12/12/17

By Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America

It seems as though data breaches affecting millions of Americans are constantly in the news these days. If this makes you anxious about the safety of your personal information, that's understandable.

You can protect your data by using secure internet connections rather than public Wi-Fi when you're providing sensitive information such as financial account numbers online, keeping your computer and mobile device safe against malware that may be lurking in email attachments, pop-ups and banner ads, downloading apps and other programs only from trusted sources, and being wary of anyone who contacts you unexpectedly asking for it. You can also use the security settings on social media sites to restrict who can see your posts.

In the offline world, you can reduce the possibility of identity theft and fraud by sending bill payments from public mailboxes rather than from the mailbox in front of your house and collecting your mail promptly, shredding documents that contain account numbers and other personal information when they're no longer needed and not carrying your Social Security card around with you.

But when businesses have your data, you can't control how well it's safeguarded. There are some simple steps that you can take, however, to make it harder for fraudsters to *use* your personal information if they get ahold of it.

- Create separate passwords for your most sensitive accounts. Sure, it's convenient to use the same password for everything. Crooks know that, so if they get your password for one account, they'll try it to log into accounts on other websites. Any account that has your financial information, Social Security number or other sensitive data should have a unique, strong password to keep would-be intruders guessing.

- Beef up your authentication. If your username, which is often your email address, and a password is all it takes to access your accounts, your defenses are relatively weak. Two-factor authentication – your password plus something that only you have, such as a one-time code that is sent to you as part of the login process – provides much stronger protection.

- Freeze your credit file. This prevents identity thieves from opening new credit accounts in your name because the lenders won't be able to access your credit record. Since some landlords and employers also check applicants' credit records, freezes can also stop fraudulent attempts to get jobs or rent apartments using your identity. Contact the three major credit reporting agencies – Equifax, Experian, and TransUnion – to request a security freeze. You can lift the freeze anytime you need to and reset it. In some situations you may be able to do this for free; otherwise, there will be a small fee .