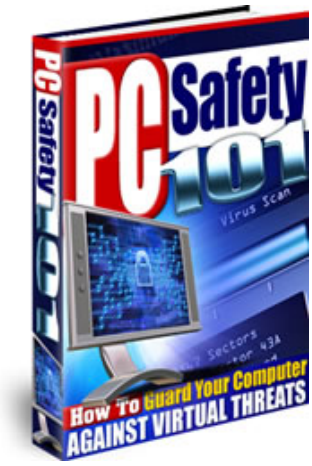


PC Safety 101

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.

Spyware is much more problematic than viruses for several important reasons:

1. The purpose of spyware is to gather information about you – the information may be fairly harmless or confidential, valuable and important
2. Spyware often works silently
3. Spyware is almost never an executable file
4. Spyware is almost entirely undetectable by traditional antivirus software methods, as well as invisible to most firewalls – so it needs to be dealt with on its own, and its presence (at least briefly) on your PC may not entirely avoidable
5. Spyware is everywhere including friendly sites, friendly software and other places, so while there are no good viruses there are some "good" or at least inert pieces of spyware

Spyware hides all over your computer system, and believe it or not, you may actually have agreed indirectly to let it!

You did it by enabling cookies on your Web browser. But disabling cookies may make certain sites not function at all and certain functions within sites unavailable such as most any login, so disabling cookies is usually not the best way to avoid spyware problems. Besides, cookies are often friendly and the spyware ones are easy to separate out with scanning software.

You also did it by downloading items like pictures, video clips and music from websites. But never downloading again isn't too practical, right?

Most common places for spyware and its various subtypes to "hide" on your machine are:

- Temporary files, especially Temporary Internet Files/Browser Cache
- Cookies (these may be friendly items also)
- Favorites listings
- Registries (these are usually the most seriously bad items)
- In some cases as image files or within image files

A typical small business PC may have upwards of 100,000 files on it, so there are plenty of places for tiny non-executable files to hide.

Spyware comes from many, many places, but the most common kinds of sites are those that are for shopping or offer downloadable information, including:

- Shopping sites and portals
- Bulletin boards and information exchange sites
- Gaming sites
- Download sites
- "Lifestyle" sites such as those aimed at teenagers or brides to be
- Sites that rely on serving customer content
- Adult entertainment sites and portals

It may not be practical to avoid all of these, but a large percentage of spyware does come from these kinds of places.

What "Friendly" Spyware/Adware Does

Regardless of where it comes from, Spyware sends information about you somewhere.

There is literally no "good" spyware if we use the definition above, but there are pieces of software that are not bad for you or your system that act somewhat like spyware – in the sense of tracking information about you – but in almost all cases you did opt in to allowing these items on your machine and they do only something legitimate.

Basically "good" spyware would be cookies and key-loggers for sites and software you have agreed to use as part of your "contract" with either, or which you are choosing to use to enable faster or more pleasant web-surfing.

Example of this would include:

- Cookies for friendly sites
- Active-X controls for friendly sites
- Java scripts for friendly sites
- Key loggers for friendly software.
- Key loggers for friendly software.
    - A "key logger" does what it sounds like, which is records things you do with your keyboard and mouse. For example, if you accept a trial on software that is good for 30 loads, the way the company keeps track of

those loads is through a key logger. You almost certainly agreed to this in the terms, conditions or registration of the software – and a large part of the time these things are invisible and won't harm your machine or transmit confidential information like passwords.

Adware may also include friendly cookies that help identify you, help you log in to websites with which you transact business like "legitimate" sites – for example, major search engines.

The reasons why people want to drive traffic are complex (as a web marketer you may be familiar with some of them) but the most important thing is you don't want your machine to be a pawn in someone else's web marketing game without your permission.

The vast majority of spyware is not friendly, and the scanning programs are very good at telling the difference.

You may not be able to entirely stop spyware from entering your system, but you can minimize it through a combination of behaviors and browser settings, then find and remove it with an easy-to-use variety of software tools.

How does spyware get on your machine?

Spyware enters your system through several major routes. These include:

- "Holes" in either your operating system or browser software.
  - The solution to most of these is "security fixes" or security patches, covered below.

- Online account registrations.
  - These can be friendly. For example, if you register at Amazon.com, Amazon uses a cookie to "remember" who you are, let you sign in faster, shop more easily and get served offers and items likely to be of interest.

- Downloading images, sound or video clips.
  - When you agree to download something from a website, the downloading process can bring with it software pieces you didn't exactly agree to download! While viruses will usually be caught by virus software, spyware will almost never be caught by them because the software is differently written.

- "Active" pages on web sites including Java and Active-X

- Some security experts advise against enabling these technologies as a result. For large corporations that may make sense, but the typical small business can find better ways to manage these risks while still enjoying full web functionality. See below for how.

What "Bad" (Virtually All!) Spyware Does

Regardless of where it comes from, Spyware sends information about you somewhere.

Some will try to "hijack" or take over your Web browser to "force" you to go to web sites you don't want to visit, like the viruses known as worms. Sometimes these sites will look like "legitimate" sites – for example, major search engines. The reasons why people want to drive traffic are complex (as a web marketer you may be familiar with some of them) but the most important thing is you don't want your machine to be a pawn in someone else's web marketing game without your permission.

You may not be able to entirely stop spyware from entering your system, but you can minimize it through a combination of behaviors and browser settings, then find and remove it with an easy-to-use variety of software tools.

Because spyware is continually downloaded onto your machine, it needs to continually be found and removed.

And the "definitions" update is even more important here than with virus programs, and, importantly, is often not automatic – so you will need to update the definitions yourself every few days.

While all the major security software companies are introducing spyware stopping products, and the latest releases of the major web browsers have some anti-spyware functionality, as of late 2005 the two best pieces of anti-spyware software remain FREE for personal use, and are quite inexpensive for business use.

Best Anti-Spyware Bets: Ad-Aware and SpyWare Doctor

Ad-Aware is published by the Swedish company Lavasoft. Continually updated since 1999, Ad-Aware is one of the simplest, user-friendly pieces of software for

finding and deleting spyware, especially, tracking cookies and registry entries. Available direct from the publisher at www.adaware.com and also from CNET's fantastic free site www.download.com Ad-Aware SE is highly recommended for all computer users. It is regularly updated, stable, and for non-business use, completely free.

Ad-Aware will remind you to check for updates, offers one-click scanning, and is incredibly simple to use. Definitions are updated about weekly.

The main drawback (at least of the free versions) of Ad-Aware is that it offers no "automatic" scanning options, and it also tends to miss malware that is not of the tracking cookie or registry entry variety.

Also, Ad-Aware is so popular that some spyware designers have found ways to create pieces of software that specifically won't be found by Ad-Aware, so you need a second piece of software, and at the moment our tests suggest that software should be SpyWare Doctor, which is also available for individual users for free.

SpyWare Doctor is published by PC Tools, which also has good freeware/shareware and also commercial products in the area of registry management and other security and performance enhancement items.

SpyWare Doctor is available in a "free" version which is in fact an unregistered version that has some limits when compared with the registered version, including not being able to run in the background continually, not automatically live updating and so forth. Some trial or free versions of SpyWare Doctor also have limits on the number of scans you can run, or the number of items the scan will allow you to process. If you get a "free" version that allows updates and no limits on the scans, you may find that adequate for your needs. If you get a limited "free" version you may find upgrading to the registered version is a good idea.

SpyWare Doctor offers ease of use, very thorough scanning, and a nice feature lacking in many other spyware detection and removal programs – very specific explanation of what the particular item does, where it probably came from, and how serious a threat it poses.

If you're the type of person who likes that level of detail, SpyWare Doctor is particularly enjoyable to use. Visit www.pctools.com to learn more and try the software.

There are many other options, and they are changing all the time. Among the better ones (which can all be used alongside Ad-Aware and SpyWare Doctor) are Spybot Search and Destroy from PepiMIK, SpySubtract from Intermute, and SpyWare Blaster by JavaCool.

Chances are Norton and all the others will be offering spyware related software products or upgrades in the very near future, and www.download.com continues to feature the best in freeware, shareware, and trial versions along with a fairly reliable review system.

There is also a great site that is fully dedicated to only anti-spyware programs, and usually has downloads of all the free ones and the time-or-function limited full commercial versions as well – www.spychecker.com.

And by the way: Any time you see a pop-up window offering "anti" spyware products, don't believe it! Most of those are in fact scams that will download software that is actually spyware masquerading as anti-spyware!

The importance of updating "definitions"

Updating definitions continually is even more important with spyware products than virus products; since spyware is updated almost daily you need to update definitions almost daily, and unlike a virus scan that can be run say once per week, running a "quick" scan for spyware – which will focus on the commonest places for spyware to hide – should be done daily.

You can then run a "full scan," perhaps once a week.

You also want to update your Windows software regularly to get security patches. Whether to turn on automatic updates or not is a complex question, since some early release updates cause more problems than they solve until the bugs are worked out.

We believe in running Windows update manually every month or so, which is likely to bring you all the major security improvements without the problems of beta or version 1.0 releases, on average.

To update Windows, within Internet Explorer select the Tools menu. Then Tools > Windows Update and the rest of the process will be easy to follow.

If you do want to turn on automatic updates, you can do that via the update process the first time you visit the Windows update site, or, you can enable it via the Control Panel on your PC.

There are a few things you can do with your browser as well.

Security at the Browser Level

We mentioned that you can set some parameters within Internet Explorer to minimize the downloading of certain kinds of spyware, but that this will limit functionality of your web surfing and may even make some of your favorite sites unavailable.

There are also some general preferences and routines you should consider.

Disabling Bad Scripts – But Enabling Good Ones

There is a two-setting solution that will probably provide you with some enhanced security while still enabling the kind of surfing and browsing you are used to doing.

What you want to do is disable IE's ability to run scripts without your permission, first.

1. In Internet Explorer click the Tools menu > Internet Options > Security
2. Select A Web Content Zone and Custom Level.
3. Disable four items:
    a. Download unsigned Active-X controls
    b. Initialize and script Active-X controls not marked safe
    c. Active scripting
    d. Scripting Java applets

Then set your Java permissions option to "High Safety." Now you have better security – but half your favorite sites won't work. There's an easy if slightly time-consuming solution to that.

Next do this:

4. In Internet Explorer click the Tools menu > Internet Options > Security > Trusted Sites > Sites
5. Enter (by typing them in one at a time!) all of the site URLs of the sites you know and like that require scripting.
6. Disable "require server verification" for these sites
7. "OK" your way back to the browser window

As you encounter more sites you like that require scripting to function properly, you'll simply need to go back and use steps 4-6 again.

Just Say No!

In addition, you can make simple preferences adjustments within your browser that will minimize the appearance of malicious software on your machine:

- Disable pop-ups (or enable pop-up blocking)
- Do not click in pop-ups if you don't disable them entirely
- Do not download "free" "toolbars" or other "plug ins" for your browser, since most of the time these software items will not do things you want them to do
- Do not answer strange or unexpected questions in dialogue boxes, whether they pop up in pop-ups or appear on normal web pages. Close the page, browser or window, and if you can't, JUST SAY NO! Literally. Almost always the "yes" option is opting into something very bad.

Glossary of Terms

Like any area of technology that is rapidly changing, malware is constantly introducing new words and concepts into the language we use to talk about computer issues. This can be educational at best and incredibly confusing at worst.

To make it easier to understand what's being discussed if you come across news items, stories or instructions in the press or on the Internet, we offer the following basic glossary of terms:

Adware

Adware is the general term for any "spybot" software that exists to track your shopping, browsing and spending habits by sending this information to a remote server. Technically speaking, adware often is bundled with software you intentionally downloaded (which acts as a peer-to-peer file swap, a sort of secret version of what Napster did with music files), and sometimes as we said earlier you agree to host the software in the fine print of your EULA with some software products. Increasingly adware is simply placed on your PC when you download any content from many websites, or even if you just visit those sites.

While most adware is not truly "malicious," the combination of its hidden nature and more importantly the fact that adware will frequently cause erratic (slow) or annoying (pop-up) behavior means most of it should usually be removed unless you deliberately accepted it, for example, in order to be able to use a piece of free software.

BHO or Browser Helper Object

This is a small piece of software that loads itself every time you start your web browser. They can range from fairly harmless – tracking the ads you are served, for example – to annoying and destructive.

Most BHO objects will be found and removed by any of the anti-spyware programs commonly in use.

Cache or Browser Cache

Also known as Temporary Internet Files, the original idea here was to make web browsing faster by storing certain elements of image-heavy sites locally, so they load more quickly than they would from the web. The problem is that in combination with spyware and adware, the nature of the files and the sites they came from can be transmitted as part of your surfing profile, which you may not want for any number of reasons.

There are many utilities that routinely clear the cache, but this is easily done by hand in Internet Explorer. Click on Tools > Internet Options > and in the middle

of the dialog window on the General tab, click Delete Files and check the box for "delete all offline content." This clears your cache.

Cookies

Cookies are usually tiny text files that contain information about you, that a web site you visited deposits on your hard disk to "recognize" you the next time. Many cookies are harmless but some are not.

Anti-spyware programs will usually find all bad cookies, tracking cookies, and unnecessary cookie fragments, and delete them.

Dialers

If you use a dial-up Internet connection you will want to make sure to protect yourself against dialers, almost all of which are malware and of a type that can cost you money.

The basic functioning of a dialer is to disconnect your modem from your ISP and connect you to another one, usually at ridiculous rates (like a 900 number).

Very occasionally a dialer will be a legitimate business tool that you will agree to use, for example, certain content (usually adult content) will require you to accept a connection to the content provider's own ISP, which makes the "free" content well more expensive than free, but this may be something certain users are willing to do in some situations.

Good anti-spyware programs will find and remove dialers. If you are not using a modem to connect to the Internet, the dialers can do you no harm in any case.

EULA

EULA is an abbreviation for "end user license agreement," the detailed contract terms between a user of software and the publisher or owner of the software. Increasingly, these contracts contain legalese that hides agreements to have your behavior tracked and so forth, which is how you may inadvertently agree to certain malware being present on your system.

In this case removal of the malware will usually disable the software it came with, and the software may or may not tell you that that is what happened.

The important thing is to CAREFULLY READ all EULA text from all but the most well-known vendors before clicking that you accept.

(A lawyer would suggest reading the stuff from Microsoft and Adobe and so forth also, but our attitude is productivity in real life requires their products so you may as well agree; also they do not generally abuse their "monopoly" status, at least not in this context).

Identity Theft

Identity theft is a complex subject, but in simplest terms it means taking a person's actual ("real life") identity and using it to commit fraud of various kinds, usually involving money transactions but not always.

Malware

An abbreviation of "malicious software," software designed to harm your computer, you, or to hamper the normal functioning of your system. We define "harm" to include all tracking of your personal information without your explicit consent.

All viruses and most spyware can be included in this category. While some adware would be less than malicious in intent it is fairly irritating in practice, so we consider all of it to be in the general category.

A cookie you willingly accept from say, Amazon.com, would not be malware as it has neither malicious intent nor malicious results.

Personally Identifiable Information (or PII)

This is information that can used to contact you specifically, or that can be associated with you specifically in terms of behavior. Your name, phone numbers, physical addresses, email addresses, etc are PII. PII is necessary for any kind of identify theft, but it is also necessary to offer you personalized service in some software and web situations.

Other information that may be of interest to marketers would be considered non-PII, such as you demographic profile unassociated with any data about you personally.

Privacy policies or agreements (which are included in EULAs frequently) will discuss whether a particular software package or website uses PII or does not.

Registry

The registry is a database on your PC that keeps track of everything about your computing environment like hardware, software, user profiles, settings and so on.

Many spyware programs infiltrate the registry either to gather information or to modify it, which can cause mayhem with your computer or possibly cause it to stop functioning until resolved.

Spyware

Spyware is software that records information about you without your consent, which can include passwords, keystrokes, browsing habits, and much more. Some is merely annoying and some is very dangerous.

Spyware goes by many names: snoopware, PC surveillance, key logger, system recorders, Parental control software, PC recorder, Detective software and Internet monitoring software.

Trojan or Trojan Horse

Named for the original Trojan horse – the "gift" that inside it contained an invading army – Trojans are pieces of good-seeming software that have a nasty surprise inside that may be a virus, a worm, spyware, or even a program that connects to a remote machine and allows access to your whole system.

Antivirus programs will generally stop Trojans before they are loaded, and can usually remove them once they are.

Worm

Generally speaking, a program that makes copies of itself.

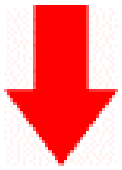
We are confident that your next ghostwriting project will go incredibly well – and that with the right ghostwriter in your business "bag of tricks" you'll reach your business goals faster, better, and certainly more articulately!

There are a lot of secrets to using ghostwriters. I hope this report has given you some valuable information that will help make you more money on the Internet.

Thank you for taking the time to read this ebook. We'd really like to hear what you think about it. Feel free to email us with your thoughts. We'd really love to hear from you.

Your Friends,
Michael Rasmussen and Jason Tarasi

Continue Below For Your $197 Value Bonus



Get Your FREE "Surprise" Bonus

Download the Private Label Reprint Rights To 20 Brand New Internet Marketing Reports

You can use these premium reports to...

- create your own viral ebooks
- create your own killer newsletters
- create an auto-responder series
- drive traffic to your website
- sell them for profit or give them away
- and much, much more!...

This is BONUS if available for a *Limited Time Only!*

To get **FREE Instant Access** please click on the link below:

Click Here To Download Your FREE Bonus

Michael Rasmussen and Jason Tarasi

www.ResellRightsBlowout.com