10:00 AM: Antivirus software updates its definition files, and possibly notifies you of such, making you feel a little more at ease. *What it doesn't tell you is: This update ONLY protects you from known viruses prior to the 10:00 AM update.*

11:00 AM: A new virus is introduced and implanted into a poisonous website, email, etc. Anti-virus companies have not found the "cure" yet. *So, your computer is not protected against this virus, and if you happen upon this avenue, your computer could get infected.*

Most infections attack the computers Windows Sockets (winsock), thus **disabling your computer's ability to browse the internet, receive further antivirus updates, hijacking your homepage, etc.** In some cases, it disables the task manager and can even hide and or delete all of your files. Often times, bogus (rogue) anti-virus looking software opens and pretends to tell you that you are infected, wanting you to purchase protection. If you do this, your credit card information can be compromised.

Additional Information:

Although most viruses have similar characteristics and heuristic behaviors, anti-virus software can possibly detect these behaviors and put the files in a "suspicious" location, often referred to as the quarantine until user interaction is taken.

Some infections are not actually from a virus. They can also be from Malicious Software sources (known as malware), spyware, adware, root-kits, etc. In some instances, these "non-infections" can morph themselves into viruses if not addressed quickly enough.

Examples of virus transmittal:

The following list contains a few examples of potential transmission methods that can contain "poisonous" code, aka computer viruses, malware, spyware, etc.

- Pornographic websites
- Game / Game room websites, chat rooms, etc.
- Emails containing "zip", "com", "exe" and other file attachments
- Programs that allow the free download of software, music, movies, etc.
- Social Networking websites with the installation of certain 3rd party applications
- Bogus pop-ups informing you that you have "won" something
- Websites not originating in the United States

Recommendation:

It is the recommendation of Ozark Computer Works to run two software suites. One to catch the Malware, spyware, etc. before it has a chance to morph into a virus. Another to catch and remove viruses. We are here to help get your computer running back to normal and install the protection to help aid in keeping your computer clean.

Who creates these viruses?

It is illegal to create software that gets installed onto private computers without the owner's consent. Unfortunately, these American laws do not apply to "hackers" in overseas locations. Viruses are created by people with the full intention of being "mean", and with the purpose of stealing information, causing harm and frustration. Hackers are in the USA too. Often, from people with nothing better to do with their time than to be mean. It is our opinion that this meanness is a form of terrorism. Every year, hundreds of American hackers are arrested for doing this, but the penalties of such acts are very minute at this time. There is no penalty at all for the hackers not in the USA because it is often impossible to track them down.