# Did you know?

**Your Assignment**

Your assignment is to create a PowerPoint Presentation on Computer Viruses. **It needs to be at least 8 slides**. Keep in mind that you **DO NOT** put every single word into a PowerPoint. Only the most important items should be included in your presentation. I have outlined the Virus section for you to be a help of how to do the rest of the article.

The **Bold Words** are helps to you. (You should probably include those in your PowerPoint. Use the headings as guides as well.

**Extra Credit will be given for extra work and effort.**

**VIRUSES**

**AWESOME TIMES**

Real Life Live Viruses

Strange as it may sound, the computer virus is something of an Information Age marvel. On one hand, viruses show us how vulnerable we are -- a properly engineered virus can have a devastating effect, disrupting productivity and doing billions of dollars in damage. On the other hand, they show us how sophisticated and interconnected human beings have become.

 **“A virus is a small piece of software that piggybacks on real programs. Each time the program runs, the virus runs, too.”**

For example, experts estimate that the [Mydoom worm](http://www.timesonline.co.uk/article/0%2C%2C1-979473%2C00.html) infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the [Melissa virus](http://www.cert.org/advisories/CA-1999-04.html) was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained. The [ILOVEYOU virus](http://vil.nai.com/vil/content/v_98617.htm) in 2000 had a similarly devastating effect. In January 2007, a worm called Storm appeared, and by October, experts believed up to 50 million computers were infected. That's pretty impressive when you consider that many viruses are incredibly simple.

# Viruses

What is a computer virus?

Computer viruses are called viruses because they share some of the traits of biological viruses. **(New Slide Titled: What is a Computer Virus?) (First Bullet Point)** A computer virus passes from computer to computer like a biological virus passes from person to person.

Unlike a [cell](http://science.howstuffworks.com/life/cellular-microscopic/cell.htm), a virus has no way to reproduce by itself. Instead, a biological virus must inject its DNA into a cell. **(2nd Bullet Point)** The viral DNA uses the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

Similar to the way a biological virus spreads, a computer virus must hitch a ride on a program. **(3rd Bullet Point)** A computer virus must piggyback on top of some other program or document in order to launch. **(4th Bullet Point)** Once a computer virus is running, it can infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks.

**(New Slide Called: “Why would anyone make a virus?”)** People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus's attack phase, whether it's a silly message or the destruction of a [hard disk](http://computer.howstuffworks.com/hard-disk.htm). Why do they do it?

There are at least four reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to break a window on someone's car, paint signs on buildings or burn down a beautiful forest? For some people, that seems to be a **(1st Bullet)** thrill. If that sort of person knows computer programming, then he or she may funnel energy into the creation of destructive viruses.

The second reason has to do with the **(2nd Bullet Point)** thrill of watching things blow up. Some people have a fascination with things like explosions and car wrecks. When you were growing up, there might have been a kid in your neighborhood who learned how to make gunpowder. And that kid probably built bigger and bigger bombs until he either got bored or did some serious damage to himself. Creating a virus is a little like that -- it creates a virtual bomb inside a computer, and the more computers that get infected, the more "fun" the explosion.

The third reason involves **(3rd Bullet Point)** bragging rights. Sort of like Mount Everest -- the mountain is there, so someone is compelled to climb it. If you are a certain type of programmer who sees a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it.

And then there's **(4th Bullet Point)** cold, hard cash. Viruses can trick you into buying fake software, steal your personal information and use it to get to your money, or be sold on the digital equivalent of the black market. Powerful viruses are valuable -- and potentially lucrative -- tools.

**(New Slide Titled: “What are the Consequences?”)** Of course, **(1st Bullet Point)** most virus creators seem to miss the point that they cause real damage to real people with their creations. **(2nd Bullet Point)** Destroying everything on a person's hard disk is real damage. (2nd Bullet) Forcing a large company to waste thousands of hours cleaning up after a virus attack is real damage. Even (3rd Bullet) a silly message is real damage because someone has to waste time getting rid of it. For this reason, the legal system continues to develop more rigorous penalties for people who create viruses.

# Virus History

The Evolution

Traditional computer viruses were first widely seen in the late 1980s, and came about because of several factors. The first factor was the spread of [personal computers](http://computer.howstuffworks.com/pc.htm) (PCs). Prior to the [1980s](http://electronics.howstuffworks.com/gadgets/other-gadgets/80s-tech.htm), home computers were nearly non-existent. During the '80s, real computers started to spread to businesses and homes because of the popularity of the IBM PC (released in 1982) and the Apple Macintosh (released in 1984). By the late 1980s, PCs were in businesses, homes and college campuses. People would put viruses on floppy disks that would attack the start-up files located on the ROM. This type of virus is called a **BOOT SECTOR VIRUS.** Another factor that helped spread viruses was the use of computer bulletin boards. Bulletin boards are kind of like Face Book pages for people and companies, but more easily accessed. People could dial up a bulletin board with a [modem](http://computer.howstuffworks.com/modem.htm) and download programs of all types. Games were extremely popular, and so were simple word processors, spreadsheets and other productivity software. Bulletin boards led to the precursor of the virus known as the **Trojan Horse**. A Trojan horse masquerades as a program with a cool-sounding name and description, enticing you to download it. When you run the program, however, it does something uncool, like erasing your hard drive. You think you're getting a neat game, but instead, you get a wiped-out system. Trojan horses only hit a small number of people because they're quickly discovered, and word of the danger spreads among users. The third factor that led to the creation of viruses was the floppy disk. In the 1980s, programs were small, and you could fit the entire [operating system](http://computer.howstuffworks.com/operating-system.htm), a few programs and some documents onto a [floppy disk](http://computer.howstuffworks.com/floppy-disk-drive.htm) or two. Many computers did not have hard disks, so when you turned on your computer, it would load the operating system and everything else from the floppy disk. Virus authors took advantage of this to create the first self-replicating programs. If one of the infected programs is given to another person on a floppy disk, or if it is uploaded so other people can download it, then other programs get infected. This is how the virus spreads -- similar to the infection phase of a biological virus. A **LOGIC BOMB** is started by some sort of trigger which will activate the attack phase, and the virus will then do something -- anything from displaying a silly message on the screen to erasing all of your data. A **TIME BOMB** trigger might be a specific date or a number of times the program has been started up.

# E-Mail Viruses

Careful what you open

The I LOVE YOU VIRUS, which appeared on May 4, 2000, was simple. It contained a piece of code as an attachment. People who double-clicked on the attachment launched the code. It then sent copies of itself to everyone in the victim's address book and started corrupting files on the victim's machine. This is as simple as a virus can get. It is really more of a Trojan horse distributed by e-mail than it is a virus.

The MELISSA VIRUS took advantage of the programming language built into Microsoft Word called VBA, or Visual Basic for Applications. It is a complete programming language and it can be used to write programs that do things like modify files and send e-mail messages. It also has a useful but dangerous auto-execute feature. A programmer can insert a program into a document that runs instantly whenever the document is opened. This is how the Melissa virus was programmed. Anyone who opened a document infected with Melissa would immediately activate the virus. It would send the 50 e-mails, and then infect a central file called normal.dot so that any file saved later would also contain the virus. It created a huge mess.

What fueled this virus was the human willingness to double-click on the executable. The same kinds of exploits have also been passed over instant messaging networks like AIM and Windows Live Messenger. Commandeered accounts will send out links to viruses in instant messages; anyone who clicks the link and installs a [Trojan](http://computer.howstuffworks.com/trojan-horse.htm) application will have their own account hijacked and unwittingly spam their own friends with the compromising link.
Worms

A worm is a computer program that has the ability to copy itself from machine to machine. Worms use up computer processing time and network bandwidth when they replicate. A worm usually exploits some sort of security hole in a piece of software or the operating system. Worms normally move around and infect other machines through [computer networks](http://computer.howstuffworks.com/home-network.htm). Using a network, a worm can expand from a single copy incredibly quickly. The Code Red worm replicated itself more than 250,000 times in approximately nine hours on July 19, 2001.

A worm called Storm, which showed up in 2007, immediately started making a name for itself. Storm used social engineering techniques to trick users into loading the worm on their computers. And boy, was it effective -- experts believe between 1 million and 50 million computers have been infected.

# Are they popular today?

Viruses haven't had the same kind of impact in recent years for a number of reasons. People are a bit better educated about viruses. Free anti-virus software is easy to download. Microsoft recommends its own Security Essentials, while companies like AVG and Avast offer their own free alternatives. Computer software, in general, is designed with the Internet in mind and is less susceptible to viruses.

There are more viruses than ever out there for anti-virus software to keep track of. These programs will automatically update themselves regularly -- often even daily -- to guard against the latest virus mutations on the Internet.

In a modern era of smartphones and tablets, it's actually easier than ever to browse the Internet without getting a virus. Why? Because viruses are written for specific platforms. A virus intended to exploit something on Windows won't work on Apple's Mac operating system -- the code that makes up the two systems is completely different. Similarly, the code that makes up mobile operating systems like Android and iOS is different from the code on [PCs](http://computer.howstuffworks.com/pc.htm). Viruses that would cripple your computer won't work on mobile devices.

But mobile devices aren't completely secure, themselves. There are viruses out there that can extract personal information from [Android phones](http://www.lifeofandroid.com/news_detail/android-gingerbread-virus-poses-fresh-smartphone-threat/). Because Apple's iOS is a closed source platform, unlike the open source Android, it's more difficult to target with viruses. Besides, Windows is still a juicier target. While mobile viruses will certainly become more popular as smartphone sales increase, as of 2011, they're a very minor concern.

# Protecting my PC

There are three important things you can do to protect your computer and electronic devices. The first is to install an Anti-Virus Software. There are hundreds of options and the best option depends on your budget and your platform (what Operating System you have).

Second. Firewalls need to be set up on your computer. Firewalls are digital walls or blockers that allow permission or block information from different computers.

Last, you need to be cautious what you open on the internet and e-mail. You should never double-click on an e-mail attachment that contains an executable. Attachments that come in as Word files (.DOC), spreadsheets (.XLS), images (.GIF), etc., are data files and they can do no damage. However, some viruses can now come in through .JPG graphic file attachments. A file with an extension like .EXE, .COM or .VBS is an executable, and an executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The only defense: Never run executables that arrive via e-mail.