In this issue of the BSD ISO Cybersecurity Newsletter…

- **False Support –** Social Engineering scammers are continuing to find ways to gain access to a user's computer to either install malware that could steal sensitive data or ask you for personal information to steal your identity. Please read the following story about Dr. Monroe's fake tech support experience and how you can avoid becoming a victim of a fake tech support scam.
- **BSD Information Security Standards –** Are you looking for Security Standards to assist with your department's security? The BSD Security Liaisons Group, consisting of IT professionals from the University of Chicago, BSD and UCM, is working to develop information security standards for the division.

False Support

"Hello, this is Rick from Microsoft, am I speaking to Dr. Monroe?" Physician James Monroe rolled his eyes -- a telemarketer. "Yes, but look, I really don't have time right now for a sales call," Monroe responded impatiently.

"My apologies, Dr. Monroe, but I'm actually from Microsoft Tech Support, working with your University's IT department to defend against a very nasty computer virus that's going around. You've probably heard about it on the news this week."

Dr. Monroe paused. He had heard something about a virus on the radio that morning, some kind of "Trojan horse" used by Russian hackers to get into the IRS and steal a bunch of data. It hadn't struck him as anything he should be worried about himself, but he certainly wasn't an expert on cybersecurity, and the caller ID on his phone checked out, reading "Microsoft Tech Support."

"Yeah, I think I did...but shouldn't someone from the CBIS help desk be calling me about this?," he asked.

"Well, this is such an urgent crisis, your IT people asked us to help reach everyone in your system about how to protect computers from the virus as soon as possible," Rick said. "Now if you're near your computer and you just have a couple of minutes, I can walk you through the precautionary steps you need to take, totally free of charge."

Preventative Measures

The University of Chicago does not enlist external computer technical support companies to provide technical support to employees.

To learn more about Social Engineering, visit BSD ISO Social Engineering Tips.

To learn more about fake tech support scams visit FTC Tech Support Scams.

Dr. Monroe shrugged and opened up his laptop, following the caller's directions to an official-looking website where he filled out a form and downloaded a small file. But something made him hesitate before double-clicking the file. Something felt...off. "OK, I've installed the program," Dr. Monroe bluffed, "is that all?" "Yes sir, thank you for your time, sir," Rick said rapidly before hanging up.

Dr. Monroe paused, then dialed up the CBIS help desk tech who had helped him set up a backup system a few weeks ago. Briefly, he explained the strange call and the instructions he had been given, feeling silly and paranoid. But when he got to the part about downloading the file, he heard what sounded like a spit take from the other side of the line.

"DO NOT CLICK THAT FILE," the tech said sternly. "DELETE IT IMMEDIATELY."

The tech explained that "Rick from Microsoft" was working an increasingly common scam: claiming to be from a tech support service. Instead of protecting Dr. Monroe from a virus, "Rick" was directing him to malware which would have opened his computer's contents to a remote user, granting who knows who access to sensitive personal and patient data. Nobody outside of the CBIS help desk will ever instruct you to install software, he said.

A close call, Dr. Monroe thought, and a phone call he wished he hadn't answered.

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
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu