Information on fraudulent job postings

Nuance has become aware of a fraudulent scheme being perpetrated by an individual or entity claiming to be an employee of the Nuance Talent Acquisition department. The bad actors are fraudulently offering employment opportunities to applicants and then asking for sensitive personal and financial information and asking applicants to transfer funds to the bad actors.

While we are taking actions to shut down use of deceptive websites and URLs, we wanted to alert job applicants of this matter.

Please be advised that all legitimate correspondence from a Nuance employee will ***always*** come from "@nuance.com" email accounts. Bad actors will often use email accounts with addresses that are similar—but not identical—to legitimate accounts. Please look closely at the sender's address and don't respond to, or otherwise engage with, any communication that purports to be from a Nuance employee unless it comes from an "@nuance.com" email address.

If you are concerned about the validity of the contact from Nuance please contact the Nuance recruitment team via the following email box: globalemployops@nuance.com.

Please read the following information about these fraudulent recruitment activities.

What is recruitment fraud?

Recruitment fraud happens when actors offer fake job opportunities to job seekers. This is normally done online through job search websites (e.g. Glassdoor, Craigslist), fake websites, unsolicited emails or phony company email addresses. The actors posing as recruiters often request recipients to provide personal information, make payments or offer to send checks as part of their fake recruiting process. **Nuance never sends checks nor asks for applicants to provide copies of applicants' checks, nor does Nuance ever request money transfers or payments from applicants to secure a job, either as an employee or as a contractor.**

How to identify recruitment fraud

- Imposter recruiters offer a candidate a job and send a signing bonus check. When the check bounces, they ask for the candidate's bank account information or solicit copies of statements as a way to confirm the deposit was made.
- Imposters send a fraudulent check to the job seeker asking them to deposit the check into the applicant's account and wire funds back to the sender. The fraudulent check doesn't clear but the outbound transfer—of the applicant's own funds—has occurred.
- Imposter recruiters request personal information, such as address details, date of birth, resume, passport details and bank details, early.
- Candidates undergo interviews via Instant Messaging (e.g. instant messaging, Skype, etc.) programs.
- Email correspondence is often sent from an email address that is similar to an official Nuance address, but differs by one or more characters. Emails are also sent from accounts set up via public and/or free email hosts, such as Gmail.com.

What should you do?

- If you are concerned about the validity of a contact from Nuance please contact the Nuance recruitment team via the following email box: globalemployops@nuance.com.
- Please be prepared to provide supporting information from the correspondence you have had with the actor(s). Other helpful information to provide includes:
    - Complete copy of the email correspondence. Do not change or edit the message in any way. Save messages from the imposter for further investigation, if necessary.
    - Copy of any email addresses or the URLs of any websites that you believe to be phony or fraudulent.
- If you believe that you have been the victim of fraud, we encourage you to contact your local law enforcement and provide them with all relevant information.

What you should NOT do

- Do NOT accept checks or send any money. Nuance does not send checks or ask for money transfers or payments from applicants to secure a job, either as an employee or as a contractor.
- Do NOT disclose your personal or financial details to anyone you do not know.
- Do NOT respond to unsolicited business propositions and/or offers of employment from people with whom you are unfamiliar.
- Do NOT communicate further with imposter recruiters if you believe the communications may be fraudulent.