

# HOW TO AVOID GETTING SCAMMED DURING YOUR JOB SEARCH



PRECISION WRITING SERVICES LLC

Jennifer Alonzo Reule, CPRW | Find me on LinkedIn

Did you know a job search puts you at a higher risk of getting ripped off, scammed, suckered, or “phished”? (“Phishing” is the term for fraudulent — but official-looking — emails that attempt to acquire information such as usernames, passwords, and financial details.)

Online security firms report there has been a 125% increase in social media phishing attacks since 2012. Jobseekers are particularly vulnerable because job applicants are accustomed to being asked very personal information during an interview, so an inquiry from a prospective employer that asks for personal details doesn’t seem unusual.

Job search scams target everybody. People of all ages, income levels, and educational backgrounds have fallen for them. Scammers don’t single out anyone, and you don’t have to be dumb to fall for a scam. Plenty of smart people have fallen for scams.

However, jobseekers who are most at risk for being conned are those who are desperate, and that includes people who can least afford to lose money to these kinds of scams. That is especially sad, because these are people who may be living paycheck to paycheck and might need money quickly. If someone is not expecting to lose his job, he can be especially vulnerable because he is desperate. The long-term unemployed are also at risk, because the scam might appear to be a “lifeline” that offers immediate income.

There are several common job scams that jobseekers might face. Work-from-home scams are one of the top rip-offs that target jobseekers.

## Work-From-Home Scams

Today more Americans are working from home. An estimated 30 million people work from a home office at least once a week (certainly more now due to the COVID-19 pandemic), and many work satisfaction surveys reveal that employees would trade a lower salary for the flexibility of telecommuting. It's no wonder that work-from-home scams are proliferating.

Some work-at-home scams involve “pay-to-play” schemes. An example would be if you are asked to send money in exchange for a special kit, supplies, or software that you can use to earn money working from home. Sometimes the company will promise to reimburse you when you are hired, but the job offer never materializes. Or the scammer might ask you to pay a subscription fee to access a website or a list of work-at-home opportunities.

The most common scam you've probably heard about is where you're asked to deposit a legitimate-looking check and then wire money or buy products online. You're then left holding the bag when the check bounces. Your bank will require you to cover the full amount of the check plus bank service fees.

Some of the most common work-at-home schemes target folks looking for extra holiday income, especially since many of these are advertised as part-time and work-at-home jobs. You have a lot of people who want to make an extra \$100 for buying presents at the holiday time, so you'll probably see more of those advertised around the holidays than you would at other times of the year. However, any time a scammer can make money, they're going to take advantage of it, holiday or not.

The most common work-at-home scams are “envelope-stuffing” jobs, assembly jobs (where you purchase supplies to assemble a craft or item, but when you submit the completed items for payment, they are rejected as “not being up to standards”), rebate processing, online survey-taking, and medical billing.

Be particularly cautious if the “employer” requests payment for something in the form of a pre-paid Visa card. It is very difficult to recover the money lost to a fraudulent transaction with a pre-paid debit card as there is often no paper trail.

Some work-at-home business opportunities promise a refund if you’re not satisfied; however, jobseekers who have attempted to obtain a refund are usually not successful.

Remember this: If something sounds too good to be true, it probably is!

## **Identity Theft**

Identity theft occurs when someone uses your name, Social Security number, date or birth and/or other identifying information — without your permission — to commit fraud.

One of the biggest areas of growth in identity theft is tax theft. An identity thief may use your Social Security number to file an income tax return and obtain a refund using your information. If someone uses your Social Security number to file your tax return before you do, the IRS records will show the first filing and refund, and you’ll get a notice from the IRS saying more than one tax return was filed for you.

Or, your Social Security number may be sold to an undocumented individual. If someone else uses your Social Security number to get a job, the employer may report that person's income to the IRS. When you file your tax return, you won't include those earnings, and the IRS will notify you that you received wages but didn't report them.

If your identity has been stolen, and you receive a notice from the IRS about unreported wages, or that your return has already been filed, contact the IRS Identity Protection Specialized Unit at (800) 908-4490.

So be cautious when you are asked to provide your Social Security number during a job search, especially if it's asked for in an application or online form. Carefully check out any companies that send you an unsolicited job application or offer before providing any personal information (especially your Social Security number). Also, don't give your bank account information (even if you're asked to provide it so that the company can deposit your paycheck directly into your checking account).

Be careful of how much personal data about yourself you disclose publicly on social media sites. Identity thieves can use that information to answer "challenge" questions on your financial accounts, gaining access to your money.

### **The "Bait and Switch" Job Offer**

Some jobseekers are being targeted with "bait and switch" scams because they're not sophisticated in discerning what is or isn't a legitimate job opportunity. Scammers are putting together job postings that look like they're from real companies.

These jobs are scams when the job isn't as promised. For example, a recruiter might post a job listing for a job that doesn't actually exist — they just want to collect résumés to build their database of candidates. On Craigslist, Monster, or CareerBuilder, these scams might be posted to gain leads for multi-level marketing opportunities or to build a database of jobseekers they can sell.

Fake job postings are more likely to appear on Craigslist because the listing is free. The scammer might have to pay a couple hundred dollars to list it on Monster.com — and some of them actually do.

For jobseekers, Craigslist can be a legitimate source of job opportunities, especially for folks who work in hourly, part-time, or contract positions. Unfortunately, scammers are causing jobseekers to miss out on legitimate work opportunities when they ignore Craigslist as a source of job postings because of the possibility of fraud.

## **How to Avoid Being Scammed**

Research is probably the biggest defense you have against getting scammed. Start with a simple Google search and find out if you're pursuing an authentic opportunity — or if other folks have been targeted with the same scam. Job postings with lots of errors, misspellings, and/or typos are often scams. Also, when you search on Google for a job posting, see if the identical ad comes up in numerous other cities. If it does, it may be a scam.

Act cautiously when receiving job offers that sound too good to be true. If you receive an email “out of the blue” with a job offer, investigate it thoroughly before responding, or simply delete it.

They might even use the real company's name and logo, but the email comes from a Yahoo! or Gmail account. Some of these scams are also coming through disguised as LinkedIn connection requests or job postings. You have to look very closely at the details in order to determine that it's actually not an authentic opportunity.

Some scammers don't even bother to make it look like the job opening is with a major company; instead, they'll just make up a job prospect in the hopes of hooking unsuspecting jobseekers. This take on "catfishing" (where an unsuspecting individual pursues a relationship with a fictional boyfriend or girlfriend) is popular because it costs the scammer little or no money and is very effective.

The purpose of these fake listings is to collect the jobseeker's Social Security number, credit card data, and/or bank account information, which is then used to access your bank account or steal your identity. This is sometimes done by requesting that the applicant pay to have his or her credit score checked or a background check done. The jobseeker is then directed to a scam website where personal information will be harvested and stolen.

The scammer posts dozens or hundreds of listings for free on Craigslist (it doesn't charge for job postings in most U.S. cities), and if they get even a small percentage of folks to fall for the scam, they can make tens of thousands of dollars.

"Bait and switch" offers can exist on any niche job board, or even the "big boards" like Monster.com and Careerbuilder.com.

As mentioned before, be mindful of the information you share on social media. Using sites like Facebook, Twitter, and LinkedIn can be beneficial in your job search, but they can also make you the target of scammers. A lot of the information you put on social media related to your job search is public, and if you put out the word that you need a job fast, it will make you a bigger target.

Again, use social media proactively as part of a targeted plan for pursuing the job that you want.

### **Avoiding Being Re-Victimized**

Sometimes scammers sell lists of people who have been scammed before. The second round of scammers offers to help you recover the money you've lost in the original scam. Instead, you're re-victimized. Unfortunately, the kind of folks who are perpetuating these scams don't care about people; they only care about money. So they're going to take advantage in any way they can in terms of separating you from your money or, again, re-victimizing you if you've already been scammed once.

If you have been scammed, report the crime. Contact your local police and the Federal Trade Commission ([www.ftc.gov/complaint](http://www.ftc.gov/complaint)). If you have provided access to your financial information (for example, providing your bank account information to facilitate direct deposit of your "paycheck"), contact your financial institution and ask for help in eliminating the scammer's access to your account (which may include closing the impacted account and setting up an alert on the new account). Keep a written log noting the names and phone numbers of everyone you've spoken to, and keep copies of all reports you file.

Sometimes, the scam can be quite elaborate. You may be asked to participate in several phone interviews, or complete a pre-employment test. However, being asked to jump through several hoops does not mean a job opportunity is legitimate.

If you are deliberate about investigating things that might be helpful to you in your job search — whether that's working with someone to help you with your résumé or LinkedIn profile, or you're exploring work-at-home opportunities — doing your homework is certainly important.

For work-at-home opportunities, research is especially relevant. You can certainly find real work-at-home opportunities listed online, but you'll need to do a little homework to make sure they're authentic.

Having a plan is also a good defense. The more focused you are on your job goal, the less desperate you are. That may involve working with a career services professional to develop your plan, or perhaps getting help from a resource in the community, like a workforce development office, churches and community organizations that offer assistance, or even your college or university's career services office.

Having assistance in developing a plan is going to help you be a lot more methodical about implementing that plan. Consequently, you will be a lot less desperate and you won't necessarily chase prospects or respond to unsolicited opportunities. You are more likely to be scammed by things that come into your email inbox than leads you're pursuing through, for example, networking or LinkedIn.

Manage your online presence to minimize opportunities for identity theft. Use passwords that contain letters, numbers, and symbols — and do not use the same password for multiple sites. If a scammer asks you to set up a username and password for accessing a company website, and you use the same password for your financial accounts online, they can access them without your knowledge.

Request your free annual credit report from the three national service providers (Experian, TransUnion, and Equifax). Obtain yours via [www.annualcreditreport.com](http://www.annualcreditreport.com). You can receive a free copy of your credit report every 12 months from each credit reporting company, which allows you to spot possible identity theft. Some jobseekers choose to pull a report from one bureau every four months, so they receive all three reports for free in a calendar year.

Checking your credit report is important because some companies will request access to your credit report as a condition of employment. As such, identifying and correcting errors is critical.

If you have been victimized, you can place a fraud alert on your credit report, which lets potential credit grantors know that you've been a victim of identity fraud. (You can remove the alert at any time.) Once you notify one of the national service providers, they will notify the other two companies. If you place a fraud alert, you are entitled to a copy of all of the information in your credit report at each of the three major credit reporting companies. You can also place a security freeze on your credit report, which prevents new credit applications from being issued.

Consider signing up for an ongoing credit monitoring service, which will provide you with email alerts if identity theft or fraud is suspected on your accounts. Some credit monitoring services also include identity theft insurance, which will reimburse you for time and money spent recovering your identity.

Unfortunately, there are many scammers waiting to con desperate jobseekers. You must keep your wits about you to protect your job search, reputation, and financial well-being. A little research and planning can go a long way toward keeping you safe.

**HAPPY (AND SAFE) JOB HUNTING!**