Article Side

How viruses and other malware work

by Sean Burke

Article published on April 30th 2012 | Technology

In the 21st century, most computer users â€“ from eight year old children to silver surfers â€“ know how damaging computer viruses can be. Being infected by a computer virus or another piece of malware (â€œmalicious softwareâ€•) can have devastating consequences, from permanently harming your computing device to stealing your personal details. However, many people are unaware of what these viruses actually are, and how they work. Hereâ€™s a quick introduction to computer viruses and how to avoid catching them.

Viruses have been termed such because they share characteristics with biological viruses. In the same way that bodily viruses, like the common cold, can spread when one human interacts with another, computer viruses are also transmitted when there is communication between an infected device and an uninfected one. A biological virus attaches itself to a cell in the body; similarly, a computer virus needs to attach itself to a programme in order to launch.

Viruses and other malware have spread rapidly over the last two decades, since the internet became popular in peopleâ€™s homes. Studies estimate that in 1990, there were 357 unique malware pieces on PCs in the UK. By 1995, this number had jumped to 8069 unique malware pieces; in 2000, 56, 342; in 2005 164,00; and in 2010, 54 million unique malware pieces were said to be on PCs, Macs, smartphones and tablet computers.

Such malware can act in various ways. In fact, many viruses are technically harmless and are written as a prank or an experiment to test new devices. The first iPhone virus, Ikee, targeted unlocked iPhones in Australia and simply placed a picture of 1980s pop star Rick Astley on the infected userâ€™s home screen. The virus didnâ€™t do any permanent damage; however, even these pranks are damaging in the wasted time each user has to spend removing the virus from their computer or mobile device.

Many viruses are much more significant. For instance, you may be sent an email with an attachment from a trusted friend â€“ only to find out that the attachment is a virus, which has been unwittingly sent from your friendâ€™s computer. These viruses may wipe your hard drive, modify your files and send out corrupted attachments to your contacts list, and may be able to extract personal details â€“ such as confidential banking information â€“ from your computer.

Viruses and malware may have flourished over the last 20 years, but internet security and antivirus software have also seen major developments during the same period. Resultantly, itâ€™s become simpler for computer users to protect themselves from these online threats. However, itâ€™s also important to use common sense when using the internet in order to avoid viruses. For example, donâ€™t open a suspicious-looking email attachment, even when itâ€™s sent from a friend; avoid saving passwords or confidential details on your computer or mobile phone; and try not to use the same passwords for all your website memberships.

Sean Burke - About Author:
Sean Burke writes for a digital marketing agency. This article on a internet security has been commissioned by a client of said agency. This article is not designed to promote, but should be considered professional content.

Article Keywords:
Internet security, malware, computer virus, virus, iPhone virus, computer virus statistics, how viruses work