



Virus Detection and Prevention Tips



- 1. Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
- 2. 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.
- 3. 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.
- 4. Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and a 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.
- 5. Update your anti-virus software regularly.** Thousands of viruses are discovered each month, so you'll want to be protected.
- 6. 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. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
- 7.** When in doubt, **always err on the side of caution** and do not open, download, or execute any files or email attachments. Not executing the files is especially important. Check with your product vendors for updates which include those for your operating system web browser, and email. One example is the security site section of Microsoft located at <http://www.microsoft.com/security>.
- 8. Stay away from Bit torrent sites.** Some of the more popular ones include Limewire, BitTorrent, Frostwire and Pirate Bay. These are heavily laden with viruses, malware and spyware. Downloading material from these websites is one of the easiest ways to become infected. It's in your best interest to just avoid these websites completely.
- 9. Be careful** when searching on the internet, the links that come up from your search engine may contain a virus. Never go to sites that sound suspicious.
- 10.** Due to the popularity of the social networking websites such as MySpace, Facebook, and Twitter, virus makers target them more than any other website. Online gaming and gambling websites also are high risk websites. **It's best to avoid these kinds of websites altogether.**
- 11.** If you happen to see a popup message when on the internet about being infected and to buy their software to protect yourself, do not fall for it! Most of the time these messages are easy to see as they tend to have bad grammar and spelling errors. Common names are XP Antivirus, Security Tools, ThinkPoint, Security Shield, Win 7 Security 2011, and similar variations. If do see one of these popups, do not click on them, **immediately shut down your computer. If you click on any part of those windows you will give the virus permission to install and bypass your antivirus program.**
- 12.** If you see any suspicious pop-ups appear on your screen, **do not click on them.** If you do, it is very likely you will infect your computer. Instead use the following keyboard command, which will allow you to close the pop-up, without having the click on it or infecting yourself. The keyboard command is **ALT + F4.** If that fails, then shut down the computer.
- 13.** If you are in doubt about any potential virus related situation you find yourself in, please do not hesitate to contact us here at Computer Resources. Our phone number is **719-471-9066** and we will answer any question you may have.