FRAUDULENT JOB POSTINGS

Safeguarding Your Job Search
This information is provided to assist you with conducting a safe job search, protecting your identity, and increasing your awareness of fraudulent job postings and scams.

Please use caution as you search UVA AlumniJOBS, and other online job boards, for employment opportunities. If you feel uncomfortable about a job opportunity you are exploring, DO NOT click on any links and DO NOT provide any personal information.

What to Do if You Encounter a Scam
1. If you suspect that a posting on UVA AlumniJOBS is fraudulent, contact ACS at alumnicareers@virginia.edu or 434.243.9000.
2. If you believe you are the victim of fraud resulting from a job listing, contact the local police.
3. If you sent money or credit card information to a possible fraudulent employer, contact your bank and/or credit card company immediately to close the account and dispute the charges.
4. If the incident occurred completely over the Internet, you should file an incident report with the: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

Researching Employers
We strongly recommend that you research any organization carefully before applying.
1. Check the company website. Is there a website? If yes, does it match the job posting? Is it professionally developed, with good communication, and complete information, including job and career listings? Is there a site index and complete company information – or just information on job opportunities? Scammers often create quick, basic web pages that at first seem all right, but on review lack depth and pertinent information. Red flag!
2. Is it listed as a legitimate business: Look them up on recognized sites such as Better Business Bureau (BBB), local Chambers of Commerce, and other employer listings. Also check out professional associations if the company is a niche player.
   a. BBB: http://www.bbb.org/us/consumers/
   e. AFCEA – http://www.afcea.org
3. Internet Searches: Search the internet/Google by organization name for recent news articles to verify legitimacy. Search also by organization and key phrases like “ACME fraudulent job postings” or “ACME Scam job postings,” to find previous reports or incidents of scams.
4. Hoosonline: Use the Hoosonline Alumni Directory (advanced search) to find UVA alumni currently working at the organization (http://www.hoosonline.virginia.edu). If you find alumni affiliated with the organization, contact them to find out more about the work that they do.
5. LinkedIn: Use LinkedIn alumni pages (www.linkedin.com/alumni) to search for UVA alumni at the company. Do the same for other groups to which you belong. Also search for the organization in the LinkedIn company pages (www.linkedin.com/companies).
6. Verify the contact e-mail address: Does it have the same domain name as the organization? For example, the contact person at Acme should have an email that is jsmith@acme.com, not jsmith@hotmail.com.
7. Contact the organization: Call directly and ask if the person who posted the job works there. If no employees or customer organizations were listed on the site, ask for a list, or references. If the organization balks – red flag.

Identifying Fraudulent Jobs/Scams:
Fraudulent jobs are designed to obtain your personal information, identity and/or steal your money. Use these tips to identify potential job scams:
1. Too good to be true: Just say no to job postings that look like an easy way to make a lot of money with very little effort. They are usually scams. If it looks too good to be true, then it probably is. Also, do not respond to suspicious and/or “too good to be true” unsolicited job emails.
2. Know your contact: If someone asks for sensitive personal information, get the person’s name, organization, phone
number and email and say you’ll get back to them. Then investigate to be sure they are legitimate.

3. **Asking for SSN and DOB:** It is legitimate to ask for SSN and DOB after you are hired, but unless a prospective employer is doing a credit/background check there is little need to provide your Social Security number. If SSN and/or DOB are on the application, leave them blank. If you can’t apply without completing, call the employer, explain your concerns and ask what it is used for. Asking for SSN and DOB doesn’t mean the employer is fraudulent, but does raise a flag.

4. **Asking for financial information:** Real prospective employers never want your financial info. Do not provide your credit card number, bank account number, PayPal account or PIN number over the phone or online to a potential employer. Or wire, transfer or courier money. Never. Ever. Red flag!

5. **Fees for job search help:** Do not pay to get a job, or for a company to “help” you get a job. If the organization charges a fee, please consult with ACS before proceeding.

6. **Asking for direct deposit too early:** Do not agree to have funds or paychecks direct deposited into any of your accounts by an unknown employer. Especially before you’ve been hired – this is something you do during the first day/week of work.

**Personal Safety with Employers**

Always use good judgment in all of your interactions with employers.

1. Be cautious when posting your resume online. If you are unsure about an employer, limit the amount of contact and other personal information on your resume.

2. Do not provide a description of your appearance online or over the phone. Personal information such as height, eye color, ethnicity, etc. does not pertain to the job search.

3. Request business references for unknown organizations before interviewing with them. Schedule interviews with employers in public places only. Make sure someone knows of your plans to interview and the location.

4. If your instincts tell you something is suspicious, it probably is.

**Advice for Specific Aspects of Job Scams**

- **Case Study:** How a Job Scam was identified – and the advice to people who had already applied [http://www.rileyguide.com/realjob.html](http://www.rileyguide.com/realjob.html)
- **Tips for Accountant/Finance Job Seekers to Avoid Pay Forward Job Scams** [http://www.worldprivacyforum.org/jobscaamtipspayforwarding.html](http://www.worldprivacyforum.org/jobscaamtipspayforwarding.html)
- **How to Avoid Job and Work at Home Scams** [http://jobsearch.about.com/cs/workathomehelp/a/homescam.htm](http://jobsearch.about.com/cs/workathomehelp/a/homescam.htm)

**Disclaimer**

Alumni Career Services (ACS) provides UVAAlumniJOBS free of charge to employers and UVA alumni seeking employment opportunities. Job postings on UVAAlumniJOBS are based on information provided by the employer or the employer’s agent.

While we strive to keep fraudulent postings out of UVAAlumniJOBS, ACS cannot guarantee that every employer and posting is a legitimate posting or organization. ACS is not responsible for safety, wages, working conditions, or other aspects of employment or internships. It is the responsibility of each alumnus/a to research and verify the organization(s) and job posting(s) to which he/she is applying.

Alumni are advised to exercise due diligence and use common sense and caution when applying for or accepting any position. For the privacy and protection of alumni when applying to a job online, it is advisable that they do not give their social security number to a prospective employer, provide credit card or bank account information, or perform any sort of monetary transaction.

All job and internship listings are posted at the discretion of ACS. We will not post jobs that appear to discriminate against applicants on the basis of race, color, religion, creed, age, national origin, disabled or Vietnam Era veteran status, sexual orientation, gender identity, disability, or gender. ACS also reserves the right to refuse to post jobs that do not support the best interests or UVa alumni or the mission of the UVA Alumni Association.