ISSUE: September YEAR: 2019

Security Awareness Newsletter

"Lets go invent tomorrow instead of worrying about what happened yesterday" - Steve Jobs

LOYOLA UNIVERSITY CHICAGO 1870 AD MAJOREM DEI GLORIAM

Preparing people to lead extraordinary lives

October is National Cyber Security Awareness Month!

Protecting Your Privacy

We live in a world where our digital lives are seamlessly connected. The apps we use on our phones, the websites we visit, and the networks we connect to all make digital life exciting and the possibilities endless. It's essential to consider one's privacy given all of these outlets for personal information to be compromised. By securing your devices and being aware of the access that apps and online accounts (such as social media accounts) can access, you can significantly reduce the risk of your private information/data being compromised.

Securing your digital life might sound complicated, but these few steps can help you:

- Use strong passwords. We recommend a minimum of 8 characters that has a combination of upper and lower case letters along with a special character and numbers.
- On your mobile device, if possible, enable its biometric authentication (Touch ID/Face ID on iOS or fingerprints on Android) to ensure that your private information cannot be physically accessed by people that should not be seeing it.
- When available, enable multi-factor authentication for online accounts to greatly decrease the chances of your accounts being compromised.

These simple considerations can do a great deal to keep your devices and accounts out of reach of cybercriminals and others who should not be viewing your personal information.
We all use multiple apps and visit different websites every day. When downloading apps and using various sites, consider the permissions that you grant to these services. For example, ask yourself: does your fitness app really need access to your e-mail? The same goes for websites; when creating profiles online, many sites ask to use your personal information for various purposes. Only grant access to reputable services and be aware of the risks that you are taking on when you accept terms and conditions of large numbers of apps and websites.

Digital life is all around us, and there's no reason to hide from it or try to disconnect. By carefully considering your actions on connected devices, you can significantly reduce the risk of having your private information compromised online.

Social Media Security

Social media is an important part of everyday life for many. Today, social media outlets such as Twitter and Facebook intake millions of data entries from people around the globe. With this vast amount of incoming data, such services are a prime target for cybercriminals looking to take advantage. Here are some of the many ways to help keep your data safe:

- Make your account visibility private
- Keep passwords unique across accounts
- Enable multi-factor authentication
- Limit or completely disable location services
- Only add or friend people you know in real life
- Turn off syncing software to avoid auto-filled data entries

SECURITY & DONUTS INFO SESSIONS

October is Cyber Security Awareness Month! Learn how to keep your information, your identity, and your computer safe from hackers and identity thieves. Join us for a brief & interactive event, have a donut and coffee and learn how to keep safe online.

- **LSC**, October 8, 9:00am-10:00am, DSC 214
- **WTC**, October 15, 9:00am-10:00am, CLC 0727
- **HSC**, October 22, 9:00am-10:00am, CTRE 428
- **Zoom Sessions**, October 29, 9:00am-10:00am

Wi-Fi Security

Public wireless networks make it easy to stay connected on the go, but beware: public wireless networks and hotspots are not secure. Connecting to an unsecured network makes it possible for others to see what you are doing on your device and access unencrypted data transmissions while you are connected. Limit your connection to public Wi-Fi and be careful of what you are doing when you are connected to such networks. Try to avoid logging into important accounts such as bank accounts and email when connected to public Wi-Fi. Also, consider using a virtual private network (VPN) or personal mobile hotspot if you would like to be more secure while connecting on the go. The use of a VPN can significantly increase your security by encrypting your network traffic. When browsing the Internet on a public or unsecured Wi-Fi connection, consider avoiding website URLs that do not begin with https://. Websites that do not use HTTPS do not encrypt your information, making it visible to potential attackers on an unsecured network.

In summary, here are some of the important points of Wi-Fi security:

- Avoid public networks
- Use a VPN
- Do not log into personal accounts such as a bank accounts
- Enable mobile hotspots instead of using public Wi-Fi

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

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