

FRAUD AND SCAM ALERT

In today's connected society, online scams are increasingly common. Komodo Health has recently become aware of the fraudulent use of its name on job sites that are not associated with the company. Prospective applicants should carefully research the legitimacy of any unsolicited recruiting communications that appear to come from Komodo Health.

The job offers come from online scammers falsely pretending to recruit on behalf of Komodo Health, by people claiming to work for, or to be affiliated with, Komodo Health. These people notify individuals that their qualifications were found suitable for a certain Komodo Health position. The online scammers reach out to job seekers via various methods (text message, email, messaging apps and other online communication tools) in which job seekers are asked to divulge their own personally identifiable information (PII) or to pay money as part of the initial online interview process. This type of masquerading is a common practice in cybersecurity and unfortunately can lead to one releasing PII and bank account information for purchasing equipment and making expense claims in pursuit of a job.

Please note that neither Komodo Health nor any of the organizations that recruit on its behalf ever ask for PII or money prior to a formal interview process, which includes an exchange of formal email communications from a verifiable Komodo Health email address. All individuals who receive an offer of employment from Komodo Health, whether directly or indirectly, are always required to go through a formal recruitment process. All communications should originate from a verifiable Komodo Health email address and not from any other email address (e.g. hotmail, yahoo etc.)

What to do (and not do)

Do not respond to unsolicited job offers from people or e-mail addresses you do not know or trust.

Do not disclose your personal or financial details to anyone you do not know or trust, or on a website you do not trust. If you have, consider reporting the incident to your local law enforcement and the [Internet Crime Complaint Center \(IC3\)](#).

Be on the lookout for suspicious signs – e.g. communications from non-Komodo Health email addresses (e.g. from a yahoo.com address); poor use of English; and requests for personal data and money.

Our position

Komodo Health's name and other company information are being used fraudulently in these situations. Although we sympathize with anyone victimized by scammers, Komodo Health is not responsible for their conduct and does not accept any responsibility for it.