Parent and Family Bulletin

USF STUDENT AFFAIRS & STUDENT SUCCESS
UNIVERSITY OF SOUTH FLORIDA
PARENT & FAMILY PROGRAMS

Protect Your Student from Email Job Scams

USF Career Services is dedicated to helping you and your student understand the difference between a legitimate job or internship opportunity and what might be a scam.

Your student may receive emails, phone calls, text messages, or other notifications of potentially fraudulent job opportunities even if they are not actively searching for a job or internship. Here are a few things you should keep in mind if your student receives a message they believe could be a scam.

If it seems too good to be true, it probably is.

Fraudulent employment opportunities often make claims that sound like they could be the perfect opportunity, from very high hourly pay rates to the option to work entirely from home. While this type of opportunity may exist in the real world, students and families should question these kinds of "benefits," especially if your student has not applied or interviewed with the organization. Even if your student has been proactive and engaged in networking activities, legitimate opportunities will require a formal application and/or interview.

No application or interview process? Probably not a real job.

The application process is extremely import for all parties involved, as it offers the opportunity to determine if the candidate and the position are a good fit. Many fraudulent opportunities have wording to indicate that they are trying to "fill the vacancy quickly," and may skip the entire job application process. Emails about these opportunities may even be presented as "job offers" that require no application or interview, or simply asks the individual to reply with a resume or contact information. Scammers use this high pressure tactic to get your student to provide valuable personal information, such as phone numbers, email address, home address, bank information, or social security number, to commit further fraudulent activities.

Keep an eye out for “spoofed” messages.

Fraudulent job opportunities are getting more sophisticated. Occasionally, scammers will disguise their identity through a process known as "spoofing," where the message seems like it is from a known, trusted source, such as a professor, legitimate employer, staff member, or fellow USF student. Spoofing can be used with emails, phone calls, text messages, and even websites.

Students should remain vigilant and verify that a message they have received about an employment opportunity is actually from that sender before sharing any personal information.

Know when to give out personal information.

If your student is asked to supply personal information - from an alternate email address or phone number to Social Security number or personal banking information - that should raise some red flags,

especially in an initial message from a potential employer. The information that an employer might need to move someone through the application process, such as a phone number for a phone interview, would typically be supplied during the application process. If your student receives a random message asking for them to respond back with personal contact information, and they've had no previous contact with the organization, the request may be a scam and they should proceed with caution.

Your student should never give money to get a job.

If your student is asked to send money, use their own money to purchase supplies, or cash a check or money order on behalf of an organization, the opportunity is most likely a scam. Your student should never have to give money or cash a check or money order to get a job or internship. In rare cases students may need to purchase their own supplies, but that will be discussed during the interview process. If your student is offered money in the form of a check or money order to purchase supplies, contact your bank before depositing it to verify its legitimacy.

The only time that your student should give out their banking information is when setting up direct deposit as a part of their on-boarding process after they have been signed an official offer letter. This typically happens during new employee orientation or on-boarding under the direction of a human resources staff member at the hiring organization.

What to do if your student has responded to a scam job posting.

If your student has received a scam job or internship opportunity but has not responded to it, they can safely ignore the message and mark it as spam.

If your student has responded to a scam opportunity, you and your student should first determine what information was given to the scammers. If all they have is your student's name, email address, physical address, and/or phone number, you or your student may want to report the scan to the FBI's Internet Crime Complaint Center (IC3) via their online form.

If there has been any kind of monetary exchange, your student should to reach out to their local police department's non-emergency line to file a report. If they live on-campus, they can contact the University Police Department at 813-974-2628 to file their report. Please note, the University of South Florida is unable to reimburse students who experience financial losses due to scam activities. Students in need of financial assistance should contact Bull2Bull Financial Education.

Next, notify USF Career Services so that we can help get the word out to other students and families as needed. It may be helpful for us to see the original message, so please forward any suspicious email or text message screenshots to careerservices@usf.edu.

Your student can also consider reaching out to the Center for Victim Advocacy & Violence Prevention if they have been affected by a scam email.

How to identify a legitimate email from Handshake.

Email messages sent from the Handshake platform will always come from an

@____.joinhandshake.com address. They also typically contain a "footer" message that contains Handshake's physical address (P.O. Box 40770, San Francisco, CA 94140) and the option for students to update their notification preferences.

If your student received information about a job or internship opportunity, they can verify the organization's identity by searching for them by name in Handshake. Students can also see available jobs the organization has posted and apply to the jobs directly and safely through the Handshake system.

Our partners at Handshake have a webpage with additional information on how to stay safe when applying for jobs and internships, which students can access here.

If you or your student are having trouble determining whether an opportunity is legitimate, contact USF Career Services for help before responding.

Submitted by: Peter Thorsett, Community Engagement and Career Readiness