http://security.bsd.uchicago.edu

In this issue of the BSD ISO Cybersecurity Newsletter…

- **The Power of Two -** E-mail scammers, or "phishers" are growing increasingly sophisticated in their attempts to trick you into revealing your password and other sensitive information. Please read the following story about Steven's phishing experience and how Two-Factor Authentication can prevent your personal information from being stolen.
- **BSD Information Security Standards -** Do you manage administrative passwords? Implement the new BSD Password Management Standards to safeguard your systems from hackers.

The Power of Two

It looked like any other e-mail from the University: the right logo, the usual administrative tone, from an official-sounding e-mail address, asking him to update some information. Still groggy before his first cup of coffee one Monday morning, post-doc Steven Perez clicked the link in the message, logged in, filled out a form, and forgot all about it.

That is, until the next month, when Steven's rent check bounced and a call to the bank revealed that his paycheck wasn't deposited as usual. Retracing his steps, Steven realized he had been "phished" -- fooled by a counterfeit e-mail into sharing his CNet password with an outside party.

Whoever it was, they were up to no good, as Steven and the BSD Information Security Office discovered that his direct deposit was recently switched to another address through the Employee Self Service portal. What's more, the crook likely now had access to a pile of sensitive information about Steven and his family, including phone numbers, addresses, benefits information, his date of birth, the last four digits of his social security number, and more.

A long, frustrated morning of phone calls followed to straighten out his paycheck, cancel credit cards, change passwords and auto-pay information across dozens of sites, and purchase pricey fraud protection services. Throughout, an embarrassed Steven whispered into the phone to hide his mistake from his officemates, but his friend Mike couldn't help but notice all the damage control from the other side of the cubicle.

Preventative Measures

The University of Chicago will never ask you for your password over e-mail, but opting into Two-Factor Authentication, for both University services and other secure websites, gives you extra protection against identity theft and fraud.

To learn more about Two-Factor Authentication, and to request this service, visit https://itservices.uchicago.edu/services/2factor-authentication.

“Dude, you were phished?,” Mike asked as he leaned over the divider.

“Just stop, Mike, I don’t need any more grief today,” Steven replied, rubbing his temples.

“No jokes, I promise; those e-mails aren’t Nigerian princes with spelling issues any more,” Mike grinned. “I’m just surprised you weren’t already on two factor!”

Mike explained two-factor authentication, an extra layer of security increasingly used by a number of websites and now available for several UChicago services. “All you do is provide your mobile phone number and download the Duo app onto your smartphone. Every time you log in to Workday, myUChicago, or other sites on a new computer, you will be prompted to either receive a verification phone call, a text message from Duo with a unique security code or a quick notification from the Duo application to accept or decline the login,” Mike said.

“I usually select the Duo application notification option because it literally takes 2 seconds. I just tap accept on my phone when I get the notification and I’m in! The site then knows you’re you and not some hacker,” Mike said. “To make it even easier, when you login you can tell the site to trust that computer for 30 days and the next time you login you don’t have to do anything extra at all.”

“Anything to prevent another morning like this,” Steven said with a sigh. “And no more answering e-mails before coffee either.”

BSD Information Security Standards

The BSD Security Liaisons Group, consisting of IT professionals from the University of Chicago, BSD and UCM, is working to develop information security standards, based on the security principals of NIST (National Institute of Standards and Technology). These standards are designed to improve the BSD’s Security Framework. The group has worked together to publish the STA-01 BSD Minimum Security Standards for Systems, STA-02 BSD Security Standards for Databases, STA-03 BSD Security Standards for Networked Printers and STA-04 BSD Password Management Standards. Please visit the BSD ISO website at http://security.bsd.uchicago.edu/Security Policies for the published and draft standards.

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

Contact the BSD-ISO team via the following phone numbers or e-mail addresses:
You may also send an e-mail to the BSD Security mailbox: security@bsd.uchicago.edu
Visit the BSD-ISO website: http://security.bsd.uchicago.edu

Plamen Martinov, Director of BSD Information Security	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Bruce Thompson, IT Security Operations Analyst	O: 773-834-5398	bthompson@bsd.uchicago.edu
Travis Le, IT Risk and Security Analyst	O: 773-834-7127	tle2@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu