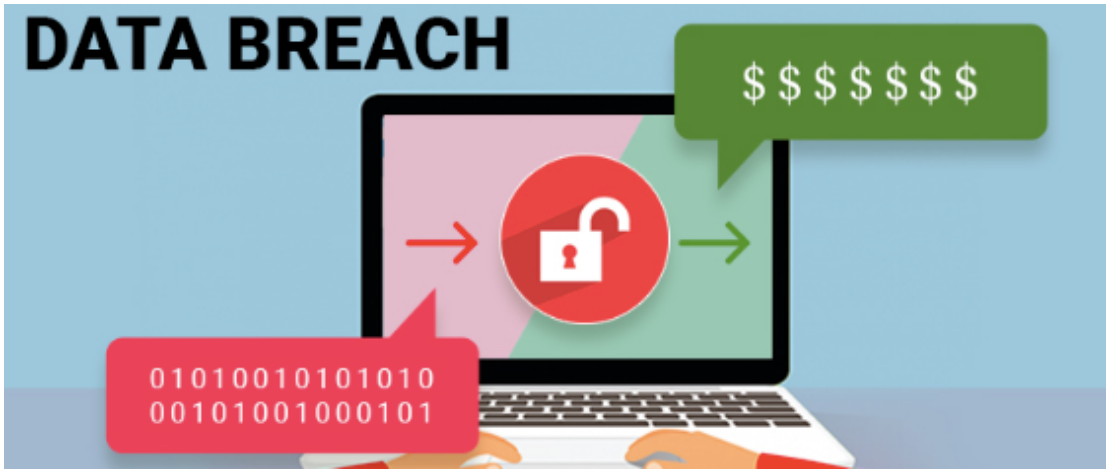
Volume #4 - Issue #177
September 14th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

What To Do If You Have Been Caught In A Data Breach



Data breach can happen to anyone, anytime. Here are steps every consumer should take after they have been notified that a data breach has been discovered:

First, set a fraud alert with a credit reporting agency every 90 days. If you are a victim of identity theft or believe you are a target of identity theft (which is everyone), then the Fair Credit Reporting Act legally entitles you to set a fraud alert with a credit reporting agency (CRA) free of charge. The fraud alert requires creditors to go through an additional identity verification procedure that essentially verifies that you are you. The fraud alert only needs to be set with one CRA (this CRA is required to inform the other two CRAs), it expires after 90 days and it takes less than 1-minute to complete. Fraud alerts are by far the most effective defense tactic against financial identity theft. During the time the alert is in effect you will be notified of any attempt to get credit in your name.

Second, close all accounts affected by the breach. Thieves collect their returns when they access your breached accounts. Many individuals do not close their breached accounts because they wrongly believe there is a minimal chance of their accounts being overtaken. If you close these accounts, then you have effectively marginalized their efforts and protected yourself from the pain and suffering of identity theft.

Third, change your passwords. Criminals adjust their methods based on behaviors of their targets. With your username and password, which was obtained in the breach, a good criminal can drain your financial accounts within minutes. Change your passwords and utilize different passwords for all of your different accounts.

Fourth, monitor your identity for fraudulent use. Most people only associate their identity with their credit report. It is also as important to check your medical, criminal, and driving records. In the case of medical identity theft, the ultimate result can be death, and criminal identity theft can lead to improper incarceration. Make certain to monitor all forms of your identity for fraudulent use. Make sure you do a web search of yourself every couple of weeks. *(It is probably a good idea to get at least one professional search done that includes the Deep Web. That is where your information will be sold if that is the hacker's intent.)*

Things you should not do:

Do not rely on free identity theft defense services. Breached organizations often have a knee jerk reaction of contracting with identity theft companies to offer rather useless identity theft defense services. They are primarily monitoring services, and by definition, monitoring alerts you of a change in status after-the-fact. In other words, it alerts you that you are a victim, but does nothing to prevent it.

Do not go crazy. It is normally not necessary to close all of the your bank accounts and credit cards, and legally change your name. If only your name is part of the breach, it is likely all that is necessary is for you to practice normal identity theft prevention and detection tactics.

Do not pretend like it didn't happen. The polar opposite of the previous point is to act like it didn't happen and do nothing. Everyone is at risk of identity theft, but a data breach indicates that a criminal stole information with the specific intent of harvesting identities. If you stick your head in the sand, then the law of averages will eventually catch up to you and you will become an identity theft victim. An ounce of prevention is worth way more than a pound of cure.

Do not trust the breached organization. There are countless examples of breached organizations delaying communication alerts, downplaying the severity and downright lying to the victims of the breach. In essence, they got caught asleep in the guard tower and now they want to convince everyone that it is not a big deal.

Thank you for subscribing to our email!