

Virus Prevention -- What You Need to Know

What is a computer virus?

A computer virus is programming code that is hidden inside a file or lurking on an infected web site waiting for an unsuspecting web traveler to come along. Many viruses are designed to automatically spread themselves to other computers once, thus magnifying the problem. In fact, the infection generally occurs behind the scenes, without your notice, that is, until your computer starts behaving strangely or friends begin asking you why you're sending them strange email messages. While most computer viruses are merely just annoying and non-threatening, other viruses exist that can completely trash your hard drive, destroying data and corrupting files, rendering your computer inoperable.

PCs versus Macintoshes

Most computer viruses affect PC users running the Windows operating system. That's not to say that Macintosh users aren't at risk. However, it's a sad truth that the folks who write computer viruses primarily target Windows computers, simply because they outnumber computers running different operating systems (such as Apple and Linux). While most viruses do not affect Macintosh users, they are still able to participate in helping to spread the virus to others. So, no matter what operating system you're using, everyone should be knowledgeable about how to prevent and handle computer viruses.

How can my computer become infected?

In a word -- carelessness. Most viruses mask themselves inside an email attachment and the recipient simply opens the attachment without giving much thought to what s/he is about to do. Boom! You're infected! Remember, viruses usually cannot infect your computer unless *you* do something to help them. In the "olden days" of computing (a few mere years ago) floppy disks were the medium of choice for infection. However, in today's hi-tech world, electronic mail and web pages have become the preferred medium.

Infected email attachments are often times cleverly disguised. Their file names appears legitimate and the accompanying text message arouses your curiosity by asking for your advice, or tempts you with promises of nude photos or funny jokes so that you'll open the attachment. Other times, they have very official or important sounding file names which may even appear to be work-related. Believe it or not, some viruses will examine your computer's hard drive, grab bits and pieces of files you have and send them to other people.

How do viruses spread?

Once your computer has been infected, the virus may spread by copying itself onto every floppy disk inserted in the computer. Or, it might "send itself" to everyone in your email program's personal address book, completely without you knowing it. Some viruses will send messages to your friends every so many days until you remove it from your computer.

Can I get a virus just by reading an email message?

Most often, you cannot get a virus just by reading an email message. The infection is typically hidden in the file attached to the text message and, when you open *that* file, you become infected. There has been a virus or two that can infect your system when you simply read an email message, however, they are few and far between and exploit security holes in your email software program (i.e., Microsoft Outlook). To protect yourself from those rarer types of viruses, keep your email software program up to date and make sure to install security patches, which we'll talk about in the next section.

Simple rules to protect your computer

Okay, so most of the risk is associated with opening up email attachments. But how can you tell if the attachment you've been sent is a good one or a bad one? In many cases, you just can't tell, but here are some helpful rules to follow:

- Purchase and install anti-virus software on your computer (i.e., McAfee and Norton). Anti-virus software is always monitoring your computer for signs of possible virus attacks. Most software offers a wide variety of options, such as automatically scanning email attachments or scanning floppy disks when they are inserted in the disk drive. But more is needed than just the initial purchase and installation of this software. You must keep it current! At the time of purchase and installation, the software is programmed to recognize hundreds of up-to-the-minute viruses. However, new viruses keep cropping up weekly. If you never update your software, while you'll have protection from older viruses, you'll not be protected against newer virus strains. Most manufacturers will offer these updates for free to registered users and they can be downloaded over the internet.
- If the attachment is from someone you don't know, delete it! We're always told, "Don't take candy from strangers." The same rule applies to attachments!
- If the attachment is from someone you DO know, don't assume it's virus-free. Before opening it, it would be a good idea to contact your friend to verify whether they did, indeed, send you the attachment and ask them what it is. Remember, even if you know the person who sent it to you, many viruses spread themselves by automatically sending themselves to people in email address books.

- Keep your web browsers up to date. If you're using Internet Explorer, log into Microsoft's "Windows Update" web page and go to the "Product Updates" section and install the recommended critical system updates.

The pros and cons of anti-virus software

While we highly recommend anti-virus software, it's only a partial solution. If you install it and never update it, it's only doing half its job. You will still be unprotected against the latest and greatest viruses. As a general rule, you should check weekly to see if there are updates. Download them and install them as soon as possible.

A computer virus or a computer hoax?

A close relative to the computer virus is the computer hoax. Hoaxes are just that -- false stories that get passed around the internet via email. Some things that can tip you off that the message is a hoax are:

- You are encouraged to email the message to "everyone you know" (which qualifies as a chain letter and violates Dickinson's Responsible Use Policy)
- It happened to or was passed on by "my boss's mother's friend's manager."
- There is not a link for more information from a well-known computer security website.

Practice responsible computing! Before joining the party and forwarding an email warning to everyone you know, go to a well-known computer security website and see if they have any further information (see next section for some reliable sites). Most likely, you will find some information about the so-called virus or story to see if it's true.