IT Information Sheet 3

Computer Viruses

Introduction

A computer virus is a program that is designed to damage or disrupt the normal functions of your computer and its files.

Like biological viruses, computer viruses attach themselves to a host, usually a program file, data file, or a file in your computer's operating system. From here, it replicates itself, spreading the infection to other files.

How viruses are transmitted from computer to computer

Viruses can find their way onto your computer in many different ways.
Viruses can be transmitted by email, in downloads from the internet, through network connections, by floppy disks or by CDs, particular those that have been burnt on a computer infected by viruses.

Common types of computers viruses

Computer viruses can cause very serious damage to your computer's program and data files, as well as affect your computers hardware, such as your hard drive. What a particular virus will do to your computer depends on how it was programmed when created.
The basic types of viruses are -

Worm Viruses

Worm viruses are self-contained programs that remain hidden and propagate via email or duplication, modify existing software so that when run, the legitimate program spawns copies of the virus, which is then forwarded on in email or other files.

Boot viruses

Boot viruses attack the boot sectors on your hard drive and interfere with your computer's basic operation, making your operating system run strangely or even corrupt it all together.

Macro viruses

Macro viruses tend to attack data files, like word documents and spreadsheets, causing you to loose files or cause your word or excel software to not work properly.

Trojan viruses

Trojan viruses pretend to be other software, hence their name as in the Trojan Horse. Trojan viruses pretend to be a legitimate piece of software, but in reality can attack your hard drives, deleting files and re-writing system files, causing your computer to become unstable, particular when operating system files are deleted.

As a general rule, computer viruses only attack files in your computer. They do not attack your computer's hardware, like the monitor, mouse or keyboard.

However, some viruses will attack the files that operate your computer's hardware, causing hard drives to re-format, video drivers to be deleted or your operating system to stop running. While this may cause your monitor to stop working properly, it doesn't mean you need to get a new monitor.

E-mail Viruses

Email is probably the most common method for spreading viruses. Plain text email messages don't normally spread viruses. Most email viruses are spread via attachments to email messages, or in email messages containing embedded executable code. For a virus contained in an email message to attack your computer, it will normally require your computer to executive some code, like open an attachment or open a html link embedded in the message. To protect yourself against email viruses it is important that you do not open attachments from senders you don't know, or come from a free email source, like hotmail or yahoo. If you use an email client to check your email, avoid clients that automatically open attachments (like Outlook Express).

Steps taken by CSU to minimise viruses

While CSU takes every precaution to protect against viruses, it is impossible to stop viruses all together. CSU does maintain up to date anti virus definitions and performs regular scanning of email servers and internet traffic to minimise the University's exposure to viruses. Even with these precautions, students and staff are encouraged to obtain and regularly use an anti-virus program for their home computers.

What to look for when buying Anti-Virus software

When buying Anti-virus software, look for a package which suits your operating system. For example, if you run Windows XP, look for a package that is recommended for Windows XP. Make sure that any software you do buy includes an update function, where you can download virus definition updates to protect your computer from future types of viruses.

Steps on how to minimise your exposure to viruses

The best way to minimise your chances of getting a virus infection is to be pro active and follow some basic steps we have outlined below. Purchase and Install anti-virus software. Make sure the software you select is compatible with your computer's operating system, and offers an update service.

- Make sure that you regularly up date your anti virus software definitions. New viruses come out every day; so its important you make sure you have updated your virus definitions. Anti-virus software that hasn't been updated for several months is practically useless in protecting your computer.
- Make sure that you regularly scan your computer for viruses using your anti-virus software. If your software allows, use its automatic protection features which will check for viruses when ever you turn on your computer
- Virus scan any new programs or other files that may contain executable files before you run or open them, particularly if it's a freeware or shareware program
- Scan floppy disks before opening them.
- Don't open emails or email attachments that have been sent by a person or organisation you don't know.
- Try to use an email client for checking your email which doesn't automatically execute or opens attachment

Beware of Virus Hoaxes

From time to time, you may receive "Virus Warning" emails. These emails, sent on by well meaning people, while seeming to alert you to a real virus treat, more often than not are merely hoaxes. Virus hoaxes are typically alerts that are passed on by naive users who think they are helping people out. The reality is that most of these warnings are designed to cause fear or simple confuse people. In some cases such messages contain instructions that, if followed, can result in damage to your computer.

If you receive a message warning you about viruses, it is recommended that:

- you do not forward the email;
- you do not follow the instructions contained in the email or forward the email to others;
- you ignore all such emails unless they are clearly from an authoritative source, and back up their claims with references to credible sources.