www.consumerreports.org

How to Use 'Have I Been Pwned' to See If Your Data Was Compromised

By Yael Grauer

5-7 minutes

Data breaches have affected most Americans over the past few years, leading to unauthorized access of log-in credentials, financial information, and personal data that can be used by criminals intent on committing fraud.

To tighten up your digital security, it's important to know which of your accounts have been affected. That's a task you can accomplish at the free site Have I Been Pwned, a resource that is widely recommended by security experts. (The term "pwn" is hacker jargon for compromising or taking control of a computer or an application.)

Created by Australian web security consultant Troy Hunt, the site analyzes information from hundreds of breaches and millions of compromised accounts, whose data often ends up posted online and traded by criminals. The site lets you enter an email address or a phone number to find out whether it has appeared in any of the data breaches the site tracks. Then you can change your passwords and take other steps to protect yourself.

Consumer Reports has been steering people to Have I Been Pwned for years, and security-savvy consumers may have used it before. However, the site has gradually become more robust, adding features and expanding its records of compromised data. And, unfortunately, data breaches continue to occur. So even if you've checked the site before, it's worth another visit.

The site has a number of functions for both one-time users and returning visitors.

Search for Your Information

The primary function of Have I Been Pwned is to tell you whether your information has been compromised. Enter your email address or phone number and you'll get a list of data breaches tied to those details. The site will also provide information such as when each data breach happened, the name of the affected company, what data was compromised, how the breach was discovered, and how many accounts were involved.

Sign Up for Notifications

You can sign up to receive an email notification every time your personal information is found in a new data breach. That'll allow you to take steps to minimize the risk of fraud or identity theft, such as changing your password on that account—and any other accounts where you used the same password.

Stop Other People From Seeing Your Data

You can opt out of letting other people enter your email address and finding out which data breaches have affected you. You provide the site with your email address, then follow a link from the email you receive to choose exactly how you want to opt out. (For instance, In addition to stopping others from

searching for breaches related to your email address, you can have your email address removed from the system altogether.)

By default, data breaches Hunt considers sensitive—such as breaches on adult sites—are not publicly searchable. Those details are revealed only to people who sign up to receive email notifications.

Have I Been Pwned is a useful resource for finding out when you've been affected by a data breach, but it's best to get ahead of the problem by making your accounts more secure. Two important steps, Hunt says, are enabling multifactor authentication and using a password manager to generate and save strong passwords.

If you do that, you may end up accessing Hunt's data without actually visiting his site. The password manager 1Password, which costs $3 per month and up, comes with a feature called Watchtower that lets you compare your passwords against a list of compromised passwords maintained by Have I Been Pwned. Then, 1Password will tell you which passwords to change right away.

Data from Have I Been Pwned is also used in browser extensions such as Okta's PassProtect for Chrome.

Hunt says one of the best uses for Have I Been Pwned is to learn about how much information you're sharing online. "There's a little bit of data minimization that almost everybody can practice," he says. "For example, do you need to give your date of birth to a site that asks for it? What is the value proposition for you as an individual handing out your date of birth?"

If the site doesn't really need a piece of information to provide you with the service you want, consider withholding it, he says.

Yael Grauer

I am an investigative tech reporter covering digital privacy and security. I'm the lead content creator of CR Security Planner, a free, easy-to-use guide to staying safer online. Prior to Consumer Reports, I covered surveillance, online privacy and security, data brokers, dark patterns, clandestine trackers, security vulnerabilities, VPNs, hacking, and digital freedom for Wired, Vice, The Intercept, Slate, Ars Technica, OneZero, Wirecutter, Business Insider, Popular Science, and other publications. Follow me on Twitter (@yaelwrites)