bearaware
Information Technology Services
Security Bulletin
September 2010 Volume 2, Issue 4

2010 BearAware Campaign

In October, ITS will once again lead the campus in the annual observance of National CyberSecurity Awareness Month. Watch for posters, lab screen savers, and Lariat ads containing reminders and information about good information security practices. Come to the BearAware Dr. Pepper Hour October 5th 3:00 PM in the Barfield Drawing Room to pick up some cool giveaways and learn more about the BearAware program. Also, check the BearAware website (www.baylor.edu/bearaware), FaceBook, and Twitter (bearaware) for additional info about October's planned activities like a PC health check event and enlightening security webinars.

Understand PCI Compliance

The Payment Card Industry (PCI) Security Standards Council has developed a set of financial and information technology standards to protect credit cardholders' data. As an entity that accepts credit cards for various events, goods, and services, Baylor must be compliant with these PCI regulations, which involve stringent standards regarding manual and electronic handling and processing of credit cards. Over the last year, much has been accomplished towards this goal, but work remains to be done. Please see the University's PCI website www.baylor.edu/pci for information about this important project and to understand how PCI compliance might relate to you personally and to the work of your department.

Found An Abandoned Flash Drive?

Flash drives are great – they are a small and convenient method to store, backup, and transport data. But sometimes they are not so great – they can carry viruses and malware that can compromise your computer and the Baylor network. Plugging in an unknown USB device can be dangerous, so don't risk it. If you find a flash drive that appears to have been lost, please send it to ITS for processing. Put it in an envelope and drop in campus mail addressed to the ITS Help Desk, One Bear Place #97268. We will securely examine it for infections and, if appropriate, review it for data that should be returned to the proper party.

A real world example of the dangers of unknown USB drives: http://www.safeinternet.org/blog/malware-riddled-flash-drive-created-worst-us-military-breach

Check that URL!

We've all seen the warnings about phishing scams through emails. One of the tactics used in these schemes involves the url, or web address, to which the message directs you. The phishers will try to deceive you with a link in the email by making it appear to belong to a valid organization, by slightly misspelling a word in a valid url, or by using subdomains in the address. Here are some examples:

www.citibank.online.com – Appears to go to the "online" section of the Citibank website but actually points to the "citibank" section of the online.com website.
www.baylor.edu/directory - Valid link text used in a message which should take you to the Baylor online directory but the actual address to which the link takes you could be a phisher's address like www.balor.com/directory.

Most applications will display the true address to which you will be directed if you use the cursor to hover over a link printed in a message. Always check this and always check the actual address displayed in the browser address bar.

For More Assistance

For ITS on Twitter (@BaylorITS_Alert) to receive tweets on technology outages and call the ITS Help Desk at extension 4357/HELP for questions related to these or other campus security or technology issues.

BAYLOR UNIVERSITY
INFORMATION TECHNOLOGY SERVICES
One Bear Place #97268, Waco, Texas 76798-7268 • www.baylor.edu/its/ • (254) 710-4357