RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

January 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 1

Inside this Issue:

Million Dollar Download

It only takes one click in a phishing attack to lose confidential Biological Sciences Division data which could result in large sums of money paid for regulatory fines and penalties. Please read the story below about how Bruce and his organization fell victim to a phishing attack.

It had all looked so legit. Bruce, a laboratory technician for an academic hospital, considered himself a pretty computer-savvy guy. He had heard all about hacking, phishing, and malware, and stayed vigilant about the personal and financial information he posted online. But the e-mail he received late one Friday afternoon didn't set off any of those alarm bells. It came from a .gov address, the official logo of a federal agency was at the top of the message, and there were none of the obvious misspellings or punctuation errors of your typical e-mail scam.

The message said to simply download and open a Word document to review new instructions for reporting health benefits on this year's tax forms. Seemed simple enough, Bruce thought, as he clicked the attachment. When he tried to open the file, Word took forever to open...but that wasn't unusual for his work computer. Glancing at the clock, Bruce decided he'd log out and read it on Monday. He gathered his stuff and dashed for the bus. It was a decision he'd long regret.

By the time he returned to work three days later, Bruce had a bad feeling. Logging back in, he found that the document still wasn't loading, and thinking back, he didn't feel so good about the origin of that e-mail any more. Swallowing his pride, he dialed up IT and admitted what he'd done. The concerned voice on the phone was just the beginning of a landslide of consequences.

First, the IT experts determined that Bruce had in fact downloaded a malicious program, one that was left free to operate over the weekend. Even worse, his computer could access to tens of thousands of electronic medical records, leaving patient information including names, billing, social security numbers, insurance, and more vulnerable to the software. It was the worst-case scenario.

While there was no hard evidence (yet) that any of this data had been stolen or used for fraud, the hospital had no choice but to disclose the breach to those affected. Local and national media covered the story, quoting patients angered and disappointed at the invasion of their privacy. The official press release only

named an anonymous "single employee" as the source of the breach, but Bruce felt like everyone at the hospital knew it had been him.

As the media storm died down, it was replaced by a the glare of a different harsh spotlight: federal investigations. The FBI looked into the origins of the e-mail and the Department of Health and Human Services (DHHS) examined the hospital's security procedures. Bruce was the subject of several difficult and humiliating interviews. Eventually, the hospital settled the case with DHHS for nearly $1 million, promising to install new security protections and employee training to prevent another incident. It was a heavy price tag for one bad decision, but one that Bruce would never forget...or repeat.

Gone Phishing…Don't Take the Bait

As part of our ongoing security awareness program, at times, we will assess the BSD's understanding of cyber security. In March, the BSD and UCM Information Security Offices will kick off a **Phishing Email Assessment and Education Campaign**. A phishing assessment is an email pretending to be a hacker; same emails that bad guys are sending. 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.

A couple of key points:

- We will send out these emails to every BSD employee.

- If you fall victim to one of these phishing emails you will be notified immediately and you will be enrolled in phishing awareness training.

Visit http://security.bsd.uchicago.edu/phishing/ for more information on how to avoid a phishing attack.

IT GRC- What are Your Security Numbers?

The BSD Information Security Office is happy to announce the rollout of our **IT Governance, Risk and Compliance (ITGRC**) platform to organize our IT Security governance, risk management, and compliance efforts in to one central system.

The platform is designed to help manage all facets of IT Security Governance, including IT Security policy, standards and procedure development, as well as provide BSD IT staff a central location to:

- Manage IT Security Vulnerabilities
- Acknowledge IT Security Policies and Standards
- Submit an IT Security Exception Request
- Submit IT Asset Inventory and Categorization Information

For more information about the platform, including tutorial documents, visit the BSD ISO website at http://security.bsd.uchicago.edu/itgrc/.

Assess Your Cyber Security Posture

The BSD Information Security Office (ISO) has developed a **Cyber Security Assessment Tool (CSAT**) to assist BSD Departments, including IT Support Groups, with assessing the current cyber security practices. The tool and the user guide is available now to download from the BSD ISO Website. The goal of this tool is to help you gather important information about your current security practices, so that we can work together to understand the cyber security level of your department's computing infrastructure and then use this information to improve it.

Our goal is to work with you to achieve the target state for your department. BSD ISO will hold workshops in the first half of Q1 of FY17 to educate staff further on how to use the tool and what it all means. Collection of results from each department will officially begin in Q2 of FY17.

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

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