UMassAmherst | School of Public Health & Health Sciences
Office of Career Planning

**How to report a job scam.** Please contact a professional staff member in the SPHHS Office of Career Planning (OCP) and include as much information as possible.
https://www.umass.edu/sphhs/careers

Include in your email:

- How did the scammer first contact you- include email address and message
- What database or websites do you think were involved if any?
- Any other information you feel is relevant

OCP will forward your information to the following groups depending on appropriateness:

- Office of Information Technology: itprotect@umass.edu
- SPHHS IT Services and Support: sphhshelp@umass.edu
- Other Career Offices and departments on campus

**Beware of employers that scam college students!**

There are various employment scams designed to gain access to peoples's money, bank account information, social security number, or identity. These scams often are posted on online job boards, websites, in newspapers, or via e-mail. As you enter a job or internship search, keep in mind…**that if a job seems too good to be true, be careful!**

Collectively UMass Amherst career offices do their best to block fraudulent employers from posting positions on Handshake or an outside job board once we become aware of them. However, due to the cleverly deceptive means by which scammers post jobs, we cannot guarantee the validity of every employer, job posted or outside website that does not screen for this.

Below are 4 examples of commonly used employment scams**:**

1. **Payment Forward Scam** (ads for personal assistants, etc..)
   This scam occurs after you apply for a position or reply to a spam e-mail. The employer will reply with instructions for a "test" before employment. As part of the test, you receive a check in the mail and are asked to deposit the check into your account (to buy supplies) and/or send a certain amount via wire transfer to another person. The employer promises that you will keep a percentage. **It is a scam because the check is not valid; and if you deposit the check and transfer the money, you will be responsible for the funds.**

2. **Application Fee Scam**
   With this scam, you are charged between $25 -$100 for a "guaranteed" employment opportunity application. People have used this scam by posing as members of the cruise line industry, the U.S. Postal Service, and other organizations. Always check with the company in which you are applying to learn more about the application process. **Employment applications should be free, and there are no "guaranteed" positions.**

3. **Phishing Scam**
   This scam occurs when you receive an unsolicited e-mail from an employer stating they saw your posted resume. The "employer" states your skills match the position for which they are hiring, but they need more information from you. The employer asks for personal information, which they may use to steal your identity. Before providing any information, be sure to research the company and verify the posting. Always be cautious when sharing personal information, such as mailing address, phone number, **and NEVER share social security number, identification number, or banking information. If you did not apply for a position, there is no reason an employer needs your address in order to interview you!**

4. **Mystery Shopper Scam**
   There are legitimate mystery shopping companies that hire college students and others to provide feedback on stores, restaurants, and businesses. However, there are scammers posing as mystery shopping companies. This type of scam can occur through an unsolicited e-mail or via a job board posting. **The fraudulent company asks you to pay a fee to become an employee. This is a scam because you should not have to pay a company to become an employee.** Another variation of this scam occurs when the employer asks you to review a wire transfer company and complete a money transfer, this action then becomes a payment forward scam as described above**.**

**How Do You Spot a Scam? Look for these "red flags".**

1. **Catchy job titles.** Scammers often use words in the job title to catch your attention, such as "Work at Home", "No Experience Necessary", "Make $1000 a week", or "Work just one hour a week".

2. **Required payment.** When payment is requested for training materials, starter kit, or other items it could be a scam.

3. **Lack of employer details.** If few details about the employer are included in the ad, posting, or e-mail, such as no company name, website, e-mail address, or location, then this may be a scam.

4. **Use of poor grammar and sentence structure**, inability to meet you in person, the signature not matching the name on the email address.

5. **Fake website.** If the website is hosted by a free domain, such as Yahoo, it may be a scam. Scammers will use a legitimate company's website information and post it as a fraudulent site. Research the company name and check **domainwhitepages.com** to

identify when the website was created. If the website was created recently or owned by someone not in the same location as the company, it could be fraudulent.

6. **Unsolicited e-mails.** If you receive an unsolicited e-mail and it comes from a free domain e-mail address (e.g., **gmail.com, hotmail.com, or yahoo.com) it could be a scam.** If the name of the e-mail signature does not match the name of the e-mail, this may be a scam. **Never click on a link in an e-mail from someone you do not know, it could be a virus or other malicious software.**

7. **Personal information requests.** Requests for personal information via e-mail, such as a copy of your ID, bank account information, or social security number, can be used by identity thieves.

8. **Guaranteed job offered.** Legitimate employers do not promise a job before discussing your skills and experience.

9. **Specific words or phrases.** Beware of words in the job description, such as wire transfers, PayPal, eBay, package forwarding, or money transfers, these are indicators of a scam.

The SPHHS OCP hopes you will use this information to keep you, your information, and your money safe. You are also welcome to contact the UMass Campus Police, or your local law enforcement agency and or launch a complaint with the Federal Trade Commission.

**Additional Links**
Below is a list of helpful resources for learning more about employment scams or to research possible fraudulent employers.

1. Federal Trade Commission
   Learn about employment scams or file a complaint.
2. Internet Crime Complaint Center (IC3)
   File a complaint with IC3 or review Internet crime prevention tips.
3. Better Business Bureau
   Research employers by reviewing reports, complaints, and accreditation status.
4. RipOff Report
   Discover complaints about companies.
5. Privacy Rights Clearinghouse
   Learn about avoiding online job scams.
6. Job Scam Examples - Typical Job Scam Examples
   Review job scam examples and share scam information.
7. http://www.ic3.gov/preventiontips.aspx
   FBI Tips and information
8. Glass Door www.glassdoor.com

**References**:

Adapted from the Winston-Salem State University Career Services, Nacelink Symplicity resources, February 2015 and these resources:

Privacy Rights Clearinghouse

Job Scam Examples - Typical Job Scam Examples

MEL revised 11/2019