7 Things You Can Do After the Equifax Data Hack

The Equifax security breach, made public last week, leaves 143 million consumers vulnerable to identify theft and credit fraud. But there are some ways you can protect yourself from the current and future threats.

Find out if you're at risk

Equifax has set up a quick and easy way to find out if you are one of the estimated 143 million consumers whose personal information is vulnerable to the breach.
https://www.equifaxsecurity2017.com/potential-impact/

Get a credit report

The odds are slim that there will be any malicious activity related to the recent Equifax breach, but it still makes sense to start by pulling a credit report from Equifax, Experian and TransUnion. They each offer one free credit report per person, per year.

Accept Equifax offer to monitor credit

To help cushion the blow of the massive security breach, Equifax is offering consumers a year of free credit monitoring through its TrustedID service. As an update to earlier reports, signing up for TrustedID does not limit a consumer's litigation options related to the breach.

Request Fraud Alerts

Requesting fraud alerts from all three credit-reporting agencies will make it more difficult for anyone to create credit under your name with stolen information.

Install a Security Freeze on Your Credit

Described by the Identity Theft Resource Center as the most robust protection that consumers can access, a security freeze prevents any new lines of credit from being issued as long as the lender checks with one of the credit-reporting agencies. Security freezes should be installed at all three agencies and could include an initial fee of up to $10.

Change Your Passwords

Skip using "123456" or "qwerty" or "111111" or any of the other most common passwords in the world. It is safe to assume a lot of people are ignoring this most basic protection. In addition to changing passwords often, experts advise making them as complex as possible and including double authentication whenever possible.

Monitor all Financial Statements

It is always a good practice to closely check all financial and banking statements for any unusual activity. **Hackers will sometimes make a small transaction on a hacked account just to see if it is active before committing more extensive fraud.**