OTIS COLLEGE OF ART AND DESIGN

Office of Career Services
otis.edu/career-services | careerservices@otis.edu
424-207-2490 | IG: @otiscareerservices

HOW TO IDENTIFY AND AVOID JOB SCAMS

WHAT AN OFFICIAL HIRING PROCESS IS LIKE

In order to avoid job scams, the first thing to know is what a typical employment process is like.

1. You apply for a job
2. The company screens your application
3. If they want to move forward they request an interview, sometimes two or three rounds of interviews that may include phone screens, assessment tests, or in-person interviewing
4. If they want to move forward you'll get a job offer. Usually the job offer is contingent on passing a background check to verify your identity, education, work history, and work authorization. STOP HERE.

   Tip: If asked for your ID or Social Security Number (or any other sensitive personal information) it's a good time to pause and make sure you've gone through an official hiring process and are working directly with an HR professional whom you can identify, meet in person or on video, and trust.

Once you accept a job offer, a legitimate job will ask you to fill out a background check authorization form or official government documents such as an I-9 (employment eligibility verification) or W-4 (federal tax withholding). However, just because an official form is requested doesn't always make it legitimate. If you've experienced any red flags, you must do your own due diligence to assess whether the opportunity is legitimate or a scam. If you suspect a scam, a good place to start is Googling the company name with the word 'scam' or 'reviews,' as well as reviewing tips to avoid or identify employer scams.

NEVER give out sensitive personal information including passwords and financial information including but not limited to: bank account, credit card, debit card, Venmo, or PayPal account numbers. The only exception after you've been hired at a legitimate company and started working is your employer may offer direct deposit to put your paycheck directly into your bank account. There is also a form for this, so never provide information over phone, email, text, through unofficial processes, before you start working, or if you suspect a scam.

It's unfortunate to become a victim of fraud. Hypervigilance for something that turns out to be legitimate is better than the other way around. Stay alert and use your best judgment. When in doubt, ask others for their opinion. If you feel you've been the victim of a scam, view steps to take.

RED FLAGS THAT COMMONLY IDENTIFY AN EMPLOYER OR COMPANY SCAM

- The email address of the sender does not match the website/company's email address provided on the actual website, or the website does not exist. A legitimate company will have their own domain such as name@companyname.com.

- Official-sounding corporate names similar to or that sound like long-standing, reputable companies, or have a professional-looking email address from a free/generic email provider such as Google, Yahoo, or Outlook.
- Have slightly misspelled web domains to mimic real companies, or logos that look similar to but slightly different than actual companies.
- Strange grammatical or spelling errors; use of strange symbols.
- Ask applicants to pay to apply or to obtain a job.
- Ask you to purchase materials, equipment, and/or other items on their behalf.
- Give you cashier's checks and/or money orders as forms of payment (fake checks), or want to make a deposit just to verify your account.
- Ask applicants to forward, transfer, or wire money from your personal account on behalf of your employer.
- Ask applicants for financial information, including, but not limited to: bank account, credit card, debit card, Venmo, or PayPal account number.
- Ask applicants to fax copies of ID and/or Social Security Number to unknown and/or unidentified parties (especially when this takes place before you've completed an official hiring process or without a secure URL).
- Includes the terms "package forwarding," "reshipping,' "money transfers," "wiring funds," and/or "foreign agent agreements."
- Offer incredibly high salaries, stipends, and/or benefits to emerging professionals.
- No written contract and/or agreement of employment.
- They make you feel rushed to take next steps or make a decision, pushed into providing sensitive information, or made to feel bad for exercising care and precaution.
- The sender tries to entice you to click on a link or open an attachment (which may contain malware).
- Someone reaches out to you unsolicited and exhibits any red flags.

TIPS TO AVOID OR IDENTIFY EMPLOYER SCAMS

- Use common sense and reputable search engines.
- Verify authenticity through finding this contact's name on the company's website and/or LinkedIn, or through a contact you know is affiliated with the company for professional reference.
- Review the company or person's website and social media; if you cannot find info about the employer or they do not have a public-facing profile, be very cautious.
- Cross-check with the Better Business Bureau and Federal Trade Commission for scam reports.
- Check if the same position looking to be filled is also on the company's main website.
- Meet the employer in person or on a video call; don't take a job without having met them somehow. Take extra precautions when applying for remote jobs.
- Make sure you receive a written contract and/or work agreement with full details of project and/or position details, federal/state guidelines, company procedures, benefits and compensation, start date, etc.
- Work with organizations that have a permanent, physical address rather than a P.O. Box which could quickly be shut down and cannot be tracked to a physical location.
- If it seems "too good to be true" it probably is.

- If what they're asking for is a little weird and doesn't make the most sense, it probably isn't legitimate.
- When inputting personal information online, always check for HTTPS protocol (the S at the end stands for “secure"). Website URLs that use “http” or a simple “www” are not necessarily secure and should be perceived with caution especially with sensitive information.

TYPES OF EMPLOYER SCAMS

- Phishing: Applicant is directed to a false web site asking for personal or sensitive information. Scam companies steal any identity information the applicant provides.
- Check Cashing: Applicant is sent a realistic-looking but fake check, asked to cash it and wire funds to another (scam) company.
- Reshipping: Packages are shipped to the applicant's residence with instructions to reship the packages to another address. Packages contain stolen property, which the police track back to the applicant’s address.
- Envelope Stuffing: Applicant pays a fee and is asked to post the same ad the applicant applied for. Applicant is paid based on the number of responses to the ad.
- Work at Home List: Applicant purchases a worthless list of opportunities to “make money from home.”
- Assembly or Craft Work: Applicant is asked to pay for equipment or materials to produce goods. Applicant’s work is then determined to be not “up to standard” and is not paid for goods produced.
- Rebate Processing: Applicant pays upfront for training, certification, or registration, and there are no rebates for the applicant to process.
- Online Searches: Applicant is asked to electronically pay a small fee to get started. Scam companies steal the credit or debit card information.

STEPS TO TAKE IF YOU IDENTIFY OR FALL VICTIM TO AN ONLINE JOB SCAM

- Notify Career Services immediately of the job title, type, and the company name/information and where you found it, especially if the job was found on the Otis College job board.
- Report the company name, contact email, and the job posting to the site/job board where the fraudulent job posting was listed so they can remove it and investigate further.
- If you shared your bank account information, close your bank account(s). For extra safety, open new accounts with a new bank.
- If you shared your personal information or provided your SSN, change any related passwords and order credit reports from all three major credit bureaus for unrecognized activity every three (3) months. Companies to order from include Equifax, Experian, and TransUnion. They can also be accessed through AnnualCreditReport.com.
- Report it to the Federal Trade Commission at https://reportfraud.ftc.gov or call 1.877.FTC.HELP (1.877.382.4357).
- Contact your local police department and file a report for any type of fraud.

- Close all email accounts used to communicate with the scammer, cease communication with them, and create a new account.
- If you received or sent an international wire transfer, contact your local Secret Service field agent.

MORE RESOURCES

Federal Trade Commission Consumer Information

Better Business Bureau Tip: Employment Scams

"How to Spot and Avoid Online Job Scams," by Biron Clark

"Job scams have increased as Covid-19 put millions of Americans out of work. Here's how to avoid one," by Carmen Reinicke