**Scenario1: posting private info on social media**

**INSTAGRAM**

****

**1 Broadcasting your location to criminals**

You hopped on Instagram to post photos of the Paris café where you ate croissants and sipped café au lait, and now you’re checking in at the Louvre on Facebook. The problem: Thieves can use social media to track potential victims.

If previous photos you’ve taken at home contain metadata showing the exact location where they were snapped, that could lead burglars right to your front door.

**Tip:** Share every last detail about your dream vacation in France — after you get back home. To protect your privacy further, avoid posting photos that contain metadata showing the location where the photo was taken. Start by disabling location metadata on photos on your camera or smartphone.

**2. Oversharing about your kids on social media**

Your child isn’t old enough to read, so there’s no harm in sharing that funny but embarrassing potty-training story, right? Wrong. Keep in mind that your social media posts essentially create a “digital dossier” on your kids, as one mother and children’s rights lawyer writes. And the information and photos you share about your kids could eventually fall into the hands of bullies, data miners, identity thieves, and even predators.

**Tip:** Start thinking about your kids’ online privacy from day one. Check your privacy settings on social media. Also avoid posting potentially embarrassing information, unclothed photos, and personally identifying information, such as full name or announcing their exact date of birth, which could put your children at risk for identity theft. Some parents use a generic nickname or fake initials when posting about a child.

**3. Leaving your accounts wide open to hackers**

You know it’s essential to use strong unique passwords for online security and privacy. If you use your dog’s name or your kid’s birthday, you might be giving criminals and hackers the keys to your accounts and the private information contained within. That could put you at risk for account takeovers, ID theft, and having your email address used to scam your colleagues, friends, and family.

But it’s hard to remember strong passwords, so consider putting “install password manager” on your to-do list and don’t keep putting it off for another day.

**Tip:** Get a password manager to help you keep track of all of your strong, unique passwords. Many password managers also include a random generator feature to help you create unique passwords of at least 12 characters that include letters, numbers, and symbols.

****