# Legal Center - Privacy, Security, & Terms of Use for IT Insights Websites

## Fraudulent Recruiting Advertisements

Job Applicants should be aware of job offer scams perpetrated through the use of the Internet and social media platforms. The scammers frequently misappropriate and use a company's logo and photos of its executives to give the appearance of legitimacy. The scam preys upon those seeking employment and uses false and fraudulent offers of employment with employers, such as IT Insights, to steal from the victims. IT Insights believes that one of the best ways to put a stop to these types of scams is to make you aware of it.

IT Insights never requires any job applicants to pay money to anyone (IT Insights, its employees or anyone else) as part of the job application or hiring process. If someone asks for money or offers to send you a check for training, equipment, etc. as part of a recruiting process, they do not work for or represent IT Insights and are likely seeking to defraud you.

IT Insights's job recruitment process involves in person and/or telephonic interviews in most cases and never interviews job applicants through chat rooms (such as Google Hangouts), or through instant messaging systems. In addition, IT Insights's job recruiting staff sends email communications to job applicants from "@it-insights.co" or "@it-insights.co" email accounts only.

## How to Recognize Potential Recruiting Fraud

The individuals who perpetrate frauds like this are continuously changing and evolving their methods, and one of the most important defenses is healthy skepticism based on the discussion above. Despite the fact that IT Insights cannot predict all the ways scammers might operate in the future, the following is a non-exclusive list of warning signs of recruiting fraud:

- You are asked to provide credit card, bank account number(s) or other personal financial information as part of the "job application" process.
- The position requires an initial monetary investment, such as a payment by wire transfer.
- The contact email address contains a domain other than "@it-insights.co" or "@it-

insights.co", such as "@live.com," "@gmail.com," "@yahoo.com," "@outlook.com," or another personal email account. Or email correspondence is from an email address that is similar to an official IT Insights address but differs by one or more characters.

- The posting includes spelling errors, grammatical errors, syntax errors, or otherwise appears to have been written by someone not fluent in English.
- The open position does not appear on the company's website listing of job positions.
- 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.
- 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 or other personal identification of yourself.
- The job posting focuses on the amount of money supposedly to be made or reflects initial pay that is high compared to the average compensation for the type of job.

## What You Can Do

- If you believe you have been the victim of a job recruiting fraud scam, you can:File an incident report at http://www.cybercrime.gov
- Call the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357) or file a complaint with the FTC online at https://www.ftccomplaintassistant.gov/#crnt&panel1-1
- File a complaint with the Federal Bureau of Investigation at https://ic3.gov
- Contact 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 charges.

---