

Spread the word with daily online safety and preparedness tips on Google+, Facebook and Twitter. Use the following blog, or create your own, and post all throughout June. Remember to include the hashtag ***#COReady #SocialMediaSafe***

## Title: Be a Savvy Social Media Surfer

### Be Safe When Using Social Media

Social media sites like Instagram, Twitter and Facebook are prime platforms for scammers to promote get rich quick schemes to unsuspecting victims.  Posts promoting “money flipping” are showing up more often in consumer’s newsfeeds. Usually the post contains a photo of cash and the caption boasts of how easily a small amount can be “flipped” into a large amount.  The profile of the poster seems legitimate including photos, followers and even thank you messages from other “investors”.

The [Federal Deposit Insurance Corporation](https://www.fdic.gov/consumers/assistance/protection/idtheft.html) (FDIC) also has concerns with social media. A fear for the FDIC is identity thieves using your social media sites to gather personal information. The information can help them access your financial accounts and passwords. Once identity thieves have these two ingredients they can steal your identity.

Some thieves even go so far as to create fake profiles to establish themselves as legitimate financial institutes or businesses that need your personal information. Identity thieves are good at luring you in and getting Social Security numbers, banking institutions, account numbers and plenty of other information including your home address.

### Ways to Protect Yourself While Using Social Media

* **Regularly check your security settings on all of your social media channels.** Security settings should be set up to block people who you do not want to see your page. Use a private setting and do not feel obligated to accept it new friend requests.
* **Block people.** If you see that someone has made their way into your network that you don’t know, block them. Don’t feel you have to provide information like your birthday and where you went to school if you are not sure of your security settings.
* **Beware of games or quizzes that may come from third party programs or apps.**
* **Do not post your vacation plans on social media.** When travelling, do not post your “checking in” to an airport or your travel dates/locations on social media. This is an easy target for thieves to go to your home to burglarize it while you are gone.
* **If you communicate with your bank or other financial institutions through social media, remember that your posts may become public even if your settings are private**. It’s best to avoid posting any personal information on any part of a bank’s social media site.

### Tips for Spotting “Money Flipping” Scams

* **Search Online –** Before contacting the social media account promoting an “investment,” search online for their username and phone number.  You might find other victims have posted complaints and other information**.**
* **Prepaid Debit Cards Equals Cash –** Remember to treat prepaid debit cards as if they were cash.  Anyone with the card number and pin will be able to withdraw the money.  If you wouldn’t give a stranger cash then don’t give them the account information.
* **Trust Your Instincts** – If it sounds too good to be true it most likely is. Users should trust their instincts and use common sense when trying to supplement their income.  Get rich quick schemes rarely have the payback they promise.

The [America Association of Retired Persons](http://www.aarp.org/money/scams-fraud/info-2016/stay-safe-and-secure-on-social-media.html) (AARP) says if you are 50-plus and on Facebook that you are in great company. Sixty-four percent of online adults ages 50 to 64 use Facebook, as do almost half of those 65 and older. But among social media fans and followers, there is fraud. ["Phishing"](http://blog.aarp.org/2016/05/13/top-phishing-scams-on-social-media/?intcmp=AE-MON-CONP-IL) scams. This scams include criminals trying to collect your credit card numbers, log-in credentials and other information in order to steal your identity. These scams have more than doubled in the past year according to social media security company Proofpoint.

### Watch out for these Scams Targeted at Adults on Social Media

* **Twitter Tricks** - With keystroke tweaks—such as adding an extra character to a corporate name—cybercrooks create fake social media accounts to pose as customer-care representatives.
* **Live-Stream Lies**. Taking a cue from media companies that stream their television shows and movies online, crooks offer their own programming—typically, they promise free viewing of a big game, hot concert or other popular event.
* **Fake Freebies and Discounts.** Scammers set up bogus social media pages that look like those of legit companies—and claim to offer free or dirt-cheap products and services to collect your name, address, phone numbers, email address and other information to be used for identity theft or sold to other crooks on the black market.

Social media has become a way for people to communicate on a daily basis with others. Be careful with what you share and just because you may keep things private, your posts on other people’s sites may get out into the world and into the wrong hands.

If you have been a victim of a money flipping scam or wish to report suspicious social media activity, you can [**file a report**](http://www.stopfraudcolorado.gov/about-consumer-protection/report-fraud) with the Colorado Attorney General’s Office.

### Social Media Safety Resources

* [Federal Deposit Insurance Corporation](https://www.fdic.gov/consumers/assistance/protection/idtheft.html)
* [Stop Fraud Colorado](https://www.stopfraudcolorado.gov/fraud-center/digital-fraud/money-flipping-scams)
* [AARP Fraud Watch Network](http://www.aarp.org/money/scams-fraud/fraud-watch-network/?cmp=RDRCT-FRDWCHNET_SEPT17_013)
* [Better Business Bureau](https://www.bbb.org/council/news-events/bbb-scam-alerts/2015/08/scam-alert-avoid-social-media-easy-money-scams/)

For more tips and preparedness information, follow us:
On Twitter: [@READYColorado](http://www.twitter.com/readycolorado)
Facebook: [www.Facebook.com/READYColorado](http://www.Facebook.com/READYColorado)
Google +: [READYColorado](https://plus.google.com/100167075139424077484)
YouTube: [www.youtube.com/READYColorado](file:///C%3A%5CUsers%5Cmtrost.DPS%5CDocuments%5CMicki%5CPrepareColorado%5CMay2015%5Cwww.youtube.com%5CREADYColorado)