RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

April 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 4

Inside this Issue:

USBs: Use with Caution

A recent study found that almost one in five people who found a lost USB stick in public used it in ways that posed cyber security risks to their personal devices, and potentially to work devices.

USB drives and devices are inexpensive, portable, and easy to use. These characteristics, however, also make USB devices attractive tools for attackers or thieves who use them in the following ways.

1. Attackers use USB drives to infect other computers.
Attackers leverage common plug-and-play components to run malicious programs or code, usually without the knowledge of the system user. The malicious software can then self-propagate by infecting other devices connected or networked to the computer.

2. Thieves use USB drives to steal large amounts of data.
Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

3. USB drives are easily stolen or lost.
The most obvious security risk for USB drives, though, is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. If the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data?

There are steps you can take to protect the data on your USB drive and on any computer that you might plug a USB drive into:

1. **Take advantage of security features**.
Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see BSD USB Encryption for more information).

2. **Use and maintain security software, and keep all software up to date**.
Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks. For detailed securing devices instructions, visit the BSD Information Security Guidelines and Procedures at **http://security.bsd.uchicago.edu/Security-Policies**.

3. **Do not plug an unknown USB drive into your computer**.
If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your department's IT custodian, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.

4. **Disable Autorun.**
The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows (link is external) , Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft® Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

Phishing Email Assessment and Prescriptive Education Initiative

We assess the BSD's understanding of cyber security as part of our ongoing security awareness program. In April, the BSD and UCM Information Security Offices kicked off a **Phishing Email Assessment and Prescriptive Education Initiative**. A phishing email assessment is a test email pretending to be a hacker, using the same tactics employed by the bad guys. The difference is these emails will not harm you in any way. They are designed to measure the organizations' awareness and help you learn how to identify these scams and protect yourself.

What Happened:

- We sent out a phishing test email titled "**Email Accounts Update Required**" to every BSD and UCM employee.
- If you clicked on the link in the phishing test email you were notified immediately that you were enrolled in a 15-minute Anti-Phishing Training.

What's Next:

- If you received a notification that you are enrolled in the Anti-Phishing Training, you can click here to login with your CNET or UCHAD ID and complete the course.
- ***For Internet Explorer Users:*** To complete the training you will need Internet Explorer version 9 or higher installed on your computer. If you need to update your IE browser, please contact your IT custodian.
- Results of this phishing test will be kept anonymous, and supervisors will not be permitted to see the results.

Visit http://security.bsd.uchicago.edu/phish/ for more information on the Phishing Email Assessment and Prescriptive Education Initiative.

BSD VPN Now Available

The Biological Sciences Division (BSD) Information Security Office, in collaboration with members of the CRI, PHS and ITS, is proud to announce a virtual private network dedicated to the BSD's staff, researchers and collaborators.

The BSD Virtual Private Network (VPN) provides BSD staff; researchers and collaborators a secure means for access to University network resources, no matter where they are in the world.

The **BSD VPN**:

- **Enables** employees and collaborators within the BSD to securely access Systems hosted on the university network.
- **Protects** the BSD by providing improved security; requiring two factor authentication as a default security setting.
- **Streamlines** access for BSD resources by simplifying credential requirements.
- **Extends Access** to research collaborators and BSD entities that would not otherwise have remote access because they lack CNET IDs.

Steps to follow for using the BSD VPN.

Step 1	Check this page to see if your department is participating. If your department is listed as "unknown," please consult with your local IT administrator for further details.
Step 2	Enroll in the BSD Two Factor Authentication.
Step 3	Install Cisco AnyConnect (BSD VPN Tool) at https://bsdvpn.uchicago.edu.
Step 4	Connect to the BSD VPN. If needed, consult the appropriate instructions for Mac or Windows.
Step 5	Go about your regular routine as if you were in the office.

Visit http://security.bsd.uchicago.edu/bsdvpn/ for more information about the BSD VPN.

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

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.