

Tips for Protecting Yourself from Viruses & Worms

Antivirus software is simply not enough. An email worm can spread worldwide in just minutes, but it takes hours for antivirus vendors to analyze, create, and deploy signature updates. Fortunately, there are five easy steps you can take to help close that window of vulnerability and help keep email worms off your system.

Rule 1: Identification - Understanding the nature of the attachment is the first step towards email safety. Any executable type attachment has the potential to be infected. This covers a wide range of extensions. Complicating matters is that, by default, Windows suppresses file extensions. Make sure you have file extension viewing enabled.

Enabling file extension viewing:

In Windows 2000 or XP:

1. Open Windows Explorer
2. Choose **Tools**
3. Select **Folder Options/View** or **Tools/Folder Options/File Types**.
4. Locate the file type(s) desired and choose **Advanced**.
5. Check the box "Always Show Extension."

In Windows 95/98/NT, to enable file extension viewing:

1. Open Windows Explorer
2. Click **View/Options**
3. View and uncheck the box for "Hide file extensions for known file types."

Executable file extensions: The following is a list of file types that should be considered suspicious when received in email and should not be opened unless you requested or expected the attachment:

- BAT - Batch File
- CMD - Windows NT Command Script
- COM - MS-DOS Application
- DLL - Dynamic Link Library
- EXE - Application
- PIF - Shortcut to MS-DOS Program
- SCR - Screen Saver

Rule 2: Intent - An executable type attachment (.EXE) should not be opened unless it was specifically requested or expected.

Since email worms are sent to addresses found on infected users' machines, just knowing the sender is no proof of intent -- they may well be infected. In fact, odds are an email worm will arrive from someone you know and the sender is oblivious to the viral email being sent from their machine. Worse, today's worms spoof the From address, so it may well be that it's not even from the person you think it is. If there's any question as to the intent, see Rule 3 below.

Rule 3: Necessity - This is the simplest rule to follow, but one that many people ignore. If you do not need the attachment, don't open it. Delete the email instead.

Rule 4: Secure your client - To date, many email worms and viruses have taken advantage of security vulnerabilities found in Microsoft Outlook and Outlook Express. However, any mail client that supports HTML and scripting should be considered at risk.

Rule 5: Patch your system - Microsoft routinely releases approximately 100 security patches per year. Keeping abreast of these and understanding which are applicable to your system can be a daunting task. To help ease the pain, Microsoft provides a [Windows update site](#). The site will automatically scan your system and provide a list of recommended updates specific to your operating system. Install any updates marked as "Critical." And remember: security is never passive. It's an ongoing process and new vulnerabilities are constantly discovered. Visit the [Windows update site](#) monthly to ensure all necessary patches are installed.

Adapted from About.com's Executable file extensions web page.