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

Privacy Tip #405 – Compromised Passwords Continue to Provide Easy Opportunities for Threat Actors

Article By:

Linn F. Freedman

Verizon's 2024 Data Breach Report, a must-read publication, was published on May 1, 2024. The report indicates that "Over the past 10 years, the use of stolen credentials has appeared in almost one-third (31%) of all breaches…"

Stolen credentials mean a user has given their username and password to a threat actor. When that happens, the threat actor has complete authenticated, unfettered access to all of the data the user has access to in the system. The result is that the threat actor can access data without being detected by tools put in place to detect malicious intrusions. This is a nightmare for organizations. Compromised passwords are an issue because threat actors gather and use them in brute-force attacks. When a user's password is compromised, if the user has used that password on any other platform, it gives threat actors an easy way to get into any account for which the user has used that password. That is why we always tell users not to use the same password across platforms.

It is important to change passwords frequently and to follow your organization's procedure for changing passwords. It is also crucial not to use the same password across different platforms.

A recent article by Cybernews shows how vital this mantra is. According to the article, "Cybernews researchers discovered what appears to be the largest password compilation with a staggering 9,948,575,739 unique plaintext passwords. The file with the data, titled rockyou2024.txt, was posted on July 4th by forum user ObamaCare." The passwords came from a mix of old and new data breaches."

Apparently, the threat actors compiled "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 further states that it 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."

Here are the recommendations from Cybernews:

The Cybernews research team advises to:

- Immediately reset the passwords for all accounts associated with the leaked passwords. It is strongly recommended to select strong, unique passwords that are not reused across multiple platforms.
- Enable multi-factor authentication (MFA) wherever possible. This enhances security by requiring additional verification beyond a password.
- Utilize password manager software to securely generate and store complex passwords. Password managers mitigate the risk of password reuse across different accounts.

National Law Review, Volume XIV, Number 193