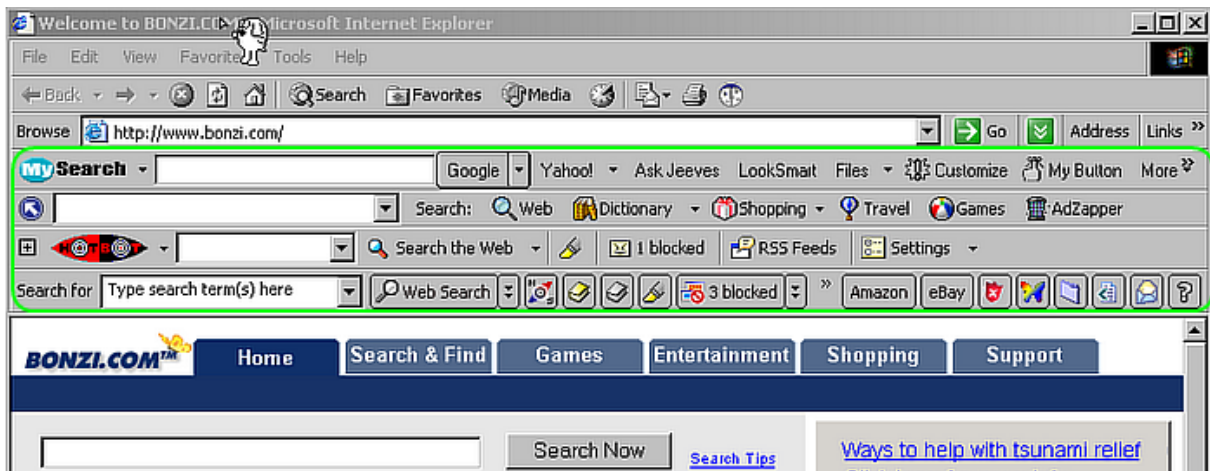
By far, the most popular web browser is Internet Explorer (IE for short), by Microsoft. IE has been exploited for security vulnerabilities numerous times, and it is not likely to end. The best way to protect yourself is to keep IE up-to-date by downloading periodic updates.

In addition to viruses and worms, many advertising and marketing companies have provided toolbar's that are installed in Internet Explorer. These toolbar's are used for searching the web, blocking pop-ups and other functions. However, they are also a magnet for spyware (some of the toolbar's are spyware themselves) and ad ware. We recommend you remove these toolbar's if you have them.

- [We have authorized one toolbar, the Google Toolbar. We also feel that the Yahoo toolbar would be OK. Anything else should go.](#)

Below is a screen shot of several toolbar's you may see in IE (toolbar's are highlighted in green). If you see any of these, click on the link below to learn how to remove them.

See [Removing Malware](#) for ideas on how to get rid of internet toolbar's from your system.



4.2 E-mail Warnings

There are several ways to check e-mail. You can use an internet based e-mail like Yahoo or Hotmail. You can also use a computer-based e-mail program to check your mail. One of the more popular ones is Outlook Express (OE for short), by Microsoft. OE is easy to use, and free (it's pre-installed on all Windows computers). Like its browser counterpart, OE is susceptible to viruses and worms. The difference is that typically the virus or worm cannot execute unless you open the e-mail that it is attached to. To avoid infecting your computers, use the following tips:

- Never, ever, ever, ever, open an e-mail unless you know the person that sent it! Opening infected e-mail from strangers is probably the number one way to get viruses or worms.
- Check for suspicious subject lines in e-mails, even from people you know. Some viruses propagate themselves by attaching themselves to and sending e-mails to everyone in the address book of an infected computer. You may know the sender, but if the subject looks suspicious delete the e-mail and ask the sender to resend it.

In the case of virus prevention via e-mail, an ounce of prevention is worth a pound of cure!

See [Removal Tools](#) for ideas on how to get rid of viruses and worms on your system.

5 Removing Malware

5.1 Overview

OK, so you didn't read this document and now you have computer problems. You suspect that someone was playing on the internet and now 3 of your 4 computers run slow and you can't work. What do you do?

Lucky for you, there are a few tools that you can use to help you clean up your system. These tools come in two categories:

>> [Windows Uninstaller](#)

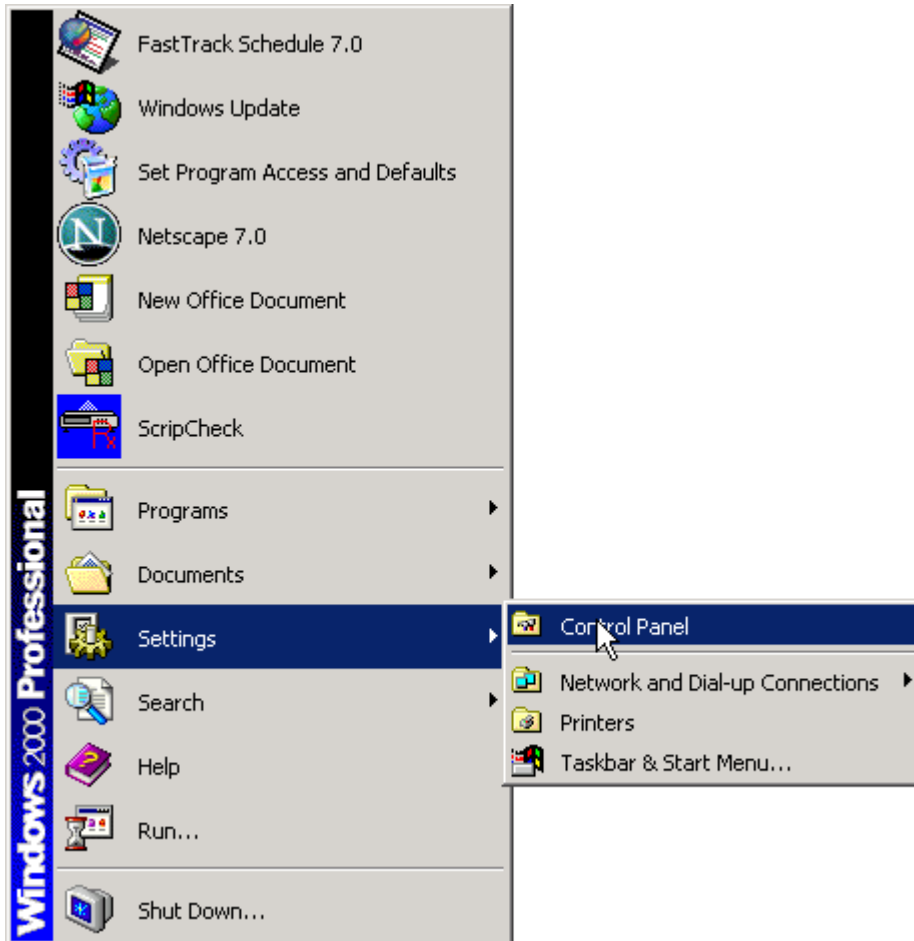
>> [Third-Party Removal Tools](#)

We won't discuss the details of how to use everyone one of the tools, but we will give you a basic idea of what is available and how to get them.

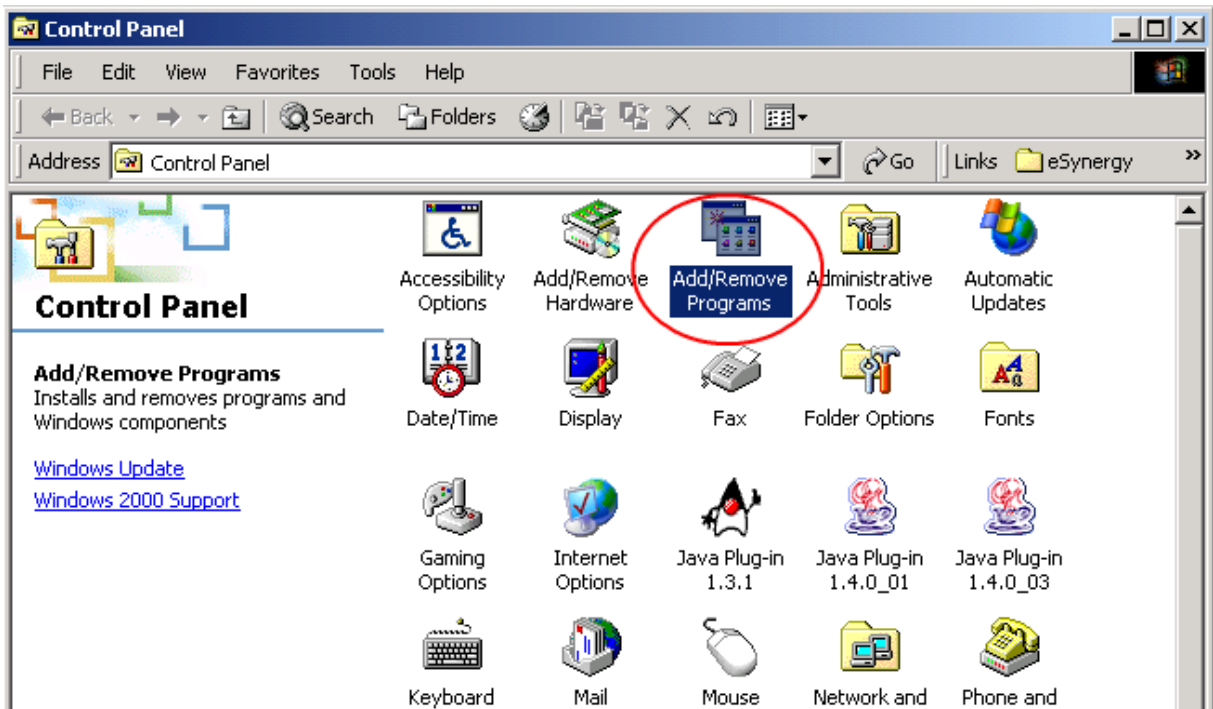
5.2 Uninstall

Windows has a control panel made specifically for removing programs. This is useful for removing malware programs and toolbar's. Here's how to get to this control panel and use it.

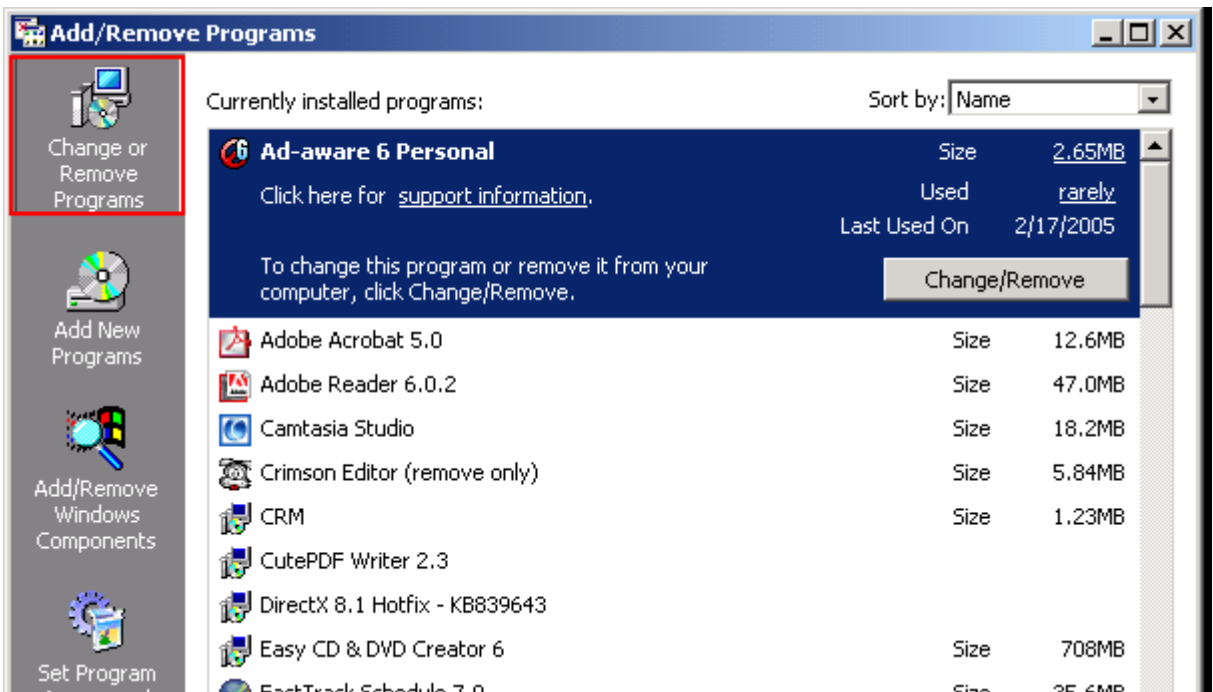
Click on the Start button>Settings>Control Panels



From the Control Panel Window, click on Add/Remove Programs



From the Add/Remove Programs, make sure that the "Change or Remove Programs" is selected. Then scroll through the list of programs and click "Change/Remove" to remove the program from your computer.



5.3 Removal Tools

There are a variety of third-party removal tools for viruses and worms, spyware, and ad ware. Several useful ones are listed here.

► *Warning: Some of these programs have free versions and paid versions. If you are getting the program for your business you need to pay for it if applicable.*

Firewall

A firewall is not actually a removal tool, but we mention it here because it is a great device for keeping out unwanted hackers. There are people and programs that go around the internet looking for unprotected computers. They then install malware that can shut your system down. Firewalls are designed to stop this kind of activity. There are two types of firewalls: hardware firewalls and software firewalls.

- Hardware firewalls are better for networked computers with high-speed internet such as cable or DSL.
- Software firewalls are fine for one computer on a dial-up connection. Several popular ones include Norton Internet Security, McAfee, and Zone Alarm.

Whichever you choose, we suggest you get one.

Anti-Virus Programs

AVG

This is the program we are putting all of our customers on. It seems to be less intrusive than Norton Internet Security. It does require that you have a firewall installed on your network as it does not provide a software firewall. You must pay for this program on each computer it is installed on.

Norton Anti-Virus

This is part of the Norton Internet Security Suite. It is also available as a stand-alone product. We have used this in the past, but it has a couple of anomalies that are kind of irritating. It must be purchased and then renew the subscription (for virus definitions) each year.

McAfee

We don't use this program, but it is another alternative that others use successfully. You must purchase it and then renew the subscription annually.

Spyware Removal Tools

Spybot

Spybot is a program designed to remove spyware. It got a very good rating from PC Mag, and as far as we can tell it is free for both personal and commercial use. You can download it from [here](#).

Ad-aware

Like Spybot, this program is designed to remove spyware and ad ware from your computer. It also got a good rating and seems to work pretty well. There is a personal version for free and a commercial version for businesses. You can download it from [here](#).

Both of the programs we mention here are very good, and relatively easy to use. However, they both catch stuff that the other one missed, so we suggest you use both together. Run them periodically to keep your system clean.

Index

- A -

Adware 2

- B -

BonziBuddy 5

- F -

File Sharing Apps 3

 Kazaa 4

 Morpheus 4

- I -

Introduction 2

- M -

Malware 2

- S -

Spyware 2

- U -

Utilities 4

 GAIN 4

 Gator 4

 Weatherbug 4

- V -

Virus 2

- W -

Worms 2