ISSUE: 3-12 YEAR: 2015

University Information Security Office Newsletter

Technology gives us power, but it does not and cannot tell us how to use that power. Thanks to technology, we can instantly communicate across the world, but it still doesn't help us know what to say.

–Jonathan Sacks

From the ISO's Desk

This month's newsletter is a departure from previous issues where in the past we have had a theme of sorts. This month we focus on 3 differing topics.

The first article reminds us that our data is valuable and if lost through a hardware failure, loss or deletion, can be the source of considerable delays and rework trying to recreate the information.

The second article introduces the concept of 2 factor authentication. Although we may not always be aware that we are using this more secure logon method, many of us that use online banking use it regularly.

Last is an article on the safe use of Wi-Fi networks. Although convenience is a wonderful thing, if we are not vigilant in our use of public Wi-Fi, we can be subjected to identity theft among other things if we connect to an unsecured public network. Please let us know If you have any comments or suggestions for topics.

University Information Security Office

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

Backing Up Your Files

Created by Jim Pardonek

Until it happens, many of us only consider backing up our data after we've lost it. With the reliable nature of computer hardware nowadays, it's easy to fall into the trap of thinking that your hardware won't fail and that it will run until you are ready to move it over to the new machine that you recently bought. The fact is, although storage technologies have improved over time, many of them still contain much of the mechanical features that a hard disk had in the 1980s. This makes the drive prone to mechanical failure over time as the magnetic head sweeps back and forth very quickly over the Frisbee shaped disk platters inside the drive. The best way to ensure that you are preserving your valuable data is to either back it up to another device or save it to a location that is backed up for you.

Remember that when backing up University data one needs to review the data handling guidelines prior to deciding where to back up Loyola data. The reason being that the University needs to be cognizant of the types of data we have and the impact on our students and staff should that data be stolen or lost.

When manually backing up your files, you need to consider these steps as you perform the backup.

1. Decide what files you'd like to back up.

2. Prioritize how you store your important files in specific locations to make backing up much simpler. Keeping the most important data under a single file structure makes it easier to prioritize and back up that data more often.

3. Insert your backup media (USB stick, writable CD/DVD, or portable hard drive) and perform the copy. Don't forget that if you are manually backing up your files you should devise a way to remind yourself to do it occasionally so that you don't forget.

Another way to back up your information is to find or purchase a backup program. Purchased versions of these programs will compress the data so that you can optimize your backup storage space. Another advantage of purchasing a backup program is that many of these programs contain scheduling and automation options to make backups a no-brainer.

Finally, and by far the easiest way to ensure your files are backed up is to use network services that are automatically backed up to store your files. For University related information it is recommended that you store your files either on your departmental N: drive, or your individual U: drive. Both the U: and N: drives are backed up daily by ITS. The University also allows the use of the University purchased instance of BOX (luc.box.com), for storage of University information that is not classified as Loyola Protected. For Loyola Sensitive information, you should check with your supervisor to make sure it is permissible for storage in BOX. Public information can be stored in BOX without restriction.

For your own personal information you can use services such as Google Drive, Dropbox, or Microsoft OneDrive. Remember currently the University does not allow the storage of University information on any cloud service other than the luc.box.com account.

Two-Factor Authentication

Created by Jacob Schuldt

With the increasing number of account hacks and the decreasing amount of knowledge required to complete these attacks, it is becoming very important to secure accounts at one of the most important layers of protection: the log-on process. Passwords are becoming easier to hack as time goes on, and even "strong" passwords aren't as safe as they used to be. Because of this, various organizations have begun implementing two-factor authentication as a more secure way for users to log on to their accounts.

What is it?

Two-factor authentication is a method of authentication that requires more than just a password for a user to access their account. Matt Cutts from Google says, "two-factor authentication is a simple feature that asks for more than just your password. It requires both 'something you know' (like a password) and 'something you have' (like your phone)."

There are various items that can be the "second factor." For example, you can have a code sent to your phone via text message or have an e-mail sent with a special code, which you then enter into the website. Some applications, such as Facebook, can require you to access their mobile application and obtain a unique code from their code generator before you can access your account from a new device.

Where can I use two-factor authentication?

To prevent account hacks, many organizations have begun making this option available to users, and it is strongly suggested that you use this service on all accounts when possible. Some of the websites that have this option are: Google, Facebook, Twitter, Steam, Microsoft, and LinkedIn. Many websites will have the option to turn on this service under privacy or account settings.

Summary

Two-factor authentication is an additional, strongly recommended layer of security on top of your password, and ensures that an attacker cannot simply access your account by cracking your password. In addition to this, it is recommended that you have different passwords among accounts, because if a user has one password, and they have your e-mail password to the account that the special code goes to, your account is still in jeopardy. Two-factor authentication and password variation together make your account nearly impenetrable to password attacks.

Using Open Wi-Fi

Created by Chris Campbell

With the widespread availability of today's Internet, many of us tend to take it for granted. An ever-increasing number of stores, restaurants, hotels, and other locations are offering free wireless access to their customers. This can be quite useful, but there are a few security implications to consider before you connect any device to an open Wi-Fi network.

Wireless access that is intended for guest use does not usually require a password, as it would have to be distributed somehow. This means that everything transmitted and received over that connection is visible in clear text to every single Wi-Fi enabled device in the area. For your home wireless network, configuring strong security (typically WPA2-PSK, also known as WPA2-Personal) prevents nearby devices from being able to see everything you are doing. Before anything is transmitted over a secured Wi-Fi connection, it is encrypted and appears as meaningless data to anyone without knowledge of your wireless password.

When you connect to a public network intended for guest use, the most you are likely to encounter is a usage agreement. However, this is typically intended to protect the entity providing the Internet access and should not be mistaken for a secured connection. It is also surprisingly common for an attacker to set up a public wireless network that exists for the sole purpose of collecting your valuable information. Public networks should never be used for anything you would not want to become public knowledge. At all costs, avoid activities that may expose sensitive information (such as making purchases or conducting online banking).

Loyola University makes two wireless networks available to its community: 'loyola' and 'Eduroam'. Both of these are protected by our Network Access Control system, which requires you to register each device before it is trusted on the network. However, the 'loyola' network is unencrypted. This means that even though we have controls in place to only allow Internet access for trusted users, your data may still be visible to other devices in the area. To combat this, Loyola provides an encrypted wireless network: 'Eduroam'. One downfall of typical wireless networks that utilize a shared password is that everyone with that password has the ability to decrypt the connections of other users. However, our 'Eduroam' network is not susceptible to this, as each user authenticates using different information. This means that once you connect to 'Eduroam' (and authenticate with your full Loyola email address and password) your information is not visible to other devices in the area, whether they are on or off the network.