Combatting Deceptive Employment Schemes: AlayaCare's Response to Fraudulent Job Offers

As of December 2023, AlayaCare has been made aware of fraudulent recruitment activity including job postings and job offers. Scammers will create fake company profiles on leading job boards to approach victims, impersonating legitimate company employees and positions. The content of these communications can be quite convincing, where scammers will often use postings, public company information, and logos to mirror those of an existing organization. In all cases reported to AlayaCare, the positions were not legitimate roles within our company. Our team has compiled information to aid in deciphering legitimate versus fraudulent recruitment communication:

- AlayaCare never requires applicants to pay money or send personal identification such as identification, banking information, SSN/SIN as part of the application or interview process.
- While AlayaCare may make contact via a recruiter working on behalf of AlayaCare, this recruiter will always have an @alayacare.com email address tied to their LinkedIn account. If you are unsure if a contact is legitimate, you are welcome to email recruitment@alayacare.com to confirm.
- Communications, including scheduling of interviews and offers, will be made from an alayacare.com domain email address. Our team is not affiliated with any other domains. Scammers often create similar domains to increase the appearance of legitimacy.
- AlayaCare interviews are generally hosted virtually or via phone. Our team will communicate with you to schedule these from an accredited AlayaCare phone number and/or alayacare.com email address.
- Virtual interviews are hosted via Zoom or Microsoft Teams. We do not use WhatsApp, Skype, Hangouts, text, or any other platform to deliver virtual interviews.
- Current vacancies being recruited for are posted on our www.alayacare.com careers page.
- Key indicators of a job posting being fraudulent include those that:
    - Ask for an initial monetary investment, such as pay by wire transfer.
    - Contain spelling, grammatical, syntax errors, or if the posting reads in a way that is not in plain language.
    - Requests for personal information beyond a resume and basic contact details, such as photographs, copies of identification, or sensitive information such as banking information or SIN/SSN.
    - An obvious misalignment between the position and the organization (example: a "Sound Engineer" being sought).

As a global company attracting talent across Canada, the United States, Australia, New Zealand, and Brazil, our team takes candidates' privacy and security seriously. If you feel that you have been targeted by a potential fraudulent recruitment tactic, we encourage the following steps:

- Reach out to recruitment@alayacare.com to validate communications as being legitimate.
- Report and block suspicious communication via LinkedIn or other job boards.
- Do not click or download any links sent via email, job board messengers, or text.
- Report and block suspicious email handles.
- If you have provided information to a suspected scammer, document and report this to your local authorities and monitor accounts for suspicious activity.

If you suspect that you may have been targeted by one of these fraudulent communications, you can also refer to this message from LinkedIn which addresses recognizing and reporting spam and scams on LinkedIn.
https://www.linkedin.com/help/linkedin/answer/a1344213/recognize-and-report-spam-inappropriate-and-abusive-content?lang=en-us&intendedLocale=en

AlayaCare People & Culture Team