Stay Secure While Job Hunting

When looking for new opportunities, follow these simple steps to protect yourself from fraud.

Depending on your situation, hunting for a new job can be either liberating or stressful. Either way, you should follow a few tips to keep your personal information safe and give scammers the pink slip they deserve!

Research, research, research

Search for the company that posted the job listing online using the company name only. Results that return multiple websites for the same company (e.g., abccompany.com and abccompanyllc.com) may indicate fraudulent job listings.

Ensure you aren't entering info on a spoofed website. Scammers will often spoof legitimate websites to deceive victims. You might notice small discrepancies, typos, or strange web addresses. Search for the job on the official company's career listings page and apply there.

Don't enter your information if something feels off about a job listing. Instead, contact the hiring company (using an email address or phone number on their main website, not the suspicious job listing). Don't be afraid to ask about the legitimacy of the job listing—this shows you read carefully and conducted due diligence! If the listing seems off and doesn't come from a company you can find from a web search, we recommend skipping it and moving on to other job postings.

Never pay to play

A common scam is to post a job listing that involves sending checks, money orders, or other forms of cash around. If any job posting describes a situation like this, some form of fraud will likely occur.

Never send money to someone you meet online (even if they claim to be a company), especially by wire transfer, prepaid cards, or money transfer apps.

If you receive paper checks with instructions to purchase items or transfer money, you should assume they are fraudulent. To see if they are real, contact the financial institution on the check to ensure the availability of funds.

Never provide credit card information to an employer.

Until you are sure of the identity of your employer, do not provide bank account information to them.

Another red flag for job search scams is if the "hiring manager" asks that you move communication to an encrypted messaging app. Stop contact with the other party if this happens.

Treat your personal info like cash

Remember, legitimate companies will only ask for your sensitive personal information (think Social Security numbers and bank account information for payroll purposes) AFTER hiring you, not before your employment contract is signed.

Before entering sensitive information on an HR portal or other website, evaluate the entire website and do a web search of the company. Contact the business directly if you have any questions about its legitimacy.

Think about who can see your contact information on your resume. You probably don't want your personal phone number and your home address on a resume you post online or send to hundreds of potential employees. Consider creating an email address solely for job hunting and possibly a forwarding phone number instead of your real one. When you do this, you build layers of protection around your identity.

Staying safe on LinkedIn

Oscar Rodriguez, vice president of product management, has a few tips to share for staying safe on that popular platform.

1. **Check for verified information on job postings.** A verification badge on a job posting means there is verified information about the company or job poster. This includes if the poster is affiliated with an official company page, has verified their association with a particular workplace, or has verified their identity through one of our identity verification partners.
2. **Share with care.** Consider what personal information you are being asked for. Never give out bank details before the onboarding process.
3. **Say “no” to suspicious requests.** Scammers can use tactics that legitimate employers wouldn’t, like asking you to download encrypted software for an interview or offering jobs with high pay for little work. Job offers after just one remote interview are very rarely a legitimate deal. You can report spam and inappropriate content.
4. **Enable message warnings.** Enable LinkedIn’s optional automated detection of harmful content, which may detect potentially harmful scams.
5. **Look for red flags.** Be cautious of job postings that sound too good to be true or require upfront payments. Common scams include roles like mystery shopper, company impersonator, or personal assistant. Additionally, be wary of anyone asking you to send money, cryptocurrency, gift cards, or to invest.
6. **Filter by jobs with verifications.** You can now filter your job search to show only jobs with verifications. The filter allows you to search exclusively for jobs posted by companies with a verified LinkedIn Page and current job posters associated with those companies. When toggled on, only jobs with these verifications will appear in your search results, and the filter will be visible in the search header.

LinkedIn has many more tips for staying safe!

Staying safe on Indeed

Scott Dobroski, the vice president of global corporate communications at Indeed.com, has advice for job hunters.

"Indeed removes tens of millions of job listings each month that do not meet our quality guidelines,” Scott says. “In addition, Indeed will not do business with an employer if their job listings do not pass our stringent quality guidelines. We encourage job seekers to report any suspicious job advertisements to us, or if they feel it necessary, to make a report to the police."

1. **Never send any form of payment to a potential employer you apply to on Indeed.** Not only is charging fees a violation of Indeed’s rules for companies, but these are often scams.

2. **Never accept money upfront for work you have not performed.** This tactic is commonly used in financial scams and can put you at considerable legal risk.
3. **Look for verifiable company email addresses.** Larger, more established companies usually have email addresses with top-level domains that match their websites. Generally, communications from such large, established companies do not come from publicly available addresses like Yahoo or Gmail. If someone with a generic address contacts you, ask if they can communicate via a company domain email address. If they can't or won't, proceed with caution.
4. **Be cautious when pursuing positions with salaries, perks, and flexibility that seem too good to be true.** Ask questions to confirm that the position is salaried (not commission only) and that there is a physical base of operations when a "work from home" opportunity is advertised.

You can find more tips on Indeed's website.

Dream employer or scammer?

The truth is that scammers know many job hunters are desperate, and some are out there trying to take advantage. If a job seems too good, easy, or well-paying to be true, it might very well be fake, especially if it comes from a company not easily found online.

Posts on job boards aren't always legitimate websites that catalog job openings can't easily verify the legitimacy of every single opportunity. If you see a job on a job board, go directly to the company's website to see if the job is also posted in their careers section. If it isn't, this is a good sign the post is not legitimate.

Just like you would look out for shady operations if you were pounding the pavement looking for work, keep an attitude of awareness and skepticism while hunting for a job online. With some caution, you can stay safe while leveling up your career!
