

It's not a Virus – it's Malware!

By Kim Brand
Computer Experts, Inc.
January 10, 2010



Most companies have become completely dependent on personal computers and the Internet. My office frequently gets panic phone calls from small businesses who have had one or both break. The exception may be a hair cutting franchise we serve. Reacting to a PC problem at one of his stores, the CEO reminded the disconsolate manager that they could 'still cut hair!'

But most 'knowledge workers' are simply stuck when their PC is busted. A marketing executive at a large non-profit called to ask why the Anti-Virus software we installed was asking her to pay more to remove an infection it found – hadn't we already charged them for it?? Her PC had actually become infected with the rogue SecurityTool fraudware. It dominated her desktop with a fake (but authentic appearing) urgent report of problems it found and solutions that were only a click – and \$50 credit card purchase – away.

A 'rogue' is so named because it pretends to be your friend by identifying and offering to remove a virus. But SecurityTool is actually a malicious scheme to sell you worthless software, steal your identity and waste your money. She picked it up by clicking on an innocent looking search result.

Protecting your computer from a mere virus is so nineties. Today, you need protection from multiple forms of malicious software; this new family of threats is called 'malware.' In addition to rogues, these include: adware, trojans, worms, bots and backdoors. It doesn't seem like that long ago all when all we worried about were pop-ups and SPAM. Now we have to deal with phishing, hijacked websites and illegitimate BHOs (browser helper objects.)

A typical BHO is MyWebSearch; I've seen some users' browsers littered with four or five of these speed-search tool bars. They get installed in your browser then redirect your searches to sites they want you to see. They track your web usage and slow down your system.

Many of my customers ask: 'Why do people do this?' There is the risk of identity theft and the potential that the contents of your PC may be compromised for gain – but this is minor league. Today, organized crime wants to sell the services of PC 'zombies' to attack a corporate or government website and extort its owner for millions of dollars. These 'bot-nets' are enabled by cheap/fast/ubiquitous broadband and users who don't maintain their PCs. As mentioned above, simply running an anti-virus program is no longer enough.

Here is our advice to Windows users to keep their PCs healthy and fast:

1. Keep your operating system updated. Microsoft spends millions of dollars fixing their OS for a reason – take advantage of this free service.
2. Keep your Anti-Virus program updated – which means you need to pay their subscription fee annually. AVG makes a free antivirus program for home users you can download from Free.AVG.com.
3. Run MalwareBytes' AntiMalware – you can download it for free. It's worth paying for: \$24.95.
4. Microsoft's latest anti-malware program: "Microsoft Security Essentials" is also free. Download it from Microsoft.com.
5. Don't use Internet Explorer – download the alternative (and free) Firefox browser from Firefox.com.

An ounce of prevention is worth a pound of cure. If you have already been infected with malware you probably lack the skill to remove it. Repairs can take from minutes to hours and cost hundreds of dollars. Few of our customers can afford to be down for very long, so getting an infected PC working again is usually a mini-crisis. This is happening more and more.

PCs and high speed Internet may be a better bargain than ever but remember to budget for training, protection, backup and repairs. That new PC will help make you more productive only as long as you aren't banging your head on the keyboard!



Kim Brand is an IT consultant, President of Computer Experts, Inc., and inventor of the FileSafe server – a technology product/service he rents to small businesses who would rather not invest the capital or time required to manage their own IT infrastructure. You can reach Kim at 317-833-3000 or Kim@ComputerExpertsIndy.com.