

Tips to Identify a Potentially Fraudulent Job Posting

1. You are asked to provide your credit card, bank account, PayPal, or other personal financial information.
<i>Legitimate jobs will not ask for this kind of information on an application, by phone or email.</i>
2. The contact email address contains a non-business email. Sometimes the posting may even appear to be from a reputable company, but the email address does not match the domain used by representatives of the company.
<i>Legitimate recruiters are directly associated with the company for whom they work. Therefore, the email addresses used should match the company's domain.</i>
3. You are asked to forward payments, by wire, courier, bank transfer, check, PayPal, etc...
<i>Never forward payments – they want to access your bank account and money. Do not forward, transfer or send by courier (i.e. FedEx, UPS), or “wire” any money to any employer, for any employer, using your personal account(s). Never transfer money and retain a portion for payment.</i>
4. The position requires an initial investment, for instance, having to purchase equipment or products in order to earn a wage or paying for necessary training.
<i>Legitimate jobs never ask for an initial investment. Some companies may ask you to pay a fee to obtain their sample product for demonstration. In essence, they are still asking for money so you can have a job.</i>
5. The “company” website is not active, does not exist, or re-routes users to another website.
<i>If the listed website is not working, does not exist, or the URL goes to another unassociated website, then the employment opportunity is most likely not real.</i>
6. The posting includes many spelling and grammatical errors.
<i>If the employyr kant spel, du u reely wanna werk 4 them? Poor spelling and grammar suggests the job announcement was written by a non-professional and therefore the job is probably not legitimate.</i>
7. A high salary or wage is listed for a job that requires minimum skills.
<i>This is designed to entice you, to get you to apply. Think wisely – how many legitimate companies can afford high wages for low skilled jobs? Why would they pay these wages?</i>
8. The position appears as a traditional job, but upon further research, it is independent contractor opportunity.
<i>Independent contractor jobs (“1099 type self-employment) mean you will be self-employed and accountable for associated IRS tax obligations. You will not have benefits and are not really an employee of the company.</i>
9. You are offered a large payment or reward in exchange for allowing the use of your bank account (often depositing checks or transferring money) or you receive an unexpectedly large check.
<i>Legitimate employers do not need to use your bank account! Also, these checks typically bounce – but you are then held responsible for all the bank charges and any money used, wired, or processed.</i>
10. It is difficult to find an address, actual contact information or the employer contacts you by phone, however, there is no way to call them back. The number is not available or disconnected.
<i>A legitimate business wants to be reachable for clients, business partners, and applicants so the number will be active!</i>

(Source: Georgia State University Career Services; Kevin Gaw, PhD & Melanie Jauch)

What to do if you Discover You've Been Scammed

- 1) Contact Career Services at (319-352-8425) or email derek.solheim@wartburg.edu
- 2) Contact Campus Security (319) 352-8372 and the local police.
- 3) If you have sent money to a fraudulent employer, contact your bank and/or credit card company immediately.