ISSUE: August YEAR: 2020

Security Awareness Newsletter

LOYOLA UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

"Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them. " - Steve Jobs

Multi-Factor Authentication is Here

We've all used some form of Multi-Factor Authentication, often times we don't even realize we are using it. From ATM machines to gas pumps and the grocery store, if you've used a debit card, you've used Multi-Factor Authentication or MFA.

What is Multi-Factor Authentication?

The definition for MFA is a more secure method of confirming a user's claimed identity that requires that two or more pieces of evidence (or factors) be presented to an authentication mechanism. The "factors" can include; knowledge (something the user and only the user knows), possession (something the user and only the user has), or inherence (something the user and only the user is). Some common forms of second factors are a one-time passcode (OTP) sent via SMS, a phone call, or a mobile app.

Why is Loyola Switching to Multi-Factor Authentication?

MFA helps defend against account takeover attacks especially in cases where the attacker has obtained an account password, they are still unable to log in without the second factor of authentication. According to research done by Microsoft, over 99% of all phishing-related account takeover attacks are prevented when an entity deploys MFA.

Where do I use MFA?

Loyola will require MFA for off-campus access to certain applications. As the first phase, off-campus access to Office 365 applications, such as Outlook email, OneDrive, and SharePoint will require MFA.Other applications will begin to require MFA over the next year (e.g. Lawson, LOCUS, DocFinity).

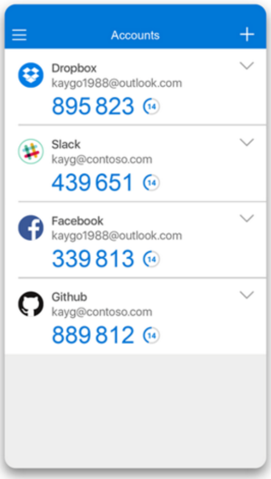
How often am I asked for MFA?

If you use a client application (e.g. Outlook, OneDrive, SharePoint), you will need to verify only once every 60 days or if changes occur in your account, such as changing your password or logging out of the client. If you use a browser for login, you potentially need to verify every time, unless you check the box next to "Don't ask again for 60 days" to postpone the next verification for 60 days. This only works if you use the same browser on the same computer.

What is the benefit for me and Loyola?

Multi-Factor Authentication helps the Loyola community protect themselves from account takeover attempts perpetrated by hackers. During COVID-19, hackers have taken advantage of remote working conditions to employ even more tactics that will catch recipients unaware in their unprotected environment at home. There are greater protections when you are on Loyola's University network, but we have to step-up our efforts to protect our accounts especially during this time. If you talk to anyone who has dealt with compromised information you would find most, if not all of them, to be deeply appreciative of the steps taken protect an individual's private information. Not to mention the monetary cost to compromised individuals, and the cost to Loyola, is exorbitant.

Microsoft will require Multi-Factor Authentication for access to any of their services by the Fall Semester – this includes Microsoft Outlook email. This not only makes it an appropriate step for Loyola it will be out of our hands because it is a Microsoft requirement as well. The University took steps to address it now, in a controlled manner to avoid a larger disruption at start of school. Based on statistics collected by Microsoft, there are over 300 million fraudulent sign-in attempts in their cloud services each day and 99.9% of account related attacks can be prevented by using Multi-Factor Authentication.



Dropbox
kaygo1988@outlook.com
895 823

Slack
kayg@contoso.com
439 651

Facebook
kaygo1988@outlook.com
339 813

Github
kayg@contoso.com
889 812

Coronavirus Phishing Emails

What to look for in a phishing email

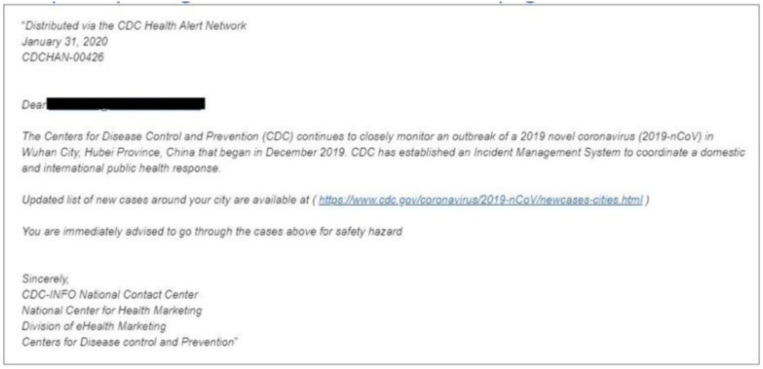
With the ongoing crisis of coronavirus, it is important that everyone's online accounts are safe and secured. The reality of the situation, however, is that many malicious entities on the internet are using this as an opportunity to phish the everyday internet user. Use the following tips and reminders to keep your account secure:

- Current phishing scams will often include an urgent call to action, such as "Buy Now, Limited supply".
- Remember to hover over hyperlink text (or long-press on mobile) to see where the URL will direct you if you click on it.
- Be on the lookout for misspellings, such as legitimate business names that are missing or off by just one or two letters.
- Awareness of these phishing attacks is critical, if ever unsure about a particular email, forward the email to the ITS Service Desk for verification.
- Remember that the University will never ask you for your password.
- Look out for the UISO monthly newsletter, as well as frequent posts on the Information Security blog.

Examples of a coronavirus phishing email

Think before you click! Cyber criminals are always looking to take advantage of people seeking information on COVID-19. They are trying to impersonate organizations such as the CDC, WHO, and others by trying to trick users on clicking on a link. Slow down. Don't click. Instead, go directly to a reputable source. Here is a real life example of a coronavirus phishing email:

CDC Alert phishing email



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

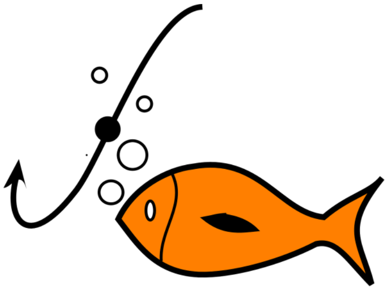
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

It is vital to keep not only your LUC account safe, but your personal accounts as well. One suggestion is to use a password vault, such as LastPass. With a secure password vault, multiple random passwords can be used to safeguard each account using a unique password with high complexity. For more information about LastPass (including detailed signup instructions, FAQs, and video walkthroughs) visit the ITS LastPass page at https://www.luc.edu/its/services/password/lastpasspasswordmanagementvault/.

Symanovich, S., 2020. "Beware Of These Coronavirus Scams". *[online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>*



● ● ● | LastPass Available to Students, Faculty and Staff!

Loyola offers LastPass to all students, faculty, and staff. With almost everyone working remotely due to the pandemic, it is crucial to keep your online credentials safe and secure. LastPass can take the burden of remembering passwords off the user and also provide an extra layer of security. LastPass offers users the ability to generate, remember, organize, and fill passwords. All you will need to remember is one master password to access all of your account passwords managed by LastPass. All students, faculty, and staff can now sign up for a LastPass Premium account!

Sign up for LastPass

- Signing up for LastPass is quick and easy!
- Simply go to https://lastpass.com/partnerpremium/loyolachicago and follow the instructions on the screen.