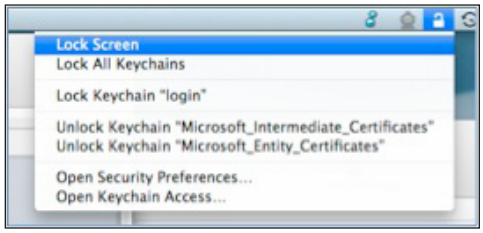
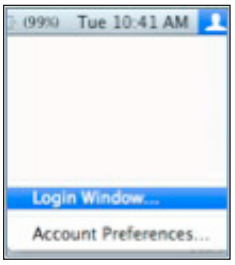
bearaware
Information Technology Services
Security Bulletin
September 2009 Volume 1, Issue 4

Locking Macintosh Screens

It is important to lock your computer screens if you walk away from them, even for a short time. The process on a Windows PC is to either press the Ctrl/Alt/Delete keys together and then press Enter, or to press the Windows key and the "L" key at the same time. With an increasing number of Macintosh computers on campus, it is also critical to understand how to secure them against misuse. Do one of the following to lock your Macintosh screen:



Option 1



Option 2

Option 1: The preferred method is to select "Lock Screen" from the menu that appears when you click the padlock icon in the Menu bar at the top of your Macintosh screeen (see below). If the padlock icon is not visible, launch the KeyChain Access Application, which is located in the Utilities folder within the Applications folder. Choose "Preferences..." from the KeyChain Access menu and Select "Show Status in Menu Bar."

Option 2: Locate the Profile icon in the Menu bar on the top of your Macintosh screen. Select "Login Window" from the drop-down Menu.

Upcoming BearAware Campaign

ITS will conduct the annual observance of October as National CyberSecurity Awareness month. This will be the third year Baylor ITS has participated in this observation. Scheduled BearAware activities for October include:

bearaware
http://www.baylor.edu/bearaware/

- A brownbag luncheon on identity theft
- Dr. Pepper hour in Bill Daniel Student Center with the chance to view award-winning videos made by college students
- A free PC health check event in Bill Daniel student center
- A variety of promotional items
- A special speaker on malware (see below)
- Creative posters emphasizing the reality of identity theft on our campus

Watch for more information on this year's BearAware campaign in the coming days and plan on taking advantage of these important educational opportunities. And - look for this year's posters and screensavers around campus! Visit http://www.baylor.edu/bearaware/ for more information.

Malware

The term "malware" stands for malicious software and, yes, it's bad for your computer. Malware is software designed to penetrate a computer without the owner's knowledge. It includes a variety of hostile, intrusive, or annoying program code such as viruses, worms, rootkits, spyware, trojan horses, fraudulent adware, etc. Malware can hijack your browser, cause endless pop-up ads, redirect search attempts, track websites you visit, and make your computer unstable and/or slow enough to be unusable.

The most common way to get your computer infected with malware is through email or the Internet. The sources of malware are designed to look legitimate. So, be suspicious of web pop-ups asking you to download something or emails asking you to click a link that you weren't expecting. While not foolproof, having up-to-date virus protection will assist in preventing malware infections. In addition, keeping operating systems and applications patched will help to prevent malware. 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 malware. When in doubt about what to do, call the ITS Help Desk at (254) 710-4357 (HELP).

Follow us on Twitter at http://twitter.com/BaylorITS_Alert to receive notifications when there are issues and network outages.