PATCHES

Patches are software add-ons designed to fix software bugs, including security vulnerabilities, in operating systems or applications.

Patching for new security vulnerabilities is critical to protect against malware. Many high-profile threats take advantage of security vulnerabilities. If your patches are not applied in a timely manner or not up to date, you risk leaving your computer open to hackers.

PATCHES ARRREN'T JUST FOR PIRATES!!!

Many software suppliers routinely release new patches, with Microsoft issuing fixes on the second Tuesday of each month ("Patch Tuesday"), and Adobe issuing quarterly updates to Adobe Reader and Acrobat on the second Tuesday after a quarter begins.

To stay abreast of the latest vulnerabilities and patches, subscribe to vulnerability mailing lists. Most reputable vendors offer such a service.

Apple OS X users can click the Apple logo in the upper-left corner of their desktop and select Software Updates.

For example, Microsoft security information is available at www.microsoft.com/technet/security/bulletin/notify.mspx. Microsoft Windows home users can use Windows Update (Windows Vista/7) or Security Center (Windows XP) to turn on automatic updating.

Organizations should make sure that all computers connecting to their network abide by a defined security policy that includes having the latest security patches in place, including for operating systems and applications.

Image Source: www.mcafee.com

◼ End of Transmission…

Information Security: It's a Shared Responsibility