## **Beware of Fraudulent Recruiting Advertisements**

Lawrence Livermore National Laboratory (LLNL) is aware that there has been an increase in recruitment fraud. These scams prey upon those seeking employment and use false and fraudulent offers of employment to obtain personal/financial information or money from their victims. This type of fraud can be carried out through websites, newspapers, fake e-mails claiming to be from hiring organizations, or phony social media profiles.

The best way to put a stop to these types of scams is to make job seekers aware that they exist, provide tips on how to identify and avoid them, and make clear how organizations recruit for positions so that you can more easily identify fraudulent recruiting advertisements.

## LLNL's hiring practices:

- Never requires job applicants to pay an application/training fee or submit personal documents like bank account details, passport number, Social Security number, tax forms or credit card information as part of the interview process.
- Involves at least one interview (virtual or in-person) and never interviews job applicants through chat platforms such as Google Hangouts, or via correspondence through text and instant messaging systems.
- Only sends email communications to job applicants from domain "@llnl.gov" or via their applicant tracking system, . Occasionally LLNL uses third-party vendors that will contact you about job opportunities. If a recruiter contacts you to apply, you will always be directed to our career page to apply through our career site.
- Encourages all applicants to visit LLNL's careers page at <u>www.llnl.gov/join-our-team/careers</u> if they saw the job posting on another site prior to applying to ensure the job posting is accurate and valid.

## How to Recognize and Protect Yourself from Potential Recruiting Fraud

As technology gets more advanced, the scams change, and methods evolve. It is wise to be able to recognize warning signs of recruiting fraud. The following is a non-exclusive list of warning signs:

- You are asked to provide a credit card, bank account number(s) or other personal financial information as part of the job application process.
- The contact email address contains a domain other than "@llnl.gov" or "notifications@smartrecruiters.com," such as "@live.com," "@gmail.com," "@yahoo.com," "@outlook.com," or another personal email account.
- The job position requires an initial monetary investment, such as payment by wire transfer.
- The job posting includes spelling errors, grammatical errors, or syntax errors.
- The job posting does not mention required qualifications and job responsibilities, but instead focuses on the amount of money supposedly to be made.
- The job posting reflects initial pay that is high compared to the average compensation for the type of job.
- You are offered a payment or reward in exchange for allowing the use of your bank account (e.g., for depositing checks or transferring money related to promised employment).
- You are asked to provide a photograph of yourself.
- The supposed "employer" contacts you by phone or through a chat room or instant messaging service and gives no way to call them back or the number they do give is not active or goes only to a voicemail box. For example, such supposed "employers" often direct that you "meet" them in chat rooms at specific times.

## What You Can Do

If you see a job scam or lose money to one there are various actions you can take, including:

- Filing an incident report at http://www.cybercrime.gov
- Calling the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357) or at ReportFraud.ftc.gov
- Filing a complaint with the Federal Bureau of Investigation at https://ic3.gov
- Contacting your local police to report the fraud.

- Contact your bank or credit card company to close your account and dispute any charges related to the fraud.
- Contacting a lawyer to assist in determining what actions are appropriate.
- Contacting the job board company to inform them of suspicious activity on their site.
- Contact LLNL at <u>careers@llnl.gov</u> to inform LLNL of the suspicious activity.