Additional Tips

-Remain alert to any unusual mail or emails received and read through things that may initially appear as junk mail.

-Set privacy settings when adding/uploading a new app.

-Do not click on links you are not sure about, even if they are sent by a trusted source.

-Do not trust phone calls or emails phishing for private information. Hang up and call the business from a phone number you have used before or that is printed on the back of your credit card or on a business statement.

-Verify friend requests. Remember, email addresses can be faked.

-Safeguard your passwords.

-Closely monitor bank accounts and credit card statements.

Contact Us

Colorado Bureau of Investigation
Identity Theft and Fraud Unit

Victim Assistance Program
303-239-4242
Si hablas español
303-239-4312

24 Hour Toll Free Hotline

855-443-3489

Email

CBI.StopIDTheft@state.co.us

Mailing Address
Colorado Bureau of Investigation
Identity Theft and Fraud Unit

690 Kipling Street #4000
Denver, CO 80215

Follow us on Facebook

www.facebook.com/CBI.IDTheft

Visit us Online

www.colorado.gov/cbi

Revised February 27, 2019

PROTECT YOUR PERSONAL IDENTIFYING INFORMATION

Colorado Bureau of Investigation

Identity Theft and Fraud Unit

Victim Advocates
can be reached at
303-239-4242
Si hablas español
303-239-4312

or

24 Hour Toll Free Hotline
855-443-3489

Tips

Protect your Personal Identifying Information by following these tips:

Open an **online "My Social Security" account** with the Social Security Administration: ssa.gov/myaccount

Check your Credit Reports: Consumers are entitled to one free credit report annually from each of the major credit bureaus: annualcreditreport.com

Consider placing **Fraud Alert**: A business must try to verify a consumer's identity before extending credit: consumer.ftc.gov/articles/0275-place-fraud-alert

or

We recommend placing **Credit Freezes**: Once a freeze is placed, no one, including the consumer, can access the consumer's credit report to open new credit until the consumer uses their assigned Personal Identifying Number (PIN) to unfreeze and refreeze their account. Information: consumer.ftc.gov/articles/0497-credit-freeze-faqs

No cost to consumers to place credit freezes or to unfreeze or refreeze credit reports.

Bureaus have up to one hour to release the freeze when a consumer calls in their request. They have three days, if the request is made in writing. Freezes last until the consumer temporarily lifts or permanently removes them.

Credit Locks: This involves a cost with each bureau. It is unknown how secure the lock is. It is NOT necessary to protect a person's credit. **Fraud alert** and **credit freezes** are still viable NO COST options that provide excellent protection.

File an ID theft report with your local law enforcement agency: If you are told they won't be able to investigate, tell them you need the report/case number for documentation purposes. Make sure to get your case report number.

File an ID Theft Affidavit with the Federal Trade Commission at: identitytheft.gov

Consider opting out of pre-approved credit offers: optoutprescreen.com

If you are notified of **tax fraud** by the IRS and therefore have concerns about tax ID theft, log onto this site for more information:

irs.gov/newsroom/when-to-file-a-form-14039-identity-theft-affidavit

Multi-factor Authentication: Contact all existing banks, credit card companies, lenders and investment firms, to add extra security called 2-step or multi-factor authentication. You want your accounts flagged in case someone tries to change your mailing address, request a new card or access your account.

Passwords: Use a combination of letters, numbers and symbols that no one can figure out. Experts recommend about 25 characters in length. Change it when you believe or have been informed your password was breached.

Public Wi-Fi: Do NOT use it. It is safer to use private Wi-Fi or a Virtual Private Network (VPN).