http://security.bsd.uchicago.edu

In this issue of the BSD ISO Cybersecurity Newsletter…

- **The Wi-Fi Snooper –** Wireless networks are convenient, but they are also inherently insecure. Hackers can easily snoop insecure wireless networks to steal confidential data and/or your personal information. Please read the following story about how student Jennie Parker narrowly escapes a cyber security incident.
- **BSD Information Security Standards –**The BSD Security Liaisons Group, consisting of IT professionals from the University of Chicago, BSD and UCM, has developed a new standard to assist with the inventorying and categorization of BSD information technology assets.

The Wi-Fi Snooper

Jennie Parker loved her new neighborhood coffee shop. When she needed to get out of the noisy, distracting environment of the laboratory and knuckle down on writing her thesis, it was the perfect retreat. Good espresso, comfy seats, friendly staff, and best of all, free Wi-Fi. The place was so chill, you didn't even have to ask for the password!

Across the coffee shop sat another regular visitor, staring deeply into his laptop. Max liked the cafe's password-free Wi-Fi too, though for completely different reasons. Using software he found on the internet, he could easily access all of the information sent to and from computers on the Wi-Fi. He could eavesdrop on the Internet connections from cafe shop patrons and screen information they sent. The place was crowded this afternoon, Max thought, and it promises to be a fruitful visit.

After staring at a blinking cursor for several minutes, Jennie decided she needed a break. Her roommate's birthday was coming up, and she needed to pick out a present soon. Maybe something from the yarn shop that just opened up downtown? Jennie went to their website, picked out some gifts, and was ready to enter her credit card, when she noticed something strange. Shouldn't there be a lock icon next to the site address in the browser?

Jennie heard somewhere that you shouldn't trust a site with your information if it was only "http," not "https." Oh well, so much for the yarn, she thought, and picked out a book from Amazon instead.

Preventative Measures

It is your responsibility as a user to exercise caution when connecting wirelessly. To learn about the steps you can take to safely use the internet on a public Wi-Fi network, visit BSD ISO Staying Safe On Wi-Fi

To learn more about the University's cVPN visit University of Chicago IT Services VPN/cVPN.

When Max noticed the woman at a nearby table pull out her credit card, he paid special attention to the Internet connection information popping up on his screen. Spotting the web address for a store, he was pretty sure a credit card number was soon to follow. But he winced when the user switched to an https site -- the subsequent data was encrypted, and thus impossible for him to crack. Not this time.

Back to work on her thesis, Jennie realized she would need to reference some data on her lab server. Dang it, she thought, I'm not ready to head back to the craziness of the lab just yet, and navigating to the server address from the cafe just brought up a forbidden access error. Then she remembered the UChicago VPN, a "virtual private network" to create a secure connection to the UChicago network.

By entering in her cNet ID and password (on a https site, she noticed), Jennie could access her data remotely and feel confident about its privacy. Relieved she didn't have to head back to her office just yet, she cheerfully ordered another coffee and dug back into her thesis.

Max perked up when he noticed some interesting traffic to university sites from the IP address he was watching for credit card information. Now he dug through the packets looking for passwords -- one slip, and he could access all of the user's private information and e-mails. But again he was foiled, as encrypted data showed up once again. "I guess people at this cafe are getting smarter," he thought, closing his laptop and sulking out the cafe door.

BSD Information Security Standards

The BSD Security Liaisons Group, has published the STA-05 BSD IT Asset Inventory and Categorization Standards. This standard is for creating a consistent inventory of IT assets, and categorizing these assets based on industry standards for information security. For more standards to secure your IT assets, visit our site at http://security.bsd.uchicago.edu/Security Policies.

What to do if you become aware of an information security incident?

Contact the BSD-ISO team via the following phone numbers or e-mail addresses:
You may also send an e-mail to the BSD Security mailbox: security@bsd.uchicago.edu
Visit the BSD-ISO website: http://security.bsd.uchicago.edu

Plamen Martinov, BSD Chief Information Security Officer	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu