

The Anti-Virus Conundrum

Why virus infections get past anti-virus software.

By Bill Hely

One of the most common reactions I get from clients when I tell them a virus is the cause of their "problem" goes like this: *"But I'm using an anti-virus. I've always had one! The man in the computer shop put it on for me"*.

"The Man In The Computer Shop", by dint of the fact he is "in computers" and speaks all that jargon stuff, is perceived as an *"Expert Who Can Be Trusted"*. I mean, do you argue with your plumber about pipe diameters and flow rates? Do you quiz your electrician about safe electrical loads? No. He is the expert and you expect him to know.

Please Heed This Warning:

Do not carry any of the trust you may place in a qualified tradesperson over to the computer industry. Look on the computer business as being more akin to the motor trades. You don't expect the car salesman to be an expert in tune-ups, or the mechanic to repair a tear in your upholstery. Each to his own.

Many computer retail sales people are quite competent when it comes to configuring a PC, but there is no necessity for them to be anything more than good salespeople.

Unless you work in a company that has ready access to a competent IT support professional, there is much you will have to do yourself to get your computer safe. There is also much you will have to become aware of for it to stay that way.

My favorite saying with respect to anti-virus protection is this:

"An anti-virus program is only as good as the day it was made".

Usual response: *"Huh?"*

OK, I'll explain.

A virus is just a computer program and, reduced to basics, a computer program is just a special type of document containing alpha-numeric characters which, taken collectively, is called "code".

The publishers of anti-virus software carefully analyze the code of a known virus program and determine a "fingerprint" or "signature" that can be said to be characteristic of that particular virus. That information is added to a database of signatures of other viruses that have also been analyzed and categorized by competent technologists.

An anti-virus program compares data on your computer's hard drive (and in memory) with the information stored in its database of virus signatures. If a match is found, the likelihood of a virus is high and an alert is issued, or some other pre-programmed action takes place.

There is also a more complex detection method called *heuristics* which, rather than looking for specifically defined characteristics (i.e. the fingerprint or signature mentioned above), looks for "virus-like behavior". If your anti-virus program offers a heuristics option, do make sure it is enabled. Unfortunately some anti-virus programs that offer a heuristics feature don't have that option enabled by default.

The Anti-Virus Conundrum

Now if I remind you that new viruses are being released onto the Internet every day of the week, can you see how your anti-virus program will soon become useless against an ever-growing number of viruses for which it will have no characteristics?

So a variation of my favorite saying might become:

An anti-virus program is only as good as the last time it was updated.

If you are to have any chance at all against the virus-type attacks flooding the Internet, you absolutely **MUST** ensure that your anti-virus installation is always using an up-to-date database.

Don't let the mention of "database" deter you—that's the province of the programmer. All you need do is configure your anti-virus program to regularly contact it's developer's website and download the latest updates, and that's very easy to do.

Any anti-virus program worthy of your consideration will have a built-in scheduler to take care of updating. The program should regularly connect to the Internet and retrieve updates. Frankly, it's just too important a task to be left to the frailties of human memory, so always use automation, such as scheduling, when it is available.

As for detection capabilities, most of the major anti-virus packages are pretty much on a par these days. For me it's the little extras that count, like ease of configuration, prompt and helpful support, etc. — and of course cost.

The specific brand of anti-virus software you use is up to you. My personal preference is a company I have been watching, using and recommending for several years now. More information here:

<http://HackersNightmare.com/AVG>

Home computer users can legally use that excellent anti-virus program completely free of charge. The site layout and the links change from time to time, but from the link above look for a reference to "AVG Free". If you can't find it on that page, use the little search box (usually at the top of the page somewhere) to search for the term "AVG Free".

Note that there is also an AVG Trial, but that's a time-limited trial of the commercial software. As a home user on a single stand-alone PC you'll be very happy with AVG Free. Businesses and professionals should select one of the commercial versions — all very inexpensive, very capable and very necessary.

Finally, a word about "security suites".

I know I'm inviting criticism for this stance, but I must say I'm not a fan of security suites for most home or small business installations. A suite is a software package that offers not only anti-virus but includes software components that purport to tackle other nasties such as spyware, adware, etc.

In my experience you do not find the best of each type of protection bundled together.

Because a company may be extremely good at developing an anti-virus product does not mean they can do as good a job with an anti-adware solution. While the corporate buyers tend to turn their noses up at free software, the fact is that some of the very best-of-breed security solutions are just that—free.

The Anti-Virus Conundrum

If the corporates, with their big budgets and in-house IT support, prefer to invest in complex and often costly integrated suites, that's fine. They have the resources to handle anything that happens.

But for my money there's a lot to be said for implementing a series of much smaller, less complex, often free utilities that, matched task for task, can usually out-perform the equivalent component parts of an integrated suite.

I discuss adware and spyware threats more specifically in another article which you should be able to get from the same source as this one.

In the interim, get yourself a good modern anti-virus scanner and, once installed, be sure to get into the configuration options and set a daily update schedule.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity issues. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*[™].

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.