RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

February 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 2

Inside this Issue:

Password Poltergeist

Having a strong, complex password helps to keep the Biological Sciences Division data safe. Please read the story below about how Maria stopped a weak password from haunting her.

A reminder box popped up: it was time to change passwords...again. Maria groaned and sipped her coffee, racking her brain for a new idea. She'd already used practically every object on her desk, every childhood pet, every favorite song, every favorite movie -- spelled with what seemed like every possible combination of letters and numbers and symbols. Maybe this time she could just get away with picking a random word out of the dictionary, right?

Flipping open her Webster's to a page somewhere in the middle, she stabbed with a finger and picked the first word longer than 12 characters: "featherweights," that should work, she thought. But as she typed it into the new password field, her office lights suddenly flickered. "That's....weird," Maria whispered to herself. The superstitious type, she picked up a German dictionary and tried a word from its pages instead.

But upon typing, things got even worse: flickering lights, her wastebasket sliding with a loud scrape across the floor, a few books seeming to throw themselves off her shelf. Standing up and shivering now, Maria's brain reached out for a new solution in a panic. Maybe a made-up word from a book? Let's see books, books, Harry Potter, "AvadaKedavra"?

Lights flickering, wastebasket now floating off the floor, books flying from shelf to shelf, and a loud moaning noise panning around the room. And this time it wasn't stopping. "What do I do???" Maria yelled.

She heard a knock at the door, and Brenda from the next-door office peeked in. "Password troubles?" she asked, unphased by the flying objects and loud noises. "HOW DID YOU KNOW?" Maria yelled, hair flying in a sudden gusty wind. "I've tried words from three different dictionaries, and nothing works!"

"Well there's your problem, hackers use dictionaries all the time to guess people's passwords," Brenda said calmly. "Try a passphrase: 19 or more characters describing a memory or a favorite joke or a list of favorite songs, with some numbers and punctuation thrown in for extra protection."

Maria stretched for her keyboard and typed in a sentence describing her childhood home. Abruptly, the lights steadied, the noises stopped, the books returned to their original position. "Password security, it's no joke, right?" Brenda said, and closed the door.

Password Guessing Cyber Attack

A password guessing attack began on Wednesday, January 27th against BSD and UCM computers on the University network, which has impacted parts of the BSD and UCM operations. The attack caused many users to have intermittent account lockouts. This particular attack is known as a 'Brute-force password guessing attack' and is highly distributed, meaning it's originating from many compromised computers around the world. Since the start of the attack, over 300 BSD accounts have been locked at least once, impacting these users' workflows and several UCM accounts were successfully compromised.

Steps Taken by the ISO:

The BSD, ITS and UCM Security Officers have initiated a coordinated response to mitigate the risk and have taken the following steps to protect account holders:

- Temporarily increased password lockout thresholds as an immediate countermeasure to minimize the impact to operations.
- Assisted employees impacted by the lockouts, ensuring they can continue to work while this attack is underway.
- Implemented network restrictions at the border to impede the brute-force password guesting attempts.
- Tuned security systems to monitor and alert the Information Security Offices in the event accounts are compromised.

The attack has subsided dramatically as a result of the above actions, but the attack is persistent and without further action additional account holders may be impacted.

Next Steps:

We believe the best course of action is to turn on the host-based firewall on computers exposed to this attack to restrict hackers from accessing the remote desktop services. **As a result, users will have to first establish a VPN connection using cVPN (and soon BSD VPN) before they can access their work computers when working remotely.**

How to use cVPN: https://itservices.uchicago.edu/services/vpn-cvpn

Note: If you are unable to use the cVPN service, please contact security@bsd.uchicago.edu. Those who currently use the hospital VPN (i.e. webvpn.uchospitals.edu) may continue to do so without interruption.

Keep Calm and Use the BSD VPN

The Biological Sciences Division (BSD) Information Security Office, in collaboration with members of the CRI, PHS and ITS, is proud to announce a virtual private network dedicated to the BSD's staff, researchers and collaborators.

The BSD Virtual Private Network (VPN) provides BSD staff; researchers and collaborators a secure means for access to University network resources, no matter where they are in the world.

The BSD VPN Will:

- **Enable** employees and collaborators within the BSD to securely access Systems hosted on the university network.
- **Protect** the BSD by providing improved security; requiring two factor authentication as a default security setting.
- **Streamline** access for BSD resources by simplifying credential requirements.
- **Plan** for future innovation and network changes.

When?	The BSD VPN service will be available shortly after pilot testing is complete in March.
Who?	All approved BSD staff, researchers and collaborators. Some departments have not yet adopted the BSD VPN. Please click **here** for the latest status, by department. The Department of Anesthesia and Critical Care will not be using BSD VPN.
How?	**If you intend to use the BSD VPN, you will need to first enroll in DUO Two-Factor Authentication and register a qualifying device.** Step-by-step instructions for enrollment are located **here.** The DUO Enrollment site is located **here.** Approved users can access the BSD VPN at https://bsdvpn.uchicago.edu, and logon to the system with their BSDAD ID and Password. Please click **here** for the BSD VPN general overview document.

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

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