

# Combating Computer Viruses

- **What is a Virus**
- **Get Protected**
- **Virus FAQ**

**Internet Access Made Easy**

- **What is a Virus?**

A virus is best defined as "A self-replicating piece of computer code that can partially or fully attach itself to files or applications".

Viruses usually operate without the knowledge or desire of the user, and mostly causing harm to the user's computer system.

A virus is actually a computer program. Like any other program, it contains instructions that tell your computer what to do. The difference is, a virus will cause your computer to do something you don't want, and it can usually spread itself to other files on your computer - and other people's computers.

Some viruses can be considered as quite harmless and simply display a message, presenting little more than a nuisance. More recent viruses have been far more destructive and presenting a payload to the computer, leading to destruction of files and subsequent data loss, personal information becoming public or even causing damage to the computer itself. Some can even open "back doors" to the infected computer providing hackers with access to maliciously exploit the system.

And as the name suggests, computer viruses share many traits with their biological counterparts:

**They Evolve:** New and more sophisticated computer viruses continue to be written all the time representing a continually evolving threat.

**They Infect:** Instead of infecting the cells of an organism, computer viruses infect the files of a computer system including those stored on removable media (i.e. floppy disks, zip disks, recordable CDs).

**They Replicate:** As with biological viruses, computer viruses attempt to replicate themselves (infect) into as many other computer files as possible, including those of the current host or of other accessible (i.e. networked) computer systems. And most importantly they spread via e-mail. Some viruses take addresses from the address book of an infected computer and send out new messages with its destructive payload attached to all e-mail addresses, often "faking" the senders address.

- **Get Protected!**

Whatever scanning is in place on the transit path, i.e. at the mail server side of the ISP, it can by nature of the technology, only provide partial protection. In particular when it comes to the detection of highly complex embedded worms. The only solution is a virus protection at the receiving end – your computer. If you don't already have virus protection software on your machine, get some. We at Infocom will be available to assist you to select the best software and we offer installation services. Please get in touch with our Customer Care team to provide you with all relevant details.

#### **Update your anti-virus software**

Almost 1000 viruses are discovered every month. And due to higher complexity of the virus software code and sophisticated encapsulation techniques they are even more difficult to avoid. It is therefore absolutely essential that you keep your anti-virus software up to date. Most of the virus protection programs such as Norton and MacAfee and many others do have an automatic notification and/or update feature that will automatically link to the respective Internet site and alert add new virus detection code whenever the software vendor release new virus update files.

#### **Don't open attachments!**

One of the best ways to prevent virus infections is not to open attachments, especially when viruses are being actively circulated. Even if the email is from a known source, be careful. Once a computer system has been compromised, some viruses take all e-mail addresses resident on infected computer and send out new messages with its destructive payload attached. And this happens in the background of all other processes unnoticed. Always scan the attached files first for viruses. Unless it's a file or an image you are expecting, delete it!

In particular never open email attachments with the file extensions VBS, SHS or PIF. These extensions are almost never used in normal attachments but are frequently used by viruses and worms. Never open attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS.

#### **Scan your system regularly**

If you're loading anti-virus software for the first time, it's a good idea to let it scan your entire system. It's better to start with your PC clean and free of virus problems. Often the anti-virus program can be set to scan each time the computer is rebooted or on a periodic schedule. Some will scan in the

background while you are connected to the Internet. Make it a regular habit to scan for viruses.

- **Virus FAQ and Common Misconceptions**

**“There is only one type of virus...”**

There are three main types of computer viruses to differentiate: Trojans, Worms and Macros.

**Trojans** – are programs that stay on your system and either allow other users to gain access to your system or cause damage by deleting or corrupting files. Trojans are usually found within attachments sent via e-mail and generally do not replicate themselves. They are often difficult to spot as they can take the form and name of another (usually essential) system file.

**Worms** – are viruses spread either via e-mail or network connection. They have different risk levels and infecting abilities. Worms are the most common form of computer viruses and also the most damaging. Famous names are: Melissa, Loveletter and more recently Sircam, Nimda and Magistr. New variants of these worms are discovered all the time and because of the nature of the Worm viruses they spread very rapidly.

**Macros** – are viruses embedded within documents, usually Word or Excel files. They are activated when the document is opened. As with Worms, the degree of causing damage can vary dramatically. Some Macros replicate themselves by attaching the macro code to all documents and standard templates so every new document created will already be infected with the virus code. Some Macros also have the ability to attach an infected “empty” document to all outgoing mails.

**“I don’t open e-mails from people I don’t know...”**

Although this will certainly help to protect you, many viruses e-mail themselves to every e-mail address found in the address books, or mailboxes (in-box, out-box etc.). That means a virus can come from anyone you have regular e-mail contact with.



**"I have a firewall installed or my ISP has firewall security..."**

Firewalls do NOT protect against viruses. They are designed to provide and monitor access control policies to computer networks ("hacking") but they are fully transparent to e-mail traffic and would let infected mails pass through.

**"My ISP has already got anti-virus protection..."**

This does only provide a certain degree of protection. At Infocom we have the most state-of-the-art virus mail scanning installed. However, due to the nature of the virus code and sophisticated embedding techniques, certain viruses can only be detected during a download process of e-mails or attachments. And it would not protect you at all against viruses transferred via shared storage media (floppy disks, zip disks, CDs etc.) or through network connections. To guarantee sufficient protection it is therefore essential to install an anti-virus program on your computer.

**"I've got anti-virus software on my system..."**

Very good. Then you are protected for the next week or so. New viruses are discovered every day and you need to make sure that your virus definitions are regularly updated. This is absolutely essential otherwise your anti-virus software and protection is worth close to nothing if the last update was only done a couple of months back. Most of the well known anti-virus software brand names provide cost free Internet Live-Update facilities for a year or more and this can be extended for a very small fee.

**Your Infocom Customer Care Team**



Uganda's leading Internet provider

Tel: 342681 Fax: 342192

[www.infocom.co.ug](http://www.infocom.co.ug)

[sales@infocom.co.ug](mailto:sales@infocom.co.ug)

Dial-up access (countrywide):

049 5100 (local call rate within UTL network)

031 217100 (MTN)