10 ways to keep holiday hackers at bay

By Gary S. Miliefsky

We've all lost our identity at least three times, with more than 930 million records breached, lost or stolen to hackers and cyber criminals, says consumer advocacy non-profit Privacy Rights Clearinghouse.

Why don't we do all we can to stay safer online?

According to StaySafeOnline.org, more than a quarter of Americans say they lack the information necessary.

So, here it is – everything you need to know to enjoy the Christmas shopping experience without losing your privacy and identity or putting your children's safety at risk:

• Assume you've already been compromised. Whether it's your baby monitor, your SmartTV, 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 those devices' and apps' privacy policies, and the permissions you grant them, much more seriously.

• Change your passwords – all of them. 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 "o" with a zero. 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. Assume most of your smartphone or tablet apps are creepware – 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. Replace apps that ask for too many permissions and take advantage of too many of your privacy settings – like GPS, phone and sms logs, personal identity information – with similar apps that don't.

• Opt out of sharing your information. Opt out of every advertising network that you can. Visit the National Do Not Call Registry and register your smartphone and home phone numbers at www.donotcall.gov. If you use a Google email account and have an Android phone, even with your GPS off, it's tracking your every move. (Log in to maps.google.com/locationhistory/b/0 and see for yourself.) Go into your smartphone or tablet settings and turn this feature off. In your Android phone, go to Settings, then Location, select Google Location Reporting and set Location History to off. The same holds true for the Apple iPhone, iPad and iTunes. You need to find the location and privacy settings and turn off access under Settings, then Privacy then Location.

• Your browser is a double agent – keep it clean. It is spying on you for advertisers unless you block and remove cookies and delete the cache frequently. In your web browser settings, delete your history, all cookies and passwords and the cache. You should do this frequently so you don't leave personal information sitting around on your computer, smartphone or tablet.

• Remove third-party Facebook plugins. Third-party plugins are mini applications designed to eavesdrop on your behavior in Facebook and possibly grab information about your habits within that social network. Some websites you visit will

require you to log in using Facebook, and then you have to trust them to connect to your Facebook account. This is very risky. Read their privacy policy and make sure they are a legitimate business before you risk doing this.

• Only shop on the websites of companies you already trust. If you don't know where the merchant is located, don't shop online there. If they don't have a corporate address or are located in another country, it is risky for you and you may never see the goods you think you purchased. Also, if their shopping cart experience is not an HTTPS browser session, then everything you type in, your name, address and credit card information, is going over the internet unencrypted – in plain view.

• Turn off geotagging – your photos are full of information. Twitter and Instagram as well as your iPhone will give away your location. Most people don't realize Twitter and Instagram both use geotagging for everything you send out. Geotagging stores the latitude and longitude of your tweet or image. Pictures you take on an iPhone usually store geotagging information, as well. The less information you give out about where you are located, the safer you are.

• Don't use cash or debit cards – use credit cards, wisely. Credit cards allow you to travel with less cash, and if you're purchasing online, it's safer to give your credit card than your debit card information. The same holds true when you visit your local retail outlet. The reason? If you experience identity theft, credit card laws allow you to keep all of your credit, with no responsibility during an investigation. With a debit card, your bank can tie up your money in the amount equivalent to the fraudulent transactions for up to 30 days.

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 and serves on the advisory board of MITRE on the CVE Program, and is a founding

board member of the National Information Security Group.