USA
TODAY

10 billion passwords have been leaked on a hacker site. Are you at risk?

Betty Lin-Fisher
USA TODAY

Published 5:12 p.m. ET July 11, 2024 | **Updated 5:14 p.m. ET July 11, 2024**

In the latest cybersecurity scare, a file with nearly 10 billion passwords has been posted to a hacking site.

Researchers at Cybernews said they discovered the file, posted on July 4, with 9,948,575,739 unique plaintext passwords.

Cybernews experts said they believe this data dump, called RockYou2024, is the largest password leak of all time.

"The Cybernews team believes that attackers can utilize the ten-billion-strong RockYou2024 compilation to target any system that isn’t protected against brute-force attacks. This includes everything from online and offline services to internet-facing cameras and industrial hardware," the online publication said in a report.

What is the RockYou2024 leak?

The 10 billion passwords included in a file uploaded by a user named ObamaCare are not all new, Cybernews said.

Cybernews said its team "cross-referenced the passwords included in the RockYou2024 leak with data from Cybernews’ Leaked Password Checker, which revealed that these passwords came from a mix of old and new data breaches."

The passwords on the document have likely been collected from more than 4,000 databases over the last 20 years, Cybernews said.

“In its essence, the RockYou2024 leak is a compilation of real-world passwords used by individuals all over the world. Revealing that many passwords for threat actors substantially heightens the risk of credential stuffing attacks,” Cybernews said.

Credential stuffing is when hackers take information, such as passwords, from one data leak and attempt to log onto other websites, which can be very damaging to businesses and consumers, Cybernews said.

The recent wave of hacks targeting several sites including Ticketmaster were the result of credential stuffing attacks, said Cybernews.

Three years ago, a leak of 8.4 billion passwords called RockYou2021 was posted on a hacker site. At the time it was the largest password leak.

Cybernews said its analysis determined that the 10 billion leaked passwords in the RockYou2024 document included 1.5 billion new passwords leaked from 2021 through 2024.

Leak is the latest to share information already available

The 10 billion passwords leaked are a series of data dumps from previous hacks and are not new, but it is stil a big deal to have that many passwords in one document posted on the Internet, Scott Augenbaum, a retired FBI agent, cybercrime prevention trainer and author of The Secret to Cybersecurity, told USA TODAY.

"The big moral of the story is this needs to be a wake up call that no matter what a great job you do keeping yourself safe, someone's going to lose your user name and password," Augenbaum said, referring to companies whose sites are hacked.

The danger is that many people use very common passwords or if they're using a more difficult password or passphrase, they use the same one for multiple accounts, said Augenbaum. When those passwords are compromised, hackers can get into multiple accounts, he said.

"The passwords are out there," he said. "That means the cybercriminals right now are banking on the fact that they're going to capture one of your passwords. Are you using that same password for multiple platforms?"

It's important to have a different password for each account, said Augenbaum.

"This has an impact because just think about how many of our parents have the same password for multiple platforms or even our kids," he said. "This will have a greater ripple effect across consumers than anyone could imagine."

Augenbaum is particularly worried about the senior population, which is more likely to use the same password and could be vulnerable to scammers.

Cybersecurity: Data breaches and ID theft are still hitting records. Here's how to protect yourself.

How do I protect myself?

Here are five steps Augenbaum suggests consumers take to protect themselves:

> **Reset All Passwords:** Immediately change passwords for all accounts associated with the leaked passwords. Ensure each password is strong and unique. A good password should be at least 12 characters long and include a mix of letters, numbers, and symbols. You can check Cybernews' leaked password check at https://cybernews.com/password-leak-check/. Augenbaum suggests starting by putting in the passwords for your "mission critical" accounts such as banking and personal finance, email and social media. If your password is among those leaked, change it on all sites where you use it. You can also use https://haveibeenpwned.com/ to put in your email address to find out if your information has been in any data breaches and change passwords there.
>
> **Enable Two-Factor Authentication (2FA):** Wherever possible, enable 2FA, which prompts you to verify yourself on a second device. This adds an extra layer of security by requiring an additional verification step beyond your password.

Use a Password Manager: Utilize password manager software to securely generate and store complex passwords. This reduces the risk of password reuse across different accounts.

Beware of Account Compromise: Always verify suspicious emails, even if they appear to come from someone you know. Check for signs of phishing and avoid clicking on unexpected links or attachments.

Educate and Encourage Safe Practices: Encourage your friends and family to adopt these security measures and stay on guard for social engineering attempts. Cybercriminals often exploit the weakest link and unprotected accounts can lead to further breaches.

Betty Lin-Fisher is a consumer reporter for USA TODAY. Reach her at blinfisher@USATODAY.com or follow her on X, Facebook or Instagram @blinfisher. Sign up for our free The Daily Money newsletter, which will include consumer news on Fridays,here.