RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

April 2017 | SECURITY.BSD.UCHICAGO.EDU | Volume 3, Issue 4

Inside this Issue:

New Secure Data Delivery Mechanism

The Center for Research Informatics (CRI) in conjunction with the BSD Information Security Office (ISO) is excited to announce a new secure data delivery mechanism for the Clinical Research Data Warehouse (CRDW) team.

UChicagoBox — a cloud-based file storage and sharing service is available to BSD departments. UChicagoBox combines powerful content management, flexible collaboration tools, and the security you need for sensitive files, all in one easy-to-use platform. Box provides unlimited and free online space for storing or sharing files. Files stored on Box can be synced and accessed from several locations, including desktops, mobile devices, and laptops.

The CRDW team will now upload your data to a secure folder within UChicagoBox. You will receive an email announcement when your data is ready with instructions for data retrieval.

To start this process for your data, send an e-mail to the CRI's CRDW team at **datarequest@bsd.uchicago.edu**.

For more information on UChicagoBox, visit the BSD ISO website:http://security.bsd.uchicago.edu/bsduchicagobox/.

Cloud Applications and Click-Through License Agreements

Cloud applications are becoming commonplace for business use. These applications are typically cheaper and easier than having the University or Medical Center "build" a new application. While this may be true, there are still a few things you must considering before purchasing cloud application subscriptions on behalf of the University or Medical Center.

Click-Through License Agreements
If you've ever subscribed to a cloud application, then you've seen a Click-Through license agreement. Commonly referred to as the End User License Agreement (EULA), a screen usually appears somewhere between registration and payment that requires you to read (or at least attest to have read) and agree to some lengthy Terms and Conditions. These Click-Through agreements are legally binding. By clicking "I Agree", you are asserting you have authority to agree to the Terms. This is fine when purchasing subscriptions for personal use, but if the University of Medical Center is paying for the subscription, you may be putting the Organization at risk.

Agreeing to Click-Through terms constitutes approval without review of legal terms and may bind the Organization, as well as the individual "clicking". While the vendor may claim, the terms are not negotiable, this doesn't mean the Organization will find them acceptable. Further, usually the vendor reserves the right to amend the terms, potentially resulting in more liability for the Organization without any notice.

How to Handle Click-Through License Agreements
To avoid the risks previously mentioned, you should:

- Involve your Organization's Legal team early in the process when planning to purchase software or services of any kind
- When purchasing cloud services on behalf of the Organization, always be on the lookout for license agreements and/or terms and conditions that must be accepted in order to complete the purchase
- Ask your Legal team to review license agreements and/or terms and conditions prior to making purchases

If you have any other questions, please contact the Organizations' Information Security or Legal Office.

Department	Email
BSD Information Security Office	security@bsd.uchicago.edu
UCM Information Security Office	help@bsd.uchicago.edu

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 2016, 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 Happens:

- We send out a phishing test email 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.

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

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