



## How To Keep Your Computer Free From Pests And Predators

Monday, April 30th, 2007

People talk plenty about [antivirus](#), spam removal, antispyware, root kit removers, and all of the neat ways you can blast pesky parasites from your machine, stop them from slowing down the works and invading your privacy. But what about prevention?

Do Americans view technology in the same way as we do medical industry — where we can't be bothered with maintenance or upkeep? Do we turn a blind eye to the potential issues, waiting until all hell breaks loose before we call in an expert to undo the damage caused by our own neglect?

If so... why do we do this? Isn't it better to take a proactive stance instead of wasting our hard-earned dollars on quick-fix band-aid solutions?

Like many home computer owners, I was once blissfully unaware of the disasters that can befall you when there is no "computer upkeep and maintenance" program in place. But then I became self-employed and I realized then that there is no bigger threat to my future success than NOT doing anything to prevent computer break-ins.

If you're a consultant, you "owe it to your clients" to ensure that the equipment where their confidential information and important documents are stored stays free from prying eyes, identity thieves and people with nothing better to do than inflict harm. So now the questions you may be asking (assuming you know as little about computers as I did when I first "took my business online"):

- What can I do to keep my information safe?
- How can I make sure my computer is operating at peak performance?

### **First things first: How would you be able to tell there's been an invasion?**

1. Everything slows down — hard drive makes unearthly groaning sounds.
2. Your "temp folder" has mysteriously migrated to someplace new.
3. Suspicious looking folders you never saw before, right in the Documents and Settings folder — labeled with long arbitrary strings of letters.
4. [Browser](#) hijack — your homepage turns to something new.
5. Creepy spam that "always seems to know what you've been Googling."

Let me just say it without any fanfare: If you either suspect or know that your computer is infected with a virus, trojan horse or rootkit, there's an easy way to wipe it totally clean:

## **Reinstall the operating system disk.**

What's the [operating system](#) disk? It's that CD you received with your computer, the one with your Windows Vista, XP, 98 or whatever system your PC runs on (OS 9 or X if you're a Mac user).

Reinstalling sounds simple enough — like a fool could do it, right? Ah, but the problem comes when you realize that in doing a reinstall, you lose all your precious data, including:

### **1. Every program that you ever installed to “enhance” your user experience.**

Examples include the Microsoft Office suite of programs if you use that, your antivirus utility if you installed that from a link online, your PDF creation program, any [design applications](#) you use such as Adobe Dreamweaver, Fireworks and so forth).

### **2. All your documents.**

This could potentially mean client work, invoices, records, project drafts, your own marketing... everything will be gone, wiped out. Oh, and let's not forget music files and images, whether personal, or for marketing purposes. All gone, in one fell swoop!

Is there a way around this? But of course. **Backup and removable storage.** If you're unfamiliar with the terms, it may sound like a complicated process but it really isn't.

For less than \$200 you can purchase removable storage that's so simple to use it's almost ridiculous. Here's a great one: Maxtor OneTouch. Just plug in the device, pop in your installation disk, follow the prompts, restart when/if asked, and you're good to go. Then, select all the files you want to store and “move them” to their new location on the Maxtor portable hard drive — in one easy click.

Later, after you've done the clean sweep of your operating system, just plug in the storage device again, reinstall the CD it came with, and presto — there are all your files, safe and snug in their protective area on the Maxtor removable hard drive.

The other thing you have to do after a system reinstall is to retrieve all the old applications from whence you got them — either on a CD that you've hopefully stored in a safe place, or by going back to the emails you received when you purchased them online, clicking the links and re-downloading. This includes the software that you installed with your printer, scanner, digital camera, microphone if you have one of those, and all other “accessories.”

And, after that, you're still not done. You may have to retrieve old logins. For example, if you design Web sites, and you've reinstalled the Adobe Macromedia suite, your clients' FTP logins are no longer stored in Dreamweaver. You have to find them and re-enter each Web site's information one by one.

Your email will also be temporarily inaccessible. If you use Microsoft Outlook, you'll need to set up all of your accounts all over again, which may take a while if you've forgotten your logins and passwords.

Now, it would seem that this reinstall business is a huge headache. And if 6 to 8 hours of work (10 or more if you're a disorganized wreck) just to get your computer spic and span sounds preposterous, then maybe what you want to do is call in an expert. But all of this messiness

“could” have been avoided, or at least the aftermath of a reinstall can be greatly reduced. Here’s how:

- Store all your program disks together, in a safe place where they won’t be damaged. This includes the system operating disk that you received when you purchased your computer, plus every other program and accessory that came with an installation CD. If programs become corrupt, these disks are needed to reinstall them to their original, disease-free state.
- Require a Master Password before logging onto your operating system each time you boot up.
- Get a notebook where you can keep a running list of all your logins and passwords. Store it in a safe place and update regularly.
- Don’t let your browser or [email program](#) “save my passwords” — if a hacker ever gets in, he’s sitting pretty. Enter them in each time you log in. This will help you store them in your memory, too.
- Keep client files and business records organized in an alphabetized hierarchy of folders in the My Documents folder of your C drive. Develop a consistent system for file and folder storage that you use all the time.
- When you receive a new document by email, immediately do a SAVE-AS and name/save the draft to the appropriate client folder, even if you don’t plan to work on it “right now.”
- Use that handy storage device you bought to back up client and other business files on a regular basis.
- Start > Settings > Control Panel > User Accounts: Shut the Guest Account off.
- Make sure remote access to your computer is unchecked.
- Don’t save anything in the “bookmarks” area of your browser — especially if it’s “sensitive information,” like your PayPal login page.
- Don’t pay your bills or do your banking online.
- Configure your browser to dump temp files (cookies) each time you exit.
- Keep your [firewall](#) on and your antivirus running. There are less “invasive” antivirus programs than Norton and McAfee. Try Avira or AVG from Grisoft for small businesses.
- Do an adware scan (AdAware from Lavasoft is a good program), disk defrag and disk cleanup at least once a month. But more frequently is better! You can find the defrag and disk cleanup programs under Start > Programs > Accessories > System Tools.
- Don’t use the Windows Firewall — there are better ones on the market. Try ZoneAlarm from Zone Labs.
- Dump all “stupid” programs you never use but that came with your system — like those crappy card makers and Microsoft Money. You can do this by clicking SETTINGS - CONTROL PANEL- ADD OR REMOVE PROGRAMS.
- Run Windows Updates on a regular basis. You’ll probably want to do this at the same time when you’re doing your defrag and disk cleanup.
- Keep lots of paper and printer ink on hand so you can print out instructions and tips when you find them on the Internet.
- Buy a file cabinet and hanging file folders with labels so you can organize and store your information — especially those instructions on how to monkey around with your computer!

On a final note — everything you need to know about computer maintenance, protection, troubleshooting, program help, etc. can be found via Google or even the “lesser” search engines. For example, if you need to know the exact steps one must take to reinstall your Windows XP operating system on an HP machine, just type those key phrases into Google. Fire up the printer and out spits a critical piece of documentation that you will be able to just whip out in a hurry when “bad stuff” seems to be happening to your equipment.

It takes time and patience to manage your own system with minimal help from a computer specialist. But I find that these "so called" specialists don't always come back with the results you were hoping for. To minimize your risk and keep your money where it belongs — in your pocket — brush up on your tech skills and become empowered about your business.

*Copyright 2007 Dina Giolitto, Wordfeeder.com Copywriting and Marketing. All rights reserved.*

*Dina Giolitto delivers copywriting direction, support and implementation to businesses throughout the United States. Sign up for the [Copywriting and Marketing Ezine](#) from [Wordfeeder.com](#) today.*

-----

**Need technology marketing and copywriting support? Email [Dina@Wordfeeder.com](mailto:Dina@Wordfeeder.com).**