Massive breach leaks 773 million email addresses, 21 million passwords

By Alfred Ng

Published: 2019-01-17 · Archived: 2026-04-06 01:16:31 UTC

The best time to stop reusing old passwords was 10 years ago. The second best time is now.

Alfred Ng Senior Reporter / CNET News

Alfred Ng was a senior reporter for CNET News. He was raised in Brooklyn and previously worked on the New York Daily News's social media and breaking news teams.

2 min read

In one of the largest public data breaches, a collection containing more than 87 gigabytes of personal information was leaked online.

The data dump, titled "Collection #1," was hosted on the cloud service Mega, and had 772,904,991 email addresses, and 21,222,975 passwords. The treasure trove of private information was discovered by Troy Hunt, a security researcher and founder of the "Have I Been Pwned" service.

The login credentials appear to have been stockpiled over years, as some passwords and emails come from 2008, Hunt said on his blog. The information comes from more than 2,000 different sources, Hunt said. You can check if you were affected by the breach by entering your email address on Have I Been Pwned. And you can see if individual passwords were compromised by clicking here.

Breaches continue to happen on a massive scale as companies collect data on millions of people and fail to protect them properly. Marriott experienced one of the largest personal data breaches in history, losing personal information belonging to 383 million guests, while hackers hit Yahoo and stole data belonging to 3 billion accounts. The big numbers don't always equate to dire after-effects; the breach of Yahoo accounts, for instance, isn't likely to have the same potential for damage as the compromising of 147.7 million Social Security numbers taken in the Equifax breach.

Watch this: Biggest hacks of 2018

03:25

But just because your information is stolen doesn't mean that you're helpless.You can, and should, change your passwords.

When potential hackers have access to this massive amount of login data, they're not sitting at a computer trying to log into every account one by one. They're using bots to do it through a technique called credential stuffing, which automatically blasts multiple services with the same set of login information.

"Massive data breaches like Collection #1 create huge spikes in bot traffic on the login screens of websites, as hackers cycle through enormous lists of stolen passwords," said Rami Essaid, a co-founder at bot security company Distil Networks.

The company found that websites experienced three times as many login attempts after public breaches happen.

The idea is that if you've reused those old passwords for different platforms, a potential hacker would use the leaked passwords to break into your newer accounts with these bots.

With this recent leak, it's a reminder for people to change their passwords, or start using a password manager that can automatically generate secure passwords for you.

The best defense...: Data breaches can sucker-punch you. Prepare to fight back.

That Marriott breach: Hackers stole more than 5 million passport numbers.
