ISSUE: MAY YEAR: 2022

Security Awareness Newsletter

LOYOLA UNIVERSITY CHICAGO 1870 AD MAJOREM DEI GLORIAM

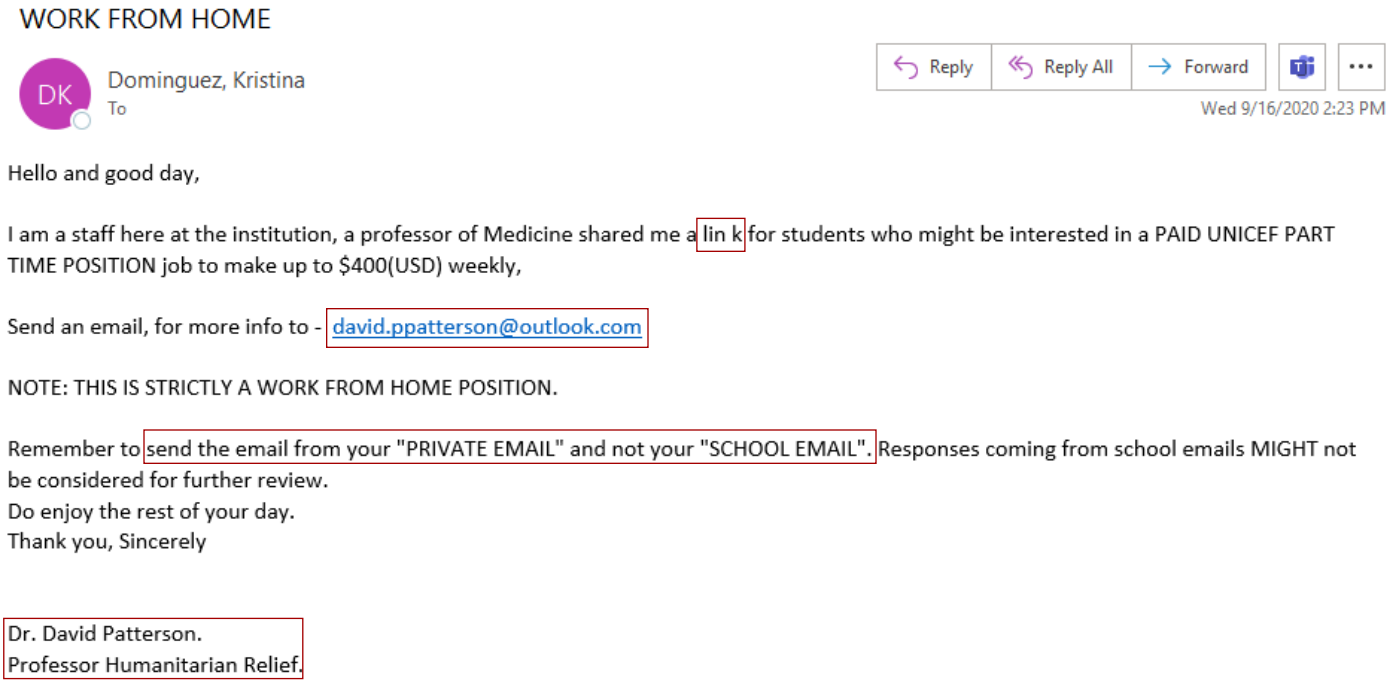
Preparing people to lead extraordinary lives

For every lock, there is someone out there trying to pick it or break in.— David Bernstein

How to Spot a Job Scam

1. The email is from a Gmail, Yahoo, or Outlook address. Legitimate companies should email from their corporate email account. LUC will not post jobs from employers that do not have corporate email accounts.

4. The email contains grammatical or spelling errors. A very common attribute of scam emails is that they do not bother to spell check or grammar check their outgoing emails.



WORK FROM HOME

DK Dominguez, Kristina
To

Reply | Reply All | Forward

Wed 9/16/2020 2:23 PM

Hello and good day,

I am a staff here at the institution, a professor of Medicine shared me a lin k for students who might be interested in a PAID UNICEF PART TIME POSITION job to make up to $400(USD) weekly,

Send an email, for more info to - david.ppatterson@outlook.com

NOTE: THIS IS STRICTLY A WORK FROM HOME POSITION.

Remember to send the email from your "PRIVATE EMAIL" and not your "SCHOOL EMAIL". Responses coming from school emails MIGHT not be considered for further review.
Do enjoy the rest of your day.
Thank you, Sincerely

Dr. David Patterson.
Professor Humanitarian Relief.

2. The email does not address you by name. The email may say your information was obtained from a job board, school database, or Career Services office. If so, they should address the email to you directly, rather than “Hello Student” or “Good Morning.”

3. The company name is a legitimate company. To make the scam more believable the email will use the name of a legitimate company. However, the person contacting you has no relationship with the company they are claiming to work for.

5. There is no contact information for the sender. Any legitimate email from a company’s Human Resources or Recruiting department should have a signature line with the sender's name, title, and contact information.

Stay Safe! If it is too good to be true, be cautious. When in doubt, look for these signs, and use your best judgement. Verify the offer by contacting the company directly. Look for a contact in HR, call them up and ask if this is a legitimate job offer. For more information about identifying job scams, please visit: https://www.luc.edu/its/uiso/awareness/protectyourself/jobscams.shtml

Source: University of Houston

Multi-Factor Authentication

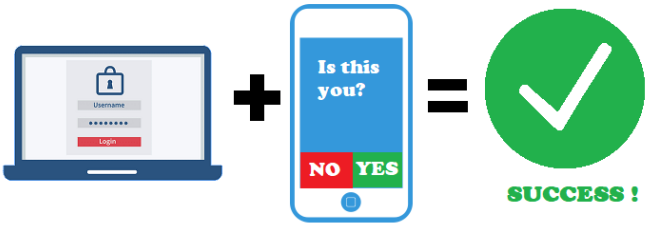
What is Multi-Factor Authentication?

Multi-factor authentication, also known as two-factor authentication (2FA), is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials can be one of three things:

1. **Something that you know,** *such as a password.*
2. **Something that you have,** *such as a phone or token.*
3. **Something that you are,** *such as a fingerprint or iris.*

When you enter in your LUC username and password, you will also need to have a push notification you click on or enter a *six-digit code* that you receive on your cell phone in the form of a text message.

Push authentication works in the way that when you try to login, instead of a page appearing asking you to enter in a code, it sends a signal to your phone and all you need to do is click the notification. Please note that **you should not click the push notification if you did not try and log-in yourself.** The reason for this is because it is possible a hacker is trying to gain access to your account and personal information.



If you opt out to receive the text message with a six-digit code, you simply need to enter in that code when authenticating.

MFA helps protect you by adding an additional layer of security, making it harder for bad guys to log in as if they were you. Your information is safer because thieves would need to steal both your password and your phone.

Source: JSCM Group

Guess that Cybersecurity Term

1. The address of a webpage. Check the validity of it before clicking on it.
2. Fraudulent text messages purporting to be from reputable companies in order to trick individuals into revealing personal information.
3. A fraudulent email purportedly from a reputable company attempting to get personal information.
4. Facebook, Twitter, Instagram, etc. (Two words)
5. Should be constructed of upper and lower case letters, numbers, and special characters.
6. Threatening behavior facilitated through electronic means such as texting.
7. A type of malicious software designed to block access to a computer system until a sum of money is paid.
8. Verifying identity.
9. Security tool that creates a secure, encrypted connection between you and the Internet (acronym).
10. Harmful computer programs such as viruses, worms, and trojans used by hackers to gain access to your computer and cause destruction.

Guess that Cybersecurity Term Answers:

1. URL
2. Smishing
3. Phishing
4. Social media
5. Password
6. Cyberbullying
7. Ransomware
8. Authentication
9. VPN
10. Malware

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