@bsolute pc solutions
T: 647 288-2882

Viruses online and offline

and dealing with them when they infect

To keep the bugs away and preparation for virus removal in case of infection:

- Avoid attachments with extensions of type (.exe, .com, .vbs, .bat, .scr)
- Keep the Data files for the virus scanner up to date
  [Most antiviral programs require data to "let the program know what to look for". Most of the major companies producing this type of software also release the Data files to the public free of charge]
- Learn how to use the program correctly
- Be careful where you choose to download from
- Scan EVERY binary file that you download for viruses (Most antiviral programs will do this automatically)
- NEVER open a file you have received off the Internet until you have scanned it for virus contamination
- Avoid downloading files from sites such as KaZaA, Limewire, Morpheus etc. but if you do, beware of files that match the name you searched for EXACTLY and check the file size; if it is too small for the type of application it could be (incomplete, damaged or a VIRUS in disguise)
- ALWAYS scan a CDRW that has been used in another computer BEFORE using it in your computer
- ALWAYS check the various *hoax pages* listed below so as not to proliferate a hoax yourself.
- The ONLY EMAIL VIRUS contained in text is the BOGUS text itself and the space it occupies on the 'Net.
- Make a complete backup of your system when it is performing well (preferably on HD) and keep it in a safe place storing according to the media manufacturers specifications. The reason tape is preferred here is that boot sector viruses do not normally store on tape.

If you find a virus:

- The Anti-virus software should be able to identify the virus by name and then be able to give instruction on ridding the system of the pest.
- Follow the manufacturers instructions to clean the system with the virus control software you purchased
- If you do not understand exactly how to do it, get a professional to do it, else you may never see your data again.
- Try to determine how the infection occurred so as to prevent it from recurring, refer to the recommendations above to help with the determination if necessary.
- Clean ALL the diskettes that you use after cleaning the hard drive.
- Notify EVERYONE you may have shared any files with.

From McAfee Associates, Inc.

Ten Common Virus Myths

1. VIRUSES CAN HIDE INSIDE A DATA FILE.

   FALSE: Data files can not spread a virus on your computer. Only executable program files can spread viruses. These are files that contain a binary header explaining to the operating system that they contain executable code. If a computer virus infected a data file, it would be a useless effort. By definition, a virus is something that must replicate. Since a data file is not executed, only loaded, the virus would not be able to replicate.

2. VIRUSES DO NOT INFECT ZIP FILES.

   FALSE: The files inside the ZIP file could be infected. To secure your system from infected ZIP files, first copy the ZIP file into a directory of its own, then using PKUNZIP extract the files into that directory. You now have all the files and nothing has been executed. SCAN the files that were extracted. Nothing is executed when you unzip, so it is safe to SCAN the extracted files before the user runs them.

3. MY FILES ARE DAMAGED, IT MUST HAVE BEEN A VIRUS ATTACKING MY FILES.

   FALSE: This is the most common virus misconception. Damaged files can be caused by many things. Damaged files could be the result of a power surge, power drop, static electricity, magnetic forces, failing hardware component, bug in another software package, dust, fingerprints, spilled coffee, etc. Power failures and spilled cups of coffee have destroyed more data than any viruses.

4. VIRUSES CAN SPREAD TO ALL TYPES OF COMPUTERS.

   FALSE: Viruses are limited to a family of computers. A virus designed to spread on Windows PCs cannot infect an IBM 4300 series mainframe, nor can it infect an Apple Macintosh. Word Macro viruses are an exception. Macro viruses can spread on any platform that runs Microsoft Word.

5. MY BACKUPS WILL BE WORTHLESS IF I BACKUP A VIRUS.

   FALSE: Suppose a virus is backed up with your files. It could not be a boot infecting virus because the back-up software will not back up the boot sector. If you had a file infecting virus, you could restore important documents, databases, and your data, without restoring an infected program. Remember myth #2, viruses can not hide in your program data, only in program files. You may reinstall programs from master disks. It is monotonous work, but not as

hard as some people believe.

6. READ-ONLY FILES ARE SAFE FROM VIRUS INFECTIONS.

   FALSE: The ATTRIB command very rarely halts the spread of viruses.

7. VIRUSES CAN INFECT WRITE-PROTECTED DISKETTES.

   FALSE: Since viruses can modify read-only files, people tend to believe they can also modify write-protected floppy diskettes. The disk drive senses a protected diskette and refuses to write on it. This is controlled by the hardware. You can physically disable an IBM PC drive's write-protect sensor, but you cannot override it with a software command.

8. ANTIVIRUS SOFTWARE WILL PROTECT ME FROM ALL VIRUSES, ALL OF THE TIME.

   FALSE: There is no such thing as a foolproof virus protection program. New viruses are constantly being designed to bypass them. Antivirus products are constantly being updated to protect against the latest virus threats. The best protection is a security policy and a system for protecting yourself from virus threats. Use a good set of backups as your first line of defense. Rely on antivirus software as a second line of defense.

From the Chalkboard

Thinking you will get a virus from opening and reading text e-mail is like thinking you will catch a cold from someone by talking on the phone with them.

If you have Microsoft Internet Mail or Netscape Mail in their native version (i.e. unmodified and virus free), you cannot get a virus by opening and reading an e-mail message. Attachments (called applications in posts above) are not launched unless you double click on them. Do not double click on these attachments unless you trust the sender and are expecting the file. And even then, you should run a virus checker program just as you would any programs you download off the internet.
The "from" address in e-mail can be faked. If you get something from Microsoft about a bogus virus forget it. Watch The Site or read one of the links John posted about viruses.
Also, if someone were trying to spread a virus through e-mail don't you think they would change up the subject line?

Lets' review
- You can't get a virus from text only e-mail
- It is ok to open e-mail
- You can get a virus from attachments
- It is not ok to open attachments unless you know what it is and trust the sender

- Run a virus checker on any programs you download off the internet or receive as
an attachment to e-mail
- "From" addresses can be faked
- Don't believe everything you read in e-mail
- Someone smart enough to write a virus wouldn't use the same tell-tell subject line

A final note:
If someone were gonna make a for-real e-mail text virus they would put it in a message titled "VIRUS ALERT" and make it look like it was from your friend (or Microsoft).

Tel: **647 288-2882**