APRIL ISSUE YEAR: 2018

University Information Security Office Newsletter

"You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable. "

– Daryl White, DOI CIO

Social Media Best Practices

Chibuzo Anaeto

While we all love our Facebook, Snapchat, Instagram, Twitter, and other preferred forms of social media, we should not forget the danger that comes with them as well. As these technologies continue to grow, cyber thefts and hackers have grown in parallel. Some are making a full-time career of it, and many users continue to fall prey to them. In this world of technology, it is imperative to understand the intricacies surrounding negative side of social media, as well as some social media best practices to avoid falling prey.

First, how secure are your passwords? If you feel the same way I feel about the burden of remembering passwords, then we would all want to use our names as passwords. Maybe we have made efforts to create a complex password, then used that password for all our social media accounts. After all, how many complex passwords do you want to remember? It is always advisable to use strong and unique passwords for your social media accounts. Using a strong password makes it more difficult for hackers to easily decode or guess your password, hence making it tougher for one to fall victim. The world of technology is always evolving, and different techniques are being applied by hackers to trample on compromised victims who don't apply salient measures to protect their accounts.

Never use the same password and/or username for all your social accounts. Using different usernames and passwords is a fantastic protection technique for social media. This kind of habit should be practiced consistently to avoid the wide-ranging effects of a compromise. Imagine if by any chance your Facebook account becomes compromised and your login details get into the hands of someone else. The rest of your social accounts would also be compromised because the same credentials are in use everywhere. Because of this, it is necessary that users protect their accounts using complex, unique passwords for each account.

While we love to share our social pages with our friends and other users, it is important to pay attention to which friends we choose to accept on social media pages. This will help reduce the amount of information about you that is publicly available, which can in turn reduce your risk for other types of attacks.

How about social accounts and platforms that we are no longer active on? Always remember to close accounts that are not being used, as forgotten accounts can easily be preyed upon.

Users should always have the most recent updates for their social apps, as security patches protect one from known threats.

Useful Information

University Information Security Office

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

Loyola Information Security Blog

http://blogs.luc.edu/uiso/

For current information regarding security risks at Loyola

Loyola Aware

Cai Wang

Beginning in April, our Loyola Information Security Awareness Program – Loyola Aware — is now hosted on a new platform. New training modules are available for all faculty and staff. Updated interactive training modules include engagement questions to deepen learning and change behavior, while also reducing module run times to increase impact.

Loyola Aware is Loyola's Information Security Awareness Program, which was started in 2015 and designed for all faculty and staff. The purpose of the program is to increase the employee's security awareness by providing short video snippets that bring to light specific topics in Information Security. By increasing awareness, the program allows everyone to recognize IT Security concerns and respond accordingly.

To Access Loyola Aware

1. Go to https://access.sans.org/go/loyolauniversitychicago, and log in with your UVID and password.
2. All current LUC employees should already be enrolled in Loyola Aware. If you are having any trouble with logging in to the site, please email DataSecurity@luc.edu.
3. There should be two sections on the home page: "Required Training" and "Recommended Training". Different training modules are assigned to each user based on your role at Loyola. Loyola Aware general modules are located under the recommended training section.
4. All modules require a minimum score of 60% to pass.
5. After completing all training that was assigned to you, you will be provided with a certificate of completion.
6. Assessments remain available for unlimited attempts. Users can click on the Gradebook to check their scores and get immediate feedback.

For additional questions or assistance, please contact the University Information Security Office: DataSecurity@luc.edu

In the News

Simon Jakubczak

When signing up for any social media, there are some options to opt out of sharing your personal data with its creators, but is your data truly safe with them or even others? Consumers of social media such as Facebook, Twitter, and even Instagram should understand that once something is on the Internet it will be incredibly difficult to remove. Likewise, once any data is acquired maliciously, virtually nothing can be done to enforce the deletion of it.

In recent news, a company by the name of Cambridge Analytica reportedly managed to acquire data from over 50 million users of Facebook. The goal of the data acquisition was to "identify the personalities of the American voters and influence their behavior", and it was also collected under the notion that it would be used for "academic purposes". What Facebook didn't know was that the information was instead used to create personality profiles in order to shape campaign messages during the Trump-Clinton Campaign. What troubles some more minds is the link between the corporation of Cambridge Analytica, Russia, and Ukraine, as well as the founder of Wikileaks (Julian Assange).

Some users are speculating that the "data leak" was in fact a breach of Facebook systems, when in reality it was a misuse of information by Cambridge Analytica. The terms of service and platform policies are set in place to protect the information of each user who agrees to them. Any information that was collected was agreed to by the users, and no sensitive information or passwords were stolen in this case.

Aside from not using social media, we have compiled 4 steps to take you in the right direction towards securing your data on social media.

1. Limit what personal data you add to your profile.

2. Turn off all location services.

3. Try to limit the number of Third Parties that are linked to your accounts.

4. Turn off as many sharing settings as possible.

Rosenberg, Matthew, et al. "How Trump Consultants Exploited the Facebook Data of Millions."*The New York Times, The New York Times, 17 Mar. 2018, www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.*