PENTEST EXPERTS

# COMMON PASSWORD PATTERN REPORT

# FOREWORD

In the vast and ever-expanding digital landscape that defines our modern world, passwords remain the ubiquitous cornerstone of digital authentication. Despite the advent of multi-factor authentication (MFA) and biometric solutions, these simple strings of characters overwhelmingly remain the primary method for securing access to our online lives and critical systems. While exact percentages fluctuate across industries and platforms, estimates consistently place the reliance on password-based authentication for individual and enterprise accounts well over 80%.

The seemingly humble password carries an immense burden of responsibility for our security. It acts as the critical first line of defense, the initial gatekeeper safeguarding our most sensitive information. From personal financial data and private communications to critical corporate assets, intellectual property, and national infrastructure, the integrity of our digital world fundamentally hinges on the strength, uniqueness, and proper management of these credentials. A compromised password can instantly grant unauthorized access, leading to data breaches, financial losses, identity theft, and severe reputational damage.

This report delves into the intricate world of password security, examining current shortcomings, prevalent vulnerabilities in human behavior, and the evolving threat landscape. As cyber threats continue to proliferate, ensuring the robustness of our password security practices is not merely a technical consideration but a collective imperative for individuals and organizations alike.

## Predictability of human behavior

In the realm of digital security, passwords stand as the ubiquitous first line of defense. Their efficacy, however, often hinges not on the predictable nature of human behavior.

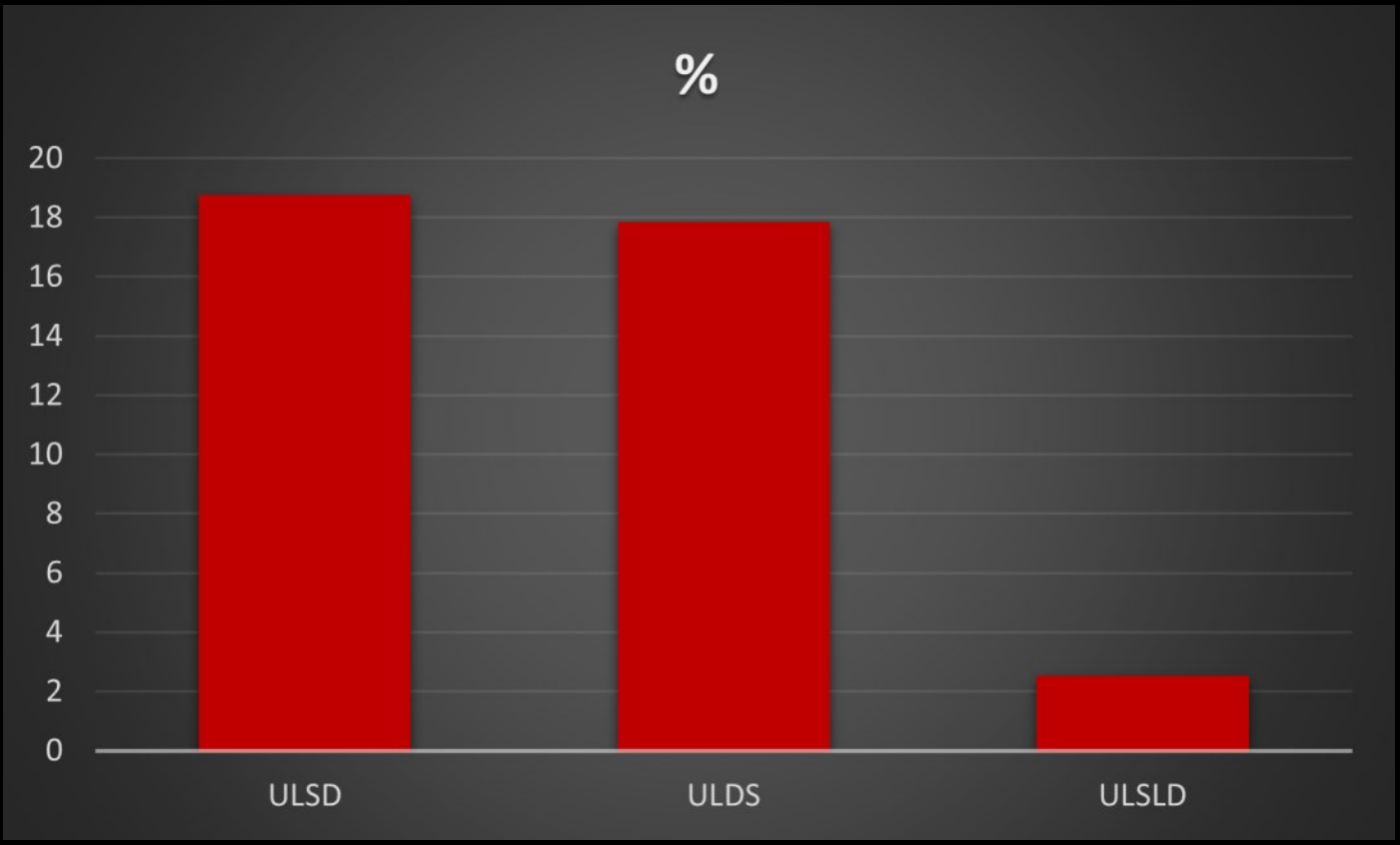
The human mind, wired for efficiency and recall, frequently seeks simplicity and patterns, a trait that directly conflicts with the computational demand for randomness and complexity in secure credentials.

We have analyzed more than 4.5 million unique real-world passwords from various data leaks for this report to uncover the most prevalent patterns in cracked passwords. The nature of the data used for this analysis introduces a very strong bias – so please take the numbers with a grain of salt! please take the numbers with a grain of salt!

# HUMANS TEND TO FOLLOW THE GUIDANCE

Many websites request from a user to create a password with "*upper- and lowercase characters, special characters and digits*" or "*upper- and lowercase characters, digits and special characters*".

This instructions are taken from many users by the letter – analyzing the top 3 patterns in the leaked and cracked passwords we uncover the following:

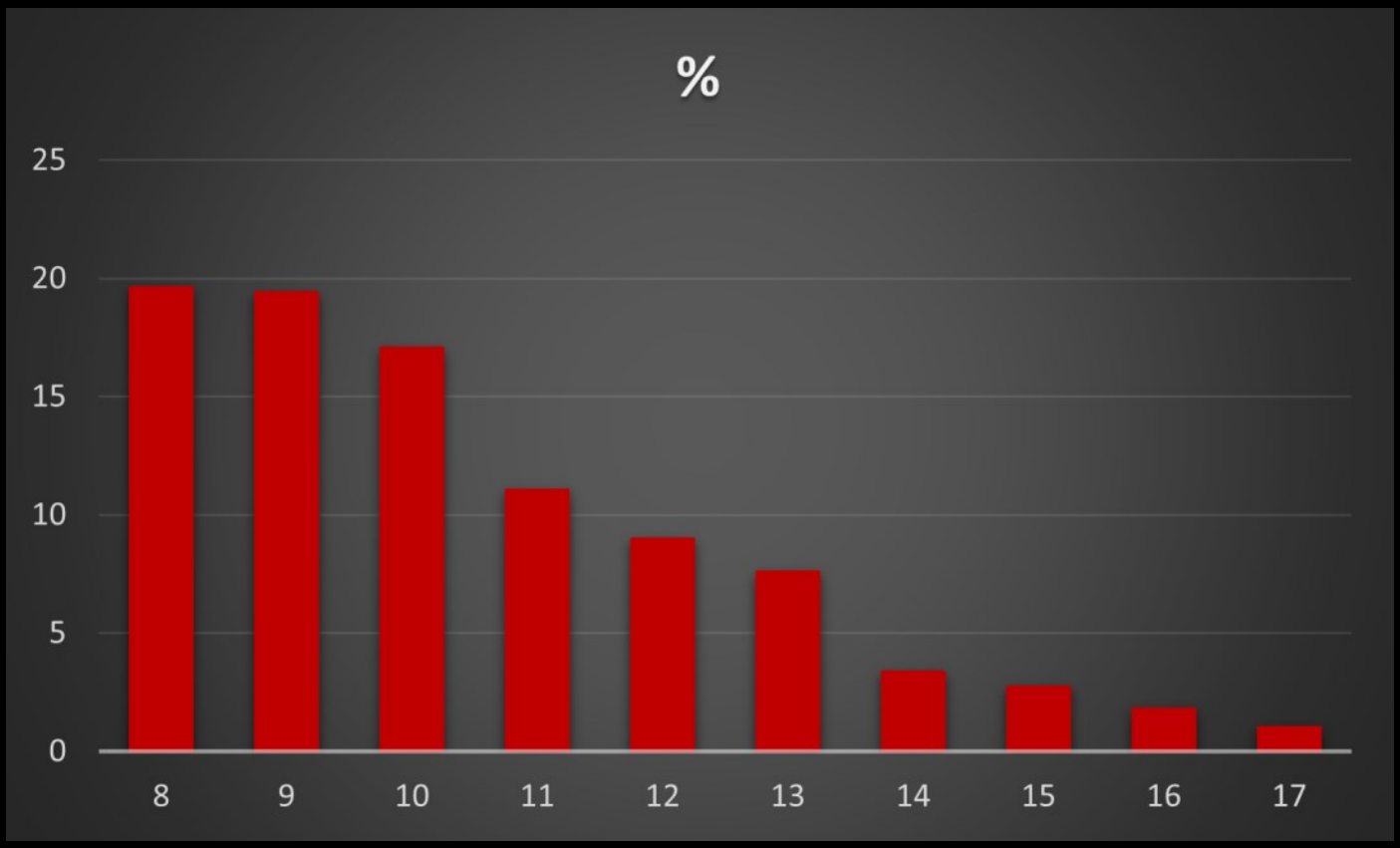



U ... Uppercase letter | L ... lowercase letter | S ... special character | D ... digit

In total 1,650,201 passwords or **36.53% were following exactly one of the aforementioned 2 orders**. Faced with abstract complexity rules, humans seek the simplest, most consistent structure to aid recall, like applying instructions in a literal, sequential order. This cognitive shortcut sacrifices true randomness for convenience, making the password easy for us to remember, but unfortunately also predictable for attackers.

# AS SHORTER AS BETTER

Given a common minimum password length requirement of 8 characters, many users do not want to go the extra mile with a longer password. Thatfor the top 10 password lengths are:

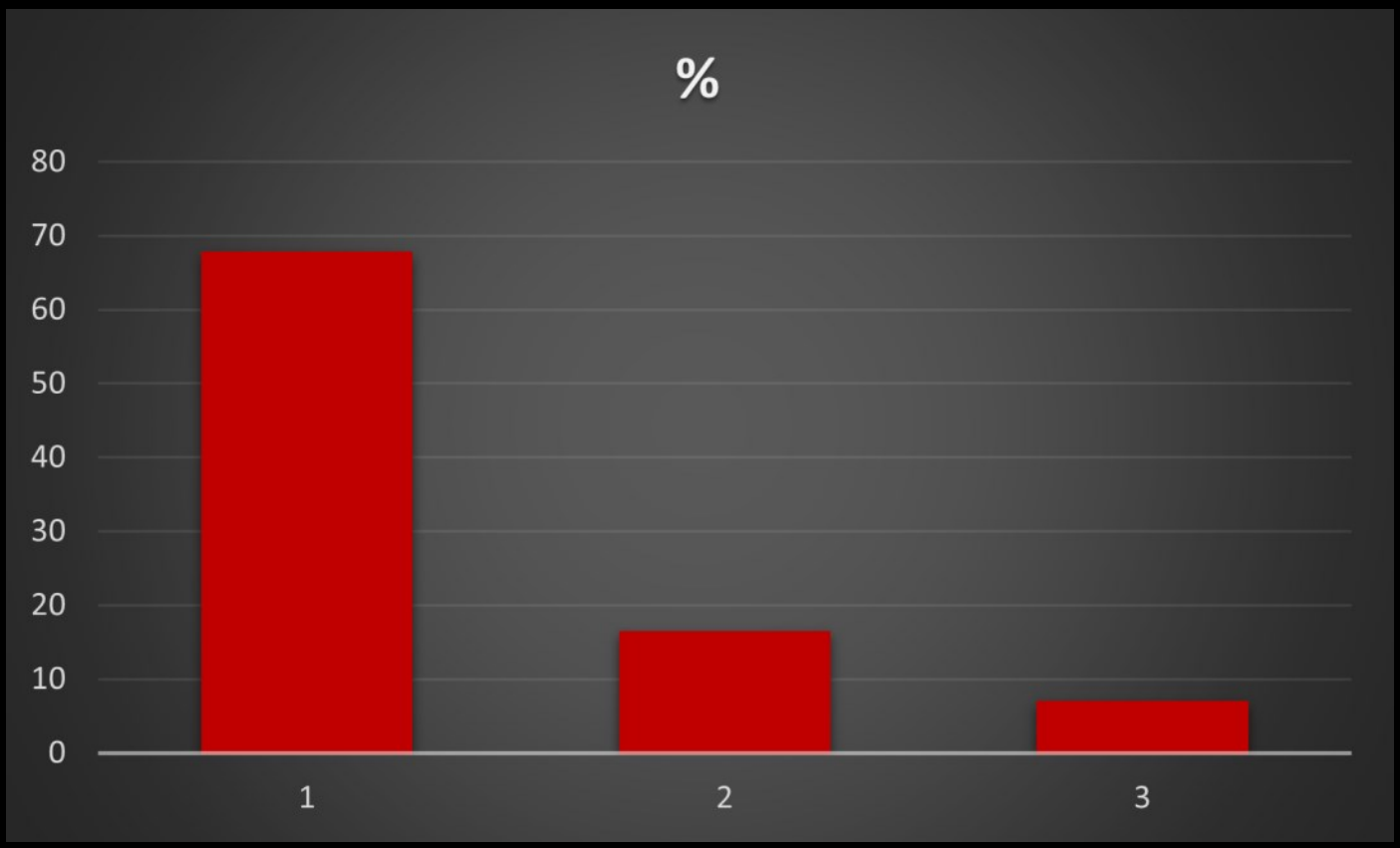



The overwhelming concentration (aprox. 50%) of passwords are with 8-10 characters at or just above the common 8-character minimum requirement. Those short passwords are in reach for brute-force attacks (trying every possible combination of characters) even with modest hardware and thatfor not considered save anymore.

From a security standpoint, this creates a critical vulnerability. Password strength grows exponentially with length; even a few additional characters can dramatically increase the time and computational resources required for a brute-force attack.

# MOST PASSWORDS ARE BASED ON WORDS

Analyzing the top 3 counts of Uppercase characters paints a very dramatic picture:



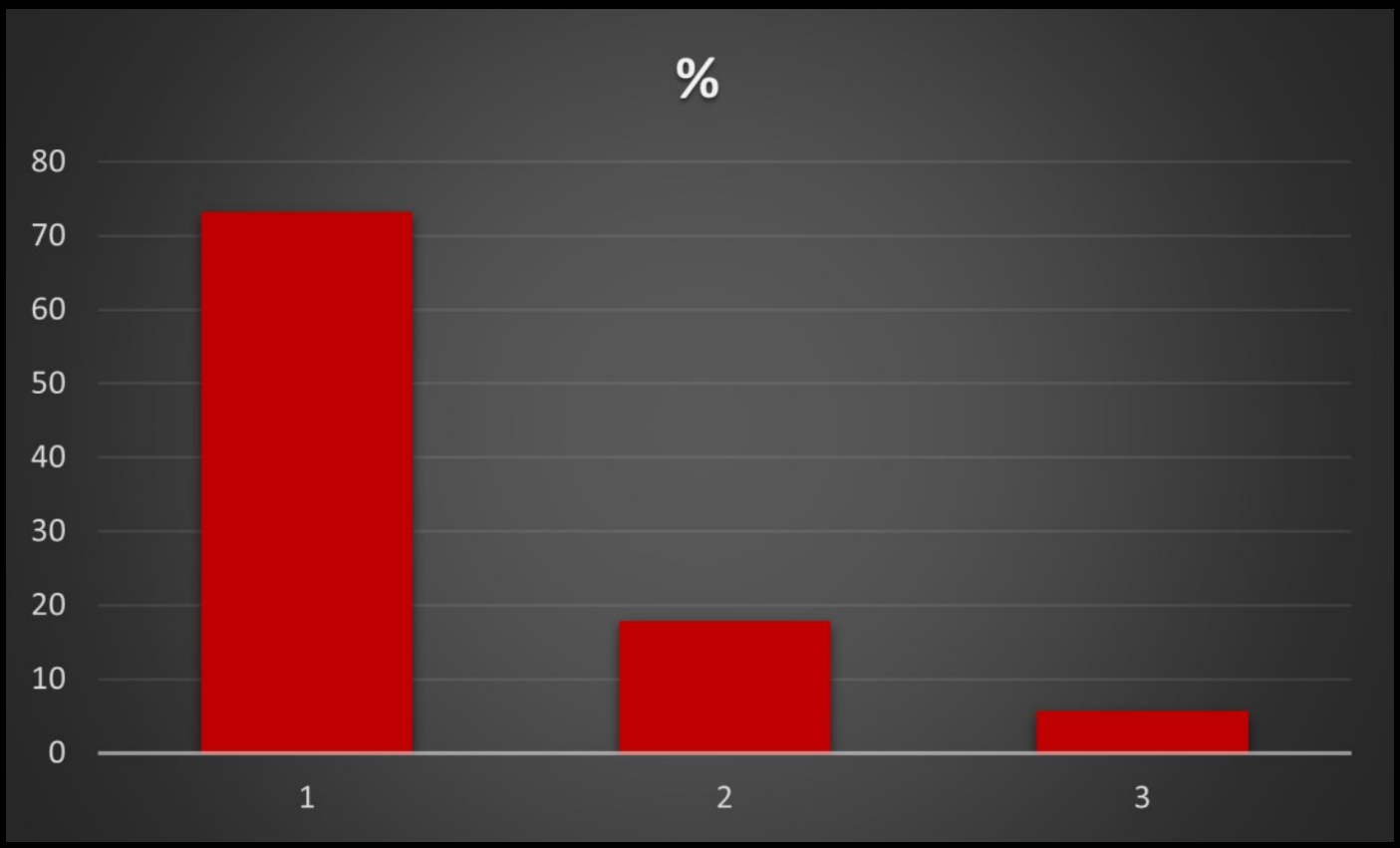

Over 67% of the cracked passwords use a single uppercase letter, indicating that the cracked password was based on a single word with an initial Uppercase letter.

A good 77% of all those passwords contain a word with an initial uppercase letter, followed by 3 or more lowercase letters. This is easy to explain as this pattern follows the way we tend to write Names or some words and as a creature of habit, humans have a hard time to ignore that trained patterns.

Attackers are acutely aware of this human tendency, prioritizing dictionary attacks, which take common words, names, etc. and decorate them with digits and special characters over brute-force attempts (which try all possible combinations of characters in any possible order), because dictionary-attacks are much faster then brute-force attacks!

# SECIAL CHARACTER USAGE

Analyzing the top 3 counts of special characters reveals:




Good **73% of the passwords used only one special character**!

Furthermore those are the most used special characters, making up more than 90% of the usage:

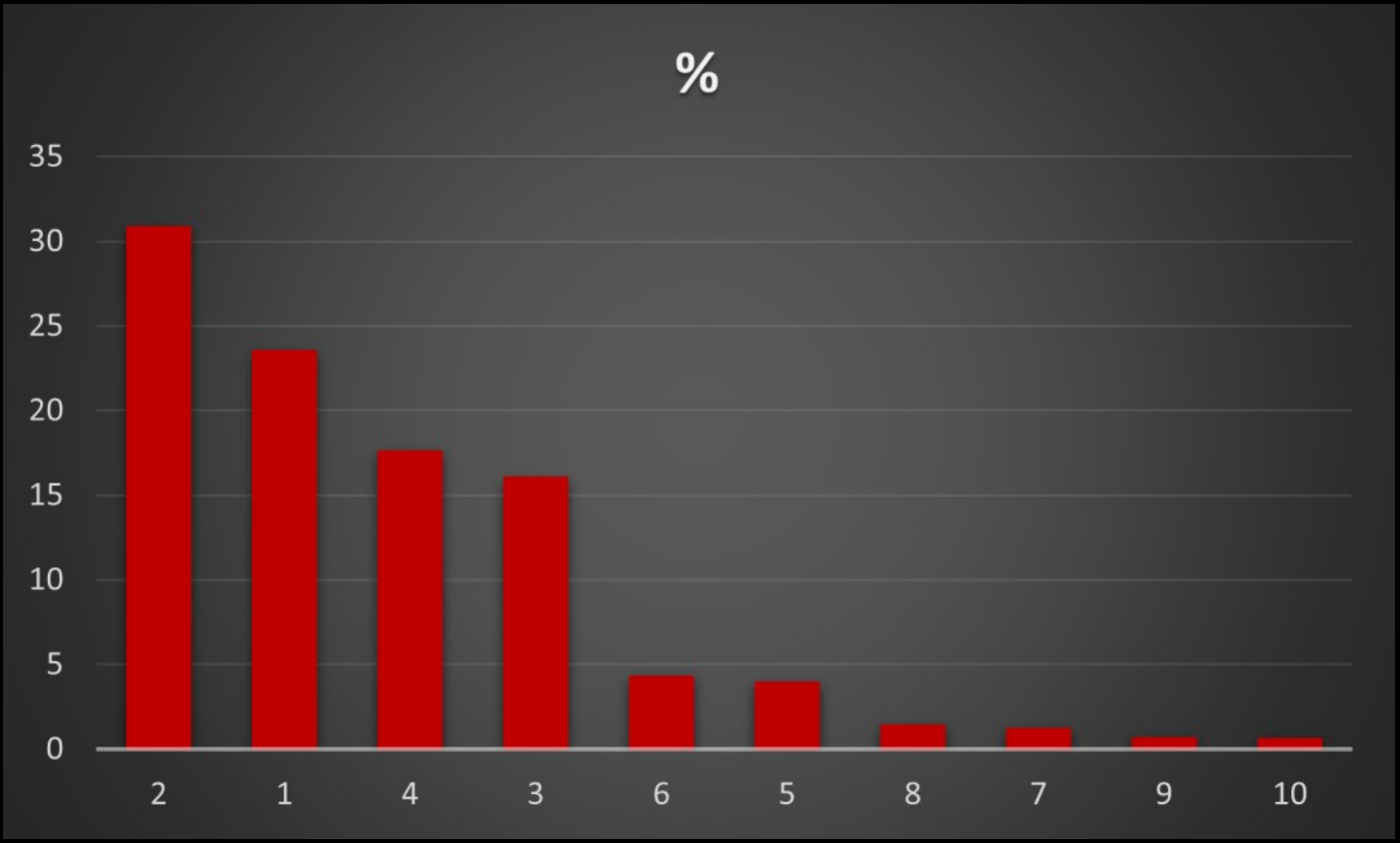
```
! @ . _ # $ - * & :
```

The top 10 most used combinations of a digit with one special character (19% in total) are:

```
1! @1 #3 _1 #1 3! .1 2! @2 -1
```

# DIGITS USAGE

Analyzing the top 10 counts of digits in a password shows:




Almost **88% of the passwords use 1-4 digits**!

The top 10 combinations of 3-digits, making up over 15% are:

`123 201 200 198 199 234 100 036 010 000`

The top 10 most used combinations of a digit with one special character (19% in total) are:

`1! @1 #3 _1 #1 3! .1 2! @2 -1`

Over **8% of the passwords contain a year between 1900 and 2025** and the fact, that the dot and - are in the top special characters indicate the use of dates to an even higher degree!

# FAZIT FOR PENTESTERS

- Over 36% of passwords use the orders
  uppercase, lowercase, number and special character or
  uppercase, lowercase, special character and number
- 67% of passwords use exactly one uppercase letter
  51% use a word (1 uppercase letter, followed by 3 or more lowercase letters)
- 88% of passwords use 1-4 digits
  54% use 1-2 digits
  8% use a year from `1900`-`2025`
  most common number pattern are `123`, `1234`, `000` and `0000`
- 73% of passwords use exact one special character
- Most used special characters are: `! @ . _ # $ - * & :`

# FAZIT FOR USERS

- Following the above mentioned patterns, is the best way to get your password hacked.
- Use a password manager to generate and store your long and secure randomly generated passwords to stay safe.