Windows/PC and Apple/Mac Best Practices

This month, our campus CISOs offer some best practices to prolong the life of your computer and keep your personal information safe.

**BOTH**
- Ensure software updates are current.
- Install antivirus software, keep it current, and scan weekly.
- Create an additional non-administrative account for daily use. Remember: Admin or root accounts are for tasks, not browsing the network and reading email.
- Disable automatic login & Guest accounts.

**WINDOWS/PC**
- Regularly install updates to both the Windows operating system and all installed applications (Adobe products, Office, Java, etc.).
- Use Firefox with Ad-Block & NoScript extensions, or Google Chrome, or the latest application compatible version of Internet Explorer and understand the security features.
- Browse with tools such as Site Advisor or Web of Trust (WOT).
- Clear cache and temp files with CCleaner and run malware scans.

**APPLE/MAC**
- Turn on the firewall.
- Use the OS X screensaver with a password: This habit ensures that your machine remains inaccessible whenever you’re away from the keyboard by requiring a password after sleep or screen saver begins.
- Enable auto locking of your login Keychain.
- Turn on File Vault.
- Use secure virtual memory, e.g. iCloud and back up regularly.
- Use a strong password for your local account: A strong password has a minimum of 8 characters, usually mixed case and alphanumeric.