ISSUE: 3-12 YEAR: 2020

University Information Security Office Newsletter

If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it.

Tim Cook

From the CISO's Desk

This month's newsletter focuses on four topics aimed to help you secure yourself during these challenging times.

The first article shares information about the rise in unemployment fraud and identity theft along with some tips on what to do if your identity is stolen.

The second article introduces some ways we can secure our networks in our virtual environments during the pandemic. Remote work security focuses on what we can do individually from home so that we are increase our security despite being away from the workplace.

Third is a new segment of tips in our Newsletter called Phish Bytes. These tips are a great start to increasing online security for everyone in our community.

Finally, we promote National Cyber Security Awareness Month with different themes and links for each week.

University Information Security Office

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

Identity Theft Security

Created by Aleksandra Stosovic

Loyola University has become aware of several attempts to file unemployment claims for individuals who are still employed at the university. These are known as "impostor claims" and there has been an increase all over the country in such activity during the COVID-19 pandemic.

In a fraud attempt, someone else applies for unemployment benefits using stolen employee information from public breach data and employment data pulled from department listings on public employer websites.

How To Know If You're a Victim of Identity Theft

Employees may discover they have been targeted in a few different ways. For example:

- They may receive notification from Human Resources. If HR becomes aware of an unemployment filing for an employee who is actively working.
- They may also receive information by mail from the state unemployment agency stating that a claim has been filed on their behalf.

What To Do If You're a Victim of Identity Theft

Human Resources has employment verification systems in place for unemployment claims and will contact individuals if a false claim is received.

If an employee becomes aware that someone is using their identity to collect unemployment benefits, they should report this immediately to Human Resources.

How to Protect Yourself From Identity Theft

- **Protect your Social Security number.** Don't carry your Social Security card or other cards that show your SSN.

- **Use caution when giving out your personal information.** Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails, and in postal mail. Most institutions wouldn't ask for your SSN or other personal information over the phone, and many emphasize that they do not ask for this information. Do not send your SSN or credit card information via email. If you wouldn't feel comfortable putting this information on a postcard, you probably wouldn't want to send it by email either.
- **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.
- **Protect your postal mail.** Retrieve mail promptly. Discontinue delivery while out of town.

The Federal Trade Commission has a website providing more information on identity theft. You can find it at:

https://www.identitytheft.gov/

To learn more about specifics around unemployment fraud at Loyola

https://www.luc.edu/hr/resources/unemploymentinsurancefraud/

Work From Home Security

Created by Jalan Cruz

Most Loyolans have been under quarantine or remote-work conditions for seven months, and this will likely continue for the near future. Our teaching, learning and work environments have been primarily virtual. As Loyola and the rest of the world have shifted to an online environment, this provides new opportunities for bad actors to take advantage of remote and distributed work environments that can be less secure.

Following are some tips to help secure your remote environment:

1. Secure your home's wireless router. Change the default settings of the router's password and username to increase your home network's security.
2. Update your devices that connect to the router. From your laptop to your gaming device, everything needs to be updated to the latest software update. Almost all updates for these devices include some sort of security check.
3. Run weekly security scans. In the same way that the novel coronavirus is highly contagious, think of how quickly a virtual virus can move through your network. With more schools being entirely virtual, more internet traffic is being funneled through your home network bringing more threats directly to your home.
4. Try to separate work devices from your personal devices. While it may be tempting to overlap the two, separating these two very different worlds can help reduce potential risky and malware-heavy search engines.
5. Invest in a sliding webcam cover. Web video chats are necessary, but limit the camera time to those very important meetings and occasional Facetime.
6. Use Loyola Secure Access (LSA). By remotely connecting to our networks, we will be able to add additional protection to your devices. LSA is well equipped for determining malicious attempts and this will only help your home set up with appropriate security precautions.

Whether we like it or not, cybersecurity threats are prevalent, and as the circumstances of the world are changing, so are the attacks that are designed to affect us. While we are in the safety of our homes the importance of cybersecurity is as important than ever. In the link below, is a general tutorial on how to change your router's default password and settings.

Below is how you can gain access to your router and start making changes to your home network security.

To change your router's password:

1. Right-click the Start button then select Command Prompt. On the Command Prompt window, enter "ipconfig" and press the [Enter]. The numbers indicated on the Default Gateway section is your router's IP Address.
2. Enter your router's IP Address into your web browser
3. Log in with the default Username and Password
4. Go to Settings
5. Select Change Router Password or a similar option
6. Enter the new password
7. Save the settings

UISO's Phish Bytes

Phinn Says Don't be Shark Bait! Increase your own Cybersecurity knowledge with some Phish Bytes

- Increase password strength by using a phrase that is a least 12 characters long - they are easier to remember and much stronger when paired with other password requirements.
- Use Multi-Factor Authentication when available.
- Use LastPass to securely store your passwords: https://lastpass.com/partnerpremium/loyolachicago
- The easiest way to spot a phishing email is the sender's email address. Watch out for multiple domains in the address. Ex. sampleaddress.luc.edu@gmail.com

It's Cyber Security Awareness Month

Cybersecurity Awareness Month – observed every October – was created as a collaborative effort between government and industry to ensure every American has the resources, they need to stay safer and more secure online. This October as we encourage all users to own their role in protecting connected devices. "Do Your Part. #BeCyberSmart."

Weekly themes include:

- October 5 - 9 (Week 1): If You Connect It, Protect It and Fishing and Phishing
- October 12 - 16 (Week 2): Securing Devices at Home and Work and The Many Forms of Malware
- October 19- 23 (Week 3): Securing Internet-Connected Devices in Healthcare and Social Engineering (and all its moving parts)
- October 26 - 30 (Week 4): The Future of Connected Devices and Your data is Valuable Protect It!

For more information on what Loyola is doing to help raise awareness like us on Facebook, follow us on Twitter, and check out the Cyber Security Awareness web page: https://www.luc.edu/its/uiso/awareness.shtml