Take Control of Your **Personal Info**

CYBER SECURITY MARCH 2019

Identity theft has become a fact of life during the past decade. If you are reading this, it is a safe bet that your data has been breached in at least one incident. Does that mean we are all helpless? Thankfully, no. There is a lot we can do to protect ourselves from identity theft and to make recovery from cyber incidents quicker and less painful.

First, take control of your credit reports. Examine your own report at each of the "big three" bureaus. You get one free report from each credit bureau once per year. You can request them by going to AnnualCreditReport.com. Make sure there is nothing inaccurate in those reports, and file for correction if needed. Then initiate a credit freeze at each of those plus two other smaller ones. Instructions can be found at Krebs on Security. To keep an eye on your credit report all year, space out your credit bureau requests by requesting a report from a different credit bureau every four months.

Next, practice good digital hygiene. Just as you lock your front door when you leave home and your car when you park it, make sure your digital world is secured. This means:

- Keep your operating system up to date
  When OS updates are released, they fix errors in the code that could let the bad guys in.
- Do the same for the application software you use
  Web browsers, plug-ins, email clients, office software, antivirus/antimalware, and every other type of software has flaws. When those flaws are fixed, you are in a race to install that fix before someone uses the flaw against you. The vast majority of hacks leverage vulnerabilities that have a fix already available.
- Engage your brain
  Think before you click. Think before you disclose personal information in a web form or over the phone.
- Think before you share on social media sites
  Some of those fun-to-share-with-your-friends quizzes and games ask questions that have a disturbing similarity to "security questions" that can be used to recover your account. Do you want the answers to your security questions to be published to the world?
- Use a password manager
  Keep a strong, unique password for every site or service you use. That way a breach on one site won't open you up to fraud at other sites.
- Back. It. Up.
  What do you do if you are hit with a ransomware attack? (Or a run-of-the-mill disk failure?) If you have a recent off-line backup, your data are safe, and you can recover without even thinking about paying a ransom.
- Full disk encryption is your friend
  If your device is stolen, it will be a lot harder for a thief to access your data, which means you can sleep at night.
- Check all your accounts statements regularly
  Paperless statements are convenient in the digital age. But it is easy to forget to check infrequently used accounts such as a health savings account. Make a recurring calendar reminder to check every account for activity that you don't recognize.
- Manage those old-style paper statements
  Don't just throw them in the trash or the recycle bin. Shred them with a cross-cut shredder. Or burn them. Or do both. Data stolen from a dumpster are just as useful as data stolen from a website.

If you have been a victim of identity theft:

- Create an Identity Theft Report by filing a complaint with the Federal Trade Commission online (or call 1-877-438-4338).
- Use the Identity Theft Report to file a police report. Make sure you keep a copy of the police report in a safe place.
- Flag your credit reports by contacting the fraud departments of any one of the three major credit bureaus: Equifax (800-685-1111); TransUnion (888-909-8872); or Experian (888-397-3742).