Understanding how users choose passwords: analysis and best practices

Alessia Michela Di Campi[1,†], Flaminia L. Luccio[1,*,†]

[1]DAIS, University Ca' Foscari of Venice, Venice, Italy

Abstract

In an era where digital services and password-protected platforms are becoming ubiquitous in various aspects of our lives, from healthcare technology to home environments, security has emerged as a paramount concern. To remotely access these devices, users must go through an authentication process, which typically involves the use of passwords. These passwords must meet two essential criteria: usability and security. Usability implies that passwords should be easy for users to remember and use. Security requires that passwords be resistant to unauthorized access. This study aims to investigate potential links between human behavior and password selection, as well as users' perceptions of password security. To address this issue, we analyzed multiple data leaks and surveyed 217 users across various age groups and backgrounds. Data analysis reveals that, regardless of educational or professional background, most people tend to opt for simple, easily guessable passwords. Surprisingly, users with a technology background chose the weakest passwords. Based on the results of our analysis, we propose recommendations for both users and IT professionals. These suggestions can help users create stronger passwords and help IT professionals formulate effective access policies.

Keywords

passwords, human behaviour, usability

1. Introduction

Passwords play a crucial role in our daily lives as they are the key to accessing various computer systems. To ensure security, it is critical to examine and understand how to create passwords that are not easily guessed [1, 2]. In recent years, several papers have proposed models and techniques for measuring password strength, aiming to provide real-time feedback to users and guide them in selecting stronger passwords (see, e.g., [3, 4, 5, 6]). However, one of the primary concerns for users is the fear of forgetting their passwords, leading them to choose easily memorable ones. Unfortunately, this practice makes them vulnerable to various efficient attacks (see e.g., [5, 7, 8, 9]).

Passwords' memorability is influenced by their composition and patterns. In this work, we will analyze common words and patterns used in password creation. This analysis is crucial as some attacks exploit these commonalities and can even guess encrypted passwords. By examining the most commonly used patterns and word categories in password creation and their potential correlation with language, we aim to gain valuable insights into password security vulnerabilities. Thus, this work focuses on analyzing known data leaks and responses from participants to a questionnaire in order to address the following research questions:

***RQ1**: Which are the most common patterns and word categories used for password creation, and do they depend on the used language?* Passwords' effectiveness is closely linked to users' cognitive abilities and behaviour. Understanding how cognition and behaviour affect password security can lead to insights into vulnerabilities and strategies to improve digital security.

***RQ2**: How does user cognition impact password security and usage?* Experts and regular users have different approaches to password security based on their knowledge and experience. By analyzing

ITASEC 2024: The Italian Conference on CyberSecurity

*Corresponding author.

†These authors contributed equally.

alessia.dicampi@unive.it (A. M. D. Campi); luccio@unive.it (F. L. Luccio)

0000-0002-0877-7063 (A. M. D. Campi); 0000-0002-5409-5039 (F. L. Luccio)

these differences, we can identify opportunities for targeted interventions and educational initiatives to enhance cybersecurity for all users.

***RQ3**: Are there differences between experts and regular users?* We aim to explore how computer knowledge may affect attitudes towards choosing passwords.

This comprehensive analysis aims to shed light on password security and help users and IT professionals in making informed decisions to enhance the protection of computer systems. The contributions of our work are: i) A comprehensive analysis of multiple data leaks: we analyzed multiple data leaks to understand password choice behaviors, patterns, and vulnerabilities and provided a comprehensive understanding of password security practices. ii) Exploration of cognitive aspects: we delved into the cognitive aspects underlying password choices, identifying common mistakes and proposing techniques to prevent them. iii) Investigation into factors shaping password selection: we explored the factors influencing individuals' password choices, including demographic variables and level of IT experience through a questionnaire survey.

This manuscript is organized as follows: in Section 2, We discuss recent studies on psychological factors that influence password choice, as well as studies on password structure. In Section 3, we discuss the analysis made to pre-existing data leaks. In Section 4 we introduce the analysis and results of the proposed questionnaire, and in Section 5 we try to answer to RQ1, RQ2 and RQ3. We conclude in Section 6 giving some general recommendations and discussing future work.

2. Related Work

In this section, we discuss recent studies on the psychological factors that influence password choice, as well as studies on the best password structure for security purposes.

Cognitive dissonance. Many websites enforce strict password guidelines, frustrating users [10, 11, 12, 13]. Psychological factors, such as cognitive dissonance, i.e., the psychological discomfort stemming from the simultaneous adherence to conflicting sets of beliefs, values, or attitudes, influence password choices [14]. Users often exhibit cognitive dissonance regarding password behavior, knowing the risks of reusing passwords but persisting in the behavior. Despite awareness of best practices, like changing passwords regularly, many users do not adhere to them.

Neutralization mitigation. Different strategies are proposed to reduce risky behaviors in password creation. An empirical study by [15] found individuals applying psychological mechanisms like denial of responsibility. This mechanism involves individuals justifying their non-compliance with company password guidelines by asserting ignorance of such guidelines. Educational interventions can reduce such behaviors and promote secure password practices [16].

Cognitive depletion and training memory. Another important aspect studied in password choices is the influence of cognitive depletion [17], often referred to as *cognitive exhaustion* [18]. According to Baumeister's theory, individuals have limited mental resources for decision-making and self-control. This limitation leads users to fear forgetting their passwords, resulting in password reuse across various websites. A study conducted by Wash et al. [19] found that people were reusing each password on average on 1.7 out of 3.4 different websites. Users tend to reuse passwords they enter frequently or those that are more complex. This pattern was evident in our questionnaire, where participants often used the same password for multiple questions. Cognitive depletion arises due to limited mental memory capacity. Nelson and Vu [20] in 2010 proposed image-based techniques to simplify password memorization, leveraging humans' strong image recall ability [21, 22, 23, 24, 25, 26]. Image-based passwords are easier to remember compared to text-based ones, triggering the stream of consciousness [27].

Attention processes. Experts in a particular field tend to enter a state of *energy conservation*, as the process of focusing their attention is cognitively demanding. On the contrary, when people lack significant knowledge on a topic, their attention it is often heightened, allowing them to remember even the smallest details [28]. Consequently, experts in a particular field may focus solely on the end goal, such as registering on a website, inadvertently overlooking a critical aspect: security. This behavior is rooted in the intrinsic nature of the attention processes.

Pattern frequency analysis. To access certain systems, complex passwords are required to enhance security against guessing attacks. Password strength is typically measured by entropy [29, 30, 31]. Users often slightly modify passwords across accounts to improve uniqueness while maintaining security, though this practice is understudied [32]. However, meeting complexity requirements does not guarantee strong passwords, for instance, `P45sw0rd1` appears secure but can be easily guessed due to common patterns [12, 33]. Moreover, techniques such as Leetspeak, that replaces characters with symbols, do not significantly enhance security [34, 35, 36, 37, 38, 39].

3. Dataset Analysis

We analyzed various datasets to scrutinize the relationship between common patterns in password creation across multiple data leaks. Our aim was to extract insights applicable to any data leak using diverse datasets, departing from the practice of tailoring results to specific datasets observed in prior research such as [35, 40, 41].

3.1. Dataset Selection

After an accurate selection we downloaded different datasets which are publicly available on GitHub, and that contain a substantial number of passwords. The datasets are the following ones: *RockYou Dataset* [42]: Contains 32,603,048 passwords leaked from accounts of RockYou, a company known for developing widgets for MySpace and social networking applications; *Hotmail Dataset* [43]: Includes 8,930 passwords from a data breach of Microsoft's web-based email service; *PhpBB Dataset* [44]: Comprises 184,388 passwords leaked from PhpBB, a popular free forum management system; *Ashley Madison Dataset* [45]: Contains 375,831 passwords leaked from Ashley Madison, a dating service; *Most Common Words Dataset* [46]: Consists of over 4000 English words; *Most Common Names Dataset* [47, 48, 49, 50]: Includes over 8000 English, German, and Spanish names.

3.2. Password Analysis and Results

We analyzed different data leaks to extract commonly used password patterns. Our focus was on the frequency and position of characters, as well as their similarity to commonly used words. We also ensured our findings were not uniquely linked to a particular dataset.

3.2.1. Password Patterns

To answer to RQ1 we followed different steps in a systematic manner. To describe the steps we first need to introduce some notation, and then we explain the analysis.

We followed the notation of [35], where passwords are defined using a concatenation of different symbols: *L, N, U* and *S*, where *N* represents numbers, *L* lowercase letters, *U* uppercase letters, and *S* symbols. We define a *pattern class* as a variable-length (eventually empty) sequence of numbers N^+, lower or upper case letters L^+ or U^+, and symbols S^+. Moreover, a *password pattern* is a combination of strings of the type N_n, L_n, S_n, or U_n. For example N_3 represents a numeric string composed of three characters, and U_5 denotes an uppercase letter string composed of five characters.

For each data leak, we calculated the average length of passwords and which ranges of length were the most frequent ones in order to create datasets with sufficient data for statistical analysis. Then, following the research outlined in [51], we delineated diverse password construction methodologies. First, we categorized passwords by pattern class using a simple algorithm that converts a string input (password) into the corresponding pattern class. For example, `Password1` becomes $U^+L^+N^+$, and `Pas5word@1` becomes $U^+L^+N^+L^+S^+N^+$. This facilitated faster understanding of password structure, and we calculated frequencies to determine the most common patterns.

Then, we performed common substitutions of numbers and symbols with characters (see Table 5 in the Appendix). After substitution, we removed any numbers or symbols at the beginning or end of the

password and analyzed the resulting passwords to generate statistics. In the case of comparisons with other dictionaries, were counted how many comparisons had hits. In the case of single string analysis, were divided the strings into characters and analysed the structure. To measure the minimum number of single-character edits (insertions, deletions, or substitutions) needed to transform one word into another, we used an edit distance algorithm. In particular, we used a modified version of the Levenshtein Distance algorithm [52], taking two files and a threshold as input. The first file contained common words, and the second file contained processed plaintext passwords. The algorithm found potential matches in the dictionary based on a chosen threshold, indicating common substitution methods used in passwords. We also used this algorithm to categorize passwords, considering common words along with commonly used names, colors, superheroes, etc. We analyzed the distribution of capital letters, lowercase letters, symbols, and numbers within passwords to better understand password structures. We analyzed passwords containing numbers and symbols positioned either at the beginning or end of a sequence to derive detailed statistics on employed numerical values, or symbols.

Then, we conducted an analysis on special format patterns, including passwords with specific structures such as dates in various formats and combinations of birth months, days or years. We analyzed repeating patterns, reversing patterns, and mixed patterns that combine various types of patterns.

Finally, we investigated whether users of different languages exhibited distinct password patterns. After analyzing word lengths in datasets of frequently used words in languages other than English, we focused on Spanish and German datasets, applying to them the same analytical procedures used for English passwords.

3.2.2. Dataset Analysis Results

Pattern Analysis Results. Our analysis of password lengths revealed that they typically range from 7 to 8 characters, with the majority falling between 5 and 12 characters. We excluded passwords shorter than 5 and longer than 12 characters for our examinations. From the pattern analysis results, we identified the dominant pattern class as one characterized by the presence of both letters and numbers L^+N^+ and only letters L^+ (details in Table 1). We noticed that as the password length increases, the occurrence of lowercase letters ascends towards the end of the password, while the occurrence of numbers decreases. Uppercase letters exhibit a descending pattern from the first character to the end of the password. We also observed that pattern classes starting or ending with numbers or symbols were frequent. Regarding prefixes and suffixes, numeric prefixes are more common than symbolic prefixes across all databases, with suffixes being predominantly numeric. For instance, in Rockyou, approximately 22.90% of passwords have numeric prefixes, while only 0.72% have symbolic prefixes. As for suffixes, 57.98% are numeric characters, while 2.38% are symbolic characters. Additionally, an inline diff analysis revealed that in 90% of cases, password symbols corresponded to characters resulting from common substitutions, such as “@” for “a”, “$” for ’s”, “!” for “l”, and “[” for “p”.

	%				
Pattern class	L^+N^+	L^+	N^+	N^+L^+	$L^+N^+L^+$
Rockyou	33	26	17	4	1
Ashley Madison	37	33	12	4	2
PhpBB	24	41	11	5	2
Hotmail	20	42	19	3	2

Table 1
The pattern classes. They may not total 100%, as we are only displaying the top five patterns.

Frequent Categories. We employed the Levenshtein Distance algorithm to categorize passwords based on input word files, such as lists of personal names. In analyzing personal names, we found that certain names were more prevalent than others across the datasets. The most common names in the RockYou dataset were Love, Mari, Angel, and Anna. In PHPBB, Love, Star, and King were prevalent. Hotmail showed Mari and Love as the most common names, while Ashley Madison exhibited Love,

King, and Mike. Furthermore, we observed that passwords with five characters tended to contain names more frequently than passwords of other lengths. Match percentages decreased as password length increased, indicating longer passwords were more complex and less likely to contain common names. Additionally, an examination of potential connections between names, dates, and numbers showed that passwords containing numbers with names became more common as password length increased across all datasets.

Analysis of other Languages. Regarding the analysis of the Spanish and German languages, even though the datasets contained fewer words, we uncovered noteworthy patterns and trends. We found that the most used patterns are the same as those used for the English language.

4. Case Study

4.1. Questionnaire

We created a questionnaire for users across different age groups and backgrounds to gather insights into their password creation practices and attitudes toward password security. The questionnaire was distributed through multiple social networks including Facebook, Instagram and Twitter and we collected 217 responses. Notice that, a potential bias may have occurred in the questionnaire responses, particularly when we requested passwords that adhered to the reported policies. Participants might have chosen safer but more difficult-to-remember passwords, given that they knew they would not need to recall them in the future.

Ethics. To gather data, we distributed an anonymous questionnaire to request responses from our target participants. We chose this anonymized approach to ensure the privacy and candidness of respondents, thereby encouraging a more open and unbiased exchange of information. Participation in the research by filling in the questionnaires was purely voluntary. The questions had no mandatory answers, so those who did not want to answer could skip and go to the next question. Participants did not get any reward by participating in the research.

4.1.1. Passwords Shapes and Categories

We proposed some questions involving user-invented passwords. By doing so, we were able to build a dataset of passwords to be analysed. To answer RQ1, we analysed the new dataset to deduce patterns, distributions of numbers and symbols, and the most commonly used words. The questionnaire free answers were analyzed following the pattern notation explained in Section 3.2 with letters representing lowercase letters, numbers, uppercase letters, and symbols. Passwords were categorized into pattern classes, and common substitutions of numbers and symbols were examined. Using editing distance algorithms, patterns were identified and special formats like dates and combinations of birth months were investigated. While for multiple-choice answers we applied averages and standard deviation. For some questions it was necessary to go deeper by applying additional statistical tools to visualise whether there were substantial differences between groups of answers or persons. As for the categories, we proposed a list of possible categories based on the results of data leaks and asked participants to specify whether they sometimes, never, or always use a specific category among those proposed. We also asked to explicitly specify the patterns they usually use, giving them a choice of lowercase, uppercase, number, and symbol for the various positions of a password of arbitrary length.

4.1.2. Human Cognition: Perception, Behavior, and Knowledge

To address RQ2, we asked the participants to describe their perception and behaviour w.r.t. the choice of a password.

Password Comparison. To gauge user perception of password strength, as in [53], we presented a list of 8 couples of passwords. The pairs were composed of similar passwords and we asked participants to compare them and select the strongest one. The participants rated the passwords on a 7-point Likert

scale [1]. 8 of the 12 proposed passwords were taken from [53] as a reference, while the other 4 were created by us.

Preferences and Practices in Password Security. We asked about the user's password-strength preferences - whether it should be easy to remember, secure, or both. For the participants who responded positively regarding the ease of remembering passwords, we conducted a follow-up inquiry asking why a password should be easy to remember through a multiple-choice question. This question provided predefined options as well as the opportunity for the participants to include free-text responses, allowing for a more detailed explanation of their reasons. We investigated also common beliefs about the strategies malicious users employ to guess passwords (e.g. software, brute force, common words).

External Stimuli. We designed an experiment in which users were directed to three distinct websites. The first website centered around dog training [54], the second one featured CD sales [55], and the third one was focused on helicopter sales [56]. We instructed participants to indicate the password they would use if they were to subscribe to each website in the questionnaire. This was undertaken to evaluate the impact of visual cues on their password selection. Our goal was to analyze how visual stimuli, encompassing images and content, affected their choice of passwords.

Expert Users. To answer to RQ3, we decided to investigate whether users who are presumed to be experienced employ better policies and patterns than non-experts. By expert users we mean people who responded that they were completing or had completed studies in computer science. We are aware that computer science encompasses many categories, so not necessarily everyone has to be a security expert, but still we expect a greater knowledge of good strategies than participants in other fields.

4.2. Results

In this section, we present the findings from our study, which aimed to investigate the relationship between human behaviour, password selection, and user perceptions of password security. We used Python3 and IBM SPSS statistics for string examination for data analysis [57].

Sample. In total, 222 individuals, with different types of jobs (64%) and students (36%), took part in the questionnaire, but 5 of them interrupted the compilation after the first questions, so we removed them from the analysis and considered only 217 responses. The average age of participants was 25 years, ranging from 17 to 62. The cohort was equally divided between men and women, with 44.2% of the sample belonging to the female gender, 55.3% to the male gender, and 0.5% preferred not to answer. In addition, the educational level of the participants was recorded, with 42.4% of the responders having a high school degree, 37.3% a bachelor's degree, 12% a master's degree, Ph.D. degree (1%), or they stopped their study at primary school (1%) or secondary school (6%). In terms of careers, participants included employees, executives, and workers. We assessed participants' computer proficiency levels, categorizing them as advanced, autonomous, or average users. Participants classified as advanced users were 45.2%, 40.6% as autonomous users, and 12.4% as intermediate users, with the remainder possessing basic computer knowledge. The participants were instructed to answer each question spontaneously, without any prior review of their responses. However, they were free to revisit their answers at any point during the study. The summarised questionnaire is shown in Table 6 in the Appendix.

4.2.1. Password Patterns and Categories

We now consider the password patterns and the categories of words used in their construction to respond to RQ1. We explicitly asked the participants about the type of password pattern they usually use; it has been observed that most of the passwords analyzed start with a capital letter followed by lowercase characters, numbers and then symbols (as shown in Table 2a). Participants were also instructed to invent passwords based on their preferences. We collected a total of 643 passwords and analyzed their different patterns and frequencies. The most common pattern was a combination of one

[1]The scale offers two moderate opinions, along with two extremes, two intermediate, and one neutral opinion to the respondents. Selecting 1 would indicate that the first password is considered more secure than the second one. At the same time, 4 suggests they are equally secure, and 7 implies that the second one is more secure.

Type		Position			
		First	*Middle*	*S-last*	*Last*
U	N	**129**	61	22	5
	%*	**59**	28	10	2
L	N	60	**119**	17	21
	%*	28	**55**	8	10
N	N	32	28	**92**	65
	%*	15	13	**42**	30
S	N	14	24	77	**102**
	%*	6	11	36	**48**

(a) Typical password pattern of the N=217 users.

Pattern Class	N	%*
$U^+L^+N^+$	108	17
$U^+L^+N^+S^+$	40	6
$U^+L^+S^+N^+$	34	5
L^+N^+	20	3
U^+L^+	19	3
$U^+L^+N^+L^+S^+$	12	2
Others	410	64

(b) Most common password patterns and related frequencies of 643 passwords.

Table 2
Characters positions and pattern frequencies (*Percentage does not have to give always 100% due to rounding.).

Comparison	PW1	PW2	Perceived stronger	Actually stronger (RGN)
C1	p@ssw0rd	pAsswOrd	PW1	PW2 (4×10^3)
C2	punk4life	punkforlife	PW1	PW2 (1×10^3)
C3	iloveyou88	ieatkale88	PW2	**PW2** (4×10^9)
C4	astleyabc	astley123	Neither	PW2 (9×10^5)
C5	jonny1421	jonnyrtxe	Neither	PW2 (9×10^5)
C6	brooklyn16	brooklynqy	Neither	PW2 (3×10^5)
C7	abc123def789	293070844005	Neither	PW2 (8×10^2)
C8	puppydog3	puppydogv	Neither	PW2 (7×10^2)

Table 3
Passwords comparison results. RGN = ratio of guess numbers.

or more uppercase letters, followed by one or more lowercase letters, and then one or more numbers ($U^+L^+N^+$). This was followed by the pattern of $U^+L^+N^+S^+$, and then $U^+L^+S^+N^+$ (see Table 2b).

We also checked each password to determine which symbols were present and counted them. It emerged that the exclamation point, at sign, and hyphen were the most commonly used symbols.

Regarding the categories of words used to create passwords, the results are that 76% of the respondents used names of relatives, 28% random numbers, and 25% numbers that remind of important dates. Table 7 in the Appendix lists all results.

4.2.2. Human Cognition: Perception, Behavior, and Knowledge

Passwords Comparison. To respond to RQ2 we asked the participants to compare a set of eight pairs of passwords, and we analysed the distributions of the various responses. Only one password was correctly perceived to be more secure than the other. In fact, as can be seen from Table 3, only in the third comparison did the users correctly perceive the second password as the most secure. In all other cases, they either noticed no difference or perceived the less secure one as more secure.

Preferences and Practices in Password Security. According to the survey results, 64% of participants believe that a password should be highly secure, while 31% consider a moderate level of security to be sufficient. Regarding ease of remembering passwords, 37% prefer passwords that are very easy to remember, while 42% find a moderate ease level acceptable. Interestingly, 55.30% of participants prefer easy-to-remember passwords due to fear of forgetting them, 28.90% opt for using the same pattern across all websites, and 23.20% find password recovery processes bothersome. As the survey included opportunities for open-ended responses, the remaining percentage of individuals provided their reasons. Many mentioned the challenge of remembering unique passwords for numerous websites they are registered on, leading them to use one password for multiple accounts or select simple passwords to avoid frequent recovery procedures. Regarding potential methods attackers might use to guess

C_n	G1		G2		F-value	p
	M	SD	M	SD	(1,97)	($\alpha = 0.05$)
C1	3.81	1.53	4.20	1.53	1.58	.213
C2	4.63	2.07	3.95	2.26	2.37	.127
C3	4.57	1.87	4.41	1.77	0.19	.657
C4	4.00	1.84	3.91	1.64	0.06	.799
C5	4.17	2.00	4.05	1.70	0.10	.751
C6	5.89	1.45	5.43	1.30	2.64	.107
C7	2.62	1.50	3.41	1.99	4.89	.029 *
C8	2.87	1.77	2.23	1.33	3.98	.049 *

Table 4
Anova between non experts (*G1*) versus experts (*G2*) for each passwords comparison of Table 3 (*: significance level reached).

passwords, 41.90% of participants believed attackers would try commonly used passwords, while 33.20% thought attackers would use words and names familiar to the participant's native language. However, a significant proportion (66.40%) admitted to consistently using the same password, often incorporating commonly used words.

External Stimuli. An intriguing finding from our study was related to a specific survey question which considered possible correlations between the name of a website and the corresponding login password. 84% of the respondents expressed concerns about the security of such a practice, however, a contrasting 24% created passwords closely related to the specific website name. Furthermore, we noted that 6.91% of the participants used identical passwords across all three websites despite their initial security concerns. Additionally, 13% of the respondents answered negatively when we asked if they often use the same password, and 62.77% of those who admitted of reusing the same password for multiple accounts, created three different passwords for the various websites.

4.2.3. Expert Users

To answer to question RQ3, for each of the passwords asked in the questionnaire, we have decided to investigate the relationship between IT knowledge and the right view of password security. We expect expert users to be the most knowledgeable about how to choose good passwords. To assess the relationship between IT knowledge and password security, we performed a one-way ANOVA[2] test for each of the eight pair of passwords PW1 and PW2 of Table 3. We recall that PW2 is always more secure and values of answers range from 1 to 7, and 4 indicates that the passwords are equally secure.

The goal was to determine whether individuals with different levels of IT knowledge, specifically non experts (*G1*) versus experts (*G2*), exhibited significant variations in their ability to select secure passwords. Our null hypothesis (H0) posited that there would be no significant differences in password security perceptions between these two groups, while the alternative hypothesis (H1) suggested that significant differences would be present. An ANOVA analysis was conducted to examine differences between the password comparison (C1, C2,..,C8), and on the expertise of the participants as the dependent variable. The significance level (α) was set at 0.05. The results of our ANOVA analysis are summarized in Table 4. The C_n column lists the categories of elements that were compared between the two groups, G1 and G2. The G1 and G2 (M and SD) columns provide the means (M) and standard deviations (SD) of the category values for the two groups. For example, in the row for category C1, for group G1, the mean is 3.81 with a standard deviation of 1.53, while for group G2, the mean is 4.20 with a standard deviation of 1.53. The F-value column contains the F-values calculated from the analysis of variance (ANOVA) and determines whether group means are equal. In one-way ANOVA, the F-value is the ratio between variation between sample means and variation within the samples. ANOVA assesses whether there

[2]ANOVA (Analysis of Variance) is a statistical test used to determine whether there are significant differences between the averages of three or more independent groups by comparing the variations between them with the variations within the groups themselves.

are significant differences between group means, higher values indicate greater differences between groups. For example, for category C7, the F-value is 4.89. The test included 1 degree of freedom between groups (numerator) and 97 degrees of freedom within groups (denominator), where 97 corrisponds to the summation between the experts users (N=44) and non experts users (N=54) - 1. The p column contains the p-values associated with the significance tests conducted by ANOVA. The p-value is the probability of obtaining a result equal to or more extreme than the observed one, assuming the null hypothesis is true. In this context, a low p-value (typically less than 0.05) indicates that the differences between groups are statistically significant. For example, for category C7, the p-value is 0.029, indicating statistical significance at a 95% confidence level. When the p-value is less than $\alpha = 0.05$, it's indicated with an asterisk (*) to emphasize the significance of the difference. As seen in the table, the ANOVA analysis revealed that for passwords C1 through C6, there were no statistically significant differences between experts and other participants concerning their ability to select secure passwords. However, for passwords C7 and C8, the results were different. In the case of C7, expert users answered more correctly, while for C8, the result was opposite.

5. Discussion

We analyzed breach data and questionnaire results, addressing our research questions. For our first query, we identified prevalent usage patterns, commonly used symbols in passwords, and predominant password categories. Surprisingly, despite the diversity of languages used, common structures persisted. Regarding our second question, we uncovered numerous misconceptions surrounding factors believed to enhance password complexity. Finally, our investigation into the third question revealed that misconceptions about password security techniques extend even to those with substantial expertise in computer science. In the subsequent paragraphs, we delve into each question's findings.

RQ1: Which are the most common patterns and word categories used for password creation, and do they depend on the used language? Several important considerations emerge from the analyses conducted on the methods of constructing passwords and the related composition schemes. First, password pattern analysis highlighted various techniques users use to create their credentials even when they are asked to follow standard password policies. These techniques include combining letters, numbers, and symbols and more complex strategies such as adding, inserting, and repeating elements within passwords. In particular, the use of insertions, both through adding digits and symbols within common words and through approaches such as password munging, suggests a wrong awareness on the part of users of the importance of creating longer passwords and complexity to increase security. Another significant discovery is adopting practices such as replacing letters with symbols or numbers, as in the case of Leetspeak or Faux Cyrillic. While these techniques seem to broaden the complexity of the password, they do not improve it. Additionally, observing repetition patterns indicates that many users use common or recurring sequences to create their passwords. This behavior makes such passwords more easily guessable and vulnerable to dictionary-based or brute-force attacks. Regarding the difference in patterns used in different languages, it was observed that the password pattern in both Spanish and German is not significantly different from that in English.

RQ2: How does user cognition impact password security and usage? We investigated users' tendency to rely on easily memorable passwords due to fear of forgetting them, despite understanding the attributes of strong passwords. However, they lack substantial guidance on improving password security. Users often overestimate the effectiveness of symbols and numbers, underestimating the predictability of common patterns. For instance, passwords like `p@ssw0rd` are perceived as strong but remain vulnerable. Similarly, `punk4life` is weak due to predictable substitutions, while `ieatkale88` is stronger than `iloveyou88` but still vulnerable to dictionary attacks. Passwords like `astleyabc` and `astley123` receive similar ratings despite differences in character sets. Using uncommon words like `rtxe` is becoming popular, but these passwords still lack entropy. Numeric-only passwords and common patterns result in weak security. Overall, users need more guidance on choosing secure passwords, considering both common misconceptions and emerging trends. The authors of [53] found

similar results, identifying four main misconceptions. Users tend to believe that adding digits inherently enhances security, underestimate the impact of substituting digits or symbols for letters, overrate the security of keyboard patterns, and underestimate the prevalence of common words or phrases in passwords. These misconceptions contrast with current password-cracking capabilities, highlighting the need for improved understanding of password security among users. Our study delved deeper to investigate whether even experienced users made the same errors.

RQ3: Are there differences between experts and regular users? We have shown some user misconceptions and we have highlighted how IT knowledge does not directly correspond to a correct attitude towards IT security. The results highlight that expert users evaluate only one password comparisons correctly while in the other cases they gave similar, if not weaker, ratings on average than non-expert users. Specifically, in one comparison, they predominantly selected the incorrect password w.r.t. to individuals from varied backgrounds. The results of our questionnaire are different and offer new insights compared to the findings of a previous study on a similar topic (e.g. [53]). Inexperienced users tend to pay more attention to detail, while experienced users often engage in energy-saving behavior, focusing solely on the ultimate goal of site registration, which may lead them to neglect security concerns.

6. Recommendations and Conclusions

The paper delves into how human attitudes affect password creation, analyzing various data leaks to identify common patterns. A questionnaire was conducted to understand user perceptions and behaviors. Upon analyzing data from known data leaks and a recently created questionnaire, it has become apparent that despite the passage of time, the methods for creating passwords have remained unchanged. Even with the implementation of password policies, users still find ways to circumvent them and rely on predictable patterns. Additionally, even those who claim to be experienced in educating others on proper password usage have not demonstrated a complete understanding of the issue.

Our research underscores psychology's potent influence on password creation and security, offering strategies for promoting robust passwords. Password policies must prioritize length and diversity, avoiding common patterns attackers exploit. Avoiding dictionary words is crucial, despite the challenge. Admins can enhance security by categorizing accounts based on user interaction levels and offering guidance on password choices. Monitoring user patterns and banning vulnerable ones can mitigate risks. Psychological factors like cognitive dissonance contribute to users' password mistakes, which can be addressed through techniques like neutralization, as identified by [58].

Future developments could focus on guiding users to strengthen passwords and improving systems to overcome neutralization. Suggestions include auto-completing passwords, enhancing password meters, and developing adaptive policies for usability. Continuous questionnaires could be employed to assess memory retention.

Acknowledgments

The authors would like to thank all the anonymous participants to the questionnaire. This work is partially supported by projects "SEcurity and RIghts In the CyberSpace - SERICS" (PE00000014 - CUP H73C2200089001), "Interconnected Nord-Est Innovation Ecosys- tem - iNEST" (ECS00000043 - CUP H43C22000540006), and PRIN/PNRR "Automatic Modelling and ∀erification of Dedicated sEcUrity deviceS - AM∀DEUS" (P2022EPPHM - CUP H53D23008130001), all under the National Recovery and Resilience Plan (NRRP) funded by the European Union - NextGenerationEU.

References

[1] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, J. Lopez, Guess again (and again and again): Measuring password strength by simulating password-

cracking algorithms, in: 2012 IEEE Symposium on Security and Privacy, 2012, pp. 523–537. doi:10.1109/SP.2012.38.

[2] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, Of passwords and people: Measuring the effect of password-composition policies, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11, Association for Computing Machinery, New York, NY, USA, 2011.

[3] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, L. F. Cranor, Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks, in: 25th USENIX Security Symposium, USENIX Association, 2016, pp. 175–191.

[4] A. Narayanan, V. Shmatikov, Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, 2005, p. 364–372. Https://doi.org/10.1145/1102120.1102168.

[5] D. Pasquini, A. Gangwal, G. Ateniese, M. Bernaschi, M. Conti, Improving password guessing via representation learning, in: 42nd IEEE Symposium on Security and Privacy, IEEE, 2021, pp. 1382–1399. Https://doi.org/10.1109/SP40001.2021.00016.

[6] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation, in: Proceedings of the 21th USENIX Security Symposium, USENIX Association, 2012, pp. 65–80. Https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur.

[7] A. M. Di Campi, R. Focardi, F. L. Luccio, The revenge of password crackers: Automated training of password cracking tools, in: V. Atluri, R. Di Pietro, C. D. Jensen, W. Meng (Eds.), Computer Security – ESORICS 2022, Springer Nature Switzerland, Cham, 2022, pp. 317–336.

[8] D. Pasquini, M. Cianfriglia, G. Ateniese, M. Bernaschi, Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries, in: 30th USENIX Security Symposium, USENIX Association, 2021, pp. 821–838. Https://www.usenix.org/conference/usenixsecurity21/presentation/pasquini.

[9] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, R. Shay, Measuring Real-World Accuracies and Biases in Modeling Password Guessability, in: Proceedings of the 24th USENIX Conference on Security Symposium, USENIX Association, 2015, p. 463–481.

[10] H. Habib, J. Colnago, W. Melicher, B. Ur, S. Segreti, L. Bauer, N. Christin, L. Cranor, Password creation in the presence of blacklists, in: Workshop on Usable Security, USEC, volume 17, 2017.

[11] S. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor, S. Egelman, Of passwords and people: measuring the effect of password-composition policies, in: Proceedings of the sigchi conference on human factors in computing systems, 2011, pp. 2595–2604.

[12] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, L. F. Cranor, Can long passwords be secure and usable?, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2014, pp. 2927–2936.

[13] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, B. Ur, A spoonful of sugar? the impact of guidance and feedback on password-creation behavior, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015, pp. 2903–2912.

[14] L. Festinger, Cognitive dissonance, Scientific American 207 (1962) 93–106.

[15] A. M. Di Campi, Password guessing: learn the nature of passwords by studying the human behavior (2021).

[16] M. Siponen, P. Puhakainen, A. Vance, Can individuals' neutralization techniques be overcome? a field experiment on password policy, Computers & Security 88 (2020) 101617.

[17] T. Groß, K. Coopamootoo, A. Al-Jabri, Effect of cognitive depletion on password choice, in: The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016), 2016, pp. 55–66.

[18] R. F. Baumeister, E. Bratslavsky, M. Muraven, D. M. Tice, Ego depletion: Is the active self a limited

resource?, Journal of personality and social psychology 74 (1998) 1252.
[19] R. Wash, E. Rader, R. Berman, Z. Wellmer, Understanding password choices: How frequently entered passwords are re-used across websites, in: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), 2016, pp. 175–188.
[20] D. Nelson, K.-P. L. Vu, Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords, Computers in Human Behavior 26 (2010) 705–715.
[21] T. F. Brady, T. Konkle, G. A. Alvarez, A. Oliva, Visual long-term memory has a massive storage capacity for object details, Proceedings of the National Academy of Sciences 105 (2008) 14325–14329.
[22] C. L. Grady, A. R. McIntosh, M. N. Rajah, F. I. M. Craik, Neural correlates of the episodic encoding of pictures and words, Proceedings of the National Academy of Sciences 95 (1998) 2703–2708. doi:10.1073/pnas.95.5.2703. arXiv:https://www.pnas.org/doi/pdf/10.1073/pnas.95.5.2703, https://www.pnas.org/doi/abs/10.1073/pnas.95.5.2703.
[23] G. Lu, N. Sebe, C. Xu, C. Kambhamettu, Memory efficient large-scale image-based localization, Multimedia Tools and Applications 74 (2014) 479–503. doi:10.1007/s11042-014-1977-3.
[24] D. Marks, Visual imagery differences and eye movements in the recall of pictures, Perception & Psychophysics 14 (1973) 407–412. doi:10.3758/BF03211175.
[25] D. L. Nelson, V. S. Reed, C. L. McEvoy, Learning to order pictures and words: A model of sensory and semantic encoding., Journal of Experimental Psychology: human learning and memory 3 (1977) 485.
[26] L. Standing, J. Conezio, R. N. Haber, Perception and memory for pictures: Single-trial learning of 2500 visual stimuli, Psychonomic science 19 (1970) 73–74.
[27] C. Merrick, M. Farnia, T. K. Jantz, A. Gazzaley, E. Morsella, External control of the stream of consciousness: Stimulus-based effects on involuntary thought sequences, Consciousness and Cognition 33 (2015) 217–225.
[28] G. Matthews, L. Dorn, Cognitive and attentional processes in personality and intelligence, in: International handbook of personality and intelligence, Springer, 1995, pp. 367–396.
[29] L. Bošnjak, J. Sreš, B. Brumen, Brute-force and dictionary attack on hashed real-world passwords, in: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1161–1166. doi:10.23919/MIPRO.2018.8400211.
[30] B. Hitaj, P. Gasti, G. Ateniese, F. Pérez-Cruz, PassGAN: A Deep Learning Approach for Password Guessing, in: Int. Conference on Applied Cryptography and Network Security, volume 11464 of *LNCS*, Springer, 2019, pp. 217–237.
[31] D. Wang, Z. Zhang, P. Wang, J. Yan, X. Huang, Targeted online password guessing: An underestimated threat, in: Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, ACM, New York, USA, 2016, p. 1242–1254. Https://doi.org/10.1145/2976749.2978339.
[32] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, L. F. Cranor, "i added '!' at the end to make it secure": Observing password creation in the lab, in: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), USENIX Association, Ottawa, 2015, pp. 123–140. Https://www.usenix.org/conference/soups2015/proceedings/presentation/ur.
[33] M. Golla, B. Beuscher, M. Dürmuth, On the security of cracking-resistant password vaults, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, Association for Computing Machinery, New York, NY, USA, 2016, p. 1230–1241. doi:10.1145/2976749.2978416, https://doi.org/10.1145/2976749.2978416.
[34] K. Blashki, S. Nichol, Game geek's goss: Linguistic creativity in young males within an online university forum (94//3 933k'5 9055oneone), Australian Journal of Emerging Technologies and Society 3 (2005).
[35] H.-C. Chou, H.-C. Lee, H.-J. Yu, F.-P. Lai, K.-H. Huang, C.-W. Hsueh, et al., Password cracking based on learned patterns from disclosed passwords, IJICIC 9 (2013) 821–839.
[36] W. Li, J. Zeng, Leet usage and its effect on password security, IEEE Transactions on Information

Forensics and Security 16 (2021) 2130–2143.
[37] N. Ross, Writing in the information age, English Today 22 (2006) 39 – 45. doi:10.1017/S0266078406003063.
[38] M. Weir, S. Aggarwal, B. de Medeiros, B. Glodek, Password cracking using probabilistic context-free grammars, 2009, pp. 391–405. doi:10.1109/SP.2009.8.
[39] D. L. Wheeler, zxcvbn:low-budget password strength estimation, in: 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 157–173.
[40] M. Vainer, Password Dataset Generation for Further Analysis by Machine Learning Methods, Ph.D. thesis, 2022. doi:10.13140/RG.2.2.16711.16805.
[41] R. V. Guimarães, An investigation of semantic patterns in passwords, 2013. URL: https://api.semanticscholar.org/CorpusID:51963378.
[42] Kali Linux, Rockyou dataset, https://gitlab.com/kalilinux/packages/wordlists, Accessed April 2022, 2013.
[43] Hotmail, Hotmail dataset, https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/hotmail.txt, Accessed April 2022, 2020.
[44] phpBB, phpbb dataset, https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/phpbb.txt, Accessed April 2022, 2019.
[45] Ashley Madison, Ashley madison dataset, https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/Ashley-Madison.txt, Accessed April 2022, 2020.
[46] pkLazer, 4000 Most common english words, https://github.com/pkLazer/password_rank/blob/master/4000-most-common-english-words-csv.csv, Accessed April 2022, 2013.
[47] Compute.io, Common english female name, https://github.com/datasets-io/female-first-names-en, 2015.
[48] Compute.io, Common english male name, https://github.com/datasets-io/female-first-names-en, 2015.
[49] PenTestical, Common german names, https://github.com/PenTestical/german_names, 2019.
[50] marcboquet, Common spanish names, https://github.com/marcboquet/spanish-names, 2012.
[51] E. I. Tatli, Cracking more password hashes with patterns, IEEE Transactions on Information Forensics and Security 10 (2015) 1656–1665.
[52] V. I. Levenshtein, Binary codes capable of correcting deletions, insertions, and reversals, Soviet physics. Doklady 10 (1965) 707–710.
[53] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, Do Users' Perceptions of Password Security Match Reality?, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16, Association for Computing Machinery, New York, NY, USA, 2016, p. 3748–3760. Https://doi.org/10.1145/2858036.2858546.
[54] Sant'Uberto, Tutto il mondo del cane in un click, https://cani.com/, 2023.
[55] Dvd-store, Dvd-store, 20 anni, 2003-2023, https://www.dvd-store.it/, 2003.
[56] Leonardo, Leonardo elicotteri, https://helicopters.leonardo.com/it/home, 2022.
[57] IBM, Ibm-spss, https://www.ibm.com/, 2024.
[58] G. M. Sykes, D. Matza, Techniques of neutralization: A theory of delinquency, American sociological review 22 (1957) 664–670.

A. Appendix

@	**8**	**(**	**6**	**3**	**#**	**9**	**#**	**1**	**!**	**<**	**1**	**i**	**;**	**0**	**9**	**5**	**$**	**+**	**>**	**<**	**%**	**?**	**uu**
a	b	c	d	e	f	g	h	i	i	k	l	ll	o	q	s	s	t	v	v	x	y	w	w

Table 5
Common substitutions generated using leetspeak.

Question	Response
Informations about participants	Table 8 reports the information
Do you often reuse the same password?	Yes 66.4%, No 33.6%
When you create a password you think it must be:	Easy to remember, safe, or both
If you think a password should be easy to remember it's because	I'm afraid to forget it 59.3%; all sites ask me for the same pattern so I don't want to waste time thinking about a new password 28.9%; when I think about a new password, one that I use often comes to mind 20.1%; I have no imagination 9.8%; doing "recover password" bothers me 23.2%
Do you frequently reuse passwords with variations like substituting letters with numbers or symbols?	Yes 64.5%, No 35.5%
Do you use password manager?	Yes 21.7%, No 78.3%
What is the pattern you use the most when creating a password?	Table 2a show participants' answers
Categories of words	Table 7 shows how many people answered that use the proposed category
Choose which of the two passwords is more secure in your opinion	Table 3 shows which passwords were perceived to be stronger and which actually were
Select who you believe is more likely to steal one of your passwords	A stranger 65.4%; a family member 24%; a friend 21.7%; a colleague 16.6%; other people I know 21.2%
What do you think a malicious user does to try to guess your password?	Uses software 73.3%; uses brute force 29.5%; tries the most used and known words and names in my language 33.2%; tries common passwords 41.9%; tries dates and numbers 38.7%
Why would an attacker try to guess your password?	Financial reward 44%; to collects personal information 73.6%; for identity theft 64.8%; fun / proof they can 35.2%; spamming 19.9%; espionage 20.8%
Enter a password for registration on this site (dog.com, cd.com, leonardo.com), Minimum 6 characters with lowercase, uppercase, symbols, and numbers. Enter a password at least 8 characters long with upper and lower case letters, numbers, and symbols.	Table 2b reports the results of the analysis we conducted on the responses

Table 6
Summarized questionnaire.

Categories on passwords	N
Names of relatives	167
Random numbers	62
Numbers that remind important events	55
Dates	51
Nicknames	36
Proper name	33
Pets names	26
Football team / names of footballers	26
Slang	18
Colors	16
Surnames	15
Band / singers names	13
Films	12
Others	35

Table 7
Categories of words used in password - Questionnaire.

Variable	N	%*
Participant to the questionnaire	222	
Valid submissions	217	
Gender		
– Female	96	44
– Male	120	55
– Others	1	1
– Missing	0	0
Age	M=30.46 Mdn=25	SD=11
Level of study	217	100
– Primary school	2	1
– Secondary school	12	6
– High school	92	45
– Bachelor's degree	80	37
– Master's degree	27	12
– Master	3	1
– Doctorate	1	1
High school	107	42
– Computer science	51	47
– Languages	19	18
– Scientific	5	5
– Others	32	30
Bachelor/ Master degree	111	49
– Computer science	44	40
– Languages	12	11
– Cultural heritage	8	7
– Engineering	8	7
– Economics	11	10
– Environmental sciences	6	5
– Others	22	20
Job	217	100
– Student	79	36
– Employee	58	27
– Headmaster	6	3
– Others	74	34
IT knowledge	217	100
– Basic	4	2
– Intermediate	27	12
– Autonomous	90	42
– Advanced	96	43

*Percentage does not have to give always 100% due to rounding.

Table 8
Sample characteristics of the questionnaire.