12 Steps to Virus Protection

Computer viruses, worms, and Trojan horses are becoming more prevalent, more insidious, and more destructive. One of the most serious causes for concern in this area is the frequent changes in virus behavior. What was once "common knowledge" about virus exposure is now seriously out of date.

The following 12 steps reflect the state of the virus writers' art as of today, which is considerably different from virus behavior a few years ago. To minimize your likelihood of virus infection, the traditional, old advice applies, but with many new twists, which are summarized here:

1. Make regular backups of your important data files, and cycle them on a schedule that always lets you restore data to the end of the prior week, month, quarter, and year.
2. Never open an attachment from someone you don't know, regardless of the file type.
3. Never open an attachment from someone you do know, unless you first verify with them that they did actually send you that attachment.
4. If they did send you the attachment, verify that they are the original source of the attachment -- if they just forwarded something they thought was cute, it still could contain a virus, worm, or other malicious code.
5. Run a well-known Antivirus program, update your virus definitions regularly, and have the program automatically scan all incoming and outgoing e-mail and attachments.
6. Perform a Windows Update regularly, applying all Critical Updates to your version of Windows and Internet Explorer. Where possible, upgrade to Microsoft Update.
7. If you see an incoming message that looks suspicious, go to your Antivirus program's Web site and do a search on some of the words that raised your suspicions.
8. If you're using Microsoft Outlook or Outlook Express for your e-mail, turn off the Preview Pane. In Outlook Express you accomplish this by going to the View menu, then selecting Layout... and un-checking the box that says, "Show preview pane."
9. Change the default options in Windows Explorer so that you can see all viruses (and all attachments) by their full name. In Windows Explorer, choose the Tools menu (View menu in Windows 98), then Folder Options. Click on the View tab and change the selection under Hidden Files to Show All Files, then right under that box, un-check the box that says, "Hide file extensions for known file types." Also be sure that the options are selected to display the contents of system folders and not hide protected operating system files, if applicable.
10. If you receive a suspicious e-mail, delete it immediately without opening it. Note that you will be unable to follow this advice unless you've turned off the Preview Pane, as described in step (8) above.
11. Exercise some restraint in forwarding jokes, cartoons, petitions, and other "cute" or sexy messages, and encourage your friends, associates, and correspondents to do the same.
12. If you e-mail anything to a list of recipients, put their addresses in the Bcc: field of the address instead of Cc:. Many of the current viruses are sent not just to the addresses it finds in your Address Book, but also to every e-mail address it finds in any message on your system. This is the primary reason viruses are spreading more rapidly these days.

These are the most important steps to virus protection, short of corporate-level security and firewalls. Any computer with a high-speed, "always-on" connection to the Internet should have at least a software firewall installed and running full-time. You may also want to consider a hardware firewall and extra security settings in your browser for additional protection.