Why is my computer infected with viruses when I have an antivirus program installed?

Posted on Jun 05, Posted by Paul Category FAQ

What are viruses?

Viruses are malicious programs written by very talented programmers.

What is the purpose of a virus?

Modern viruses are typically designed to gain unauthorised access to your information. Once the virus has access to your information it forwads it to whoever is controlling the virus. The controller then uses the information for their financial gain.

How do viruses install themselves on a computer?

The operating system on your computer is a colection of programs. These programs work together to give you the familiar user interface you recognise as Windows (or other). Great care is taken ensure these programs are error/bug free but occasionally a bug is discovered in one of these programs that can be exploited by a virus to gain access to your computer and/or information. Microsoft and other software vendors regularly release service packs and updates that fix errors/bugs in their products.

How do antivirus programs work?

Antivirus programs have a database of existing viruses and exploits that they use to determine if a file is malicious or not. In addition to the database, antivirus programs attempt to determine if a file is malicious by examining it for virus like characteristics. If the file is not in the database and doesn't have virus like characteristics then the file is considered to be legitimate and not a virus.

Why didn't my antivirus program detect the virus that infected my computer?

Thousands of new viruses are created every day. There are publicly available programs that non-technical people can use to create viruses. There are also many publicly available tools that can be used to mutate and/or modify existing viruses.

Sooner or later a new virus is created that isn't in the antivirus programs database and doesn't appear to have virus like characteristics even though it is malicious. This new "unknown" virus can then be delivered directly to the computer via email or other conventional methods.

Most infections occur when someone discovers a new exploit/bug in an operating system or application program that allows a virus to infect a computer in a previously unknown way. The antivirus program doesn't know about this new exploit/bug, doesn't test for it, considers the virus to be a legitimate program because its not known to be a virus and allows the "unknown" virus through.

This new virus then infects the computer.

How do antivirus vendors detect/discover new viruses?

There are systems in place on the Internet that detect when a virus sends copies of itself to other computers and/or installs itself on many other computers. These systems identify the file as being malicious and notifies antivirus authors. Antivirus authors update their antivirus programs/database/exploit list so they detect the virus/exploit.

The above process is highly automated and typically only takes a few days but depending on the nature of the exploit can take considerably longer, sometimes months. Each antivirus author has their own method of handling newly detected viruses but on average they all take roughly the same time to react.

How do I make my computer virus proof?

All programs and operating systems have vulnerabilities/exploits/bugs so its not possible to make a computer completely "virus proof" however you can minimise the liklyhood your computer will be infected by using "Best Practices".

What can I do to prevent viruses infecting my computer?

- Install some form of antivirus protection: In general paid antivirus programs are better than free antivirus programs but free antivirus programs are much better than having no antivirus program at all. Modern viruses and malware are much more sophisticated than older versions. Typically once a modern virus gains access to your computer it will be smart enough to disable the existing antivirus or stop it updating so additional viruses will not be detected.
- Keep your antivirus program up-to-date: Manually check it is automatically updating frequently.Install updates and service packs: Supplied by vendors for the operating system and application programs.
- Don't download files or open attachments unless you are sure they are legitimate
- Don't display or otherwise go to websites unless you are sure they are legitimate: If it sounds too good to be true then it is.

Hope this information helps. Please call if you have any questions.

Computer Doctor / Mobile PC
Suite 1, Ground Floor Surfers Plaza Resort,
70 Remembrance Drive,
Surfers Paradise. Qld 4217
Ph: 07 55924733
Fax: 07 55924761
Email: support@computerdoctor.com.au
Web: www.computerdoctor.com.au