Antivirus software intercepts and counteract threats posed by malicious software (“malware”). Malware tries to damage software installations, steal data, or extort money

Malware threats can be introduced into your computer system in may ways, including when installing or downloading software, when opening data files that have been infected (such as word processing files), or when visiting websites that contain threats (the website owner may or may not know that the site contains threats).

There is a constant “cat and mouse game” or “arms race” going on between the creators of malware and the creators of antivirus software. The upshot of this is that most antivirus manufacturers update the “knowledge” of their products every day so as to keep up with the latest known threats.

What computer systems are at risk? In theory, any computer system that has any kind of link to the “outside world” is at risk. The most common way of creating that link to the outside world these days is by having an active internet connection. Any file opened or downloaded from the internet could, in principle, constitute a risk. Other media for passing malware include floppy discs (remember them?), CDs/DVDs, and USB pen drives (also known as thumb drives and – usually erroneously – memory sticks).

How can you stay completely safe from malware? Don’t connect your computer to the “outside world” (see above). There is no other way to be completely safe. This, however, is not feasible and certainly falls into the category of “throwing the baby out with the bathwater”. It is possible to protect your system from malware to the extent that it’s worth taking the risk of connecting to the internet.

Are Macs and Linux computers vulnerable to malware? In theory, yes. The main reason why almost all malware is experienced on Windows-based systems is that Windows in installed on the overwhelming majority of the world’s computer systems. If you were going to create something nasty, would you spend your time creating something that could attack 90% of the world’s computers or just 5%? It is also possibly true to say that Macs are inherently less vulnerable than Windows computers. In practice, most Mac users don’t seem to use any antivirus software. I don’t know about Linux users. In principle, mobile phones and

tablet computers are also vulnerable but these, too, are not usually protected at the moment.

So, assuming that you have a Windows-based computer, **what are the main features of the antivirus software you may install?**

Free or Paid

Paid software has more bells and whistles than free versions. Personally, I've never been convinced by these. I even see them as a problem rather than a benefit as the more complicated the antivirus software, the more effect it has on system performance and the more likely it is to cause problems in its interactions with other parts of the system. The same, basic, antivirus detection is usually included in both paid and free versions of software.

Apart from the cost itself, there are other potential problems with paid software that include;

- Occasional difficulties in renewing the annual licence – Norton and McAfee come to mind.
- Automatic renewal of the licence – some of these companies will put their hand in your pocket for the renewal fee without warning you. No doubt this was mentioned in the (unread) small print of the "terms and conditions" you originally agreed to, but it doesn't make it any less annoying when it happens. My experience is that companies who do this can be persuaded to give you your money back if you object to this and wish to cancel the renewal.

Scanning Action

There are two different things that can trigger your antivirus to check files. Both of these types of check are usually present and active in antivirus software:

- Real-time scanning – this happens at the very moment you open a file or download it, and is intended to discover and neutralise a threat at the moment that the threat would otherwise have been launched. Your antivirus software might also refer to this as on-access scanning, background scanning, resident protection, or other names that suggest that the protection is there all the time, ready for any threat.

- Scheduled scanning – this happens when all susceptible files are checked all at once according to a predefined schedule (usually once a week, by default).

Why have both types of scanning?

Suppose that a brand new virus appears today and your antivirus software does not know about it. This could mean that the virus will slip past the realtime scanner and be saved onto your computer. In the course of the next day or so, your antivirus software is likely to be updated with information about this new threat. If your system is set to run a scheduled scan then that scheduled scan may reveal the virus that had previously slipped past unnoticed.

To be continued next week...

Share this:

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