PC Magazine defines antimalware as

"An umbrella term for antivirus programs, spyware blockers, intrusion detection systems (IDS's) and other software that detects and eradicates unwanted input, which in almost all cases comes from the Internet." – PC Magazine

There are two types of antimalware programs – real-time scanners (also called on-access scanners) , and on-demand scanners. Real-time scanners run on your system all the time. This term covers all programs that call themselves "antivirus" programs. This is the type of protection that this blog post addresses.

There are scores of different real-time products available. How do you know which one is right for you? This is a very common question and is difficult to answer. Some of the criteria involved could include:

- ease of installation and use
- does it slow the computer down or get in the way
- what range of threats does it guard against
- how well does it detect threats
- how well does it remove threats
- what (if anything) does it cost

It must be a bit of a conundrum for the antivirus program manufacturers that the better their program, the less the customers notice it. What we want as users is to just get on with using our computers and not worry about the potential problems. I can't imagine anyone getting excited by reading through the list of threats a particular program claims to guard against. It

hurts our brains even trying to understand the nature of the threats that we are told a specific program will guard against. What we actually want is peace of mind and no hassles.

Also, I feel sure that the way you use your computer can affect the amount and type of threat you are exposed to. There is no doubt in my mind (but I have no proof for this) that having young people using a computer seems to increase the chance of catching something. I suspect that this is because young people are far more likely than older people to be using the internet in a way that involves sharing of files amongst themselves. It's no great stretch of the imagination to think that the bad people out there have realised this and target this part of the market accordingly. Maybe it would be an idea for the antivirus manufacturers to market their products towards specific groups of people that represent the different emphases of threats that those people may be exposed to. Anyway, they don't, so you can't find an antivirus program claiming to be "Supreme for Silver Surfers" or "Fantastic Fort Knox protection for 15 year olds".

So how do we make the best decisions as far as antivirus is concerned?

If you want to look into this in huge detail and make a highly informed decision then I recommend www.av-test.org. Each quarter they publish a set of results of testing many products that are available for one specific operating system (Windows XP, Vista, or 7). They then cycle through these operating system each quarter. They score each product according to protection, repair, and usability and display the results in sortable tables (see http://www.av-test.org/certifications.php)

My own experience

My own favorites tend to change a bit over time. For a few years I have been recommending AVG Free. I think that it still does a very good job technically, but their increasingly aggressive marketing often "misleads" users into installing the paid version rather than the free version and they've even used scare tactics once or twice in the last year.

I've been installing Microsoft's own "Security Essentials" on my own and clients' sytems for a while and I have to say that it certainly performs very well in at least one respect in that it is virtually transparent: it just gets on with the job, updating itself quietly in the background and only making its present felt when there's a potential problem. I don't recall a single instance (yet) of anything getting past "Security Essentials".

One product that I've not used in-depth myself but which seems to be highly liked by clients is Kaspersky Internet Security. Unlike AVG Free (natch) or Microsoft Security Essentials, it is a paid-for product but it gets increasingly cost-effective if you buy a licence for several machines.

Nothing's perfect

Whatever product you go for, keeping up with malware threats is just that – keeping up. The bad people are always going to be one step ahead. We just have to hope that our antimalware product is very very quick off the mark in detecting and dealing with new threats The only way to stay completely safe from online threats is to stay away from the internet and that really would be a case of throwing the baby out with the bathwater. So, it stands to reason that it is possible for a threat to get past your protection.

…. and we have to live with that

You may think, then, that it would be a good idea to have another line of protection in the form of a second antimalware program. Good thinking, but don't. You could break your system. If two real-time antimalware scanners go to check the same file at the same time the whole system could freeze.

So what do we do

Keep your antimalware program up to date, ensure that it is automatically updating its data files, and check that it is set to completely scan your system once a week or so. And, by the way, are you taking backups?

And what of Mac Users?

I'll be investigating the current thinking on antivirus protection for Macs in the coming weeks.

Share this:

- Click to share on Twitter (Opens in new window)
- Click to share on Facebook (Opens in new window)