Computer Viruses: What are they, how do you know, and what can I do?

What is a computer virus?
A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be “infected”. Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

What can I do to protect myself?
The very first thing that every computer user should do, regardless of which computer or operating system you use, is to install an anti-virus program. There are many free programs available, but be sure to check which ones offer frequent updates to help keep you safe. Another sure way to cut your chances of obtaining a virus is to never open email attachments from someone you don’t know, or were not expecting to receive.

Several anti-virus products have a feature that will scan incoming emails and attachments. Lastly, be sure to backup all of your important files on a regular basis. If you are unfamiliar with installing software or making backups, your local computer repair center can help. The Virus Bulletin (www.virusbtn.com) offers a list of viruses that are known throughout the computer world. The site also offers the opportunity to report viruses, should you be unfortunate enough to encounter a new one firsthand.

How does Amplex know I have a virus on my computer?
You may have received a phone call or email notice from Amplex stating that we have a concern about your computer containing a virus. There are many viruses, malware, spyware, and things called “botnets” that take control of your computer and use it to redirect and transmit information to various websites. They can run in the background without notice, thus slowing down your computer’s applications and web browsing.

A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task. Although such a collection of computers can be used for useful and constructive applications, the term botnet typically refers to a system designed and used for illegal purposes. Such systems are composed of compromised machines that are assimilated without their owner's knowledge. The compromised machines are referred to as drones or zombies, the malicious software running on them as 'bot'.

Several agencies, in an effort to thwart these attacks, have setup decoy servers called Honeypots. A Honeypot is a computer resource whose only purpose is to get exploited. It is a trap, but for computer criminals. An attacked and properly investigated Honeypot can provide valuable information about both the attack, and the attacker. No information about the end-user is reported, but the victim’s IP address is reported to Amplex. Once we receive this report, we contact our customer to let them know that their computer is infected, and they can take the necessary steps to remove the virus or botnet. Neither Amplex or the Honeypots track which sites a customer is viewing, nor is any user privacy information known. Fortunately, we do know the IP address of the victim so we can notify them to clean their computer of these unwanted files.

Who can help clean and protect my computer?
Amplex can recommend a number of local computer repair centers that can help you with cleaning viruses, file backups, hardware upgrades, and much more. We can also recommend websites and information on removing specific viruses.