

Email Viruses – What You Can Do to Prevent Them

There has been a lot of publicity about email viruses in recent years. The “I Love You” (or “Love Bug”) virus and the “Melissa” virus made world news for days, and more are being written all the time. There are currently approximately 50,000 known viruses in circulation, and many people don’t know when their computer systems are infected.

Mail viruses do more than just damage the data on your computer. Many viruses self-replicate, causing an exponentially growing deluge of email to clog mail servers globally and creating the potential for massive mail and network slowdowns and outages.

Email service providers like Hotmail, Yahoo, AOL, and even Intermail cannot censor the attachments of each of the millions of emails that can pass through their systems in a day, just as the US Postal Service can’t open and check every piece of mail that they handle. Since viruses are passed between computers without alerting the network, consumers and businesses have the responsibility to protect their computers from infection.

Preventing Email Viruses

Have you taken steps to protect yourself from viruses? You can greatly reduce your risk by doing the following:

- **Be Careful With Attachments**

One of the easiest ways to protect yourself is to NEVER open an attachment that looks suspicious or comes from an unknown source.

Mail viruses often spread by sending themselves to everyone in a victim’s address book, so these viruses arrive with the return address of a trusted source. Your colleagues may have viruses and not know it, so attachments they send you may be infected without their knowledge. Many viral attachments have .exe (executable) or .vbs (visual basic script) file extensions, so it’s wise to be careful about opening such files. However, many different file types, including .doc, can contain viruses.

- **Install a Virus Protection Program**

If your computer is connected to the Internet, you should install a virus-scanning program, which will alert you if you try to open an infected file. There is no better way to protect your valuable data and systems from viruses. [McAfee](#) and [Norton](#) are two of the most popular, but there are many to choose from. Most virus-scanning programs are fairly inexpensive, especially when you consider the protection they offer your business.

- **Set Windows Security Features**

Microsoft Windows has security features that, when set properly, can reduce your risk of infection.

- **Know Your Viruses**

Knowing what viruses are circulating, and recognizing them before you open them, is an important step in protecting yourself. Many viruses carry telltale subject lines or attachments. If you have already been infected with a virus, knowing which one it is also helps you repair any damage, and allows you to help stop the spread.

The following sites provide in-depth, up-to-date information on specific viruses:

<http://www.antivirus.com/vinfo/>
<http://www.europe.f-secure.com/virus-info/>
<http://www3.ca.com/virus/>
<http://vil.nai.com/vil/default.asp>
<http://www.cert.org/>

- **Delete Infected Messages**

If you have a message, file, or attachment that is infected with a virus, delete it. This prevents the virus from being accidentally opened again on your own computer system, and stops it from spreading. While you're at it, you should also protect your system from attack by checking Microsoft often for updates.

Microsoft is constantly creating patches and updates to close security holes found in their products. These updates are available at <http://windowsupdate.microsoft.com>. You may receive an email if we detect a virus being sent from your mail account. The information in this email will help you locate the virus and purge it from your system.