What not to post on social media to avoid identity theft.

Did you know? In 2021 alone, there were nearly 1.5 million identity theft complaints — with social media being one of the leading causes for the rising numbers. Because social media is part of our daily lives, it can be easy to forget basic safety rules. Wondering what not to post on social media to avoid identity theft? Never share these six categories:

1. **Personal information.** As a rule of thumb, refrain from sharing too much on your social media profiles. Minimal info keeps you safer. Not sure what's public information? Take time to do a sweep of your online presence. Look at your social media pages to see what's on display. Sharing things like your birthday, high school, city where you reside, and more, gives identity thieves a more complete picture of you. Then, take it a step further and search for yourself in a search engine, such as Google, to see what others can see. Remove what you don't want public.

2. **Your home.** You got that new house … congratulations! But do you really want followers/strangers knowing the exact address? To be safe, don't share your city, a full photo of your home, or other identifying items like the house numbers or mailbox in photos.

3. **Payment information.** Social media marketplaces, retailers, and more rely on the sharing of payment information through online portals and payment apps. If someone asks for payment in a suspicious way or if you feel something is off, never share payment information. Be alert while on Facebook Marketplace. Take the time to vet retailers that deliver you ads by searching for them on Google and reviewing their associated Better Business Bureau ratings before making a purchase. Giving your credit card or bank account information too freely can be dangerous. Identity theft is a growing crime and hackers are getting smarter. That means you should also.

4. **Passwords.** A common phishing scheme involves fraudulent password scams. If you receive a message telling you to reset a password … stop. Don’t do anything until you do some digging. Look at the sender of the message — is it a legitimate business? Look at your history — has this organization contacted you before? If it seems legitimate, go directly to the site (not through the email or prompt) and try logging in with the credentials you know. Do not click on any links or respond to the message with password information if you’re suspicious. Your best bet is to find the company’s email or phone number from their website and call them directly to learn more.

5. **Location details.** Traveling across the state, country, or world? You’re sure to snap some photos for sharing. But doing so, especially in real time, sets you up for identity and property theft. People online can see you’re gone and target your home or mail while you’re away. For the safest sharing, wait to post photos until you’ve returned home. Or, avoid using location details altogether.

6. **Forms of identification.** It can be tempting to share the funny photo on your driver’s license or a photo with the marriage license you and your spouse-to-be just picked up. Even if you block out other information in the photo, you may still be sharing snippets like your signature, address, parents’ names, or town of birth without realizing it. That information could help thieves puzzle together more about you. Don’t share any part of your marriage license, birth certificate, passport, driver’s license, Social Security number, student ID, or other important documentation on social media.

Always remember the basic rules of the internet.

Social media is woven into our daily lives, jobs, and relationships. It can be easy to post and forget the golden rules of safety. But reminding yourself, your children, and loved ones what not to post on social media can keep everyone better protected from scams like identity theft.

Looking for even more protection? Talk to one of our local, independent agents about value-added services for policyholders, such as identity theft protection.