

As the Coronavirus continues to spread, you may be looking for ways to make money without ever stepping foot outside your door. While remote work is a great option for many, some scammers are looking to make their own money by defrauding remote jobseekers.

Typical work-at-home schemes promise large earning potential for very little effort and expenditure of your time, taking advantage of an individual's willingness to earn a living for themselves and their families. Watch this video from the Federal Trade Commission to learn how you can be on the lookout for work-at-home scams.

Watch video

### Signs of a Job Scam

Scammers advertise jobs where legitimate employers do — online, in newspapers, and even on TV and radio. Here's how to tell whether a job lead may be a scam:

You need to pay to get the job. They may say they've got a job waiting, or guarantee to place you in a job, if you just pay a fee for certification, training materials, or their expenses placing you with a company. But after someone pays, these jobs often do not materialize.

You need to supply your credit card or bank account information. Don't give out your credit card or bank account information over the phone to a company unless you're familiar with them and have agreed to pay for something.

The ad is for "previously undisclosed" federal government jobs. Information about available federal jobs is free. And all federal positions are announced to the public on <u>usajobs.gov</u>. Don't believe anyone from another source <u>who</u> <u>promises you a federal or postal job</u>.

### Military Consumer Month

July is Military Consumer Month and a good time to focus on scams affecting military consumers. Last year, imposter scams once again topped the list of frauds that military consumers reported to the <a href="FTC">FTC</a>. More than 35,000 servicemembers, veterans, or family members reported an imposter scam.

Imposter scams come in many varieties, but work the same way: a scammer pretends to be someone you trust to convince you to send them money.

Learn more



# Overview of Colorado's Data Breach Law

Who is impacted by the changes to Colorado's consumer data privacy laws?

• Any person, commercial entity, or governmental entity that maintains, owns, or licenses personal identifying information ("PII") of Colorado residents in the course of its business, vocation, or occupation.

What is a security breach?

 A security breach is the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person, commercial entity, or governmental entity. Go to <u>coag.gov/resources/data-protection-laws/</u> for more.

Learn more about Colorado's Data Breach Law and recent enforcement actions.

# Stay Informed

For the most up-to-date information about the Coronavirus, visit the websites of the:

- Colorado Department of Public Health and Environment
- Centers for Disease Control and Prevention (CDC)
- World Health Organization (WHO)

## COVID-19 Consumer Advice from Attorney General Phil Weiser

Colorado Attorney General Phil Weiser created a <u>webpage</u>, also available in <u>Spanish</u>, offering guidance and alerting consumers about how they can protect themselves against COVID-19-related scams. Helpful topics include:

Cybersecurity while working from home Safe banking Charitable giving

## Take time to report fraud or suspicious activity

By learning how to avoid scams related to the Coronavirus, we can work together to ensure no one in our state is taken in by these malicious attempts to defraud Colorado consumers during this public health emergency.

If you notice any scams, fraud, price gouging, or other attempts to take advantage of Coloradans during this public health emergency, contact Stop Fraud Colorado at 800-222-4444 or <a href="www.StopFraudColorado.gov">www.StopFraudColorado.gov</a>.

Tell us your story



