Viruses and Malware

In the past month, ITS has seen a dramatic increase in reports to the Help Desk of faculty and staff experiencing serious issues with their computers due to virus and malware infections.

What can you do to protect yourself from viruses and malware?

1. Be VERY suspicious of any email, website, or web pop-up that asks you to download a file or document or to click links to websites.
   - If you receive an unexpected email that includes links, **do not click the links** until you have verified the message with the sender.
   - It is preferable to **type the url for the party's original website** into the browser instead of clicking a link from an email.
2. **Read emails very carefully – even when they appear to come from legitimate organizations**, including those with whom you have a relationship, like your bank, Amazon, or PayPal. The sources of malware are designed to look legitimate, but the links in the messages, behind the scenes, may actually direct you elsewhere to unsafe sites. As noted above, it is better to type the url into the browser rather than click a link.
3. You may need to **upgrade your browser**. For those who use the Internet Explorer browser, it is imperative that you make sure you are running version 7 or 8. Version 6 is no longer supported and is very vulnerable to virus/malware attacks. If you are still running IE6, please go to the ITS website and upgrade to version 7. Go to www.baylor.edu/its => Help => Software Installer.
4. **Call the Help Desk**. If you are unsure of the source of a file or why you are being prompted to download it, odds are good that it could be a virus/malware. When in doubt about what to do or how to upgrade Internet Explorer, call the ITS Help Desk at (254) 710-4357/HELP.
5. For more information on malware, review the September 2009 BearAware Bulletin. To view this, go to www.baylor.edu/its => Security => BearAware => BearAware Bulletin.

Thank you for your diligence.
ITS