

Job Search Red Flags

How to Spot a Scam

Inconsistent or unprofessional communication methods.

- The company's website looks to be very basic or does not match the job description.
- Poorly written materials, many grammatical or spelling errors are present.
- Employer calls from a blocked or unknown number.
- Recruiter's email address does not match the company's domain name.
 - Uses free web services like @gmail.com or @hotmail.com; or is inconsistent like @googleinc.com rather than @google.com.
- The interview takes place at an odd location (such as a restaurant) instead of a formal office space.
- Interview questions are asked through email.

Request for financial or personal information.

- You are asked to provide bank account or credit details.
 - NEVER share this information during the job search process.
- The position requires an initial investment, such as a wire transfer to a foreign or unknown entity.
- The company asks you to send a photo.

Low investment, high reward.

- You're offered a job without applying or interviewing.
 - Scammers may use university directories to find your contact information.
 - All legitimate roles will require an application and interview process.
- Quick review process, recruiter responds immediately after submitting.
- Completely remote, work on your own time, with little to no supervision.
- Unusually high salary or wide range of compensation for little to no experience. Examples:
 - Make six figures immediately.
 - Make between \$30k-\$100k depending on your own work ethic.
 - Large focus on amount of money to be made as opposed to job responsibilities.
- You're offered a job on the spot or expected to give an immediate response.

What to do if I feel a job posting is fraudulent?

Research the organization for legitimacy.

- Find information on Google, LinkedIn, Glassdoor.com.
- Contact Business Career Services so we can investigate.
- Verify with the [Better Business Bureau](#).

Cease communication with the employer immediately.

If money has been transferred, immediately contact the company you used to send money and ask to have the transaction reversed.

Report it!

- If you feel your identity or safety is at risk, contact local authorities. Call the Ames Police Department at (515) 239-5133 or fill out the [Scam Reporting Form](#).
- Report the scam to the Federal Trade Commission (FTC) at reportfraud.ftc.gov.

If it feels too good to be true, trust your instinct. If in doubt, contact Business Career Services or review further guidance from our national organization, the [National Association of Colleges and Employers \(NACE\)](#), as well as the [Federal Trade Commission \(FTC\)](#).