From the ISO’s Desk

Over the years, the increase and sophistication of attacks by hackers continues to increase. Hackers now have a tendency to go after individuals within an organization, rather than PC’s, by utilizing social media methods.

The only way we can continue to protect and deter our university resources is through enhanced security measures, and educating and enabling faculty, staff, and students to be equally impactful as our first line of defense.

Uninformed Faculty, Staff and Students can do harm to our network and systems by visiting websites infected with malware, responding to phishing e-mails, storing their login information in unsecured locations, or even giving out sensitive information over the phone when exposed to social engineering.

Use these tips to help us protect your identity & Loyola’s Information!

Jim Pardonek
Information Security Officer

CYBER ATTACKERS: EVEN YOU COULD BE A TARGET

Don’t think you’re a target for cyber attackers? Think again!

Many people mistakenly believe that their computer or information has no value or that cyber attackers aren’t interested in them. In reality, individuals like you are a target.

Protect yourself. Realize that your information is in danger and that even seemingly trivial information needs protection.

Be on alert when using social media. Social networking websites allow you to post and share a lot of information, from family members to favorite songs. Hackers look for highly personal information and can use it to guess passwords or even steal your identity.

STOP: Make sure security measures are in place on your devices.

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

CONNECT: and enjoy your devices with

WHAT IS PHISHING?

Don’t get reeled in!

Phishing is the fraudulent practice of sending emails (or some form of "bait") purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Phishing attacks use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses. They cost organizations around the globe $4.5 billion every year and over half of internet users get at least one phishing email per day. Spam, phishing and other scams aren’t limited to just email. They’re also prevalent on social networking sites.

10 TIPS FOR IDENTIFYING PHISHY EMAILS

1. Don’t trust the display name.
2. Look but don’t click.
3. Check for spelling mistakes.
5. Don’t give up personal information.
6. Watch for urgent subject lines.
7. Review the signature.
8. Never click attachments.
9. Don’t trust the header.
10. Don’t believe everything you see!
TAKE ACTION!

Cyber security can start with a few basic steps:

**Secure your devices.** Use strong passwords or touch ID features to lock your devices.

**Think before you app.** Be thoughtful about what personal information is shared with the different apps on your devices. Delete apps you don’t need or only used for a temporary purpose.

**Can’t catch me!** Your movements can be tracked when Wi-Fi or Bluetooth are enabled on your device. Disable Wi-Fi and Bluetooth when not in use.

**Does it pass?** Even a seemingly strong password can be guessed if a hacker accesses your personal info. Avoid names, addresses, and birth days.

**Double down.** Many email services and social media platforms allow you to log on using two-factor authentication. This adds an extra step to confirm your identity even after you enter your username and password.

**Keep a clean machine.** 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.

**When in doubt, log out!** Make sure you completely log out of any service you’re not using – don’t just close the window or tab on your browser.

**AVOIDING TYPES OF MALWARE**

**Ransomware**—Ransomware is a malware that stops you from being able to access your files usually by encrypting them, and then requests payment to decrypt the files, restoring your access. Most commonly, ransomware asks for payment in bitcoin, which is a popular cryptocurrency. Unfortunately, paying the ransom does not guarantee restoring access to your files.

**Trojan Horses** (a.k.a. Trojans)—this malware takes its name from the classic story of the Greek army sneaking soldiers into the city of Troy hidden inside a large wooden horse. Trojan malware behave in much the same way, by appearing to be legitimate apps or software that you want to install. Some Trojans allow an attacker full access to your device, others steal banking and personally sensitive information, and others are simply used to download additional malware, like ransomware.

**Keyloggers**—This type of malware records your keystrokes and sends them to a cyber threat actor, giving them access to your usernames, passwords, and any other sensitive information you have entered using your keyboard. With this information, the cyber threat actor can access your online accounts or commit identity theft.

---

**University Information Security Office**

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

https://luc.edu/its/uiso/

**Increase your security awareness:**

https://www.stopthinkconnect.org/  
https://staysafeonline.org/  
https://www.ponemon.org/