flare

20x Increase in Number of Guesses Required to Crack Passwords from 2007-2025: What Does That Mean for Password Strength?

By Andréanne Bergeron, Security Researcher

For as long as we've logged in, passwords have been both our first line of defense and our biggest weakness. They've evolved in fascinating ways over the past two decades, reflecting not just security standards, but also the tools people use as well as shortcuts they take. Looking at trends from 2007 through 2025, the story of passwords is one of false starts, steady habits, sudden leaps, and technological nudges that changed behavior.

Key Takeaways

Infections revealed distinct patterns in how threat actors craft their traps to maximize the number of victims

- Password strength (which we defined for this investigation as estimated number of guesses required by a standard password-cracking system to successfully recover a password) has increased by 20x from 2007 to 2025
- A consistent subset of users continues to use extremely weak passwords that can be guessed almost instantly, shown by the 10th percentile values remaining near zero over the two decades
- The strongest passwords have become significantly more complex in recent years, represented by the 90th percentile grows dramatically over time (from roughly 100 million guesses in the late 2000s to over 1 billion by 2023 and beyond)
- The upper range of password strength has increased sharply over time (reflecting the adoption of more secure password practices or stronger password generation methods in later years)
- Two increases in password strength stand out in 2011 and in 2019, most likely due to policy changes and implementation of password managers, respectively
- Passwords still aren't perfect: modern cybersecurity requires various layers working together to protect people, and Threat Exposure Management's role is to identify and mitigate exposures before threat actors exploit them
- This measurable difference over the years is due to cybersecurity professionals' work of awareness, advocacy, and improved cyber infrastructure

Analysis of Users' Password Behavior Changes

At Flare, we've been collecting leaked credentials across the internet since 2016. Our data lake now contains more than 216 billion lines of compromised data. To study password evolution over time, we randomly sampled 500,000 entries per year, using the leak date rather than the ingestion date into our system when possible1. This allowed us to trace the story of password strength back as far as 2007.

The Methodology

Password strength can be measured in different ways. A theoretical measure is entropy, which expresses unpredictability in bits under the assumption that each character is chosen randomly. While useful as an upper bound, entropy consistently overestimates the security of real human passwords, which are rarely random. People tend to favor predictable patterns like "Password123!" or simple substitutions.

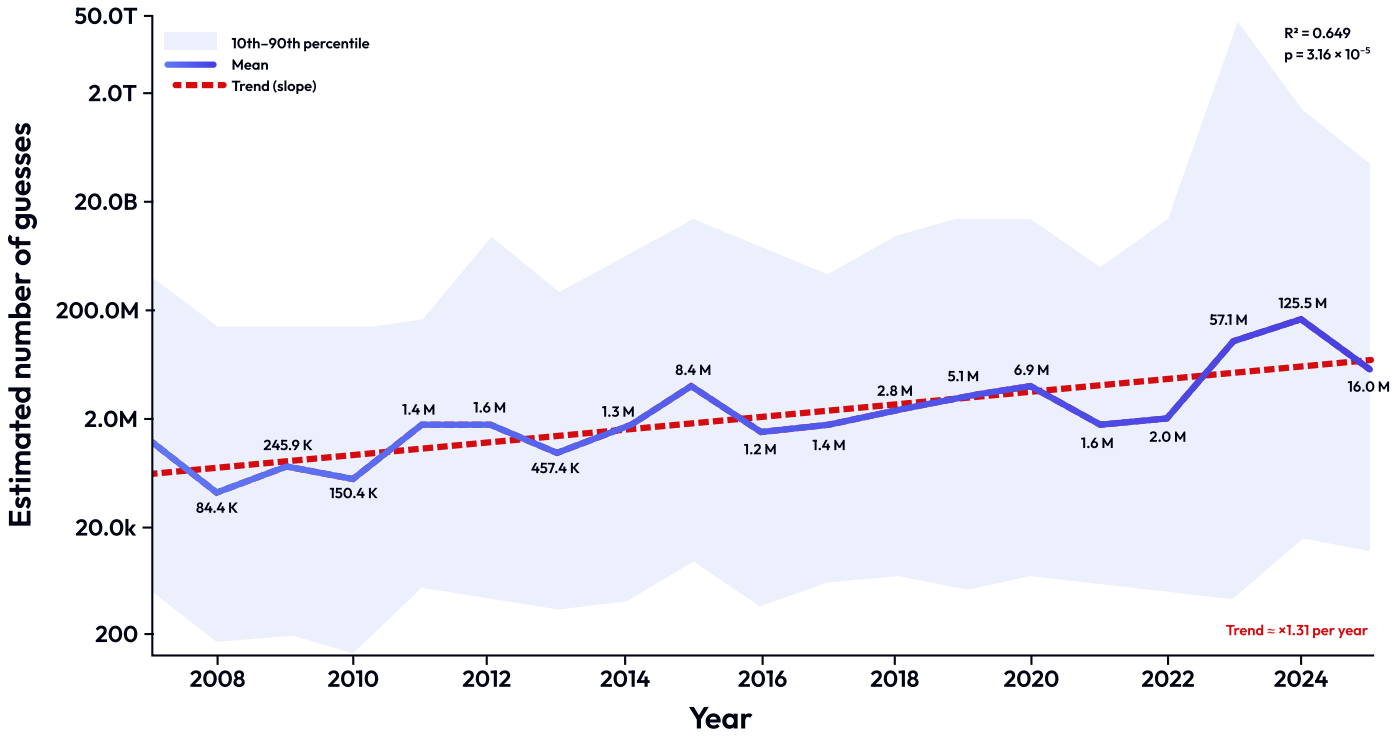
To capture a more realistic picture, we turned to a practical strength estimator: zxcvbn (developed by Dropbox). Instead of assuming randomness, zxcvbn estimates, among other things, the log10 number of guesses an attacker would need, based on:

- Entropy
- Presence of dictionary words, names and common passwords (~30,000)
- Presence of password seen in known leaks
- Pattern recognition (keyboard walks, dates, sequences, leetspeak, repeated characters)

This model offers an empirically grounded measure of password strength that better matches how real attackers operate. Using it, we performed a time-series analysis to see how password strength shifted year over year.

[1]Testing showed that our data lake samples reach stability at around 50,000 lines, while 500,000 lines provide significantly stronger reliability. We used these results to define the annual sample size.

Breaking Down the Evolution of Password Strength (2007-2025)



Evolution of password strength over time (2007-2025), calculated by estimated number of guesses required by a standard password-cracking system to successfully recover a password.

The graphic illustrates the overall trend in password robustness observed across the years. To quantify password strength, we report the estimated number of guesses required by a standard password-cracking system to successfully recover a password. This metric provides a consistent measure of the relative robustness of the password corpus over time. For ease of interpretation, all values are expressed in millions of guesses.

Indicator of Overall Password Strength: The Average Number of Guesses

The dark purple line represents the average number of guesses needed to correctly identify a password in a given year, serving as an indicator of overall password strength. Higher mean values correspond to stronger average passwords that are more resistant to guessing attacks.

The Difference Between the Weaker and Stronger Passwords: 10th-90th Percentile Range

The light-purple shaded area denotes the 10th–90th percentile range, capturing the variability around the mean and highlighting differences between weaker and stronger subsets of passwords.

Specifically, the 10th percentile marks the weakest segment of passwords (10% of passwords required fewer guesses than this value to be cracked) whereas the 90th percentile marks the stronger segment (90% of passwords required fewer guesses than this value, with the remaining 10% being even more resistant).

In other words, the 10th and 90th percentiles define the lower and upper bounds of typical password strength for each year.

Trend of Password Strength: Increase in Estimated Number of Guesses

Finally, the red dashed line represents the trend (slope), showing that the estimated number of guesses has increased in a statistically significant manner over time, suggesting a gradual strengthening of passwords across the observed period, ultimately by 20x over the observed period.

The table below provides a detailed breakdown of the numbers for each year:

Year	Mean (millions of guesses)	10th percentile (millions)	90th percentile (millions)
2007	0.75	0	737.76
2008	0.08	0	100
2009	0.25	0	100
2010	0.15	0	100
2011	1.39	0	145.61
2012	1.6	0	4,780.00
2013	0.46	0	453.13
2014	1.28	0	1,971.01
2015	8.37	0	10,000.00
2016	1.17	0	3,079.01

Year	Mean (millions of guesses)	10th percentile (millions)	90th percentile (millions)
2017	1.36	0	1,000.00
2018	2.77	0	4,839.16
2019	5.08	0	10,000.00
2020	6.85	0	10,000.00
2021	1.56	0	1,300.15
2022	1.57	0	10,000.00
2023	11.1	0	1,000,000,000.00
2024	125.43	0.01	1,060,127.25
2025	15.96	0.01	98,487.93

What Improved Password Strength Over the Years?

Across the years, the 10th percentile values remain near zero, showing that a consistent subset of users continues to use extremely weak passwords that can be guessed almost instantly.

However, the mean fluctuates considerably. We looked into noticeable increases in password strength and looked into what cultural trends or policies/standards may have affected password strength.

The First Increase in 2011: Standards and Policy Updates Amidst News Coverage of the "Year of the Hack"

By 2011, we observed an improvement with a mean climbing past one million guesses. That year, several factors might have converged to push password practices forward:

- On the standards side, PCI DSS 2.0 came into effect, prompting many organizations to review and strengthen their password policies.
- At the same time, a wave of highly publicized breaches, including the Sony PlayStation Network outage (77 million accounts) and the RSA SecurID compromise, kept weak authentication in the headlines and forced millions of users to reset credentials. Media dubbed 2011 "the year of the hack," amplifying public awareness and pressure on companies to improve security.
- It probably led NIST to finally update their Federal Electronic Authentication Guideline that had remained unchanged since 2006.

Together, these standards updates, compliance pressures, and news-driven resets likely explain the measurable surge in password strength that becomes visible in data starting in 2011 until 2015.

The Second Increase in 2019: The Rise of Password Managers (Both Standalone and Built-In)

We then observed a much larger increase from 2019. Although password managers have existed since the early 2000s (e.g. KeePass first released in 2003, 1Password launched in 2006, and LastPass was founded in 2008), they remained largely tools for enthusiasts and security-aware users for many years.

It was only in the mid-to late 2010s that they began reaching a broader audience driven by integration into operating systems and apps:

- Apple rolled out iCloud Keychain and cross-device password syncing in 2013
- Android introduced a formal Autofill framework around 2017
- iOS 12 (2018) allowed third-party apps to hook into Password AutoFill

Surveys from the late 2010s still showed relatively low adoption of standalone managers; however, by 2023–2025, around one in three U.S. adults report using a password manager (or its built-in equivalent).

This adoption trajectory aligns with what our data show: starting around 2022–2025 the upper tail of password strength increases driven by auto-generated, long passwords via manager tools.

Examining the Strongest Passwords (The 90th Percentile)

The 90th percentile grows dramatically over time (from roughly 100 million guesses in the late 2000s to over 1 billion by 2023 and beyond) suggesting that the strongest passwords have become significantly more complex in recent years.

Overall, the data indicates that while a portion of users continue to choose weak passwords, the upper range of password strength has increased sharply over time, reflecting the adoption of more secure password practices or stronger password generation methods in later years.

Making Change for Millions of People with Security-Forward Design

The broader lesson is that password strength has less to do with people suddenly becoming disciplined and more to do with technology removing friction. Users didn't wake up one day eager to memorize 20-character gibberish strings.

Instead, platforms started generating and remembering them automatically. Also, more websites started prompting stronger passwords. Once the path of least resistance aligned with best practice, security finally increased. The data shows real improvement, thanks to the growing adoption of password managers and greater user awareness.

Despite this steady progress, most passwords are still not strong enough to reliably resist modern cracking techniques. There remains significant work to be done not only in improving password security behaviors, but also in strengthening defenses against already compromised data and other areas of cybersecurity risk. For credentials that have been cracked or leaked, security teams can leverage automation to quickly identify and mitigate exposures before they are exploited.

Modern cybersecurity requires a comprehensive, layered approach designed to protect individuals and organizations through multiple, complementary safety nets. Among these layers, Threat Exposure Management plays a critical role in reducing risk and maintaining resilience against evolving threats.

The story of passwords isn't just about complexity scores or means on a chart. It's about how design choices (like building a password manager into phones) shifted the habits of millions. We've gone from "1234" to machine-generated shields, and while the journey wasn't linear, the direction is unmistakable: stronger, smarter, and increasingly automated.

Cybersecurity professionals can take pride in this evolution: education, advocacy, and better tools are making a measurable difference.