Are Your Passwords Compromised?

News of a big brand suffering a data breach is all too common today. But if you don't get an email from such a company, you could mistakenly be thinking it doesn't affect you.

The thing is, large breaches are happening all the time. Cybercriminals then put access credentials online, and other bad actors buy and exploit those email addresses, usernames, passwords, etc.

Why do the bad guys care to buy these member details? Presumably, the victims of the breach quickly change their passwords to prevent security vulnerabilities. So, what good does that info do?

Take a moment to think about how many unique passwords you actually have. Many of us have dozens of different online accounts but only a handful of distinct passwords. That means a hacker can take that stolen data from, say, LinkedIn and try the same password on your banking site.

Cybercriminals have the capacity to keep on trying. They will take one stolen password and use that data to try and hit other accounts in a massive, brute-force effort.

What can you do about it?

Stop using the same passwords over and over again. Yes, unique passwords for every account are difficult to remember, but they are critical.

One solution is to use a password manager, like LastPass. In addition, many browsers have a pop-up window offering to remember a password for a particular site. If you say "yes," the browser automatically populates access credentials on your return to the site.

If you use Google Chrome, you can also check if your passwords have been compromised. Google Safety Check compares your saved usernames and passwords against over 4 billion compromised credentials.

To check for leaked passwords, head to "Settings" in the Chrome browser, then navigate to "Safety Check" and "Check Now." You'll get a report that identifies any compromised passwords, and allows you to review and fix leaks.

MacOS users will be happy to hear that Safari added similar functionality in its latest release, and Mozilla's Firefox browser also has password checking built in.

Strengthen your passwords

Creating a strong password is challenging; almost as difficult as remembering all your different passwords. You're aiming to come up with something a human or computer can't guess!

Different sites will have different parameters. You need a combination of uppercase and lowercase letters, numbers, and special characters. Having a different mix of these helps make the password more difficult to crack. And the longer the better; That's why the passwords a browser suggests to you look like a string of gibberish.

Pay attention also to warnings from the site requiring your credentials. If they say your password is weak, believe them. Safari and Chrome suggest stronger passwords when you create a new account.

Change your passwords immediately if you are advised to do so. Password management tools are continuously improving, but there is still the human element, and that’s often the weakest link. If you don’t practice healthy password hygiene, hackers are ready to take advantage of your ambivalence.

**Please note that Hopedale Technologies receives compensation from the product links we recommend. If you click our link and purchase, we will receive a commission. We test each product and only recommend the very best ones that we use ourselves.*