

Recruitment Fraud and Safety

Recruitment fraud is an illegal scam that exploits job seekers into providing personal information or money for fraudulent 'job opportunities' on career websites. This kind of fraud is usually done through unsolicited emails and text messages, or through fake websites and social media accounts posing as a company. Those engaging in this illegal activity may request personal or sensitive information with the intent of gaining access to your bank information, credit card number or social security number.

How to identify hiring fraud

Findhelp recruiters will never:

- › Request payment for applications or interviews
- › Offer resume coaching or training for technical assessments
- › Extend a job offer without conducting an interview
- › Send a communication from an unofficial email domain (e.g. Yahoo, Gmail, etc.)
- › Request that you purchase a computer, phone or other equipment

How to verify legitimate communications from recruiter

Follow these best practices to protect yourself against fraud:

- › If you are contacted about a job at Findhelp, please verify that the email came from the domain @findhelp.com before engaging with that contact. If you receive a job-related email from a different domain, it's likely fraudulent.
- › If you are contacted by a Findhelp recruiter over a job board like LinkedIn, please confirm that the recruiter's profile has been verified with the check mark.

How to verify legitimate communications from recruiter

Be careful when someone contacts you and take steps to protect your personal information. Be sure to report any suspicious contact to the media platform that was used. You can also learn more about recruitment safety and where to report it, through the [Federal Trade Commission](#).

Findhelp assumes no liability for recruitment fraud.