ISSUE: May 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

Securing Your Home Workstation

The COVID-19 outbreak has completely transformed our everyday lives. Thankfully, technology has allowed us to keep in contact with friends and family and continue to do business remotely as we maintain social distance. With virtually all social and business interactions now taking place online, cybersecurity has never been more important. We have already seen hackers take advantage of the influx of users online with COVID-19 phishing emails and related cyberattacks. Users can feel at ease by taking matters into their own hands and being proactive about their digital security. Following these simple steps can help secure your workstation at home and keep your private information out of the hands of attackers:

Protect Devices with an Antivirus Solution

Antivirus programs protect your computer from being infected with malware - malicious software that attackers use to gain access to your data. Installing a reliable antivirus solution can protect your machine by running routine checks and handling potential infections that may be on your computer. Antivirus programs are particularly important if you are working remotely and have access to corporate data on your home machine. Take the extra precaution and feel protected by installing an antivirus solution on your device today!

You can learn more about some of the more popular antivirus solutions by visiting https://www.techradar.com/best/best-antivirus.

Keep Operating Systems and Programs Up to Date

New vulnerabilities in operating systems and applications are continually being found and patched. Developers push these patches in new updates. Updating your operating system and software keeps your machine immune to vulnerabilities that have been fixed by developers so that attackers cannot take advantage of them. Cybercriminals rely on people not updating their software. When you update software, any known vulnerabilities are patched, and your machine is kept protected. Turn on auto-updates for your operating system and other software to keep the burden of updating off of your mind!

Visit these links to learn how to keep your operating system up to date:

- PC Platforms: https://support.microsoft.com/en-us/help/4027667/windows-10-update
- Mac Platforms: https://support.apple.com/en-us/HT201541

Configure Wi-Fi Encryption

Wi-Fi networks can be a point of easy access for attackers if they are not kept secure. Make sure your Wi-Fi network is protected with a strong password. Additionally, check that your router is using WPA2 encryption, if possible. You can check if your network is using WPA2 encryption by going into your router settings. This process is different depending on your provider, but there are helpful resources and walkthroughs, just a Google search away. For example, if I had an Xfinity router at home, I would Google: "Xfinity (router model) settings". Simply having a strong password and enabling WPA2 encryption for your Wi-Fi can keep your home network and valuable information protected. Our time spent online is growing and will continue to grow as we continue to fight this public health crisis. Put your mind at ease as you stay connected by taking these simple steps to protect your cybersecurity!

Coronavirus Phishing Emails

What to look for in a phishing email

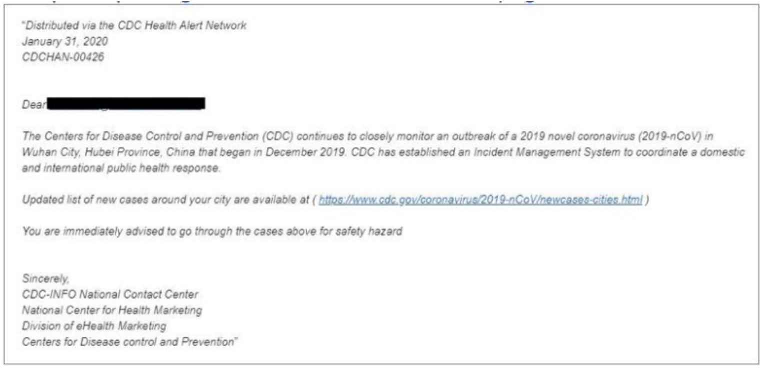
With the ongoing crisis of coronavirus, it is important that everyone's online accounts are safe and secured. The reality of the situation, however, is that many malicious entities on the internet are using this as an opportunity to phish the everyday internet user. Use the following tips and reminders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

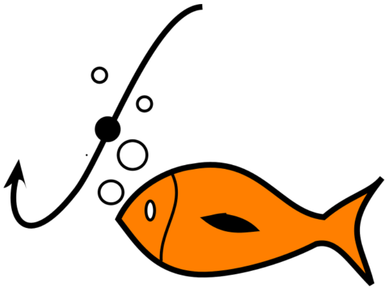
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

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.