ISSUE: 5-5 YEAR: 2016

University Information Security Office Newsletter

"People always make the best exploits. I've never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads" — Elliot Anderson

The Cloud

SANS Securing the Human

What is the Cloud?

The cloud is a powerful technology that our organization uses. Cloud computing is nothing more than using an outside service provider to store, manage or process our data. The reason we call this service "the cloud" is you never know where our data is physically stored. It is being served somewhere in the "cloud." Examples of cloud computing include creating documents on Google Drive, sharing files via Dropbox or storing your music or pictures on Apple's iCloud.

Solution

Cloud services enable our organization to be more productive, but they also come with additional risks. As such, please be sure to follow these steps whenever working with cloud services.

Permission

Ensure that you have permission before using any cloud technologies and that you use only organization- approved cloud vendors. Do not sign up for a new service without permission. Also, be sure you understand our policies on which information can and cannot be stored in the cloud and whom you can share it with.

Personal Cloud Accounts

Ensure that any work-related data is never copied or stored on any of your personal cloud accounts, such as Apple's iCloud or your personal Dropbox account. In addition, do not access any personal cloud accounts from work computers or devices unless you have prior permission.

Unique Password

Use a unique password for each of your cloud accounts. If your cloud service supports two-step verification, we highly recommend you use it. This adds an additional layer of protection to your account. Never use the same password for your cloud accounts as any of your personal accounts.

Configuration

By default, configure your cloud account so that it does not share information or files with anyone. Only share specific files with specific people or groups of people who have authorization and a need to know that information. Once they no longer need access to those files or information, remove their access to the data.

Anti-Virus

Be sure you scan any shared files with anti-virus before opening them. Since the cloud may be storing these shared files on other people's computers, these files may be infected, as other people may not have the same level of security as you. For example, an organization was once sharing files through the cloud with several different people. One of the individuals did not have their computer secured and accidently infected it and all of their files, including any files shared through the cloud. The virus worked by encrypting all the files, then demanding the organization pay a ransom to decrypt them. Since these files were shared over the cloud, it meant that all the shared files on everyone's computers were infected and encrypted.

Administration

Be careful what rights or privileges you assign to others. Some cloud services not only allow you to share files, but allow you to assign administrative rights to other people. This means you can give people you are sharing your files with the ability to allow others to access or edit them. Only give people the least amount of access they need to get the job done. If you have any questions about which cloud services you can use for work or what data can be shared and with whom, please ask your supervisor or information security team.

From the ISO's Desk

Our May Awareness topic is all about "The Cloud". The cloud has many benefits. It's Flexible, allows for increased collaboration, and gives you the ability to work from anywhere. We also need to be aware of some of the risks that the cloud creates. Using unapproved cloud services or personal cloud storage for university files puts documents at risk because of the need to have some form of control for FERPA, HIPAA and PII related content and we all need to make sure that we protect our student's and colleagues' information.

If you would like to know more about our awareness activities, please check out Inside Loyola or go to our web page: http://www.luc.edu/uiso

Safe Computing to you all!

Jim Pardonek, Loyola's Information Security Officer

Cloud Storage and Loyola

The term "cloud" is one of the latest buzzwords that the information technology industry uses to put a pretty bow on technology that is hosted elsewhere which has actually been around for some time.

One of the convenience features that was added to hosted applications is to make then available using any web browser. This enhances the ease of use that we are all looking for to help us in our work and personal lives. Many of these services have "free" editions designed to give you limited functionality or space in the hopes that you will need more and pay for it later. It is easy to take advantage of the free services so you can have access to files wherever you may be.

What could happen is that you may inadvertently store protected or sensitive information in cloud storage that has not been checked and approved by the university. This causes multiple problems, Some of which are inadvertent sharing with non-Loyola personnel, risk or a breach by the cloud service, and loss of the ability to track where protected data may be , which the university is required to do in case of a loss of personal information or during legal investigations.

Currently, the only university approved cloud storage is box. You can access your Loyola box account by browsing to luc.box.com and using your UVID and Password. ITS will be exploring other options in the future to expand Loyola's cloud storage options for students and faculty. Loyola also has a policy that governs the use of cloud storage. http://www.luc.edu/its/itspoliciesguidelines/cloud_computing_policy.shtml

Loyola Secure Transfer

Loyola Secure Transfer, our new file sharing service, allows users to securely send and receive files that are too large to send via e-mail or contain sensitive information.

The service allows files up to 2 GB to be securely uploaded, distributed, and downloaded by identified recipients—Loyola and non-Loyola users—within 10 days of the send date. Users may also further protect encrypted files by sending private messages and restricting the number of times non-Loyola users can download the file.

All faculty and staff now have access to Loyola Secure Transfer. To log in, visit securetransfer.luc.edu and use your UVID and password.

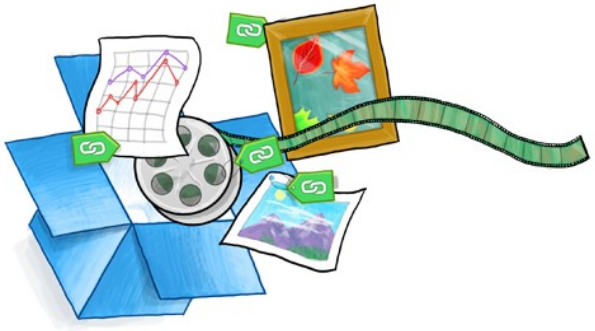
For more information and a full list of suggested uses for Loyola Secure Transfer, visit our resource page, http://www.luc.edu/uiso/resources/loyolasecuretransfer/

If you have questions about Loyola Secure Transfer, please contact the ITS Help Desk at 773.508.4ITS (4487) or helpdesk@luc.edu.

Share Files Using Links

The cloud is an amazing tool for sharing information; however, you can easily share the wrong information with the wrong people (or even the entire Internet). One common feature of some cloud services is the ability to create a web link that points to files or folders on your computer. This feature allows you to share these files with anyone you want by simply providing a web link.

The problem with this method is that there is very little security. Anyone that knows this link has access to your personal files or folders. If you send the link to just one person, that person could share that link with others or Google could harvest it. Before you know it, anyone can access the files. If you are authorized to share data by using a link, be sure you disable the link once it is no longer needed.



Loyola Aware

Our May awareness topic is " The Cloud", which will be live on May 4th.

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further information.

If you have any questions in regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)

Contact Information

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM