Office of the Chief Information Security Officer
Risk Advisory: Employment Scams

Employment Scams Targeting UW Students

In 2022, the Office of the CISO has seen a surge of employment scams targeting UW, and in some cases, members of the University community, including students, have lost money. The purpose of this advisory is to inform potential victims about specific tactics that employment scammers might use. A common goal in these scams is to get the victim to spend money based on funds that are either promised or made temporarily available to them in their bank accounts. This is often done by sending the victim a bad check or fake financial statements, but other methods may be used. Because these scams are constantly evolving, it is difficult to predict every tactic that may be used, but by reading and sharing this information, you can help raise awareness and diminish the effectiveness of these harmful attacks.
General Guidance: If you are asked to use your own money to get a job, it is very likely a scam. Please note that these scams are carried out using various forms of communication, including texts, phone calls, email, including UW email accounts, and social media messages.

Background

The Office of the CISO has sent out previous messages warning about job scams targeting students. These scams usually promise tuition discounts, rewards, and other easy incentives. In one specific case, the scammer was able to elaborately engage with a victim and cause nearly $4,000 worth of damages. This type of scam has been recently observed targeting international students, exploiting language and cultural barriers.

Fake Job Recruitment

Recently reported scams have used intricate schemes to target students or potential employees seeking attractive job positions. Students are initially contacted via email or social media platforms, such as LinkedIn or AngelList. The scammer may include recognizable logos from prominent employers in the U.S. and they may spoof email addresses from real human resources employees to make the job offer appear more legitimate. They may even conduct mock interviews or ask the student to complete fake questionnaires.

Fake Onboarding

A fake onboarding process is sometimes part of the scheme. That process may include one or more of the following steps:

1. The scammer extends a legitimate-looking job offer letter to the student and schedules an onboarding meeting.
2. During onboarding, a victim is told they will have to buy computer equipment from a company-approved site. This site may seem real, with a checkout and invoice process, and PDF payment receipts.
3. The victim is told to pay for the equipment with their personal funds. At this point, the scammer may try non-traditional forms of payment, such as Zelle or Bitcoin, as a way to get access to the funds faster.
4. If the victim does not have enough money, they may be sent a check to cash at a bank, with a sender address that includes “INC or LLC” to appear legitimate. The check may clear initially, and the victim will have access to funds, but then will later bounce. This is where the financial scam occurs, as the victim “paid” for equipment they will never receive and the scammer has obtained the victim's funds.

Other Scam Communication Techniques

Various communication methods have been used in these scams:

- SMS/Phone Call: A victim may receive a personalized message about a job offer to their mobile phone. A scammer may carry out a legitimate conversation with the victim in order to lure them into the scam.
- Email: A victim may receive a job offer from a trusted email address, such as a @uw.edu. Account compromises happen daily in the US and UW, so do not immediately trust an employment offer that arrives in your @uw.edu email. We encourage the use of the UW Career Center (see below) for finding legitimate on-campus jobs.

- Formal to Informal Communication: If you find yourself communicating with a potential employer from your UW email address, and they ask you to use your personal email, this is very likely a scam as the scammer wants to bypass protections set in place on UW email servers. Keep in mind that this tactic is used in many different types of scams.

What to do

These types of scams are always being adapted with new tactics and they are hard to stop. Just as quickly as one scam operation is taken down, another may pop up. Following the recommendations below will help reduce your chances of being scammed and sharing this information will help others in the UW community.
The U.S. Federal Trade Commission has published the following guidance for avoiding a job scam:
"Before you accept a job offer, and certainly before you pay for one, take these steps to protect yourself from job scams:

- Do an online search. Look up the name of the company or the person who's hiring you, plus the words "scam," "review," or "complaint." You might find out they've scammed other people.
- Talk to someone you trust. Describe the offer to them. What do they think? This also helps give you vital time to think about the offer.
- Don't pay for the promise of a job. Legitimate employers, including the federal government, will never ask you to pay to get a job. Anyone who does is a scammer.
- Never bank on a "cleared" check. No legitimate potential employer will ever send you a check and then tell you to send part of the money to someone else or buy gift cards with it. That's a fake check scam. The check will bounce, and the bank will want you to repay the amount of the fake check."

Current UW students and UW alumni within 3 years of graduation get access to career counseling and services through the UW Career Center. This service includes 1:1 counseling that can be used to help students apply to legitimate jobs. More information can be found at https://careers.uw.edu/.
You can assist the UW Office of the CISO by reporting fake job phishing email messages to security@uw.edu.
Important note: If you are the victim of a job scam, please contact your local law enforcement to report the crime. UW CISO cannot take any legal action; that is done through law enforcement. Students can also report this type of crime to the UW Police Department at uwpolice@uw.edu.