RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

June 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 6

Inside this Issue:

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.

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.

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 BSD

VPN, a "virtual private network" to create a secure connection to the BSD network.

By entering in her BSD user name 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.

Preventative Measures

- To connect to a wireless network, you must first select the network you want to connect to. There are often multiple networks to choose from in crowded or public places. However, always be careful which networks you connect to. Cyber criminals can create counterfeit or fake wireless networks designed to harm or monitor everything you do. To protect yourself, always be sure you are joining a trusted Wi-Fi network. Otherwise, you have to assume that devices on non-trusted networks can scan, probe or hack any other device connected to that network. By making sure you only connect to trusted wireless networks, you protect yourself against these and other attacks.

- When working remotely, use the BSD's VPN (Virtual Private Network) to connect when using a wireless network other than the UChicago's. Click here to learn more about the BSD VPN. If your department is not currently participating in the BSD VPN, you can use the University's cVPN here.

- Finally, make sure your laptop and mobile devices are using is the most current version and has the latest patches and software. In addition, be sure your encryption software is installed and you have anti-virus running on your laptop.

UCM Data Guardian for Endpoints

The next phase of the University of Chicago Medicine's Data Guardian Program launches Thursday, June 30, 2016, with the Endpoint Protection Agent. The Data Guardian Program is a collection of processes, tools and real-time education aimed at helping you protect and make informed decisions when handling restricted data. Examples of restricted data include Social Security Numbers, Credit Card Numbers, and Protected Health Information.

The next phase of the Data Guardian program is designed to extend this protection to our CBIS protected endpoints. The goal of the endpoint technology is to help you identify restricted information and may alert you via a pop up before it leaves the environment. This will help you ensure you are moving these items based on an approved process or will allow you to stop the data transfer if it was unintentional.

Specifically, we are targeting the movement of restricted information to unencrypted thumb drives, and the use of specific "consumer" cloud applications, such as Google, Yahoo or Dropbox. Please note, we will not be blocking the movement activity. Instead, we will intercept the movement and may prompt the users to provide a justification for its movement. This can also include cancelling the transaction because they were unaware of the policy and risk.

The software agent will not be able to read content on your device. Instead, it will be searching for matches of various data points to alert you to potential accidental distribution of restricted information.

IF YOU NEED ASSISTANCE: If you are encountering a negative impact to your device or workflows, please contact the CBIS Service Desk at 2-3456 to report the issue. Make sure to visit the UCM Information Security Office section of the UCM intranet for more information on this program, the Data Guardian Tip Sheet and other projects to protect our patient and employee data.

Thank you, and remember we are all Data Guardians.

UChicagoBox BSD Group Folders

As part of the BSD Research-Centric Information Security Enablement (RISE) program, established to enable and protect the research and academic functions of the BSD, UChicagoBox Group Folders are now available to your departments. The purpose for this email is to provide you with information on how to request and set up a group folder for your department.

Background:
On December 15, 2015, the BSD Information Security Office introduced Individual UChicagoBox accounts to BSD non-clinical departments. Individual Accounts allow you to store and share files and folders but once you leave the organization the data in your personal UChicagoBox account will be automatically deleted 45 days after your departure.

To ensure collaboration continues, we are now offering BSD UChicagoBox Group Folders. A Group Folder is a special folder that any BSD individual with UChicagoBox access can request on behalf of his or her group, lab, or department and is co-owned by the BSD Information Security Office. This means that, once created, the Group Folder will remain active even if the user who requested it changes departments, closes his or her Individual UChicagoBox account, or leaves the BSD.

BSD UChicagoBox Group Folders are as easy to use as individual UChicagoBox accounts and are great for the day-to-day management of shared department data.

How to request your group folder:
If you would like a department or group folder, please submit the request form, including the names and contact information of the **2 administrators (required)** for the folder.

Please see the following information detailing what you need to know about UChicagoBox and how to get started with the Group Folders.

Getting Started (for Group Folder administrators):
After your Group Folder has been created for you, the BSD Information Security Office invitation to the folder will appear in your UChicagoBox Individual account. When you accept this invitation, you will be able to configure it for security and to set up permissions for your colleagues. For additional instructions on how to manage your group folder, click here.

For more information about UChicagoBox for the BSD, visit http://security.bsd.uchicago.edu/bsduchicagobox/. Send any questions and feedback about this new service to security@bsd.uchicago.edu.

Thanks, and happy sharing!

What to do if you become aware of an information security incident? Contact the BSD ISO Team via email at security@bsd.uchicago.edu.