



## **MOST COMMON SCAMS TO AVOID**

**SSA (Social Security Administration) imposter Scam** - Someone calls stating they are from the SSA, the caller requests money or your SSN (Social Security Number) for financial gain or to steal your identity. Sometimes they tell you your SSN has been linked to criminal activity and you will be arrested or your SSN will be cancelled if you do not pay a fine.

**COVID-19 Testing Kit Scams** - Someone calls stating they will send you a packet of testing kits for a low price - the caller will request your credit card number to pay a small fee.

**Romance Scam** – A person adapts a fake online identity to gain a person’s affection and trust. Later the victim is asked for money, or to become a money mule or mover for the scammer. This swindle many times targets widows.

**Grandparent Scam**- You get a phone call from who you think is your grandchild or loved one, they request money be sent to assist with an emergency (car got towed and they are in jail). Or someone may call saying they are a medical professional and your loved one needs medical attention, but can’t pay. Without your money your loved one will die! NEVER send cash or give out any of your Personal Information. Always confirm it is your loved one who called.

**Work From Home Scam**- You received an email or text message stating you got the job, you don’t remember applying for the job, but the pay and the hours are great. The scammers request your bank information to deposit your first check- or they send you a check, and then instruct you to cash it and send them a certain amount back. The check is a fake, and you end up negative in your account and responsible for the fraudulent check. OR you may respond to an ad for a mystery shopper or other fun position that never really existed, and end up giving your information or your money to the scammer.

**Phishing Emails** – You get an email from an unknown sender stating they have an inappropriate video of you. The scammers request you send them gift cards or Bitcoins. If you do not follow the instructions, your video will be leaked to all your email contacts. REMEMBER! They do not have a video of you, it is their job to make you believe them, and to get you to fall for the scam.

**Gift Card Scam**- You receive a call from someone stating they are a government official, the caller request you pay a fine to avoid being arrested. The scammer request you go out and buy gift cards for different amounts. Once you purchase the gift cards, you are to contact the scammers and provide them with the gift card information. Government officials will NEVER call requesting payment via gift card or Bitcoins for overdue fines.

**Text Messages or Emails**—You receive a text or email from someone claiming to be a business you know, like Netflix or your bank. They say someone hacked your account, and they need you to click on a link to find out more. Don't click on that link!! This is a scam.

**Pay Your Bill**—Someone calls you claiming to be your utility company, and says your bill is way overdue and you are about to be shut off if you don't pay right away. Hang up and call the company directly.

If you or someone you know has been a victim of a fraud/scam and would like to report or talk to someone, please give us a call.

**Colorado Bureau of Investigation**

**Victim Assistance Unit**

**303-239-4242**

**Se hablas español: 303-239-4312**

**Call our 24-hour Identity theft hotline 1-855-443-3489**

**Visit us Online: <https://www.cbivictimsupport.com>**

