A Dozen Dangerous Myths About Computer Viruses

One of the reasons viruses have become such a threat to modern computer systems is the fact that today's viruses are different in almost every way from what they were a few years ago. But most computer users aren't aware of these changes. Consequently, their idea of adequate protection against viruses, worms, and Trojan horses is likely to be far less than what is necessary.

All of the following statements are beliefs commonly held about viruses, and all are myths. In most cases the statement was true a few years ago, but certainly not in 2005:

1. *They are created by bored, sociopathic teenagers and vandals* – Most viruses today are written for the express purpose of making money; many are produced "on contract" for criminals or unscrupulous operators.
2. *You'll know when your computer is infected by a virus* – Modern viruses generate more cash for their creators every minute they remain on an infected computer; they will go to extreme measures to reduce the likelihood of detection.
3. *If you've backed up your data, you don't need to worry about virus infection* – The end result of a modern virus infection is far more extensive than deleted or corrupted files on your hard drive; confidential or sensitive files may have been compromised, with no obvious symptoms on the infected computer.
4. *It's safe to reuse the same backup media every time you back up your data* – Since the symptoms of a virus infection may not be obvious, the files that were backed up last week, or even last month, could contain the virus as well.
5. *If your computer has anti-virus software installed, you don't need to worry about virus infection* – Today's viruses, worms, and Trojan horses can sometimes elude detection by even the best Anti-Virus software; and if your virus definitions are not up to date, your exposure is greatly magnified.
6. *Viruses are only transmitted through e-mail attachments* – Some viruses are activated as soon as the infected e-mail message is opened, even without an attachment.
7. *The only attachments that can hurt you are .exe files* – There are more than 40 file types, or extensions, that may contain or spread a virus; some of the most common today are .com, .cpl, .eml, .exe, .pif, .reg, .scr, .vbs, and .zip.
8. *It's safe to open attachments from senders you recognize* – Most e-mail messages that contain virus-infected attachments will appear to come from someone familiar to you; the virus "spoofs" the From address, to mislead the recipient into a false sense of security.
9. *Viruses only come through e-mail* – There are many other ways a modern virus can spread, including malicious links on Web sites, through Chat or Instant Messenger sessions, or across a Local Area Network (LAN); some generate random IP addresses and attempt to infect any computer with a corresponding address.
10. *The Preview Pane is a safe, convenient way of previewing your e-mail messages* – The Preview Pane in Microsoft Outlook or Outlook Express is a convenient feature, but it is also a major security weakness that has been exploited by numerous viruses.
11. *Viruses can only spread to e-mail addresses in your address book* – Viruses that do spread via e-mail look for the target addresses in other files on the infected computer; these may be files with an extension of .doc, .eml, .mdb, .xls, or those associated with other common office applications or databases.
12. *Only Windows-based computers are susceptible to viruses* – In a recent week, the National Cyber Alert System identified 90 new or updated vulnerabilities; of these, 12% targeted Windows systems, 50% affected Unix/Linux, and 38% affected multiple Operating Systems.