THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

September 2022

# Cyber Security Awareness Newsletter

**Protecting yourself and information from cyber security threats**

Events on the Horizon! **October is Cybersecurity Awareness Month!** As part of Cybersecurity Awareness Month, we have several webinars and events scheduled. Every Tuesday this month we will have a "**Tech Talk Tuesday at 2:00"** (easy to remember right?)**.** Anyone at the institution of all skill levels is welcome to attend. You may register for each event at the links below:

## Webinars

- October 4th 2:00PM-2:45PM "**Always Be Vigilant: Cybercriminals never stop – Neither can we!**" - Presented by: Matt Morton (UC CISO) + Karen Habercoss (University of Chicago Medicine, Chief Privacy Officer) + Dipti Ranganathan (University Chief Privacy Officer)

Register Here : https://uchicago.zoom.us/webinar/register/WN_x9jUSowJTaiK_qDjbAq9XA

- October 11th 2:00PM-2:45PM "**See Yourself in Cyber – Information you can use at work and at home to tackle cybercrime**" Presented by: Tony Enriquez, Cybersecurity & Infrastructure Security Agency (CISA.gov)

Register Here: https://uchicago.zoom.us/webinar/register/WN_d0G1KXYnS4uBy8dGJW9Qpg

- October 18th 2:00PM-2:45PM "**Threat Insight: Just when you think you know about phishing, there's more!**" Presented by: Frederick Sears (Proofpoint SE) & Craig Drake (Information Security Engineer)

Register Here: https://uchicago.zoom.us/webinar/register/WN_mCx60U-jTk-j_S4WxtPQOA

- October 25th 2:00PM-2:45PM **Oh Behave! Annual Cybersecurity Attitudes and Behaviors Report 2021 –** Presented by: Jennifer Cook, National Cybersecurity Alliance (staysafeonline.org)

Register Here: https://uchicago.zoom.us/webinar/register/WN_QT_-xa8jRh6A4c4h6hrCqw

The two webinar topics on October 11th and October 25th will be presented by speakers from **The Cybersecurity & Infrastructure Security Agency** (CISA) and **The National Cybersecurity Alliance** (NCA).

**Who is CISA? Who is NCA?**

**CISA** - Is a United States federal agency, an operational component under Department of Homeland Security oversight. Its activities are a continuation of the National Protection and Programs Directorate. They lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

**NCA** - Is a 501 USA non-profit organization that promotes cybersecurity, privacy, education, and awareness. The NCA works with various stakeholders in the government, industry and civil society. They lead a mission to create a more secure, interconnected world by advocating for the safe use of all technology and educate everyone on how best to protect ourselves, our families, and our organizations from cybercrime.

**Events**

Also on the radar is a document destruction day where the University will be hiring Shred-it! This event will be held on 3 days in October: Wednesday, October 19th| Thursday, October 20th | Friday, October 21st from 11:00AM-2:00PM each day behind the Press Building at 1427 E. 60th St., Chicago, IL 60637. We are not limited to just paper destruction. You can also bring media and hard drives. Totes for media/hard drives will be taken to 6045 S. Kenwood.


---

On to our topic for this month! For this month I want to make folks aware of software updates. One of the easiest ways to keep your information secure is by making sure your software and apps are up to date. If your machine is managed and maintained by the BSD, your operating system and some applications are already part of a monthly push for updates. However, if you have software or apps that are not part of the standard build, you will need to do those updates manually.

**Why do we need to install updates?**

To understand what updates do, it is necessary to understand the types of updates exist. Updates fall into these 4 general categories:

**Bug Fixes** – Are updates that address features in a products development lifecycle that aren't quite working as expected. These updates are normally planned and released depending on how severe the bug is to the functionality of a product. In general bugs are normally squashed to improve current functionality of a product.

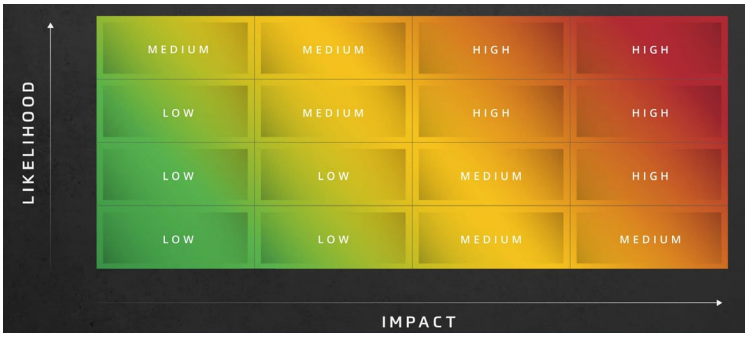
**Security Fixes** – These updates have 3 categories and are usually the result of security vulnerabilities or security flaws found in software or hardware. These types of updates are the most important to install as they are meant to prevent remote infiltration, installation of malware such as spyware, ransomware, trojan horses, worms and viruses that may take advantage of software or hardware.

- **Patches** – Temporary fix on a product that will eventually be added to the full product installer.
- **Hotfix** – A fix that can be immediately issued to a system with zero to minimal downtime. Can usually be applied while the product actively being used.
- **Coldfix** – A fix that requires a restart and has visible impact on services. These fixes can usually be applied when the system is live and active. For these fixes communication messages are usually sent making everyone aware that a reboot will be required, especially when urgent.

**Performance Fixes** – These updates are geared toward the improvement in an applications efficiency functionality. Usually, it's a development in code that could compute a function quicker and be less strenuous on memory and CPU resources.

**Enhancements Additions** – These updates are usually additional functionality added to a product. They are meant to improve the value, quality, or attractiveness of a product.

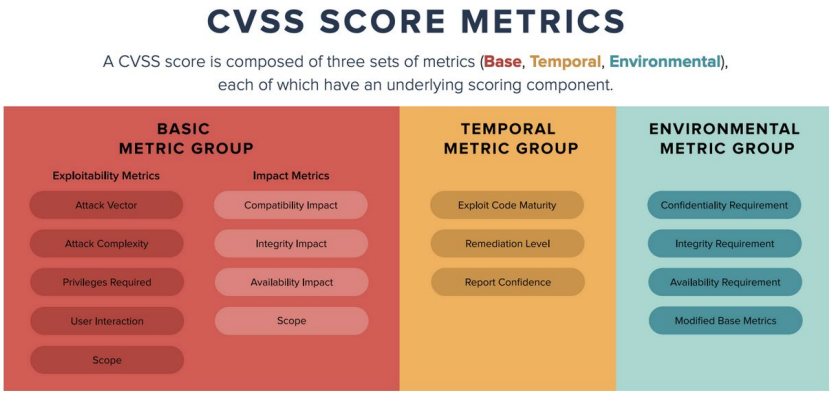
**How do you know when to apply updates?**




The second Tuesday of every month is commonly known as "Patch Tuesday". This name was coined by the industry for the frequency of updates which were released near or on that day by most vendors. This day was eventually formalized and became a monthly release of updates and information. However, when an item is severe enough that it is considered critical, an update is released outside of the normal update cycle known as an "out-of-band" update. All security updates, whether out-of-band updates or part of the monthly releases, have a severity level and a severity score known as a CVSS score.

| CVSS V3 Score Range | Severity in Advisory |
|---|---|
| 0.1-3.9 | Low |
| 4.0-6.9 | Medium |
| 7.0-8.9 | High |
| 9.0-10.0 | Critical |

These two items when combined will give you a sense of impact and likelihood of occurrence which when combined with other factors in the environment such as firewalls and other mitigating factors will give you a sense of urgency for applying updates.




BSD ISO reviews the list of updates for Patch Tuesday and suggests the urgency for implementation based on current environmental protections and impact to the organization.

**The Importance of Quality Assurance**

It is important to note that occasionally, a vendor doesn't always fully test an update and sometimes applying an update can "break" an application or hardware. For this reason, unless it is a very critical urgent update (which still gets tested), normal updates are implemented and reviewed over the course of a week in a test environment first before being implemented into the production environment. This isn't 100% fool proof however, since testing every possible configuration would be impossible, but this does give the institution a better handle on how a patch will react when implemented in the environment.

Don’t ignore operating system messages that prompt for pending updates. Always consult your IT support before applying any updates. If your system isn’t part of the managed IT support patching cycle reach out to your IT support personnel. Having your system as part of managed updates handled by your IT support will ensure that you have the most up to date and tested security patches for your system.


Please contact your IT support personnel or security@bsd.uchicago.edu for more information.