**WEAK CREDENTIALS**

By Jessica Collins

**Executive Summary**

When choosing passwords, we tend to choose our favorites in life, such as sports teams and venues, vacation spots, historical landmarks, etc. Typically, we post such specifics on our social media (Facebook, Instagram, Tik Tok), but these specifics are valuable to attackers. Attackers will use this information to gain access and steal sensitive data. Weak passwords are a serious threat and can lead to security breaches.

Attackers can exploit weak credentials by using brute force attacks, credential stuffing, and phishing. More threats include account takeover, identify theft and financial fraud. Taking years to build a brand reputation can be taken down by one vulnerability.

**Introduction**

Why do we use weak passwords for login? Simple. It is easy to remember. We do not use the passwords suggested by the computer or create different passwords for each login. Too much work, so we use the same exact passwords repeatedly. The importance of this brief is to bring awareness about creating weak passwords and the effects behind it.

But there are questions that need to be answered. What are common characteristics of a weak password? What is the best practice for passwords? How often should you change your passwords? What is one way to avoid the problem of weak passwords?

**Research Overview**

Cybernews conducted a study examining over 19 billion accounts with weak passwords being reused. This study brings to the forefront of a significant vulnerability in digital security practices globally. Security incidents such as the Snowflake breach and SOCRadar.io breach, common lazy passwords still exist. “123456” and “password” still dominate. These passwords are very predictable and susceptible to dictionary attacks. Only a small percentage created unique passwords, signaling out majority of users.

Even though we promote stronger password security, little to no progress has been made. Furthermore, the study concluded organizations should employ more authentication methods. Better password hygiene, creating strict password policies, supporting more complex passwords, and educate employees on all the risks.

**Discussion/Research Findings**

This brief is based on examining 19 billion accounts that either created or reused weak passwords. The study or findings came from Cybernews and spotlighted a significant vulnerability. The study covers percentage of individuals credentials being analyzed of how vulnerable they are to certain attacks.

**Recommendation**

The best practice for weak passwords is to make it longer than twelve characters, combining uppercase, lowercase, numbers, and symbols. Do not use any personal information or words from the dictionary. Install a password manager that can store and generate a more complex, unique password for each account you have. And as a must, enable two-factor or multi-factor authentication for extra security.