

End User Issues

From SANS:

- 1) Failure to install or keep up to date anti-virus software and signature files.

The virus protection software needs to be continually updated because as time goes on more “exploits” are found and subsequent traps are developed (by the vendors). You must keep a vigil toward maintaining a “current system”, most of these softwares can be set to automatically maintain themselves when you connect to the internet but the user needs to verify the software is always taking the action.

- 2) Opening unsolicited e-mail attachments (executing games, screen savers, etc.) without verifying the source and checking the contents.

This is just common sense but you also need to be aware that some email worms are able to “spoof” a trusted friend’s email address making it look like a friend rather than a stranger sent the file attached to an email. Be wary and safe, if in doubt email the friend to verify this is an OK file ***BEFORE*** opening the file.

- 3) Failing to install critical security patches – especially for Microsoft Operating Systems, Microsoft Office, Microsoft Internet Explorer, and Netscape

The operating systems (OSs), particularly Windows, and other software need to be continually updated because as time goes on more “exploits” are found and subsequent patches are developed (by the vendors). You must keep a vigil toward maintaining a “current system”, most of these OSs can be set to automatically maintain themselves but the user needs to verify the software is always taking the action.

- 4) Not making and testing backups

Taking a periodic backup of your entire system or at least all of your personal accumulated documents (word processing, spreadsheets, filed email, etc) so that you can restore if a system is compromised (viruses) or breaks (hard disk failure, etc.) is also common sense. The time interval of performing the backup can vary but having a “clean” set of files to restore, even if they are a month old, is extremely important. Keeping that backup media (Zip disks, CDs, etc.) at an alternate physical site such as your office or home is smart too.

- 5) Using a modem while connected through a local area network.

When you connect to two networks you risk getting an infection from one network connected system to another. Simply avoid doing this as much as possible.

Other concerns:

- 7) Password management ***DON'Ts***:
 - a) Creating passwords that are easily guessed
 - b) Failure to change on a routine basis
 - c) Writing down password and displaying them in plain view of others
 - d) Using university passwords on other systems
 - e) Sharing your password with anyone (including technical staff)
 - f) Using un-encrypted passwords from locations outside of UNI– home, cyber café's, other places of work.