- National Data Privacy Day 1
- From the ISO's Desk..1
- Cloud Storage.....1
- Privacy Tips.....2
- Safety Tips for Mobile Devices 2

ISSUE: 1 YEAR: 2017

University Information Security Office Newsletter

"Once you've lost your privacy, you realize you've lost an extremely valuable thing." - Billy Graham

From the ISO's Desk

This month we highlight Data Privacy Day. According to EDUCAUSE, Data Privacy Day (DPD) is an annual effort to empower people to protect their privacy and control their digital footprint, as well as escalate the protection of privacy and data as everyone's priority. IT stresses the importance of protecting your digital footprint, and especially the digital footprints of others by identifying and protecting those types of information that can be used to exploit an individual both economically and socially. Economically by protecting Personally Identifiable information such as Social Security Numbers and banking related information. Socially, by being careful about what you post on social media. Not only about yourself, but others as well. When private information falls into the wrong hands, it inevitably leads to identity theft which can take years to correct. Happy Data Privacy Day!

Jim Pardonek
Information Security Officer

Our January awareness topic is Privacy.

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)

Celebrate National Data Privacy Day

National Cyber Security Alliance

Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the Jan. 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Data Privacy Day is now a celebration for everyone, observed annually on Jan. 28.

The National Cyber Security Alliance (NCSA) assumed leadership of Data Privacy Day from the Privacy Projects in August 2011. A nonprofit, public-private partnership dedicated to promoting a safer, more secure and more trusted Internet, NCSA is advised by a distinguished advisory committee of privacy professionals.

Data Privacy Day is the signature event in a greater privacy awareness and education effort. Year-round, NCSA educates consumers on how they can own their online presence and shows organizations how privacy is good for business. NCSA's privacy awareness campaign is an integral component of STOP. THINK. CONNECT. – the global online safety, security and privacy campaign.

On Jan. 27, 2014, the 113th U.S. Congress adopted S. Res. 337, a nonbinding resolution expressing support for the designation of Jan. 28 as "National Data Privacy Day."

How to use Cloud Storage

Jim Pardonek

In computer-speak, the term cloud has worn many hats from the use of "dumb terminals" connected to mainframes, CPU time sharing, and Remote Job Entry in the 1950's to virtual circuits in the 1990's to what we know of today as services provided by an entity other than ourselves. Examples of this are Google Mail, Box for file storage, and Office 365 for our students.

Cloud storage is a useful, convenient and cost effective way to keep your files handy or to share them with collaborators. Files stored in the cloud can usually be accessed from anywhere, anytime and in most cases, a smartphone or other mobile device can be used. Although cloud storage companies make for convenient access to files, there is a responsibility that we, as end users, have when using these services.

First, we should separate our personal files from university-related files. Just as many of us may have a file folder in our desk marked personal, we generally don't sprinkle the contents amongst the other file folders in the drawer that contain our work.

Second, we need to make sure that we only use approved providers for Loyola information. Currently the only university approved cloud storage provider is BOX. There are however, 2 versions of BOX as they provide free space for any individual as well as the purchased separate space for Loyola University Chicago use. For university files, we need to make sure that we are using the Loyola BOX. (https://luc.box.com)

Third, we need to make sure that we look at the files that we want to store in the cloud and decide which classification type they fall under, be it Protected, Sensitive, or Public.

Per the Loyola University Chicago Cloud Computing Policy: (http://www.luc.edu/its/itspoliciesguidelines/cloud_computing_policy.shtml), it is never acceptable to store Loyola Protected data on any cloud service. This includes data such as grades, social security numbers, private correspondence, classified research, etc. These should be stored on internal central or departmental servers. Putting protected information in cloud storage could place you and the university in a position where state or federal laws and regulations are violated.

If there is ever a doubt whether a file should be saved in the cloud, you can always contact the University Information Security Office for guidance.

Privacy Tips

National Cyber Security Alliance

Help your family, friends and community be privacy-savvy. Use these research-based privacy tips to get the conversation started.

Share With Care

What you post can last a lifetime: Before posting online think about how it might be perceived now and in the future and who might see it.

Own your online presence: Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Be aware of what's being shared: Be aware that when you share a post, picture or video online, you may also be revealing information about others. Be thoughtful when and how you share information about others.

Post only about others as you have them post about you: The golden rule applies online as well.

Personal Information Is Like Money.

Value It. Protect It.

Think before you act: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.

Lock Down Your Login: Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

Safety Tips for Mobile Devices

Your mobile devices – including smartphones, laptops and tablets – are always within reach everywhere you go, whether for work, travel or entertainment. These devices make it easy to connect to the world around you, but they can also pack a lot of info about you and your friends and family, like your contacts, photos, videos, location and health and financial data. It's important to use your mobile device safely.

Secure your devices: Use strong passwords or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.

Think before you app: Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps.

- Now you see me, now you don't: Some stores and other locations look for devices with Wi-Fi or Bluetooth turned on to track your movements while you are within range. Disable Wi-Fi and Bluetooth when not in use.
- Get savvy about Wi-Fi hotspots: Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected.
- Limit what you do on public Wi-Fi and avoid logging in to key accounts like email and financial services on these networks. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection on the go.

University Information Security Office
For more information or to report a security incident:
Email: DataSecurity@luc.edu
Web: www.luc.edu/uiso
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM

References: National Cyber Security Alliance, Stay Safe Online