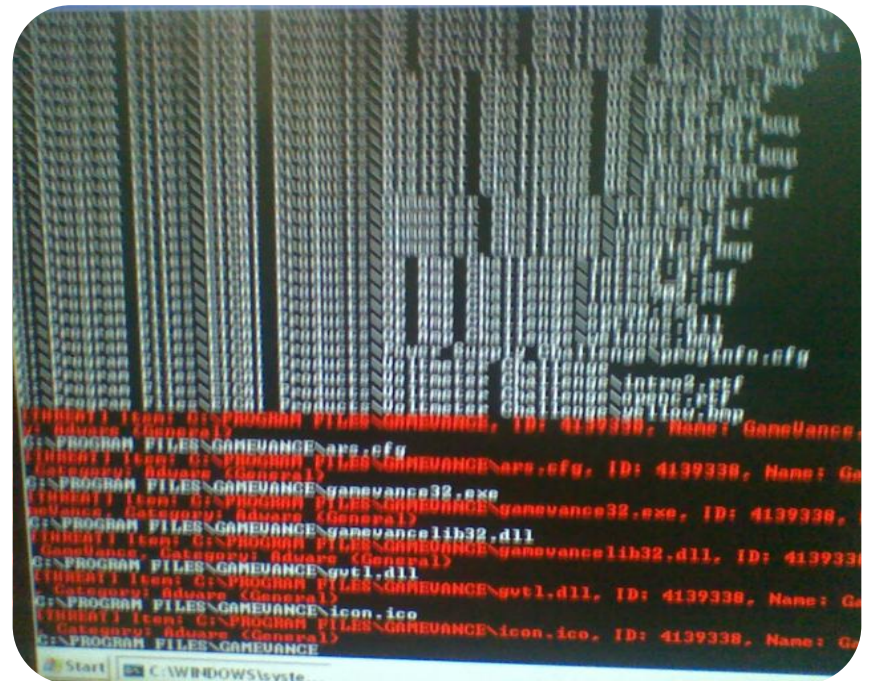


# Preventing Computer Virus

# What is a Computer Virus?

A computer virus is a small software program that spreads from one computer to another computer and that interferes with computer operation. A computer virus may corrupt or delete data on a computer, use an e-mail program to spread the virus to other computers, or even delete everything on the hard disk.

Computer viruses are most easily spread by attachments in e-mail messages or by instant messaging messages. Therefore, you must never open an e-mail attachment unless you know who sent the message or unless you are expecting the e-mail attachment. Computer viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer viruses also spread by using downloads on the Internet. Computer viruses can be hidden in pirated software or in other files or programs that you may download.



# Losses due to Virus attacks

---

- ▶ You might lose all your precious data prepared over years
- ▶ Your computer will stop working efficiently, sometimes at just 20% of the normal efficiency of the PC
- ▶ You might lose all emails & programs that you have installed
- ▶ Some Viruses have the capability of even minor hardware damages
- ▶ Viruses can be unknowingly transferred to your home computers or other friend's computers if storage media is shared
- ▶ Viruses might steal your data, passwords, credit card details etc. & send them to a hacker for misuse
- ▶ Virus infections can cause embarrassment if your friend & associates get files from you that are affected.



# Identifying Virus attack on your system

- ▶ The computer runs slower than usual.
- ▶ The computer stops responding, or it locks up frequently.
- ▶ The computer crashes, and then it restarts every few minutes.
- ▶ The computer restarts on its own.
- ▶ Applications on the computer do not work correctly.
- ▶ Disks or disk drives are inaccessible.
- ▶ You cannot print items correctly.
- ▶ You see unusual error messages.
- ▶ You see distorted menus and dialog boxes.
- ▶ There is a double extension on an attachment that you recently opened, such as a .jpg, .vbs, .gif, or .exe. extension.
- ▶ An antivirus program is disabled for no reason. Additionally, the antivirus program cannot be restarted.



# Safeguards from Virus infections

---



Antivirus



Firewall



Using USB Drives



Downloading Emails



Downloading Software



Reading Messages



Scheduling Antivirus Scans

---



# Antivirus

Always have an Anti Virus installed in your computer. Popular Antivirus are:

- ▶ Norton
- ▶ Quick Heal
- ▶ Kaspersky
- ▶ NOD32
- ▶ Avira
- ▶ Lots more

Some of the Antivirus like Avira are not only effective Software but also FREE. So do not hesitate to download & use an Antivirus always. It is a small bother compared to computer infections.

When on a Network or a Domain like DishaNet, it is best to just understand how to judge if an Antivirus software is active or not. All other details will be taken care by the IT Department. For e.g. if you have Avira on your computer, make sure that the small umbrella icon is always open.



## ▶ TIP:

*Always make sure that your Antivirus is running when you switch on your computer. If it is showing itself to be disabled, there is surely a problem. Consult an IT Expert immediately.*

# Firewall

Firewall is a system in computer to prevent viruses or hack attacks on your computer. Always have a Firewall activated on your computer. You can do this in two ways:

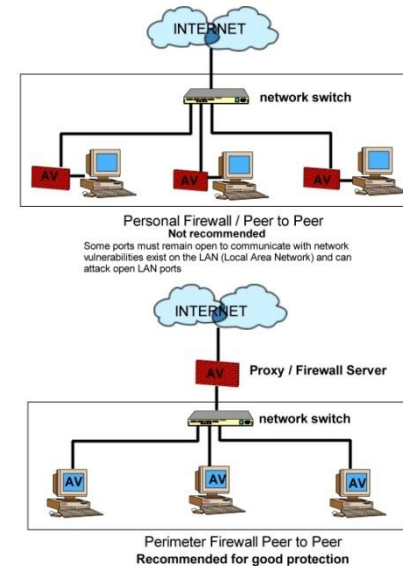
## 1. Use Windows inbuilt Firewall

All Window operating systems have inbuilt firewall. All you need to do is to activate them by going into Control Panel -> Windows Firewall & selecting the Enable Firewall option.

## 2. Use External Firewall

Most Antivirus come with their own firewall. Look for an option to enable firewall when installing the antivirus in your computer.

Always check whether firewall in either Windows or Antivirus software is activated.



### ▶ TIP:

- ▶ *In case you are not sure of which application to allow through Firewall, select the No Exceptions checkbox in the Windows Firewall category.*

# Using USB / External drives

USB Storages (Pen Drives / External Hard Disks) are the most common carriers of viruses. By using an infected USB Storage not only do you harm your company computers but also all friends / colleagues / family members with whom you share data.

To avoid infection through this medium ensure of the following

- ▶ Ensure that your Antivirus is running & enabled before inserting a USB storage device
- ▶ Run an Antivirus scan as soon as you insert a USB storage device for the first time
- ▶ Clean your storage device once a week for better security
- ▶ If you insert your storage device in someone else's computer, always scan it later in your own computer.
- ▶ Try to pick USB storage with write protection for better safety



## ▶ TIP:

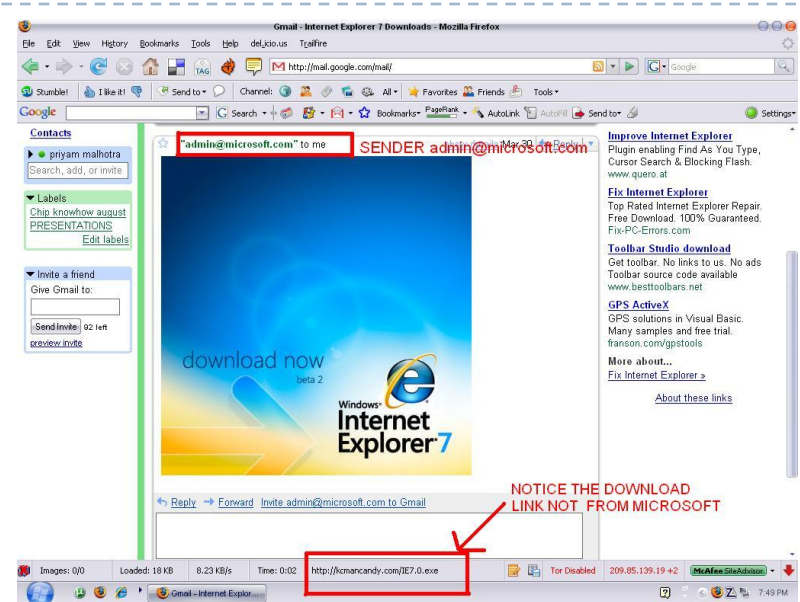
*You can install an Antivirus program on your pen drive directly. To do so contact the IT Team for a special installation.*



# Downloading Emails

Email Attachments have been found to be the most active method for spreading Virus. While email texts are harmless, it is the attachments which cause havoc. Follow these simple precautions to safe guard yourself from email viruses:

- ▶ When using Outlook always ensure that the Antivirus is enabled
- ▶ Do not open attachments unless they are sent from a known person
- ▶ Prefer to use Gmail /Yahoo for reading emails & downloading attachments as they scan all attachments while uploading
- ▶ Never open attachments other than .doc, .xls, .ppt, .pdf or properly known formats
- ▶ Never run an .exe file that comes with an attachment even from a known person
- ▶ Always scan your files before sending them to others to prevent embarrassment of sending a virus by mistake



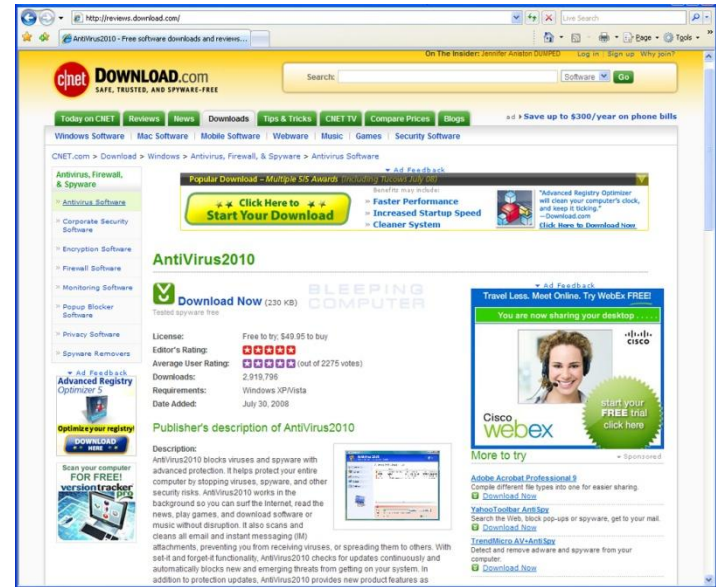
## ▶ TIP:

*You can configure your Dishamail.com email account to work in gmail for reading & sending messages. Consult the IT team or refer to the IT Manuals for the same.*

# Downloading Software

Occasionally, we download software that interest us. If doing so kindly take the following simple precautions:

- ▶ First ensure that the Antivirus is running on your computer
- ▶ Prefer to download software from reputed download sites like download.com, Tucows.com etc. or if you are downloading from a lesser known company, download from an official site only
- ▶ Never download from sites that come as advertisements, pop-ups or unwanted pages on your computer
- ▶ Always download a file, scan it with Antivirus & then only run it for safety
- ▶ Sites offering screensavers, themes, movies, songs etc. are most common sites that spread viruses. Avoid such sites & download these contents from known & reputed websites only
- ▶ Never download Cracks, Hacks etc. as they are not only illegal but also haven for malicious software



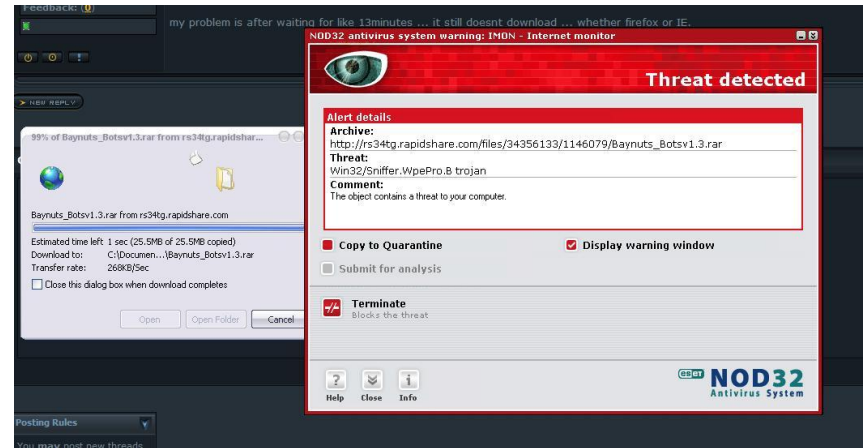
▶ **TIP:**

*Browse through download.com. It has the most exhaustive list of software on the net checked for safety.*

# Reading Messages

Your computer may sometimes annoy you with small message pop-ups with works like Warning, Error Message, Security Message etc. Please do not ignore them & shut them down. Not only does doing so prompt the computer to show you such messages more often but also potentially opens your computer to attacks. Also observe the following guidelines for the same:

- ▶ Read the message carefully, it just takes a few seconds & saves you from hours of rework in the future
- ▶ Understanding the messages is simply a matter of common sense & nothing to do with IT knowledge
- ▶ Always understand the purpose of such messages. Most important messages will always have “IMPORTANT”, “WARNING” & “SECURITY” in the headers. Take them seriously
- ▶ Understand the action being asked by the message & then click. Never allow a program to run unless you have started it



## ▶ TIP:

*Select the option “Take same action for future messages” to reduce the instances of the messages but only after you have read & understood the first message.*

# Scheduling Antivirus scans

Most Antivirus come with an automatic scheduling. Preferably set this schedule for once a week during a lunch hour. Scheduled scans will always boost the speed of your computer. Some more things you can do are:

- ▶ Schedule weekly Antivirus scans
- ▶ Schedule fortnightly defragmentation scans
- ▶ Always keep your Antivirus up to date. All antivirus have an auto update feature. Never disable this feature
- ▶ Open your Antivirus once ever fortnight to see that all tasks are being performed
- ▶ If possible use an Antispyware once in a while to check any problem

