2.2 Billion Accounts Found In Biggest Ever Data Dump -- How To Check If You're A Victim

forbes.com/sites/daveywinder/2019/02/01/2-2-billion-accounts-found-in-biggest-ever-data-dump-how-to-

February 1, 2019

Two weeks ago the Collection #1 data dump redefined 'big' as far as breached data goes: more than 770 million account details were in that database, made public for all to see. Now big has just got even bigger with the discovery of Collection 2-5 that takes the total number of hacked user accounts published to an astonishing 2.2 billion. As the name suggests, these are databases number 2 to 5 that have followed the first of the Collection breach dumps. According to Wired these total around 845GB in total, compared to 'just' the 87GB of stolen that was contained in Collection #1. When you add up all email addresses and associated passwords across the series of dumped databases it totals around 2.2 billion.

Should I be worried?

Given that 2.2 billion accounts equates to around 30% of the people on our planet, if each belonged to a separate individual, then yes you should. The good news, if there is any under these circumstances, is that the data exposed by this latest set of breach databases does not appear to be new. Instead, these are yet more compilations of data stolen during breaches that have already come to light. This does not, however, mean that you can sleep easy; credential stuffing attackers check as many email and password combinations as possible at a myriad of different sites and services. If you have been guilty of using the same login information at multiple sites then you could be in big trouble. Last year, the Distil Research Lab published a study that revealed half of all credential stuffing attacks are volumetric in nature, that is they are of the automated 'done in bursts' nature employed by bot networks. The other half were of the 'low and slow' variety which are actually harder to detect as they can bypass the triggers that alert security tools to ongoing system attacks.

How do I check if I'm affected?

The original Collection #1 data dump was painstakingly filtered and entered into the Have I Been Pwned service database which lets you enter your email address and check if your details match. The latest Collection 2 -5 dumps have been entered into the Info Leak Checker at the Hasso Plattner Institute search and this will serve the same function. I recommend you go and check all your email addresses at both sites as soon as possible.

What do I do next?

Whether your data appears in these huge dumps of breached information or not, the next steps remain the same.

Today In: Innovation

1. If you do not currently use a different password for every site or service, make sure you change this immediately.

2. If you do not currently use long and complex unique passwords, by which I mean at least 20 random alphanumeric, mixed case and special characters, then ditto.

3. If you are concerned that this all sounds too much like hard work, then think again. Hard work is clearing up the fallout from identity theft or if your email or bank accounts get accessed by a threat actor. Look to any of the major secure password vault applications such as 1Password, LastPass or Dashlane which will automate the process for you.

4. Steven Murdoch, chief security architect at security specialist OneSpan's innovation center, advises that companies should also "recognize the limitations of password authentication" and "implement additional measures, such as detection of suspicious behavior with two-factor authentication offered to customers." Terry Ray, senior vice

president and Imperva fellow, adds that "businesses should be extra vigilant over the next few weeks as these credentials make their rounds through the dark channels. Post credential leak account takeover attempts have historically spiked immediately following incidents like this..."