

# Virus Busting



# What *is* a virus?

- ◆ A virus is a normal program file with...
  - Instructions stored in the Drive's Boot sector
  - Instructions stored in the Drive's Partition sector

or

- Instructions stored as Macro in Word or Excel

# What makes a virus a *virus*?

- ◆ Viruses have a
  - Replication mechanism (how it spreads)
  - Protection mechanism (how it hides)
  - Trigger (what sets it off)
  - Payload (the damage)

# What is the process of infection?

- ◆ Instructions are copied to your computer's RAM memory
- ◆ The instructions are carried out by your computer's CPU

# What can a virus really do?

- ◆ Damage can range from
  - Nothing
  - Display cryptic message
  - Massive file deletion
  - A little damage every day for a long time
  - Leak secured information

# How are viruses classified?

- ◆ Trivial
- ◆ Minor
- ◆ Moderate
- ◆ Major
- ◆ Severe
- ◆ Unlimited

## BEWARE! Its a *hoax!*

- ◆ Never mass-forward unconfirmed virus warnings (it is sometimes the intent of the virus to spread fear and thereby bog down e-mail systems)
- ◆ Keep aware of new hoaxes
- ◆ Encourage others to e-mail responsibly
- ◆ Scan your system if you are unsure

*From ITCS's Virus Buster's Web Site (PenPal Viruses Commentary):*

General rules for determining Hoaxes:

1. The more exclamation points in a message, the more likely it is to be bogus.
2. It is **IMPOSSIBLE** to get a virus merely by reading email --a virus must execute to infect.

*Note: Some email programs allow one to open email attachments automatically ... You should scan all files you receive (or just delete them, if you weren't expecting to get them) with an antivirus program first...*

3. If you get a copy of this hoax by email, **PLEASE** reply to the sender to let him or her know it is a hoax. Provide our web address too, if you would (<http://www.umich.edu/~wwwitd/virus-busters>) so we can help stamp out this plague.

# How do I protect myself?

- ◆ Keep your anti-virus software up to date at least weekly. A free auto-updating version is available from Virus Busters.
- ◆ Avoid opening any unexpected e-mail attachment, even if it appears to come from a known sender.
- ◆ Scan an e-mail attachment with up-to-date antivirus software before opening it.
- ◆ Only download files from reputable sources and scan them before running them
- ◆ Avoid “foreign” floppies – disks that have been used in other’s computers.
- ◆ Only turn on or boot your computer with a floppy disk that you are certain is clean.
- ◆ Use the write protect tab to protect your disks.

# More Hints

- ◆ Always use licensed copies of software
- ◆ Keep your password secure
- ◆ Make regular backups
- ◆ Never ignore virus messages after scanning
- ◆ Keep anti-virus software up to date weekly

# ITCS's Virus Buster's Web Site

<http://www.itd.umich.edu/Virus-Busters/>