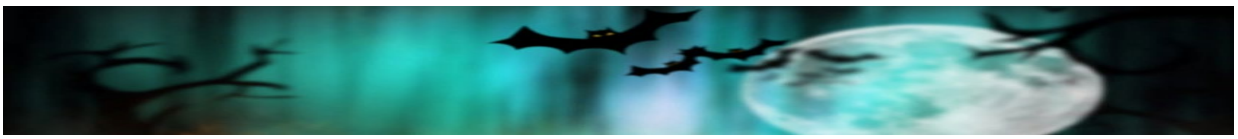
THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

October 2023



Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

This month is **Cybersecurity Awareness Month!** Before we get into the topics, I want to go over events that are being held for Cybersecurity Awareness Month: **Tech Talk Webinars**, **Cybersecurity Symposium**, and a **Secure Destruction Event**:

Tech Talk Webinars

Webinars will be held throughout the month. Please register here to attend: https://security.uchicago.edu/tech-talk-series-registration-page/

Tuesday, October 10, 2023 @ 2pm – 2:45pm Central Time
Explore a Career in Cybersecurity: It's a Different World After All
Presented by: James Clark, Cornelia Bailey, Jessica Sandy, and Vanessa Martin

Tuesday, October 17, 2023 @ 2pm – 2:45pm Central Time
Generative AI: How to be on the Inside When the Machines Take Over the World
Presented by: Matthew Singleton (Crowdstrike)

Thursday, October 26, 2023 @ 2pm – 2:45pm Central Time
America's Cyber Defense Agency
Presented by: Shaheen Chaudhri (cisa.gov)

Tuesday, October 31, 2023 @ 2PM - 2:45PM Central Time
Cyber Fraud Prevention and Response (Final Title Pending)
Presented by: Trent Fried (secretservice.gov)

Cybersecurity Symposium

Tuesday, October 24th, 2023 From 8AM- 5:30PM Central Time
Cybersecurity Symposium will be held in person @ Ida Noyes Hall
More information on the presentations can be found here:
https://cybersymposium.event.uchicago.edu/

Secure Destruction Event

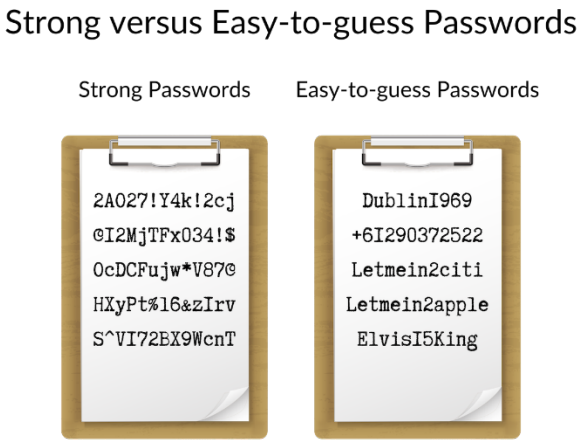
Bring your Paper, Computers, Hard Drives, and other media for secure destruction!
For all BSD, UCM or University members.

Destruction Event will be held @ 5812 S. Ellis Avenue Room N161 (End of the N Corridor)

Wednesday, October 18th from 10AM-3:00PM
Thursday, October 19th from 10AM-3:00PM
Friday, October 20th from 10AM-3:00PM

Cybersecurity Awareness Month Message

Follow these top tips to stay safe online!



- 1) Make your passwords:
  - Long: At least 16 characters
  - Complex: Use upper and lowercase letters, numbers and symbols
  - Unique: Use a different password for each account.
  - BSD Access and Control Policy
- 2) To help manage those passwords use a password manager. Recommendations :

1Password

  - 1Password: is a well-established password manager that offers a 14-day free trial and various plans for individuals, families, and businesses. It has many advanced features, such as travel mode, watchtower (data breach monitoring), biometric unlock, and more. 1Password also has a user-friendly interface and integrates with many apps and services. However, some of the drawbacks of 1Password are that it does not have a free plan. It also has higher prices than some of its competitors.

- Bitwarden: is an open-source password manager that offers a free plan with unlimited passwords, sync across devices, and two-factor authentication. It also has affordable premium plans that add features like encrypted storage, password health reports, emergency access, and more. Bitwarden is easy to use and supports a wide range of platforms and browsers. However, some of the drawbacks of Bitwarden are that it does not have a data breach monitoring service. It also has fewer integrations and policy settings than some of its competitors.

- Keeper: is an enterprise-grade password manager that also offers plans for individuals and families. It has features like encrypted storage, password health audits, dark web monitoring, secure file sharing, and more. Keeper also has a high level of security and compliance, as well as extensive integrations and policy settings. However, a drawback of Keeper is that it does not have an open-source code. It also has a less intuitive interface and a more limited free plan than some of its competitors.

	SOMETHING THAT YOU KNOW	SOMETHING THAT YOU HAVE
Two-factor Authentication (ATM)	PIN	Bank Card
Two-factor Authentication (Website)	Credentials	Mobile Device
Two-factor Passwords	Pattern	Hint

- 3) Turn on Multifactor Authentication wherever possible

- Protect your password with another password that you don't need to know! Multi-factor authentication gives you this power – think of it like placing your housekeys in a safety deposit box that can only be opened by a facial scan.
- Where should you use MFA?
  - 1. On accounts with your financial info like banks and online stores
  - 2. On accounts with personal info, like social media and healthcare apps
  - 3. On accounts with info you use for work

- 4) Update Your Software

Keeping your software and apps updated is an easy way to increase your cybersecurity posture. Software and app developers focus on keeping their users and products secure and they're constantly looking for clues that cybercriminals are trying to use to break into their systems, or they are searching for holes where cybercriminals could sneak in, even if they've never been breached before. To fix these issues and improve security for everyone who uses their services, upstanding software companies release regular updates.

- 5) Recognize and Report Phishing

Cybercriminals like to go phishing, but you don't have to take the bait. Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, you can hand over your personal information to the cybercriminals. A phishing scheme can also install malware onto your device. No need to fear your inbox, though. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

- **Does it contain an offer that's too good to be true?**
- **Does it include language that's urgent, alarming, or threatening?**

- **Is it poorly crafted writing riddled with misspellings and bad grammar?**
- **Is the greeting ambiguous or very generic?**
- **Does it include requests to send personal information?**
- **Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?**
- **Is it a strange or abrupt business request?**
- **Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.**

The advent of AI has made recognizing a phishing scheme even harder, so it is important to be extra vigilant.

As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at security@bsd.uchicago.edu .