http://security.bsd.uchicago.edu

In this issue of the BSD ISO Cybersecurity Newsletter…

- **Safe Browsing –** So many people around the world use and depend on browsers for their daily Internet activities, your browser is also a primary target for cyber criminals. Read the following story about how to safely browse the Internet (*Page 1*).
- **What's NEW …**
  - **Security Policies -** The BSD Information Security Office (ISO), UCM and University Information Security Offices have collaboratively developed a set of cyber security policy documents, which are open for comments through August 4, 2015. See the Policies section for more information (*Page 2*).
  - **Security Standards** – The BSD Security Liaisons Group published a Media Sanitization Standards. This standard defines the accepted practices for permanently deleting information when throwing away or repurposing devices used at work. See the Standards section for more information (*Page 2*).

Safe Browsing

Hi there, I'm the shared computer, that old thing sitting in your lab, your office suite, or the nearest library. You probably don't think about me very much -- I'm a big, clunky desktop in the age of near-weightless laptops and smartphones, and I run a little too slow for modern tastes. People only use me for the simplest of tasks: checking their e-mail or Facebook, paying a late bill, buying their mom a present. But you'd be surprised -- maybe even disturbed -- at the things I remember after years of people typing their passwords into me and reading their most secret and valuable information on my screen.

For one, you'd be surprised at how many people don't remember to logout of their accounts before they stop using me. Seriously, just closing the window doesn't work all of the time, you have to hit that little logout button, or shut down the whole browser software completely. When the next person comes along and opens a new browser window, they can stumble right into the earlier user's e-mail, bank account, or other private pages. Now, I've seen some pretty funny social media pranks when a colleague posts something ridiculous from their unsuspecting co-worker's account. But if someone with less scruples is the next person to use me, that's not a laughing matter.

Preventative Measures

It is your responsibility as a user to exercise caution when browsing the Internet. To learn about the steps you can take to safely browse the Internet, visit BSD ISO Safe Browsing Poster.

For more information, visit the US Computer Emergency Readiness Team (US-CERT) Tip page at https://www.us-cert.gov/ncas/tips and the Safe Browsing section.

Web browsers today are also capable of a pretty long memory when it comes to passwords. When Chrome or Firefox offers to remember your password on your personal computer, it's a convenient, time-saving feature. But on public or shared computers like myself, clicking 'OK' to remember passwords is just about the worst thing you could do. Even if you logout (good job!), those remembered passwords will still auto-fill for the next person to visit that login page.

Beyond passwords, my web browser can also remember all sorts of other stuff about what you did while using me. In normal mode, I'll remember all the websites you visited, cache the images you saw, even keep a record of the things you searched for. I'm not going to judge how you spend your time on the internet (though it should follow the University's internet policies, of course), but do you really want everyone else who uses me to be able to find that information? You can keep the browser from remembering these details by browsing in "private mode," or by clearing cached or temporary files and cookies when you're finished.

Then there's the matter of keeping my plugins up to date. Nobody likes those annoying pop-up reminders to download and install the latest version of Java or Adobe or some other software, and on a shared computer, hardly anyone will take the time to follow through on the update. The thing is, those updates keep hackers from exploiting security holes to grab the kind of private information I was talking about before. Without them, I'm liable to blab about your secrets to any hacker who asks...I just can't help myself.

Gosh, this isn't a very flattering portrayal of myself. I'm useful, I swear, don't pull the plug on me! All you need to do is follow these few simple steps when you use shared computers like me, and use common sense. Like any shared resource -- a public bathroom, the office kitchen, the subway -- you'll be much better off if you remember that many strangers have used me already, and many more will do so in the future.

Information Security Policies

The BSD, UCM and University Information Security Offices have collaboratively developed a set of cyber security policy documents that will direct and guide our organizations through the new landscape of cyber security threats and regulations. The BSD and UCM Security Offices have undertaken this project with the support of senior leadership and are committed to establishing a single set of policies for use within both the BSD and UCM. Our goal is to replace the existing and outdated policies with a set of robust policies that will enable the organization to:

- Compete for new research opportunities and grants
- Safeguard patient, student and staff information
- Support critical business processes

How to review and comment:

To access the policy documents, go to the BSD Information Security Office Policies webpage and click on the Policy Name. You will receive a prompt to log in with either your BSDAD or UCHAD account (for BSDAD accounts, please login using the syntax "BSDAD\<username>" and your BSDAD password).

To comment on the policies, select "Open in Word" from the top left hand corner of the screen and use the Microsoft Word "Insert Comment" feature (on the Review tab, in the Comments group, click New Comment). To access this feature, highlight the section of text you would like to comment on, go to "Review" and select "New Comment." In the process of your review and commentary, we ask that you consider the following to guide your comments:

- Is the policy readable and understandable?
- Is the policy acceptable, or are there items of particular sensitivity that should be further considered?
- What advice would you give to implement the policy?

Information Security Standards

The BSD Security Liaisons Group has published the STA-06 BSD Media Sanitization Standards. This standard ensures that media used to store information owned and used by the Biological Sciences Division is properly and safely sanitized or destroyed when required. For more standards to secure your devices, visit our site at BSD Information Security Office Policies webpage.

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

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

Information Security Office Team

Plamen Martinov, 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