March 2006
Volume 1 Issue 4

www.purdue.edu/securePurdue

SECURE PURDUE NEWS

All the news that's secure to print.

SECURITY TIPS

Back up the data on your mobile devices to a secured location.

Possible ideas are recordable media (CDs or DVDs) stored in a locked drawer or a password-protected flash memory device.

Wireless communications: enjoying it safely

Wireless communication is convenient, and available almost anywhere. While there are many modes of wireless communication, here are some of the most common:

Bluetooth
Bluetooth is a wireless, "cable replacement" technology that operates over short ranges, typically about 30 feet. Bluetooth allows PDAs, cell phones, computers, printers, and other portable devices to connect easily with one another only within a person's wireless personal area network (WPAN).

WiFi
Also known as "Wireless Fidelity" or "Wireless Networking," WiFi refers to wireless digital networking technology. Many public places, such as hotels, coffee houses, airports, etc., offer public access to WiFi network "hotspots" so people can access the Internet. WiFi hotspots are limited to a maximum distance of about 300 feet, making WiFi a wireless local area network (WLAN).

WiMax
Similar to WiFi, WiMax provides greater coverage distances than WiFi technology. WiMax provides broadband wireless access for up to 30 miles for fixed access points, creating larger, wireless metropolitan area networks (WMAN).

In addition to its obvious advantages, wireless technology also poses a number of security challenges. The portability, connectivity, data storage, and power that make mobile computing devices so useful also make them targets. Mobile computing devices are small and easily stolen, connect freely with unknown wireless devices, and often feature weak user access mechanisms that are easily compromised or disabled by the user.

The following are simple actions that can do much to secure mobile devices:

- Disable wireless connections when not in use to prevent attempts at unauthorized access.
- Configure devices to ask before connecting to wireless networks.
- Password protect devices to prevent unauthorized use.
- Immediately cancel communications services for lost or stolen devices.
- Never use automated login scripts; they allow thieves access to accounts.
- Always encrypt confidential information stored on mobile devices.
- Keep mobile devices close by or store them in a secure location when not in use.
- On computers, install and use current anti-virus software and all software updates and patches. Enable hardware and software firewalls.
- Exercise caution when accepting PDA applications sent wirelessly. Accept and open only known applications and MMS attachments.

For more information about secure e-mail at Purdue, visit the SecurePurdue Web site at www.purdue.edu/securePurdue.

FROM the interim CISO

By Scott Ksander, Interim Executive Director of Networking and Security

I am fond of saying that responsible computer ownership is like responsible car ownership. This analogy works well when talking about patching a computer's operating system and applications.

For instance, most cars require a "routine" oil change and have a "check engine" light that appears when it needs immediate attention. Computers run on the same basic principle: Computer users must remember to patch often-used, popular applications on a regular basis and must also be prepared to apply critical operating system patches when the computer's "check engine light" appears.

In Windows, the "check engine light" is the "Windows Update" or "Automatic Updates" feature. This feature alerts you to critical security patches for Windows operating systems. These patches often need to be applied quickly to fix known vulnerabilities. To learn more about this service, visit http://www.purdue.edu/securepurdue/docs/automaticUpdates.pdf. Apple OSX users should install security updates when prompted by "software update," or by visiting http://www.apple.com/support/downloads.

Application patching, however, requires the computer user to remember to look for new patches on a routine basis. You will want to regularly check with the manufacturer of popular applications, such as word processors and IM clients, for patches to the software. For instance, Microsoft Office updates are available at http://office.microsoft.com.

Like car maintenance, basic patching maintenance will help your computer run better and last longer.

Thanks for helping spread the word, and be careful out there!

"Oh, the usual stuff. Spam from the Joker, another e-mail virus from the Penguin, an illegal chain letter from Cat Woman...."

Spotlight :
Purdue-board

Use Purdue's newest electronic message board, Purdue-board, to see notices about things going on all over campus, including ITaP and ITSP. Visit www.purdue.edu/eboard today!