Social media sites like Facebook, Twitter and Instagram provide a convenient way to connect with friends and family. It is important to remember that scammers also use these platforms to find victims. Scammers often create fake profiles and pretend to either be someone you know, someone you want to know or an entity you trust. Because there are fake profiles it is difficult to know who you can trust. The following are some red flags that you might be targeted by a scammer on Facebook or other social media platform:

- You receive a friend/follow request from someone you are already connected with.
- You receive private messages from someone you do not know.
- You are informed about an opportunity to receive a grant, sweepstakes or prize.
- You are asked to send money to receive money.
- The person who you are messaging with asks for your phone number, email address or physical address.
- Someone you do not know shows a romantic interest in you very quickly.
- You are notified that someone is in an emergency situation and they need your help right away.
- You are receiving messages or posts with poor spelling or grammar.
- You are offered a gift, prize, money or a coupon that seems “too good to be true.”

It is critical that you only engage with people on social media platforms who you know. Make sure you use privacy settings to ensure only people who you know and trust can view your profile. If you have questions about a potential social media scam or how to lock down your privacy settings, contact an AARP Foundation ElderWatch volunteer specialist at 800-222-4444, option 2, to talk you through the situation.

800-222-4444
Denver Metro Area
303-222-4444
www.aarpelderwatch.org