Published on *The National Law Review* https://natlawreview.com

9,948,575,739 Reasons to Change Your Passwords Now

Article By:

Cameron Abbott

Rob Pulham

Stephanie Mayhew

Cybernews has reported on its researchers' discovery of what could be the largest leaked password compilation of all time, with a record 9,948,575,739 plaintext passwords in a file called "rockyou2024.txt" (see article).

This compilation is made up of both new and old passwords, appearing to add a further 1.5 billion passwords to the 8.4 billion passwords released under "RockYou2021" three years ago.

There is concern that the compilation substantially heightens the risk of credential stuffing attacks – essentially using brute force to try many different password combinations to gain access to various online accounts used by individuals who use passwords that appear in the dataset.

Cybernews' team believes the compilation allows attackers to target any system that isn't protected against brute-force attacks, including everything from online and offline services to internet-facing cameras and industrial hardware. Most websites are protected from brute force attacks, but stolen devices are at risk.

This may also allow other attackers to reverse engineer other leaked data from breaches. If a password appears in a different breach that also includes user details, hackers could specifically target those individuals.

The news isn't necessarily dire, with other security experts stating "there comes a point where the magnitude of this aggregated data becomes next to useless due to its vast size" (see article).

Nevertheless, it is essential to implement protection against such attacks.

How can you protect your business?

- Have a password policy requiring employees to update their password at regular intervals, and only allows a strong and unique password;

- Use a password manager to securely generate and store passwords;
- Enabling Two-Factor Authentication on devices;
- Ensuring privacy awareness amongst your organisation so that employees stay vigilant about phishing attacks, including upfront and ongoing training; and
- Regularly monitor financial statements for any suspicious and unauthorised transactions.

Have a Data Breach Plan and keep it up to date because despite all of the above, things can still go wrong.

National Law Review, Volume XIV, Number 200