Chase Career Center

Avoiding Fraudulent and Scam Job Postings

The Chase Career Center partners with IsenbergWorks as a resource for employers to connect with Isenberg students seeking internships and post-graduate opportunities. We strive to keep fraudulent opportunities off IsenbergWorks by monitoring newly submitted postings for some common “red flags” that are considered suspicious. “Red flags” don’t automatically disqualify a job posting; we research the company and posting if suspicion arises and then make a decision.

The Chase Career Center rule of thumb: if it looks too good to be true, it probably is! Don’t apply.

If you have concerns about the legitimacy of an employer or posting, please **report your concerns to Melissa Salva, Director of Employer Engagement** at the Chase Career Center at msalva@isenberg.umass.edu.

Tips for Avoiding Hiring Scams

- Carefully examine entry-level jobs in Sales, Marketing, Sports Marketing, or Entertainment Marketing; there are plenty of legitimate jobs in these fields, but scams tend to be focused on these areas
- If the interview process seems a bit too easy, there might be a reason why; start asking direct questions to figure out what the company and jobs are really about
- Simply walk away if your interviewer says "You'll just have to see it to believe it" when you ask what you would be doing in the job
- Use the UMass Library Business Collection and Google to research companies to which you're considering applying

Critical Actions to Avoid

- Never give your personal bank account, PayPal, or credit card numbers to a new or potential employer
- Do not agree to have funds or paychecks direct deposited into any of your accounts by a new employer in advance of your employment
- Do not forward, transfer, or “wire” any money to any employer, or for any employer, using your personal account(s)
- In general, applicants do not pay a fee to obtain a job; however, there are some rare exceptions so consult with a Chase Career Advisor if you have concerns

Additional resources can be found through the UMass Library Business Collection and the Federal Trade Commission (FTC)

12 Common Red Flags

Contact the Chase Career Center to discuss your concerns and learn the best way to assess questionable job postings.

1. You are asked to **provide a credit card, bank account numbers, PayPal account**, or other personal financial documentation. Legitimate jobs will not ask for this kind of information on an application or via email/phone.
2. The posting **appears to be from a reputable, familiar company**. BUT – the domain in the contact's email address does not match the domain used by representatives of the company. Legit recruiters are directly associated with the company for whom they work. Therefore, the email address should match the company's domain.
3. The "employer" is **using a personal email address** instead of a company email address. The recruiter's email domain should be associated with the actual company, not a personal engine like Gmail or yahoo. Employment communications are always official – so why not use an official address?
4. You are **asked to forward payments**, by wire, courier, bank transfer, check, or through PayPal. This is a clear red flag! Never forward payments – they want to access your bank and money!
5. The position **requires an initial investment**, such as payment by wire service or courier (Ex. UPS or FedEx). Legitimate jobs never require an initial investment. Some network marketing companies may ask you to pay a fee (or "pay a deposit") to obtain a sample product for demonstration; UMASS does not post such positions.
6. The "company" **website is not active**, does not exist, or re-routes users to another website unaffiliated with the "company" even though the "employer" listed a URL or website in the job announcement. This is a significant red flag because if they listed the website and it is not working or does not exist, or if the URL goes to another unassociated website, then the employment opportunity it most likely not real.
7. The posting includes **many spelling and grammatical errors**. Poor spelling and grammar suggests the job announcement was written by a non-professional and therefore, the job may not be legitimate.

8. The **job is for a start-up business**, a new small private company, or an entrepreneurial enterprise just getting underway. These are red flags simply because new business efforts are used by scam artists as an exciting creative hook – because YOU get to be in "on the ground level." These may be very legit jobs – just be sure to research them very carefully.
9. You are offered payment or a **reward in exchange for allowing the use of your back account** (often for depositing checks or transferring money). Legitimate employers do not need to use your bank account! This is an old scam with some new twists. In-home "check processing services" are a recent version of this scam.
10. You are asked to **provide a photo of yourself**. In the U.S., most legitimate jobs do not ask for a photo. Usually, any "employer" asking for this does not know the standard of practice in the U.S., perhaps indicating that they are posting from another country.
11. The **posting neglects to mention what the responsibilities of the job actually are**. Instead, the description focuses on the amount of money to be made. Legitimate employers will provide a good description of the job responsibilities and duties to see if you are a good fit for the position. The description should also state the work location. Legitimate employers will do this openly and willingly.
12. The **employer responds to you IMMEDIATELY** after you submit your resume. Note: This DOES NOT include the automatic response you may receive from an employer once you have emailed your resume. Legitimate employers take time to sort through and review applications to find the best candidates. Fraudulent employers are just seeking your personal information, not your skills, which is why they respond immediately. They are hoping the immediate response makes you feel special – a trick used to get you to share your personal information.