How To Determine If Your Passwords Are For Sale On The Dark Web

January 17, 2020 - Data breaches have become nearly a daily occurrence, and the data exposed in them can include everything from the mundane to ability to drain bank accounts. CNBC recently reported that 38 Billion records have been exposed in data breaches since 2010. That's a lot of information and it definitely includes user names and passwords for billions of accounts. But how do you find out if YOUR ACCOUNTS have been compromised and the information put up for sale on the dark web? Fortunately, there's and app for that!

Actually, there are a couple of websites for that. One from Google and another from Mozilla. The two sites function quite differently but both can provide you with valuable information.

To use the Google site, you'll need a google account. The site appears only to test passwords that have been stored with Google or in the Chrome browser. Because of this, if you don't have a Google account already, there is no real point in setting one up for this. It simply won't help you.

For the millions of us that use some of Google's many services - including Gmail, Google Sheets, Google Drive, Chrome, and the list goes on and on and onâ€¦ Google's tool is easy to access and provides a quick response.

To use it, go to http://passwords.google.com. You'll be asked to sign into your Google account. At the very top of the page after you sign in, you'll see a section titled Password Checkup. Click on the link there and you'll then see three boxes appear. The first box tells you if any of the passwords you have stored with Google have been found for sale. The second box tells you how many times you've used passwords on multiple accounts. And the third box tells you how many accounts you have with weak passwords.

If you click on the drop-down menu that appears in each of the boxes, you'll then be able to get information on the individual accounts that are compromised, reused or weak.

While this tool is useful, it isn't comprehensive. That's especially true for anyone using a password manager and who chooses to store most of their information in that manager rather than with Google.

Mozilla's tool fills in some of these gaps. You can find it at http://monitor.firefox.com.

Mozilla is less interested in passwords than it is in email addresses. And that is likely to give it better coverage than Google.

Just enter your email address on the front page of the site and you'll be told if that address is included in any data that is being sold on the dark web. I entered an old email address - one that has been cancelled for several years now - only to find out that it had been included in four different breaches. Ouch!

While the email address was old, the data breaches weren't. The most recent one occurred in November of last year and it was with a company that I simply don't remember doing business with. Fortunately for me, anyone who used that old data to log on may be able to get access to an old grocery list, but not much else.

Between the Mozilla and Google tools, you should be able to determine if any of your accounts are vulnerable to hacking. Again, if you use a password manager, then neither of these tools will provide a comprehensive way for you to know if you have accounts that are at risk. But if you do a little work and go through that password manager manually, you'll certainly be able to determine if accounts using specific sign on information require some updating.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS