Personal Information of Millions of American Voters' Recently At Risk

by jvkrakowski - Saturday, July 15, 2017

http://blog.searchbug.com/2017/07/personal-information-at-risk/

In the month of June, over 198 million Americans who registered to vote in the elections in 2016 have recently had their personal information exposed while being stored online.

This was due to a political data contractor called Deep Root Analytics that was associated with and employed by the Republican National Committee. Deep Root Analytics held and then stored a massive amount of data online without any kind of protection on it including security or even a simple password. Nothing, Nada, Zilch!

The unsecured database includes information on registered voters such as; names, addresses, dates of birth, who you may have voted for in the past elections, religious affiliation, views on gun rights, and even social media posts. If you supported a certain stance on President Trump's foreign policy, "America First", this was even included in the exposed data.

More importantly, over 9 billion points of data on over 198 million Americans has been compromised. This includes personal information that could potentially be used for identity theft or even expose information to help get individuals' bank account information.

What Has Happened In The Past

Deep Root Analytics has stated that they do not believe that there had been any hackers that claimed access to the data, however, there is no way for sure to stop future large scale attacks and exposures of big data.

Large scale identity theft seems to be a growing concern and the statistics are indeed alarming. If you remember hearing about the Yahoo mishap, over 500 million Yahoo mail user accounts were hacked in 2014. This was considered one of the largest single attacks as of late. Even last year, over 1 billion. Yes, billion… data records were stolen. Within that number, most of the attacks put up to 10 million individual's personal information and identities at risk. Additionally, in 2016 over 15 million U.S. citizens claimed to have their personal information taken from them.

The threats are real and seem to be only getting worse, so now that we know what's going on, let's go over what you can do to stay safe.

What Can You Do To Protect Yourself?

- Passwords - If you're the type of person that uses one password for every website, application, device, and account - that needs to change, now, today, do not delay!. There should never be a situation where you should use the same password twice. This can take a lot of time changing your passwords for everything you use these days but it is becoming to be a necessary task. There are even programs out there such as LastPass and Roboform that can securely store and help you remember your passwords so you don’t have to. These programs give you easy and secure access to your passwords and can even help you generate very strong passwords on the fly so you don’t have to come up with them. We highly recommend using one of these two programs to protect your online identity.

- Two-Factor Authentication - There are many applications that you probably use such as Facebook that offer a way to protect yourself with a password plus an additional piece of information by selecting a certain code or security question being sent to your phone or alternative email address. This ensures your personal information is dynamically protected. Simply check to look for Two-Factor Authentication options to turn on this extra security measure.
- Old Accounts - Take some time to dig up and find all of your old user accounts. These would be accounts you used with various websites or applications in the past. If you can’t remember off the top of your head what account you’ve stopped using in the past, then there is a likely possibility that if it was hacked you would not have a clue it was happening to you. We just mentioned Yahoo and their email user accounts being the victims of a large scale attack, we suggest either changing all of your old or unused account passwords or you could even close your Yahoo account and switch to a different email address for further protection. We’d suggest changing your Yahoo account password, then switching to a different email provider like Gmail (with a different secure password). Then add an autoresponder to your Yahoo account which would send your family and friends an email letting them know you’ve changed your email address anytime they sent an email to your old Yahoo address.

There are many other options and procedures you can take to keep your personal information safe in the ever changing online world we live in today. However, the most important thing you can possibly do is to stay informed and up to date on what’s happening around us.

For more related content on identity theft, fraud prevention, and online/phone scams please take a look at our blog to educate yourself and stay in the loop.

(Learn More: http://blog.searchbug.com/)