Virus Fact Sheet

What is a virus

Unless you've actually had a virus they can be a bit of a mystery. A tiny piece of software takes hold of a normal program like a word processing or spreadsheet package and won't let go. Each time the program runs the virus inside it multiplies, attaches itself to other programs and gradually embeds itself in your machine (and any other machine you may have on your network). They're unpleasant things that are created with the intention of being both destructive and hard to destroy.

Email Viruses

Instead of sitting alone in your computer these viruses are intended for rapid replication and will spread faster than you thought possible. Email viruses are pieces of software that arrive in an email to you (possibly called something welcoming like I Love You or perhaps in something innocuous from someone you know) and which when opened are programmed to send themselves to every contact in your address book. These are the viruses that bring large computer systems down as they rampage through before there is time to shut down. These are also the type viruses that have caused massive phone bills on unprotected sites as they send themselves, hundreds of thousands of times night and day. The destructive capabilities of theses viruses should not be underestimated they are by far the greatest threat to the average business computer system.

Worms

Cyber worms are incredibly destructive and extremely hard to prevent from entering your system. The creators of worms generally aim to expose failings or holes in a well-known product such as a program or a server. Worms are programmed to seek out these specific holes and crawl inside. They then replicate themselves and go looking for more holes across your network. The Code Red outbreak last year was a classic example of a worm. It replicated 250,000 times in 9 hours.

Trojans

Trojans generally arrive via email in a harmless looking attachment such as a game or a spreadsheet. They roam your hard drive and randomly delete files or generally create mayhem amongst its contents. Trojans can't replicate themselves automatically - but if you don't spot you have one you may unwittingly email it and cause destruction in yet another machine. Don't underestimate the damage and inconvenience that Trojans can cause, particularly within a business setting where the information stored on PC's is valuable and not easily replaced. Regular system back-ups will help to minimize problems if you do get hit.

Warning Signs

The most unfortunate thing is that all to often there are no perceptible warning signs. By the time you find out that you have been subject to a virus attack a great deal of damage has already been done. If your computer has been out of the box it came in for more than a week and you have received email or connected to the web without taking active steps to protect your system then you almost certainly have already been infected.

Top 10 Tips to Keep Your Computer Virus-Free

1. Use common sense. It's always better to err on the side of safety. If you're unsure about an attachment, delete it. Especially if it's from a source you don't recognize. If there are tempting animations on a site that look highly unprofessional, don't download them.

2. Scan floppies and cdroms before using them. This is always important, but especially if you are using the disk to carry information between one computer and another. You could easily pick up a virus from an insecure network and introduce it into your system. Running a virus scan before launching any of the programs on the disk will prevent infection.

3. Don't share floppies or cdroms. Even a well-meaning friend may unknowingly pass along a virus, Trojan horse, or worm. Label your disks clearly so you know they're yours and don't loan them out. If a friend passes you a foreign disk, suggest an alternative method of file sharing such as sending the file as an attachment (assuming your mail is scanned as it comes in).

4. Don't boot from a floppy disk. Floppies are one of the most common ways viruses are transmitted. If you are using a floppy while working on your computer, remove it when you shut the machine off or the computer will automatically try to boot from the floppy, perhaps launching any viruses on the disk.

5. Don't download programs from the Web. Unreliable sources such as Internet newsgroups or Web sites that you haven't heard of may be willing providers of viruses for your computer. Avoid downloading files you can't be sure are safe. This includes freeware, screensavers, games, and any other executable program - any files with an ".exe" or ".com" extension, such as "coolgame.exe." Check to see if the site has anti-virus software running on their side. If you do have to download from the Internet, be sure to scan each program before running it. Save all downloads to one folder, then run virus checks on everything in the folder before using it.

6. Update your anti-virus software frequently. An anti-virus program is only as good as the frequency with which it is updated. New viruses, worms, and Trojan horses are born daily, and variations of them can slip by software that is not current. Most good Antivirus systems have a feature that searches for new virus definitions every time you go online, so you are *always* up to date. A point worthy of note is that virus definition files are written after a virus has been discovered in the wild. This means that somebody will be infected before the virus is discovered and a fix is found the odds are against it being you but it is a possibility.

7. Get immediate protection. Configure your anti-virus software to boot automatically on start-up and run at all times. This will provide you back-up protection in case you forget to scan an attachment, or decide not to. And in case you forget to boot up your anti-virus software, configuring it to start by itself will ensure you get immediate protection anyway.

8. Scan all incoming email attachments. Be sure to run each attachment you plan to open through the anti-virus check. Do this even if you recognize and trust the sender; malicious code, like Trojan horses, can slip into your system by appearing to be from a friendly source.

9. Don't automatically open attachments. Be sure your email program doesn't automatically download attachments. This will ensure that you can examine and scan attachments before they run. Refer to your email program's safety options or preferences menu for instructions.

10. Install reliable anti-virus software. Anti-virus software scans files regularly for unusual changes in file size, programs that match the software's database of known viruses and suspicious email attachments. It's the most important step you can take towards keeping your computer clean and free of viruses. Your Ibcos representative will be able to call on our technical support department to advise on the best of the world's leading anti-virus software specifically tailored for your particular installation.