

Protect yourself, your company, and your friends against viruses!

Just like a human being can catch a virus, from relatively harmless ones such as a flu to fatal ones such as HIV, your computer is just as vulnerable to a virus. Unfortunately, there are some elements out there that take pleasure in destruction and wreaking havoc and making other people's lives miserable. No, I am not talking about Darth Maul, I am referring to virus programmers.

A virus is a malicious piece of code written and designed to enter your PC without your permission and unnoticed. It will then replicate itself and/or possibly cause serious damage to your files and your PC. A virus can come in many forms but they usually come attached to a file, e.g. hidden in Word macros or embedded in executable files or attached to an e-mail, or in the boot sector of a disk.

Once the infected file or disk is introduced to your system, the virus can spread by attaching itself to files on your drives, or by sending infected e-mails to people in your address book. The Internet is a great environment for a virus to spread as downloading and e-mailing and exchanging files and information is common practice. If programmed to do so, the virus will not only spread but also cause damage to your system, such as, but not limited to, deleting files, deleting hard drive boot records resulting in an unbootable system, or erasing CMOS information.

This is a serious threat and should not be taken lightly. Almost every week, a new virus strikes and brings productivity to a grinding halt. The consequences are serious. For a home user, it often results in lost data and a lot of mad friends who received the virus from you. For businesses, a virus can bring down the entire network, often resulting in hours and days without e-mail or online access, corrupted or lost data, productivity loss, etc. Viruses have caused much damage and cost businesses and government agencies billions of dollars in time and money in an effort to recover from a virus attack. Don't think that you are immune to a virus. Nobody is.

What can we all do to prevent this from happening?

The solution to the problem is two-fold. To prevent virii from spreading, companies install virus scanner software on their mail servers, and home users install virus scanners on their home PCs. Most virus scanning software can be bought in stores for a price, but why pay if there are free alternatives? See the "Security" category of our download section at downloads/security.html for links to several free antivirus solution. Another alternative is to scan your PC online by visiting Trend Micro's web site, but this option does not offer permanent resident virus protection.

Of course any virus scanner can only work if you have the latest virus definition files installed. These virus definition files, also called DAT files, are being updated on a weekly or even more frequent basis by the maker of each virus scanner software. But it is up to you to download them regularly and update your PC. Most virus scanners either have a feature that let you schedule automatic downloads of new DAT files so that you don't have to worry about it, or at least offer an easy press-one-button way of doing so. Remember, if your virus scanner does not have the latest DAT files and doesn't know about the virus, it can't catch it.

However, the makers of virus scanners are always a step behind since they can't update their DAT files until they have seen the virus and know how to deal with it. Therefore there is usually a time gap from several hours to several days between the appearance of the virus in the wild and when the cure in the form of new DAT files is available. Since no virus scanner can protect you in that time period, it is up to you to prevent the virus from getting to you.

You are responsible!

The other part of virus protection is prevention. And no system administrator or virus scanner can do that for you. You are the one and only person responsible for exercising caution to prevent this from happening. Here are the top rules of virus prevention. We suggest you print them out, staple them to your forehead, memorize them - anything it takes:

DON'T OPEN ATTACHMENTS FROM UNKNOWN SOURCES! We can't emphasize this enough.

If you get an e-mail with an attachment from a person you don't know - **DO NOT OPEN IT - DELETE IT!**

If you get an e-mail with an attachment from a person you know but you didn't ask for it and didn't expect it - **DO NOT OPEN IT - DELETE IT!**

If it really was legit, the person will follow up with you or send it again and no harm is done. If it was malicious and you deleted it - you're safe. Virii can only spread if they are activated. As long as the e-mail is not opened and the attachment is not activated, you're safe.

Virus programmers disguise their malicious software to make it look harmless. Therefore do not assume that an e-mail that is marked "Happy Mother's Day" or "Funny Joke" or "Great Opportunity" or "Free " is safe.

You need to keep your guard up. If it does not look familiar, if it sounds suspicious - DO NOT OPEN IT - DELETE IT!

A virus can come from anybody - your coworker, your mom, your best friend, anybody! Therefore do not assume that any e-mail you receive from anybody you know is safe. Virii spread by replicating themselves unbeknownst to a user by sending themselves to e-mail addresses found in the user's address book. This means that virii are most likely to get into your inbox from somebody you know! If somebody you know sends you an attachment that you didn't ask for and didn't expect - DO NOT OPEN IT - DELETE IT!

Do not open any attachment that has the extension .vbs or .shs! Virii don't have to be files ending in .exe to be executed. VBS means Visual Basic Script is another programming language, one of many, that virii are written in. Virii can actually be hidden in many types of files. Often infected files are disguised to look like a text file or a video clip to trick you into thinking they are safe and opening them. Be suspicious of every single attachment you get. If you're not sure - DO NOT OPEN IT - DELETE IT!

Please use common sense

It is crucial to be suspicious and exercise caution. The number one rule is: Delete any e-mail with attachments that you cannot say with 110% certainty that they are safe. Nobody is safe from virii, but you can help fighting them by using common sense. Remember, a deleted legit e-mail takes only a few seconds to resend. But an opened malicious e-mail can cause hours of downtime, lost productivity, unrecoverable data, and cost a company tens of thousands of dollars as a result. Be responsible, use common sense, and think before you click. The virus threat is real.