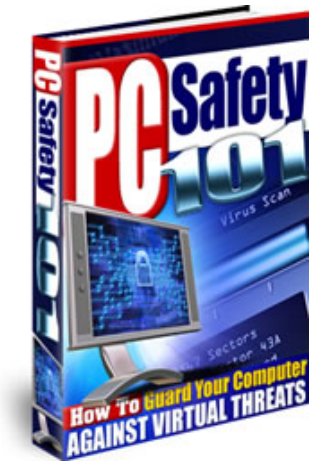

PC Safety 101

Resell Rights License Registration

WARNING: This is NOT a free book and you cannot sell or give it away to others unless you are an *AUTHORIZED DEALER!*

To get **resell rights** and become an **authorized** dealer, please click on the link below:

Click Here To Become An Authorized Reseller

You'll receive the **newest version** of this ebook and be notified of future products with resell rights.

Michael Rasmussen and Jason Tarasi

www.ResellRightsBlowout.com

Why You Need To Worry About "Malware"

As a successful entrepreneur you need to communicate all day, every day, with your customers, suppliers, partners, employees, and others. You need to keep records. You need to have reliable access to email and the internet.

Nasty little software programs are out there which will slow, snarl or even stop your computer and your Internet connection.

Some of them will track your activity, and some will even mine your personal or business information. This malicious software – or "malware" for short – is an every day problem that can, if left unchecked, render your computer worthless, harm your business, and potentially even harm your life.

Have you noticed mysterious slowdowns in your computer's performance, even when you only have one or two programs (apparently) running?

Have you noticed a lag in your web surfing, even though you have a very fast broadband connection?

Almost certainly if you have, it's because spyware or adware is taxing your system, slowing things down for you while sending information you may not want sent, to places you almost certainly don't want it sent to.

The bad news is that this stuff is everywhere now, including coming from sites of reputable companies that you have chosen to do business with. There are probably dozens, maybe even hundreds, of pieces of bad tracking software and viruses lurking on your computer right now.

The better news is that as in real life medicine, an ounce of prevention beats a pound of cure…

And the best news is that you can malware-proof your computer for very little money and without any special computer knowledge!

This report is all about understanding malware, its forms, purposes, and effects; and even more importantly the various ways you can employ to stop it, find it, and destroy it.

The answer to minimizing the presence of and eliminating damage from malware is a combination of settings, software, and surfing choices. While we do

suggest you have a firewall, a firewall is really designed to stop other kinds of problems, like malicious remote access issues (people "breaking into" your system) and like wireless security is really a different category from malware.

In this report we're going to focus on malware specifically.

First let's take a quick look at the three major categories of malware. In the biggest categorical sense, viruses and spyware represent very different basic issues.

Viruses Make Your Machine Act Badly

The purpose of a software virus is to cause damage, either to your machine, or to use your machine in a coordinated attack on other machines or indeed, on the whole Internet.

Viruses can generally be stopped before they hit your machine.

Spyware Transmits Information about You

Spyware is a buzzword that has many different facets and definitions.

Spyware is unlike a virus in that its purpose is rarely mayhem but rather information gathering, which may be for legitimate marketing purposes (as discussed in a few minutes), but more often is for purposes ranging from the irritating and invasive to the downright criminal.

There are many different definitions for "spyware" out there now, but we think a simple functional definition will help you understand the problem it represents best. Some kinds of viruses – such as Trojans, which are bad programs hidden in good ones – may actually meet the definition for spyware also, so it can be a little confusing.

One widely accepted definition is a pretty good one, as used by *Information Week* magazine and numerous spyware websites:

Spyware is software that's installed without your informed consent. Spyware communicates personal, confidential information about you to an attacker. The information might be reports on your Web-surfing habits, or the software might be looking for even more sinister information, such as sniffing out your credit card numbers and reporting those numbers.

That is about as good a summary as there is.

Of course while you read that definition and it sunk in, you probably started thinking "Hey wait a minute, how can that be, people can't just drop little software bombs on my machine!"

Actually they can and they do all the time. A colleague's computer was running slowly, in spite of good hardware, a fast processor and a T1 connection. We asked if she had run anti-spyware software and we got a quizzical look.

We loaded a couple of scanner programs and found more than 1,300 infections!

Most of these are far more irritating than they are dangerous, but they should all be dealt with, and we'll tell you how.

AdWare Can Be – But Often Isn't – "Friendly" Spyware

Adware is the less-malicious cousin of spyware. Often "adware" is designed to simply pay attention to your browsing habits at certain sites or kinds of sites and tell a server someplace what kinds of ads and other information to include on the pages shown to you.

In this sense – the most generous view – it is a form of personalized marketing, and because these things started as ad-serving assistants they are called "adware" even now, when many of them track your behavior, which is one problem, and slow your web connection to a crawl, which for many of us is the real main problem.

If you order from a clothing company a few times a year, you may well not mind if there is a cookie from that company that makes sure you see the sale items you're likely to be most interested in – but if that cookie is slowing down your ability to work, you may well want to get rid of it anyway.

Helping to distinguish between truly friendly cookies and other "spyware" and the bad stuff is something we'll cover shortly.

First let's take a look at viruses, then the more vexing and current problem of spyware and its many guises.

Viruses

You're probably familiar with viruses, as they have been around the longest and most people are familiar with "virus software," more accurately termed virus detection and removal software.

A computer virus is normally an executable program that arrives on your computer hidden within something else, like an email, or an email attachment. The typical computer virus is designed, very simply, to cause you, your computer, and other computers, problems.

You may wonder why anyone would bother to develop software specifically to cause problems, and the motives are as complex as the motives for any bad behavior. Some viruses have been developed by programmers to see what could accomplish, in a mischievous way.

Some have been developed to hurt certain companies or industries by, for example, aggrieved ex employees or nefarious competitors. Some have been developed for political or other purposes – including, debatably, actual terrorism, since "denial of service" and other virus-based online attacks can make communications stop for a while.

We're more concerned with what they do and how to stop them than why people bother to invent and disseminate them in the first place.

What Viruses Do

What viruses do varies but it is always bad, if sometimes amusing.

Some will try to destroy your computer (on the software level, although some will actually "physically" harm your hard drive disks). Some will simply replicate themselves, for example, sending copies of themselves to everyone in

your Microsoft Outlook contact lists, then to everyone in theirs, and so on (these are called worms). Some will be programmed to create huge amounts of traffic onto certain websites – such as a major corporate site, a major commerce site or a major news outlet site – to cause the site to become unusually slow or to stop working altogether.

Some viruses are supposed to be humorous. They may make little sheep dance across your screen, or make your keyboard make belching sounds when you type.

Some viruses, often called "worms" will actually make your system misbehave in specific ways – such as redirecting your attempts to visit a certain site to another site. One famous worm recently redirected Google searches in a scheme that sent surfers to a German-based site that exactly replicated Google, except served all ads from the people sponsoring the worm!

Some viruses are not funny at all, and can destroy data that cannot be recovered. While spyware and other bad software will often need to be removed rather than prevented, viruses should be prevented, and the good news is, that's pretty easy to do.

The most important, and luckily easiest, step any computer owner or administrator can do is to install, enable, update and continually run a quality security program that checks for viruses.

There are dozens of software brands out there but there are two that even now are head and shoulders above the rest, Norton, and McAfee.

Best Antivirus Bets: Norton and McAfee

Norton is now owned by Symantec, a company that itself helped pioneer virus and other computer security software.

Norton was a former competitor of Symantec's. The Norton Antivirus, which is typically offered in a major version revision each year – Antivirus 2003, Antivirus 2004, Antivirus 2005 and so on – is one of the best investments you can make for the health and safety of your PC. At around $35 per machine or less, this program will scan your whole system, as well as all incoming items like email, Internet file downloads, and removable disks, drives and CDs for viruses.

You can set the "Live Update" feature to automatically update the so-called "virus definitions," and you should. We'll talk more about virus definitions below.

See www.symantec.com for more information on the current versions of Norton branded antivirus and related security software packages.

McAfee is the other 800 pound gorilla in the antivirus software area.

Whereas Norton started with a Macintosh focus and has generally been marketed to the consumer and pro-sumer as well as small business markets, McAfee has had greater cache and success specifically in the business arena, where they have often been the #1 choice. McAfee still offers numerous "managed" virus prevention packages for larger companies as well as standalone software geared to the home office and consumer markets. McAfee is currently owned by Network Associates, the old official Internet registrar and current Internet services firm.

See www.mcafee.com for more information on the current versions of McAfee branded antivirus and related security software packages.

McAfee shopping hint: Try a Google search on "McAfee" and look for a listing that says "official McAfee site." This listing will sometimes have a special discount offer that takes you to a URL that is not obvious from the main McAfee landing/home page!

But My ISP Includes Antivirus, Doesn't It?

Many ISPs – Internet Service Providers, the people you contract with to get your dial up, DSL, cable, or satellite connection – currently offer some level of virus prevention that may be invisible to you, or may be optional but included software.

This is great but it is usually not enough. For example, many of the free or low cost Web based mail systems like Yahoo! and Hotmail offer pretty good virus protection, so your email and its attachments are scanned. That's helpful and will eliminate many threats invisibly, but an email client, web-based virus checker can't do anything to stop viruses from entering your system through web page downloads, which some viruses, particularly so called "Trojan horses" and "worms" will often do.

In most situations you therefore will still want to add your own software like Norton, McAfee or one of the many other commercial packages.

Some ISPs like EarthLink and AOL may in fact offer their own software at no additional charge that will be very similar in functions and features to Norton and McAfee – and may in fact be built using licensed components of one of them. We're not saying spend money you don't need to, we're saying make sure you have a full-function antivirus package on your PC!

No matter which package you might choose, the most important things are:

1. Turn the antivirus software on and leave it on!
2. Turn on the automatic definitions updating feature and leave it on!

It's like putting on your seatbelt. You might not need it all time, but just get in the habit and sooner or later you'll be glad you did.

The importance of updating "definitions"

Like any "cat and mouse" situation, the smarter the antivirus software gets, the smarter the makers of the viruses try to be. Whether for the intellectual challenge of it or for other reasons, new viruses are continually being developed and sent around the Internet literally, every day, and many of these viruses are specifically designed to defeat the major antivirus software packages.

The antivirus software, no matter how good, can only look for what it "knows" to look for and new viruses come out all the time. As new viruses do come out, the software uses "definitions" that allow it to recognize and deal with them.

Typically definitions will get updated a couple of times per week, which should keep your software up to date and keep your computer virus-free.

You should set your antivirus software to do a full system scan on a regular basis, maybe once per week, as well as enabling the various "automatic" scans of items like email.

You may experience a slight speed lag from time to time as the scans run, but this is a small price to pay for keeping your machine safe.

Finally, every once in a while there may be a virus that moves across the Web so fast that the major antivirus programs will all miss it. In almost every situation like this, the companies will develop a specific software tool that you can download for free, that will allow you to remove the "one that got away."

The importance of common sense

When you were young, your mother told you not to talk to strangers. That was good advice then, and it's good advice now in many situations! To minimize your computer's exposure to viruses, be sure to observe the following guidelines:

- Never open email unless you know where it is from
- Never click on executable files in email unless you know exactly what it is, and where it is from
- Never say "yes" to unexpected dialogue box questions when surfing the web
- Never say "yes" to unknown download requests

Between that, and good antivirus software, it should be pretty rare for you to have a virus on your system.

Unfortunately, Spyware and Adware are not as easily avoided.

Spyware/Adware

You may be familiar with spyware, as it has been in the news a lot in the last year or two, and finally the major software companies are responding with updates to their security software designed to defeat this annoying and potentially very damaging stuff.

While spyware is, to most people, a recent phenomenon in 2005, in fact what could be called spyware (see our definition above) effectively started back in 1996, on what at that time was the most popular ISP, America Online. There was a piece of malicious software designed to grab confidential information of subscribers, the so-called AOL Password Trojans.