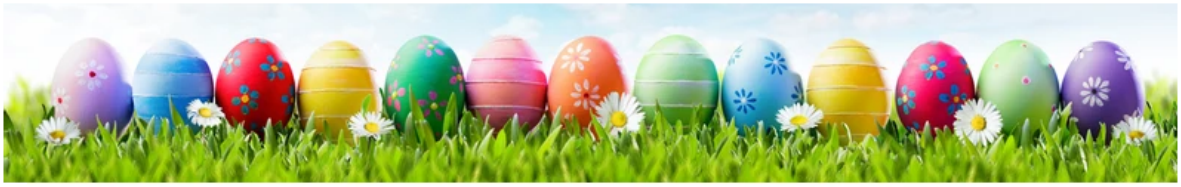
THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

April 2023

Cyber Security Awareness Newsletter

Protecting Yourself and Information from Cyber Security Threats

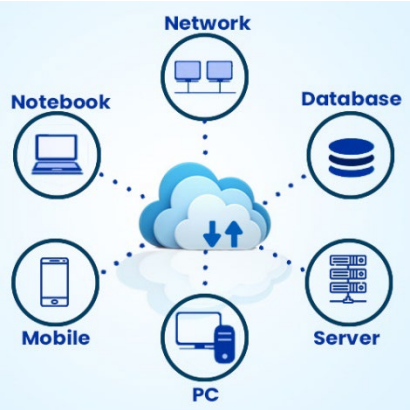


Welcome to our April Cybersecurity Newsletter! It's springtime! That means baseball starts its full swing, the easter bunny is hopping around, the birds are chirping, flowers are starting to bloom and cybercriminals are… still up to their usual tricks. Let's make sure we stay one step ahead of them with some important cybersecurity awareness themes for the month. This month I wanted to focus on the April industry campaigns that are meant to raise awareness on cybersecurity threats as well as let you know that a spring cleaning campaign is underway in the BSD to have old computing hardware destroyed and recycled. This months focus: Identity Management Awareness and Cloud Security Awareness.

Identity Management Day is observed annually on the second Tuesday in April to observe the importance of securing our employee, partners, and customer identities… but it is an important initiative all year round. With the rise of remote work, online transactions, and social media, protecting digital identities is crucial. Cybercriminals are becoming increasingly sophisticated in

their methods, making it more challenging to keep our digital identities safe. Here are some tips that should be followed for managing your identities:

- **1) Never share or reuse passwords**
- **2) Create strong passwords following BSD policy standards:** https://itcompliance.bsd.uchicago.edu/Policy/Portal.aspx?tableId=1&id=2435
- **3) Recognize and report phishing**:
  - BSD Recognize and Report Phishing
  - University Recognize and Report Phishing
- **4) Keep your software and OS up to date:**
  - BSD Minimum Security Standards for Endpoints
- **5) Enable multi-factor authentication – anywhere you can:**
  - Identification and Authentication Policy
- **6) Use a password manager** – We believe that transparency is essential when it comes to recommending security products, and we want our users to have the best possible protection for their sensitive information. That being said, last year we recommended using LastPass as a password manager based on needs, features and on current industry recommendations from reputable resources such as Gartner and others. At the end of the year LastPass suffered a security breach which had some impact on the security of the product. Although the password vaults were still secure it allowed access to them. Considering this event, we have reviewed and reevaluated our recommendations for password managers and have decided to recommend OnePassword over LastPass. OnePassword has a strong track record of security. Additionally, OnePassword offers more features and customization options than LastPass, making it a more versatile solution for users with varying needs.



Cloud Services Security Awareness Month is also observed in April. Cloud security focuses on raising awareness of the importance and best practice of securing data in the cloud. As more individuals and businesses move their operations to the cloud, it's essential to ensure that the data stored in the cloud is adequately secured. Cloud service providers have a shared responsibility with their customers to maintain security, but customers also need to take

appropriate measures to ensure their data is secure. Some folks are still on the fence regarding what cloud computing means so let me explain.

Cloud computing is a technology that allows users to access computing resources, such as storage and processing power, over the internet without the need to own or manage physical hardware. Think of it like renting a computer that is located somewhere else and accessed through the internet. This computer can be used to store data, run software applications, or perform other computing tasks. Examples of cloud computing services include online storage services like Google Drive and Dropbox, software-as-a-service applications like Salesforce and Microsoft Office 365, and infrastructure-as-a-service providers like Amazon Web Services and Microsoft Azure.

The same tips for identity management should be followed for cloud computing along with:

7) Limit access to data: Grant access to cloud data on a need-to-know basis and ensure that appropriate access controls are in place.

8) Back up data: Regularly back up data stored in the cloud to ensure that it can be restored in the event of data loss or a security breach.

9) Monitor access and activity: Regularly monitor access and activity in your cloud accounts to detect any suspicious behavior or unauthorized access.

10) Regularly update software and applications: Keep all software and applications used in the cloud up to date with the latest security patches and updates to help prevent vulnerabilities from being exploited.

11) Have a disaster recovery plan: Have a disaster recovery plan in place in case of a data breach or other security incident, and regularly test the plan to ensure it is effective

Feel free to contact us with any topic requests or suggestions at security@bsd.uchicago.edu. We want to hear from you!

-BSD Information Security Office