RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD Information Security Office Cybersecurity Newsletter

October 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 10

Inside this Issue:

National Cyber Security Awareness Month 2016

We would like to thank everyone who participated in our NCSAM activities in October.

Cybersecurity Awareness Fair

Encryption Poster Posting Contest Winners

For our encryption poster posting contest we have 2 winners. The 1st Place winner with a $100 Amazon Gift Card is Gina Duran and the second place winner is Elisabeth Sveen for a $75 Amazon Gift Card. The poster can be found on our website here: http://security.bsd.uchicago.edu/wp-content/uploads/sites/2/2015/09/BSD-ISO_Encryption_Poster.pdf

Securing Your Devices

The BSD Information Security Office wants to help protect you from any accidental confidential information disclosure and, in collaboration with the BSD Security Liaisons Group, developed the Securing Devices Guidelines. The enclosed Securing Devices Top 10 list provides a snapshot of the Securing Devices Guidelines with instructions on how to ensure greater security for your personal device(s).

Personal computing devices are becoming more and more portable and securing the sensitive information stored on those devices is more important than ever. Don't ever say "It won't happen to me". We are all at risk and the stakes are high - to your personal and financial well-being, and to the Biological Sciences Division's standing and reputation. Can you check off any of the following Top 10 securing devices guidelines that protect your devices and information?

Securing Devices Top 10 List

1. Use a Password and Screensaver
2. Install and Use Anti-Virus Software
3. Enable Built-In Firewall
4. Encrypt Your Hard Drive
5. Install UChicago VPN (Virtual Private Network)
6. Keep your Operating System and Applications Software Up to Date
7. Enable Web Browser Security Settings
8. Be Aware of the Treatment of Confidential Information
9. Backup your Data
10. Report Security Incidents

The following table provides general instructions on how to implement the Top 10 securing devices guidelines. For detailed securing devices guidelines instructions, click the icon for your specific device below or visit the BSD ISO website at http://security.bsd.uchicago.edu/Security-Policies.

Instructions for Securing Devices - Top 10 List

#1 - Use a Password and Screensaver

Choose a strong password to access your device. Require the password when your device sleeps or the screen saver is activated. Do not allow automatic login. Set your screen saver and require your password to unlock it.

#2 - Install and Use Anti-Virus Software

Download Symantec Endpoint Protection. Log in using your CNetID and password and download the file. Extract the zip file, open the extracted file(s), and follow the instructions.

#3 - Enable Built-In Firewall

Macintosh, Windows, iOS and Android devices have built-in firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.

#4 - Encrypt your Hard Drive

Visit the BSD ISO Website at http://security.bsd.uchicago.edu/encryption/ for more information on encrypting your devices.

#5 - Install UChicago VPN (Virtual Private Network)

Install cVPN software if you expect to use untrusted networks (such as guest wireless in a hotel or coffee shop). UChicago students, researchers, faculty, and staff can download and install cVPN by visiting cvpn.uchicago.edu.

#6 - Keep your Operating System and Applications Software Up to Date

Turn on automatic updating to keep your operating system and applications updated to the latest version of the release. This provides you with security updates and other improvements.

#7 - Enable Web Browser Security Settings

Choose web browser security settings that protect your privacy and enhance security. Learn more about security features in Internet Explorer, Firefox, Safari, and Chrome.

#8 - Be Aware of the Treatment of Confidential Information

Be aware that the University is bound by law or contract to protect some types of confidential information and in other instances the University requires protection of confidential information beyond legal or contractual requirements as an additional safeguard. Refer to HR Policy 601 - Treatment of Confidential Information.

#9 - Backup your Data

Backing up your machine regularly can protect you from the unexpected. Always keep a backup copy of files you do not wish to lose.

#10 - Report Security Incidents

If you use your computer to maintain or access sensitive institutional data and it is lost or stolen, inform your Manager, IT custodian and send an email to the BSD Information Security Office at security@bsd.uchicago.edu.

IT Security Service – BSD Security Assessment and Authorization (SAA)

Have you ever asked?

- Is my **existing or new system** secure?
- Is my research data safe?
- How do I obtain security configurations for grants or IRB approval?

If so, the BSD Information Security Office (ISO) can assist you with identifying security requirements with your project and ensure that these systems are protecting your data through the newly established Security Assessment and Authorization (SAA) service.

Background:

Prior to the development of this SAA service, there was no clear understanding of the security risks of many BSD information systems. The lack of clear understanding of security risks leaves the BSD systems vulnerable to cyber security attacks. To address this gap, the BSD ISO established a working group consisting of University of Chicago stakeholders to develop the risk-based BSD Security Assessment and Authorization (SAA) service. The SAA process provides a consistent approach for identifying and quantifying security risks of information systems supporting academic and research activities and to provide the BSD with a better understanding of the security risks within the BSD network.

The SAA process consists of four phases:

- Data Gathering
- Consultation
- Risk Analysis
- Authorization

The BSD ISO will work with IT staff responsible for the information system to gather information and assess whether the system is secure for your research project.

Getting Started:

To request a Security Assessment and Authorization for your system, please visit the BSD ISO website at security.bsd.uchicago.edu and click on '**For Faculty and Staff'** and then '**BSD Security Assessment and Authorization (SAA)'** for instructions, guidance and the SAA MS Excel based tool used for gathering information. You can download the Data Gathering Form to send to the BSD ISO to initiate the process.

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

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