

Virus Detection and Prevention

Do not download any files from strangers.

Do not open any files attached to an E-mail from an unknown, suspicious or untrustworthy source.

Do not open any files attached to an E-mail 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 E-mail. Better be safe than sorry and confirm that they really sent it.

Do not open any files attached to an E-mail if the subject line is questionable or unexpected. If you need to do so, always save the file to your hard drive before doing so.

Delete chain E-mails and junk E-mail. Do not forward or reply to them. These types of E-mail are considered Spam, which is unsolicited, intrusive mail that clogs up the network.

Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an antivirus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own antivirus software.

Update your antivirus software regularly. New viruses are discovered each month, so you'll want to be protected. You may also need to update the product's scanning engine as well.

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.

When in doubt, always use caution and do not open, download, or execute any files or E-mail attachments.

Always Check with your product vendors for updates which include those for your operating system, web browser, and E-mail software.