

## Keeping Your Money Safe: Working From Home Job Scam

*Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.*

*Ashlie Hagemann,  
Fraud Supervisor*

### How Does the Scam Work?

Technology has dramatically altered the workplace in many different ways. One key example is the increase in employees working from home due to advances in WiFi, mobile devices, VPN, etc. In fact, a [recent study](#) found that 70 percent of people globally work remotely at least once a week.

Unfortunately, scammers are exploiting this trend by posing as legitimate employers offering work-from-home positions to unwitting job-seekers known as the working from home job scam. This opens the door for them to take advantage of you and your confidential information through fraudulent wire transfer schemes, claims processing, envelope stuffing, refund recoveries, and other bogus offers.

### How to Prevent the Scam

The following tips provide ways to spot these types of scams and discern whether or not what seems like a great opportunity is too good to be true.

**1. Spot the red flags.** A lot of scammers will raise an obvious red flag by using a Gmail or Yahoo account instead of a traditional business email address to communicate with you. Another popular tactic is to request an interview using online chat. These red flags should alert you that the opportunity to work from home may be a scam. To counteract these tactics, insist on being interviewed by phone or video conference, or even better, in person. You should also ask for the names of your interviewer(s) in order to research them on Google or LinkedIn to ensure they are who they claim to be.

**2. Make sure the job description sounds legit.** A traditional job description will generally have a detailed list of responsibilities and expected qualifications. If you come across a description that consists of just a few bullet points or makes it seem like getting the job will be easy, it could be a scam. One way to investigate this is to ask detailed questions about what the job entails. If the answers seem vague or incomplete, it might not be a legitimate opportunity.

**3. Research the company.** Fortunately, there are a multitude of tools available to research companies in today's cyber-connected world. Obviously, the first place to check is the company's website. If they don't have one, or a very basic one with poor design, that could be a warning sign. You can also research companies through job board sites like

Glassdoor or Monster, and through their social media presence. You should also look up reviews of the company. If any of these items are missing, the job opportunity could be a scam.

**4. Never contribute or disburse your own funds.** It might seem obvious that you would not do this, but sometimes scammers will claim that you need to cover the cost of introductory training, or they may ask for an application or processing fee. This is definitely a warning sign that the opportunity may not be legitimate. It is also important to learn enough about the company to confirm that it is a legitimate business and that you have been officially hired before providing any personal information such as your Social Security number or direct deposit information.

## Keeping Your Money Safe

Following these tactics will help you determine which remote work opportunities are legitimate and which are attempts at the working from home job scam. Protecting yourself, your information, and your bank accounts is an ongoing endeavor requiring constant vigilance.

PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our [fraud resources page](#).