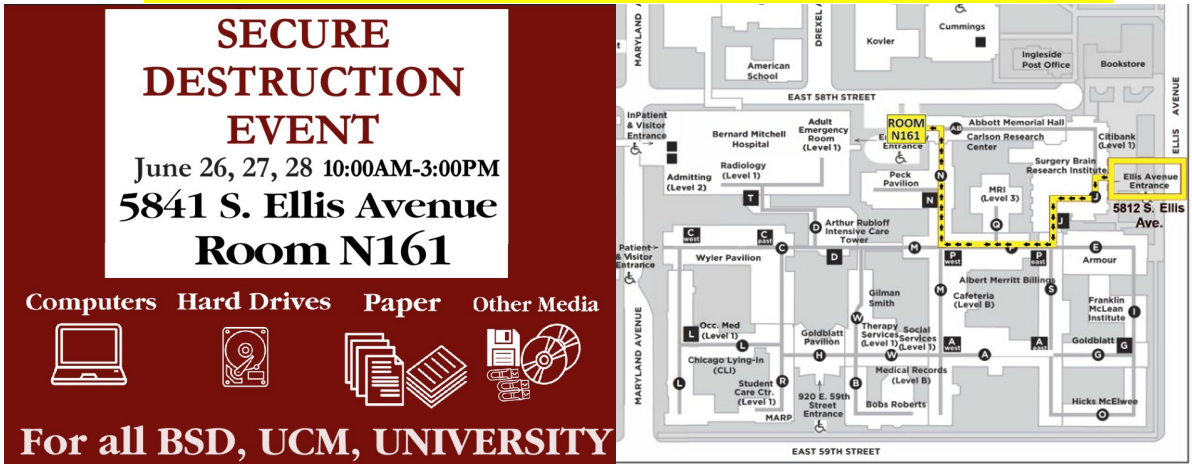
THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

June 2024

Cybersecurity Awareness
Newsletter
Protecting yourself and information from cybersecurity threats.



EVENT NOTICE: BSDIS will be hosting a **Secure Destruction Event** @
5841 S. Ellis Avenue in Room N161
This event will occur on:
Wednesday, June 26th, 10:00AM-3:00PM
Thursday, June 27th, 10:00AM-3:00PM
Friday, June 28th, 10:00AM-3:00PM

Please bring in any sensitive paper documents, hard drives, desktops, laptops, tablets, phones, monitors, USB thumb drives, CD-ROMs, and other computing media for secure destruction. If you have any questions, please feel free to contact security@bsd.uchicago.edu

Data is everything in today's digital world. Data is what drives decision making, influence, innovation, and is of paramount importance for growth. One could say that those who possess, utilize, and control data hold the keys to the kingdom of unprecedented power and potential. As the French author Voltaire alluded to, and a Spiderman movie once coined, "With great power comes great responsibility." So… this month we want to go over the importance of data discovery and data classification. Data discovery is the process of finding the data you have, and Data Classification is the process of organizing data into categories based on its sensitivity, value and importance which help to determine the appropriate protections and how data should be handled. Data classification is closely linked to data protections and data handling. The latter two will be discuss in a future newsletter. Feel free to use this information when thinking about the data you use in your daily work. Also, this month our intern Nik will be writing about passwords and password managers.


Resources to Keep in Mind:

BSD Policy for Data Handling and Classification:

- From the BSD Information Security Office: BSD Policy Document (must be on campus or use VPN to access).

University Policy for the Treatment of Confidential Information:

- Policy 601: Policy 601 Document

US Federal Government Information Processing Standard Publication Guidelines (FIPS 199):

- FIPS 199 Guidelines

HIPAA Privacy Rule by US Department of Health and Human Services (HHS):

- HIPAA Privacy Rule.

Storage Options

- University of Chicago Sensitive Data Usage Guide | Data Stewardship Council (uchicago.edu)

Data Discovery

At a very high level first we need to organize a bit by following a diagram like the above.

1) Identify the data we use.

2) Where does our data exist currently.
3) How valuable is the data.
4) Identify the security controls it needs.
5)Ensure that it is being monitored.

A quick example:
1) Social Security Numbers (SSNs).
2) Existing on a secure server named XYZ.
3) It is Protected Health Information (PHI), subject to the Health Insurance Portability and Accountability Act legislation, sensitive info which if exposed can subject us to monetary, reputation, and legal issues [Why Regulated Industries are Turning to Military-Grade Cyber Defenses (thehackernews.com)](#).
4) Needs security and privacy controls XYZ.
5) Logging access controls occur at the system level.

Data Classification

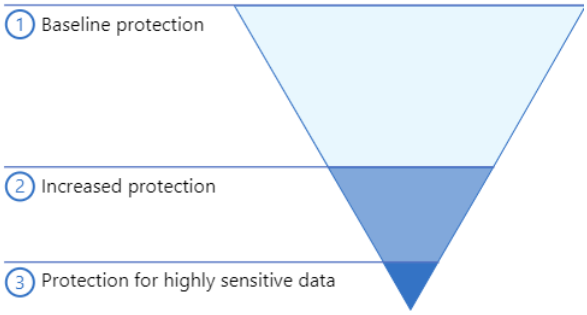
Now that we have identified our data and know what it is we need to consider if it is Restricted, Internal Use Only, or Public based on the definitions below as well as impact levels should the data be exposed.

Data Classification	Definition	Impact Levels
Restricted	Confidential information requiring the highest level of security and privacy protection. Access is only permitted as directed by the associated Data Steward or applicable University authority.	High, Moderate, or Overriding Concern
Internal	Confidential information requiring diligent security and privacy protection. Information may be shared within the University and its Medical Center on a need to know basis.	Low
Public	Information may be published and shared freely.	Public

Other items to consider are sensitivity, confidentiality, regulatory requirements as well as purpose/intended use should be considered when making the initial data classification:

- **Confidentiality and Sensitivity**: Determine the data type based on the potential impact of unauthorized disclosure. Consider whether the data contains personally identifiable information (PII), sensitive personal information (SPI), proprietary information. Data that requires protection due to its confidentiality or potential impact on individuals or organizations. This may include research data with limited access requirements or controlled dissemination.
- **Regulatory Requirements**: Identify any legal or regulatory requirements that apply to the data, such as privacy laws (e.g., GDPR, HIPAA), intellectual property laws, or data sharing agreements.
- **Purpose and Intended Use**: Consider the purpose of the research and how the data will be used. Data used for internal analysis may have different classification requirements than data intended for publication or sharing with external collaborators.

Proper classification of data helps the information security office to determine the proper controls necessary for the system where a specific type of data is being used. At a basic level the more stringent security protections are necessary on systems where sensitive data such as personal data, financial records, trade secrets, etc. exist so that they meet their regulatory or legal requirements of protections.



Besides a data usage agreement telling us what protections should be in place, how does one make the determination for the security protections that should be added? We will discuss this in the next newsletter.

Nik's Corner!

Hi, I'm Nikola Bilaver, an undergraduate 3rd year student at the University of Chicago, and I am interning at the BSD Information Security Office! Here, I will share my insights on security topics from my perspective as a student, which might be helpful to you.

Today's topic will be about passwords and password managers. In this digital age, it is common for people to have to manage several different accounts for many services. Although some services allow users to sign in with their fingerprint, face ID, or through an already signed in Google or Microsoft account, most will require a user to remember a password. This often results in two major security problems. The first is that users are more liable to create simpler passwords that are more memorable. The second is that users will often reuse passwords for multiple accounts, so if one service has a security issue that leaks the password, then all the accounts that share a username and password can be compromised as well.

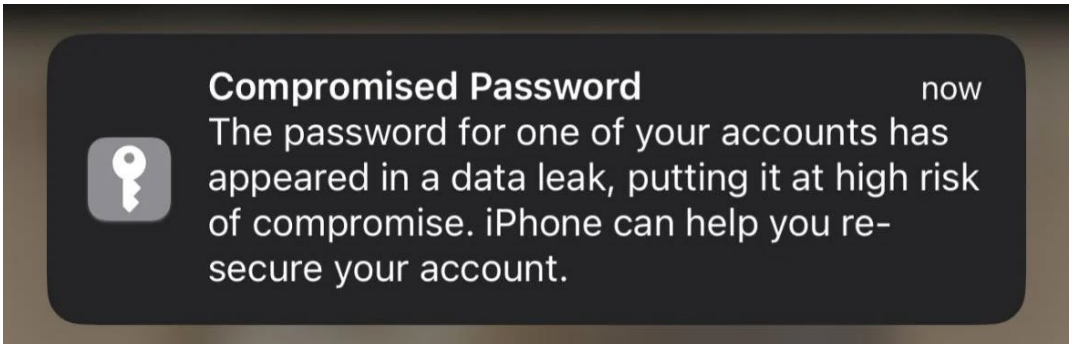
Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

In 2009, the now dissolved company RockYou had a vulnerability that resulted in the exposure of 32 million passwords. The above graphic shows the top 20 most used passwords found in the leak, and how tens of thousands of people may share the same insecure password. (Image Source)

Fortunately, a password manager is a tool that can solve both security issues while simplifying the handling of passwords. Password managers are tools that comes in many forms but share the same core principle: they securely store passwords for multiple accounts, so we don't need to remember them. We just need to remember one master password to access our other passwords, allowing each stored password to be secure and unique. Password managers often have features that synchronize with this purpose, like auto filling passwords (which can help prevent logging into fake websites), generating completely random passwords, and synchronizing those passwords across devices.



A common feature of many password managers is to notify us if our password is in a data leak, allowing us to change our password before our account is compromised.

Password managers are a great tool for bolstering security. But a common thought around password managers is "if a hacker guesses the password to our password manager, then won't they get

all of our passwords”? This highlights the importance of using a secure master password for the password manager. We will only need to remember one password, so make it secure! Another concern that may come to mind is whether a service is reputable, and if they can be trusted with our passwords. If a reputable manager is chosen, this should be a non-issue. When choosing a password manager, the following points should be kept in mind:

- It is recommended to use password managers that have two factor authentication, where an additional PIN provided through text, or an app is needed to log in. This makes it significantly harder for attackers to break into an account.
- A password manager should have a good security reputation. We should consider managers that use secure encryption standards to store their passwords and avoid ones that have had a history of multiple data breaches.
- Building upon the previous two points, the built-in password managers included with a browser or device, such as Edge Wallet, Chrome autofill, and Apple Keychain, are not recommended, as they usually lack 2 factor authentication and secure encryption standards. Usually these lack any kind of password protection at all, so if our device is being shared or left unlocked in the open, then all our passwords can be vulnerable. We recommend services that function through a website or browser extension (if they are reputable).
- While there are many password managers out there that are paid services, there are plenty of free services available that provide many helpful features with a good security reputation. But we need to be careful, as many ‘free’ password managers make a profit through tracking the accounts we create passwords for and selling that information to advertisers. We need to check the privacy policies of these services before using them.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

The above graphic shows roughly how long it would take for a hacker to guess a password. Note that these values are rough estimates that may vary depending on the exact password used.

When transitioning to using a password manager, note if we use a weak master password to protect it, or if it is used to store repeated, weak passwords, then the point of using one is defeated. The BSD password policy requires the use of a password with a minimum length of 12 characters containing uppercase letters, lowercase letters, numbers, and symbols. The BSD password policy also recommends the use of passphrases, which are passwords consisting of multiple words stringed together, which can make remembering a password easier. These should be a minimum length of 19 characters. The passwords stored in the manager can be generated to be even more secure than the password for the manager itself, as many services will auto generate passwords of this level of strength. If all the passwords used are secure and unique, then our accounts will be exceptionally well protected.

Hopefully after receiving this advice, we will be able to secure your digital life by using a password manager!

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 .