"I know where you are"

The new you may not be you at all. Hackers and cyber criminals steal millions of records and identities, according to the consumer advocacy nonprofit Privacy Rights Clearinghouse.

Stay safer online by following these practices:

- **Assume you've already been compromised.** Whether it's your baby monitor, your Smart TV, the webcam on your laptop, or apps you installed on your smartphone or tablet, your antivirus is not enough protection. It's time to take their privacy policies, and the permissions you grant them, much more seriously.
- **Change your passwords.** All of them. Now. And do it as frequently as you can tolerate. Also, if you don't want to change it often, then use any unique characters you can think of, such as a dollar sign ($) or exclamation mark (!), or replace an "oh" with a "zero" (0). This goes a long way in preventing attacks against your password.
- **Turn off wireless and geolocation services.** Protect your smartphones and tablets by turning off WiFi, Bluetooth, NFC and GPS, except when you need them. That way, if you are at a local coffee shop or in a shopping mall, no one can spy on you using nearby (proximity) hacking attacks, and they can't track where you were and where you are going on your GPS.
- **Assume most of your apps are creepware.** This is malware that spies on you and your online behavior. Do you really need them? Delete all of the apps you aren't using too often.

Source: Gary S. Miliefsky is CEO of SnoopWall and the inventor of SnoopWall spyware-blocking technology. He is a founding member of the U.S. Department of Homeland Security.