Is Your Computer Feeling Ill?

John A. Underwood, CCNA
ITS Help Desk Manager
NDSU

Computer Viruses

- What are they
- How do you get them
- What can you do to protect yourself

What are they

- There are four types of viruses

Hoax

- generally an email or newsgroup posting claiming that a new threat has been created when in fact it does not exist. The intent of the message is to scare other users into forwarding the false information to others, effectively spreading the hoax. If you receive a hoax message, please disregard it.

Hoax Examples

- “Join the Crew”
  - *Hey, just to let you guys know one of my friends received an email called "Join the Crew," and it erased her entire hard drive. This is that new virus that is going around. Just be careful of what mail you read. Just trying to be helpful...*

Hoax Examples

- “AOL4Free”

Anyone who receives this must send it to as many people as you can. It is essential that this problem be reconciled as soon as possible. A few hours ago, I opened an E-mail that had the subject heading of "aol4free.com."

Within seconds of opening it, a window appeared and began to display my files that were being deleted. I immediately shut down my computer, but it was too late. This virus wiped me out. It ate the Anti-Virus Software that comes with the Windows '95 Program along with F-Prot AVS. Neither was able to detect it. Please be careful and send this to as many people as possible, so maybe this new virus can be eliminated.

Hoax Examples

- "Worth a Try"
  - *When you forward this e-mail to friends, Intel can and will track it (if you are a Microsoft Windows user) for a two week time period. For every person that you forward this e-mail to, Microsoft will pay you $203.15, for every person that you sent it to that forwards it on, Microsoft will pay you $156.29 and for every third person that receives it, you will be paid $17.65.*

Trojan Horse

- a Trojan horse program comes with a hidden surprise intended by the programmer but unexpected by the user. Trojan horses are often designed to cause damage or do something malicious to a system, but are disguised as something useful. Unlike viruses, Trojan horses don't make copies of themselves. Like viruses, they can cause significant damage to a computer.

Trojan Horse Example

- AOL4Free Trojan Horse
  - Received via e-mail
  - With the promise of receiving “Free AOL”
  - Deleted all of your files from your hard drive

Virus

- a segment of executable code or script that implants itself into an executable file or script-enabled document and spreads systematically from one file to another. This systematic process of self-replication differentiates viruses from other virus-like computer infections such as Trojan horse programs and worms.

Virus Examples

- WordMacro
  - Attach and spread through Microsoft Word and Excel files

Virus WordMacro Examples

- **Concept**
  - And 56 of her sisters
- **Wazzu**
  - And 72 of his brothers
- **Melissa**

  Subject: Important Message From " Application.UserName

  Message "Here is that document you asked for ... don't show anyone else ;-)“

  Attachment

  Or

  Subject: Resume for Janet Simons

Virus Other Examples

- Stoned
- Michelangelo

Worm

- worms replicate themselves. However, instead of spreading from file to file they spread from computer to computer, infecting an entire system.

Worm Visual Basic Scripts Examples

- **Loveletter**

  Subject "ILOVEYOU“

  Message "kindly check the attached LOVELETTER coming from me.“

  Attachment "LOVE-LETTER-FOR-YOU.TXT.vbs“

  - Sends a copy of the e-mail message, including attachment, to everyone in your Microsoft Outlook address book.
  - Scans all drive (local and on a network) for multimedia files and replaces them with a copy of the worm.
- **Stages**
  - Attachment: LIFE_STAGES.TXT.SHS
  - Sends a copy of the e-mail message, including attachment, to everyone in your Microsoft Outlook address book.

How do you get them

- E-mail attachments
- Infected Microsoft Word or Excel documents
- Other infected programs or files

What can you do to protect yourself

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- Do not open any files attached to an email if the subject line is questionable or unexpected.

What can you do to protect yourself

- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.

What can you do to protect yourself

- Update your anti-virus software regularly. Over 200 viruses are discovered each month, so you'll want to be protected.
- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy.
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments.

Anti-Virus Software

- Symantec **Norton Anti-Virus**
- Command Software Systems **Command AntiVirus**
- McAfee **VirusScan**
- F-Secure **F-Prot**
- Computer Associate **InoculateIT**
- **ANTIDOTE**
- Panda Software Panda **Antivirus Platinum**
- Trend Micro **PC-cilllin**

Questions?

- Contact the ITS Help Desk
  - 231-8685