RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

July 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 7

Inside this Issue:

False Support *(Page 1-2)*

IT Phone Scam Alert *(Page 3)*

UChicagoBox BSD Group Folders *(Page 4)*

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.

"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."

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.

Preventative Measures

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

To learn more about Social Engineering, visit the **BSD Information Security Office website** and click on **For Faculty and Staff** to download the **BSD ISO Social Engineering Poster.**

IT Phone Call Scam Alert

It has been reported recently that scammers are impersonating the University ITS Service Desk and the UCM CBIS Service Desk. The scammers are calling staff to inform them of a password problem.

They ask the staff member to log in and change their password, and then ask to be provided with the new password to verify it is working correctly. The scammers may already have some of the staff's information, such as name and phone number extension, in order to appear legitimate.

As a reminder, no one at the University, BSD or Medical Center will ever ask you for your password. If you encounter a phone call from someone claiming to be from the University ITS Help Desk or UCM CBIS Service Desk and asks you for your password, hang up the phone. You should never provide your password to anyone.

If you have supplied your password to someone over the phone, you should take these steps **immediately**:

1. Change your password by calling your Service Desk.
2. Notify your respective Information Security Office that you suspect your password might be compromised.

If you have any further questions, contact the organizations' Information Security Offices.

Department	Contact Information
UCM Information Security Office	security@uchospitals.edu
BSD Information Security Office	security@bsd.uchicago.edu
ITS Security	security@uchicago.edu
ITS Service Desk	773-702-5800 (x2-5800)
UCM CBIS Service Desk	773-702-3456 (x2-3456)

UChicagoBox BSD Group Folders

As part of the BSD Research-Centric Information Security Enablement (RISE) program, established to enable and protect the research and academic functions of the BSD, UChicagoBox Group Folders are now available to your departments. The purpose for this email is to provide you with information on how to request and set up a group folder for your department.

Background:
On December 15, 2015, the BSD Information Security Office introduced Individual UChicagoBox accounts to BSD non-clinical departments. Individual Accounts allow you to store and share files and folders but once you leave the organization the data in your personal UChicagoBox account will be automatically deleted 45 days after your departure.

To ensure collaboration continues, we are now offering BSD UChicagoBox Group Folders. A Group Folder is a special folder that any BSD individual with UChicagoBox access can request on behalf of his or her group, lab, or department and is co-owned by the BSD Information Security Office. This means that, once created, the Group Folder will remain active even if the user who requested it changes departments, closes his or her Individual UChicagoBox account, or leaves the BSD.

BSD UChicagoBox Group Folders are as easy to use as individual UChicagoBox accounts and are great for the day-to-day management of shared department data.

How to request your group folder:
If you would like a department or group folder, please visit the **BSD Information Security Office website** and click on **For Faculty and Staff** to submit the **BSD UChicagoBox Access (Individual or Group Folder) Request Form**, including the names and contact information of the **2 administrators (required)** for the folder.

Please see the following information detailing what you need to know about UChicagoBox and how to get started with the Group Folders.

Getting Started (for Group Folder administrators):
After your Group Folder has been created for you, the BSD Information Security Office invitation to the folder will appear in your UChicagoBox Individual account. When you accept this invitation, you will be able to configure it for security and to set up permissions for your colleagues. For additional instructions on how to manage your group folder.

For more information about UChicagoBox for the BSD, visit the **BSD Information Security Office website** and click on **For Faculty and Staff** and then **BSD UChicagoBox** under **Security Programs**. Send any questions and feedback about this new service to security@bsd.uchicago.edu.

Thanks, and happy sharing!

What to do if you become aware of an information security incident? Contact the BSD ISO Team via email at security@bsd.uchicago.edu.