ISSUE: August YEAR: 2019

Security Awareness Newsletter

"Technology is unlocking the innate compassion we have for our fellow human beings." -Bill Gates

LOYOLA UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

LastPass Password Management

Information Technology Services will soon offer services provided by LastPass. LastPass is a password management service that aids in the management and security of all of a user's passwords. LastPass requires that you remember one password (your "Master Password") and in return, LastPass stores every unique password you use regularly to log into other websites.

Using LastPass provides many benefits in addition to only having to memorize one password. LastPass also acts as an organizational tool for all of your passwords. Also, every login screen will come auto-filled with the specific credentials to that website. Along with your LastPass Master Password, LastPass also requires a second authentication method (such as Microsoft Authenticator). Alongside the individual benefits of a secure password vault, LastPass also provides cooperative benefits by allowing users to share website credentials with other users.

Users can choose between multiple different security layers for each user, or for each specific website that they share. Public accounts will now be easier than ever to share between users, as a website credential admin can customize the access of each individual account with no impact to other accounts on the website.

For more information on LastPass and its functions, please click on the link below.

https://www.luc.edu/its/services/password/lastpasspasswordmanagement/

Please visit https://www.luc.edu/its/vpmo/resources/loyoladigitalexperience/ to learn more about Loyola Digital Experience (LDE) strategy.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) technology helps to protect your accounts against the most common avenue of attack: password compromise. Whether your password was obtained during a phishing attack, guessed using brute force, or a variety of other methods, MFA can still ensure you are the only one using your account to access supported applications and services. This is accomplished through the use of additional components or "factors" (such as a mobile app, phone call, or text message) to verify identity after your password is entered successfully.

Loyola is in the process of implementing a Microsoft MFA service, which was integrated with LSA on 6/25/2019. Going forward, we plan to use this technology to secure other University services such as email and OneDrive. Supported verification options include push notifications or codes within the Microsoft Authenticator mobile app, a phone call, and codes delivered via text message.

Please visit https://www.luc.edu/its/services/mfa/ to learn more about this program, as well as to view the MFA FAQs and Quick Guide.

Data Loss Prevention

We work with different types of sensitive information in our day-to-day work lives, ranging from Social Security and credit card numbers to student records. What happens if this data is accidentally or purposely misused, exposed, accessed by an unauthorized user, or sent to an unintended recipient? This is where DLP comes into play to ensure that sensitive information stays protected.

For example, if an individual attempts to share sensitive data with someone who may not be an appropriate recipient, DLP may prevent the sharing action. DLP may take a variety of actions (e.g. alerting, blocking, and encryption) to prevent users from accidentally or maliciously sharing data that could put their department or the University at risk. DLP tools are also used to stay in compliance with federal and state security and privacy laws such as HIPAA, PCI-DSS, FERPA, and others.

At Loyola University Chicago, the University Information Security Office has procedures in place to protect all student, faculty, and staff data to ensure that your information has not been accessed or compromised by an unauthorized user.

In addition to our current procedures, Loyola University Chicago will be implementing a DLP solution in the near future. More information on this solution will be provided to you before implementation.

Below are some additional benefits of Data Loss Prevention:

- Prevents important business data from being disclosed outside the institution
- Prevents data from being compromised or stolen by an unauthorized user
- Monitors the usage of (and secures) data according to established policies
- Ensures that data is managed in a uniform manner across the organization

New Protected Location for Instructions and Forms Containing Sensitive Data

Included in ongoing information security improvements and to reduce the risks of data loss, Loyola University Chicago will begin moving some of its documents and forms that deal with sensitive data to a more secure location.

In the coming weeks, some of these forms on the HR and Finance webpages will be updated to require a Loyola login to access.

This modification will ensure that only authorized personnel have access to the processes that specifically deal with sensitive information.

University Information Security Office
LUC.edu/its/uiso/

ITS Service Desk
Email: ITSservicedesk@luc.edu
Telephone: (773) 508-4487
Hours: LUC.edu/its/service/support_hours.shtml