ISSUE: February YEAR: 2021

Security Awareness Newsletter

LOYOLA UNIVERSITY CHICAGO 1870 AD MAJOREM DEI GLORIAM

Preparing people to lead extraordinary lives

"Privacy - like eating and breathing - is one of life's basic requirements." – Katherine Neville

Springtime, Spring into a New Home Office Security Strategy

3 Tips to Kick off Your Spring

Home may feel like the safest place on the planet these days, but your personal network might not be. This year, step up your home office security strategy and dedicate 2021 to protecting yourself and your organization.

Get a head start on securing your home office with these 3 tips:

1. Avoid Unsecure Public Networks

Free Wi-Fi at your favorite coffee shop may tempt you to set up there during working hours, but these hotspots also attract hackers. Unsecured public networks let cyber-criminals sneak in between you and the connection point, which means they could potentially intercept your emails, credit card information and business account credentials. No matter where virtual work takes you, use VPN (such as Loyola Secure Access) to prevent hackers from stealing your personal and business information. And above all, never trust public Wi-Fi.

2. Protect Personal Devices from People and Pets

Never leave your personal devices unsecured and unsupervised. Guests and roommates can snoop around and steal personal info – and you'd probably never suspect it. Prevent this by password-protecting computers, tablets, phones and important files, and lock them away somewhere safe when you're not home. Kids and pets, on the other hand, can accidentally share or delete important data in just one click. In addition to locking your devices, you can also pet- and kid-proof your computer by encrypting files, and setting up parental controls.

3. Shred Sensitive Documents

Buying a shredder may seem unnecessary but here's the truth: people who want to steal your identity are willing to dumpster-dive for it. Protect your personal information by destroying documents that contain your name, address, phone number, identity number and banking information. That also includes last month's electric bill, old airline tickets and ATM receipts, as well as expired credit cards, IDs and passports.

Phinn's Phish Bytes

A burglar is easy to spot, but catching a hacker who's hi-jacking your Wi-Fi can be harder. Monitor your network for these signs of compromise:

- Your computer is behaving strangely (and without your input).
- Family and friends receive messages from you that you didn't send.
- You get ransomware messages and phishing emails.
- Passwords have been changed and settings have been reset.
- Devices crash, reboot and lose power quickly.

Source: InfosecIQ

University Information Security Office
LUC.edu/its/uiso/

ITS Service Desk
Email: ITSservicedesk@luc.edu
Telephone: (773) 508-4487
Hours: LUC.edu/its/service/support_hours.shtml

Sharing isn't Always Caring — Especially Online

OPSEC Checklist: 3 Steps to Staying Secure

Social media has normalized sharing on the internet. But even the most innocent information, like photos from your trip, your weekend plans or job updates, should be thought of as oversharing in the age of social engineering. And that's because every piece of information you share online can be used against you.

1. Limit Personal Information Shared on your Social Profiles

While social media is all about chatting and sharing, you should be cautious about what you say and who can see it. Seemingly harmless information can give hackers the ammunition they need to launch a phishing attack.

In general, you should never share your location or plans, even though bragging about your upcoming vacation may be tempting. Hackers can use location data to tailor their attacks, while thieves may use it to case your place. You should also avoid sharing details about your employer. And beware of photos and details that could give people answers to your security questions: things like which elementary school you attended, the street you grew up on and so on.

While having no social media at all is the best way to keep people out of your business, the next best thing you can do is keep a low profile.

2. Declutter your Office — Especially What's in View of your Webcam

You've probably heard the horror stories about hackers gaining access to webcams, but you might not have considered the ways in which you're exposing yourself when you use yours.

In the era of virtual work, anyone can take a peek into your personal life on a conference call. That's why you should be aware about what documents and other sensitive information are visible in your frame.

Before virtual meetings, clear your workspace, secure files and check reflective surfaces to get a glimpse at what others may be able to see. This will get you into the habit of ensuring personal materials are always out of sight.

3. Get Creative When Setting—up Account Security Questions

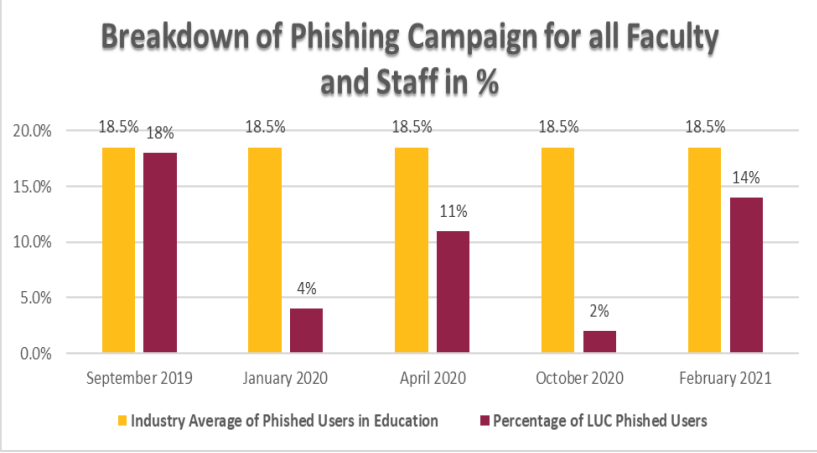
When it comes to securing your accounts, your best defense is nonsense. Instead of giving standard answers to security answers, try responding with something silly or nonsensical. When asked what your childhood pet's name was, for example, you might write "magenta" instead of "Buddy." Or you may say you met your spouse at "lasagna."

In addition to providing unique answers, you can also type them in all lowercase letters so they're easy to remember.

Less is Definitely More

When you create a new account, you're likely used to providing an email address and password, but sometimes platforms ask for more. Whether it's for marketing purposes or for "a personalized experience," as they may frame it, doesn't matter: you should never give more than the bare minimum. Any extra information is unnecessary and could be used against you in the event of a data breach.

Source: InfosecIQ



Loyola Phishing Campaign Program

Beginning in 2019, Loyola has started a phishing campaign program aimed to improve security awareness on phishing and scam emails. The graph on the left shows our performance over the past year. The University's phish rate has consistently fallen below the industry average. Keeping the campus community safe from malicious attempts to steal personal information, requires constant vigilance. We encourage you to continue sending anything you see as suspicious to us at helpdesk@luc.edu.