# Viruses online and offline

## and dealing with them when they infect

@bsolute
pc solutions

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

- Avoid attachments with extensions of type (.exe, .zip, .bat).
- Keep the OS (Operating System) and 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 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/movies/music from programs such as ***Bittorrent***. 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 DVD or USB drive that has been used in another computer BEFORE using it in your computer.
- ALWAYS check sites such as www.snopes.com so as not to proliferate a hoax yourself.
- Text only emails are safe to open.
- Make a complete backup of your system when it is performing well (preferably on an external HD or Flash Drive) and keep it in a safe place. You might want to keep 2, 3 or more copies of your files in different drives now that storage is quite cheap.

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.
- If the threat looks serious shut down your system immediately and call for professionals support as some hijacking software do more damage with time.
- 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 external drives that you use after cleaning the computer.
- Notify EVERYONE you may have shared any files with.
- Disconnect any backup drive attached to the computer.
- Don't backup your files until your system is clean.
- Never assume a system is clean just because you haven't seen any further signs in a day or two.

Ten Common Virus Myths

1. VIRUSES CAN HIDE INSIDE A DATA FILE.
   FALSE: Data files such as (Music, Pictures, Videos) can not spread a virus on your computer. Only executable program and macros files can spread viruses. 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, run a virus scan on the zip file before opening and even better if you don't have to or don't know what this zip file is about just don't open it.
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 a smartphone, nor can it infect an Apple Mac. MS Office macro viruses are an exception. Macro viruses can spread on any platform that runs Microsoft Office.
5. MY BACKUPS WILL BE WORTHLESS IF I BACKUP A VIRUS.
FALSE: Suppose a virus is backed up with your files. If you had a file infecting virus, you could restore important documents, databases, and your data, without restoring an infected program by first cleaning your system and then doing a scan on you backup drive.
6. READ-ONLY FILES ARE SAFE FROM VIRUS INFECTIONS.
FALSE: The ATTRIB command very rarely halts the spread of viruses.
7. 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 use GMail, you cannot get a virus by opening and reading an e-mail text message. Attachments 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 posted about viruses.

Iif 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).