OCTOBER ISSUE YEAR: 2017

University Information Security Office Newsletter

"It takes 20 years to build a reputation
and few minutes of cyber-incident to ruin it."
-Stephane Nappo

From the ISO's Desk

This October is the 14th annual National Cyber Security Awareness Month (NCSAM) campaign. NCSAM is a national public awareness campaign intended to encourage everyone to protect their computers and our nation's critical cyber infrastructure. Cyber security requires vigilance 365 days per year. However, the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate to shed a brighter light on what home users, schools, businesses and governments need to do in order to protect their computers, and data. This year the University Information Security Office is holding a Security and Coffee session at each campus. Each session contains a brief presentation on keeping your information safe followed by a Q&A on any information security topic. The UISO staff is also available to speak at any departmental meeting to talk about Cyber Security both at Loyola and at home. If you would like to know more about our NCSAM activities, please check out Inside Loyola or go to our web page https://www.luc.edu/uiso

Jim Pardonek
Information Security Officer

University Information Security Office

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

Safety Tips for Mobile Devices

National Cyber Security Alliance

Your mobile devices – including smartphones, laptops and tablets – are always within reach everywhere 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.

The first step is to STOP. THINK. CONNECT.

STOP: make sure security measures are in place.

THINK: about the consequences of your actions and behaviors online.

CONNECT: and enjoy your devices with more peace of mind.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

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.

Delete when done: Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterwards, or we may have previously downloaded apps that are no longer useful or interesting to us. It's a good security practice to delete all apps you no longer use.

Now you see me, now you don't: Some stores and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi 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.

KEEP A CLEAN MACHINE:

Keep your mobile devices and apps up to date: Your mobile devices are just as vulnerable as your PC or laptop. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.

Loyola Aware is Changing

Beginning in November, Loyola Aware will be moved to the new Advanced Cyber Security Learning Platform (ACLP) offered by SANS. This new platform will allow for faster delivery of both new and modified content to keep pace with the changing Cyber Security Threat landscape that we all face every day. In addition to some new topics ALCP will be easier to navigate and track your individual progress. It will also allow Loyola to meet several compliance requirements that are mandated by regulations such as HIPAA, FERPA, and PCI-DSS. Look for future announcements as to when the new Loyola Aware will be available.

LOYOLA
UNIVERSITY CHICAGO

Lock Down Your Login

Protect Accounts with Strong Authentication

National Cyber Security Alliance

What is strong authentication?

Strong authentication – sometimes called multi- or two-factor authentication – provides an extra layer of security beyond your username and password to protect against account hijacking. Many online services, including email and social networks, offer this free extra security protection to help ensure it's actually you trying to access your account – not just someone who stole or guessed your password.

How does it work?

Strong authentication requires you to have more than just your password to sign into your account. Strong authentication tools are widely available on major email and social networking sites. The most common methods you can choose from are: Security Keys (A small device that plugs into your USB port or is used in conjunction with a phone) Biometrics (fingerprint, facial recognition or other unique personal identifier) or One time Codes (A unique code sent after entering your username and password, usually by text to a mobile device that is then entered on the site to verify it's you).

Here's how to Turn on Strong Authentication

Many Internet services support strong authentication. Here is a listing of a the most commonly used sites:

Google: With 2-Step Verification on your Google Account, it takes more than just your password to sign in. This could be a six-digit code that you get through the Authenticator app or SMS. For even stronger protection against phishing, you can set up a Security Key. You can learn more about using a Security Key on your Google Account at g.co/securitykey. If you opt to receive authentication codes over SMS, be sure you're taking the steps under "Protect Mobile Devices" to keep your phone safe.

Facebook: As more individuals and businesses turn to Facebook to share and connect with others, people are looking to take more control over protecting their account from unauthorized access. Login approvals is a Two Factor Authentication system that requires you to verify your identity via a code sent to your mobile device whenever you log into Facebook from a new or unrecognized computer. Once you have verified your identity, you'll have the option to save the device to your account so that you don't see this challenge on future logins.

For more information on other sites including Twitter and others, please see https://www.lockdownyourlogin.org/strong-authentication/

Password Tips and Securing Accounts

National Cyber Security Alliance

Passwords can be inconvenient, but they're important if you want to keep your information safe.

Protecting your personal information starts with STOP. THINK. CONNECT.: take security precautions, think about the consequences of your actions online and enjoy the Internet with peace of mind. Here are some simple ways to secure your accounts through biter password practices.

Tip #1: MAKE YOUR PASSWORD A SENTENCE

A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!

Tip #2: UNIQUE ACCOUNT, UNIQUE PASSWORD

Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

Tip #3: WRITE IT DOWN AND KEEP IT SAFE

Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

Tip #4: 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.

Help Us Celebrate Cyber Security Awareness Month by Attending One of Our Awareness Events

Security Coffee Sessions

• Wed. October 18,	9:00AM-10:00AM	WTC Corboy 601
• Thu. October 19,	9:00AM-10:00AM	LSC DSC 214
• Thu. October 26,	1:00PM-2:00PM	SSOM 170