BİTLİS EREN ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

ISSN: 2147-3129 / e-ISSN: 2147-3188

Article Type : Research Article
Received : October 17, 2024
Revised : May 10, 2025
Accepted : May 29, 2025
DOI : 10.17798/bitlisfen.1569257

Year : 2025
Volume : 14
Issue : 3
Pages : 1306-1330

EVALUATION OF EFFECTIVE PASSWORD GENERATION PROCESSES IN TERMS OF CYBER SECURITY

İbrahim AYAZ [1,*], Muhammed Zekeriya GÜNDÜZ [2]

[1] *Bitlis Eren University, Department of Computer Science and Technology, Bitlis, Türkiye*

[2] *Bingöl University, Department of Computer Science and Technology, Bingöl, Türkiye*

**** Corresponding Author:*** *iayaz@beu.edu.tr*

ABSTRACT

The increasing frequency and sophistication of cyber-attacks have underscored the critical importance of strong, secure passwords in protecting digital identities. This study evaluates the effectiveness of password generation processes within the context of cyber security, focusing on various methods for creating secure passwords, from traditional alphanumeric combinations to advanced passphrases that incorporate special characters and multi-factor authentication. While long and complex passwords are essential for robust security, the research also emphasizes the importance of user awareness and consistent password management practices in mitigating risks. This study also emphasizes that information security cannot be achieved through technological solutions alone, highlighting the critical role of end-user cyber security awareness. Effective password generation and usage are central to safeguarding sensitive systems and data, and the article presents strategies for developing this skill, offering examples and suggestions to foster awareness and improve password security practices. We advocate for user-friendly yet secure password-generation techniques to strengthen cyber security resilience in the digital age.

Keywords: Cyber security, Data security, Secure password, Passphrase.

1 INTRODUCTION

The conveniences provided by technology to human beings are increasing day by day. The people of our age have achieved more comfortable living standards thanks to the technologies that have emerged as a result of cumulative knowledge. It is accepted that the discovery of the Internet is the biggest in terms of the convenience provided by technological developments to human life. Individuals who interact more with the Internet have made high-

security transactions such as shopping online using credit cards, making money transfers through Internet banking, and paying online bills an integral part of their daily lives. However, the widespread use of the Internet and its intertwining with daily life have brought information security risks. This makes the need to ensure the security of users' personal and financial information even more important. Therefore, Internet users need to be more aware of how to stay secure in the digital world [1]. Therefore, Internet users must adopt more conscious and proactive approaches, such as using strong passwords and implementing security measures like two-factor authentication. In this context, information security has become an unavoidable priority of the digital age.

Transactions carried out over the Internet require various layers of security depending on the system used. Elements such as username, password, virtual keyboard usage, and security code are the basic components that make up these layers. The first and most important step in ensuring security is to create passwords that are easy to remember but difficult to guess, and at the same time resistant to brute force and dictionary attacks. Weak passwords can be easily cracked by attackers in a variety of ways, which can lead to users' accounts being compromised. Therefore, creating strong passwords plays a critical role in ensuring digital security [2].

People need to keep many passwords in their memory to handle their transactions in the digital environment. The research shows that the average person has more than 20 passwords. If there is a password, it means that there is confidential information. If the information is hidden, the question of who it is being protected from also arises. These people try to guess passwords so that they can access the information [3].

Amico et al. [2], compare various password cracking techniques, including dictionary and brute force attacks by analyzing the relationship between search space and the number of cracked passwords. They have empirically shown that passwords that are not complex are much easier to crack. Nosenko et al. [4], by performing password guessing applications with Recurrent Neural Networks (RNN), they have been demonstrated that passphrases are more reliable. Jin et al. [5], demonstrated that weak passwords can be easily cracked using deep learning methods. Li et al. [6], experimentally show that passwords containing personal information can be cracked more easily than passwords that are meaningless.

Although passwords are the first line of defense against cyber attackers, people are too lazy to create strong passwords. Usually, the difficulty level of these passwords is simple. Weakly created passwords can be captured by cyber attackers in different ways. In this respect,

strong and reliable passwords should be produced by users, whether they are system administrators or end users. The purpose of a strong password is to increase the difficulty for cyber attackers to crack or guess it. In addition, one of the most important features of passwords is that they can be easily forgotten. If the users forget their passwords, it means that they cannot verify their identity for the relevant system [7]. This study aims to develop personalized algorithms for creating strong yet easily memorable passwords, which are among the most critical aspects of cyber security.

The remainder of this paper is organized as follows: Section 2 presents the importance of passwords in cyber security. Section 3 examines the features that a secure password should have and provides examples of secure and insecure passwords. Section 4 introduces more techniques for generating effective passwords. Finally, the results and suggestions are presented in Section 5.

2 PASSWORDS IN CYBER SECURITY

All digital or electronic activities, including network operations, are part of cyber space. Ensuring the security of cyber space is called cyber security. Security in cyber space starts with using robust passwords. A password is a confidential information that only two parties know. Thanks to this confidential information, the parties can identify each other as secure. The most effective method attackers use to gain unauthorized access to a system is compromising passwords.

The use of passwords dates back to Roman history. In Rome, guards would stop people trying to enter certain areas or buildings and ask for passwords. However, those who knew the password were allowed to enter there. Every day, the camp commander would give the guards a wooden tablet with the password on it. The guards would circulate this tablet among themselves and engrave their marks on it [8]. When the tablet returned to the commander, the commander knew all the guards had received the password. On a computer, passwords are almost as old as operating systems. The digital password system was first used in MIT's Compatible Time Sharing System in 1961. Since then, both creating and deciphering passwords has become a mutual race [1].

The most basic way to crack a password is to guess. Intelligent guesses can be instrumental in cracking many passwords, despite the low probabilities. Technology can't completely prevent user errors; Even the most advanced algorithms ultimately depend on the

password that the user creates. All passwords can be cracked, but passwords that are complex and long enough can be deterrent to low-skilled attackers. As the length and complexity of a password increase, its security and resistance to being cracked also increase. Strong passwords prevent third parties from accessing areas and information that require information privacy. A good password should be hard for others to guess, but easy for the user to remember. Passwords are personal and should not be shared. Only the related person needs to know. The generated passwords should be meaningless to others. Different passwords should be used for different types of accounts [9].

The widespread use of Internet-based applications has led to an increase in the number of passwords used. The first step in ensuring these passwords and data privacy by users is to create effective and reliable passwords. In this context, basic-level secure passwords should consist of a combination of uppercase letters, lowercase letters, numbers, and special characters/punctuation marks. Because the more different types of characters there are in the password, the harder it is to guess the password. The basic requirements for a strong password are shown in Figure 1.

Moreover, it is recommended to pay attention to the following principles when creating a secure password:

- Must be at least 8 characters long.
- Passwords should not contain consecutive or identical expressions such as 123456 , abcdef, qwerty, asdf, XXX, or ababab.
- It should not be short or consist of a single word such as Bitlis, Bingöl, Galatasaray.
- Expressions that identify the person such as name, surname, and date of birth should not be used.
- Words that can be found by a dictionary scan attack should not be used.
- Words and phrases that are easy to remember, but difficult for others to guess, should be chosen.
- Information that is directly related to the person's interests and life should not be used as passwords.
- If meaningful words are to be used as passwords, the words to be used should be abbreviated or some characters should be omitted.
- The same password should not be used for all accounts. However, since using different passwords in all accounts tire the human memory, the same password can be used in accounts with the same security level.
- The reliability of the accounts can be categorized as Very reliable – Reliable – Insecure, and a separate password can be used for each category.

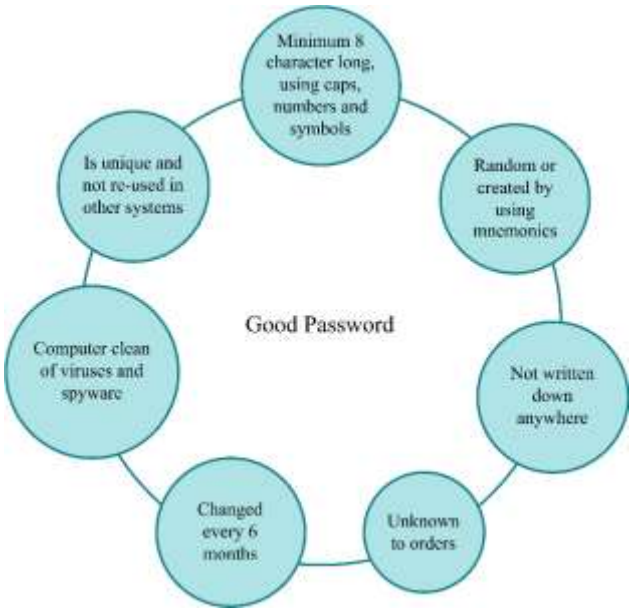


Figure 1. Key features of a strong password

In addition, it should be noted that after a password is created, the following points should be noted:

- It should be changed between 3-6 months.
- Passwords issued for temporary use should be changed immediately.
- Critical passwords should not be written down on paper or any other medium.
- Important passwords should not be given to a third party.
- The same password should not be used on all platforms.
- Logout should be done on the exited systems**.**

The reliability of a password can be measured by taking into account some key factors such as password length, character variety, predictability, resistance to brute force and dictionary attacks, and the use of the password in different environments. Online password check tools can be useful for testing password security and creating strong passwords. By analyzing how strong the password is, these tools estimate how resistant it is to different types of attacks. However, it is necessary to be careful about security when using such tools. In particular, entering the password directly on third-party websites can lead to potential security risks. For this reason, it is recommended to use a variation of the password during the test instead of using the full version of the password as a more secure method. Some of the online password check tools to measure password reliability stand out for their reliability [10].

How Secure Is My Password: This site evaluates the security of the password by estimating how long it will take to crack it. With a simple interface, this tool shows how resistant

the password is to brute force attacks. However, since the password is entered directly, it is better to be careful for security and avoid using the full password [11].

Kaspersky Password Check: This password checker provided by Kaspersky analyzes how strong the password is and points out its weaknesses. It also shows the estimated time it took to crack the password and how secure the character combination is [12].

NordPass Password Strength Test: This password testing tool analyzes the strength of the password and shows its weaknesses. It also offers recommendations for creating strong passwords and shares strategies that can be used to improve password security [13].

Bitwarden Password Strength Tester: It is a popular password management software and offers powerful password generation tools. This tool evaluates the security of the password and indicates whether the password is weak, medium, or strong. It also offers suggestions for creating a more secure password [14].

LastPass Password Strength Checker: LastPass is a platform known for its password management tools and offers a testing tool that analyzes how secure the password is. This tool identifies the weaknesses of the password and provides security recommendations [15].

3 PASSWORD SECURITY

It can be difficult for an attacker to technically break through a system. However, capturing the user's password is a more practical solution. Hackers use data from previous attacks and complex algorithms rather than making random attempts to crack passwords. It is the responsibility of users and software developers to increase security against this situation.

3.1 Features and Examples of a Secure Password

Passwords are for personal use. It should not be shared with others. At least two-step verification should be used. The security question, if any, must be complex. A secure password should be both long and contain a wide variety of characters. The reference [16] can be used to find out whether the passwords to be created are included in the dictionaries used for password attacks.

A password is like a toothbrush. No one else is allowed to use it. It must be changed every six months. Doing more than one thing at the same time with a single password (such as PC, mail, server, and VPN access passwords) means single sign-on (entering everything with a

single password), and this is a troublesome approach in terms of security. Because losing the password means losing everything. Developing different password algorithms is the most appropriate solution to this. In addition, all the passwords saved by a web browser can be easily intercepted by someone who obtains the computer's public password [17].

The length of the password makes the password strong. However, it is not always valid to say, "Long passwords are always more reliable than short passwords." Because password length is only one factor that affects security. A strong password should be meaningless but easy to remember. By taking the first letters of the lyric " şu gelen atlımıdır yavrum sorun Bağdatlımıdır ", a meaningless but easy-to-remember password can be created in the form of "şgaysB". However, a strong password should consist of letters, numbers, and symbols. Therefore, an important date or number can be combined with this password. If the number 1453 is shifted by one from the beginning and written between the expression "şgaysB", the result is the expression "1ş4g5a3ysB". If a special character is added at the end of the expression, the password '1ş4g5a3ysB?' can be created. In some cases, the password can be made even more complex by taking advantage of character similarity (such as a and @) to make the password '1ş4g5@3ysB?'.

Another example is that the password to be created on the shopping site can be chosen as a sentence such as "Ben Sabah Alışveriş Yaparken Okuldan Tanıdığım Eski Bir Arkadaşımı Gördüm" that will remind you of that site or shopping. The initials of these words are taken: BSAYOTEBAG, and then some letters can be replaced with numbers that remind them of themselves: 8SAY0TE1A6, and the last uppercase letter is replaced with lowercase letter: 8SAY0TE1a6, finally a symbol can be added at the end: 8SAY0TE1a6!

Another method is recommended to help users create passwords that are easy to remember but difficult to guess. A unique password is created with numbers and letters using a familiar phrase. For example, the phrase " Arkadaşlarım Tekin ve Yasemin bana her gün komik bir e-posta gönderiyor " can be converted to a password such as "ATvYbhgk1e-pg" by adding numbers with each letter and initial. This process is repeated for each site, creating strong and memorable passwords.

Various methods exist for generating passwords that are both secure and easy to remember. One widely employed technique is the use of mnemonics, which enhances memory retention through associations, such as rhymes or acronyms [18]. For instance, consider the well-known phrase:

“To be or not to be? That is the question.” (Hamlet, Shakespeare). This can be transformed into a mnemonic password: “2bon2b?Titq.”

In another example, numbers substitute similar-sounding words (e.g., "to" is represented as "2"), acronyms are utilized, capitalization is applied to key nouns and verbs, and prefixes are maintained in lowercase. “I had a DREAM, where all men were born equal” (Martin Luther King Jr.). This phrase may be condensed into: “1haDwamwb=”

These methods yield passwords that may appear random to others yet remain relatively easy for the creator to remember, given the underlying logic of their construction.

Additional strategies for enhancing password complexity include:

- Substituting numbers for similar-looking letters: For example, replacing "i" or "l" with "1" and, "o" with "0"
- Abbreviating words with numbers: Such as transforming "four" into "4" and, "to" or "too" into "2"
- Incorporating symbols or emoticons: For instance, "Are you happy today?" as “ru:-)2d?”

These examples illustrate fundamental techniques, and users are encouraged to personalize their mnemonic systems to devise strong, memorable passwords. Developing individualized coding methods is advisable to further enhance security.

3.2 Password Cracking Methods

In most cases, passwords reflect something easy to remember. However, guessing a password by having personal information about the user is the most common method of compromising a system for motivated hackers.

Using of passwords is of great importance in protecting the confidentiality of data and systems. When used correctly, they are one of the most effective methods of protecting the system, but sometimes they are the weakest aspects of network systems. Because the fact that passwords are somehow learned by third parties can provide them with a lot of authority. If certain principles regarding passwords are not followed and some precautions are not taken, they can be intercepted by attackers. Attackers can test hundreds of passwords per second with specially prepared password-cracking software [19].

Passwords are widely used to force access to resources. Attackers use many techniques to learn users' passwords and gain unauthorized access to a resource or data. Many of the most

common cyber attacks today are based on social engineering. It is also possible for system passwords to fall into the hands of third parties through social engineering methods based on human weaknesses. It is now a known fact that passwords can be obtained through social engineering, also known as directing people to do what is desired by someone else [20]. According to Kevin Mitnick, one of the first hackers, the weakest link in a system's security ring is the human. In this case, it is very important to inform users against attacks using social engineering and to ensure that information security awareness is created. It is clearly understood that this is a necessity, especially considering the active use of information systems in every field [21].

Some methods, also known as cryptographic password attacks, are used to aim to decrypt passwords. Brute force attack refers to the method of attempting to guess a password by systematically trying all possible combinations. These attacks are typically used to capture passwords, usernames, or other authentication credentials. This approach often involves using an electronic dictionary to test every word within it. While this process would be time-consuming for a human, a computer can execute it within seconds. Consequently, if a password is a correctly spelled dictionary word, it can be compromised within minutes through a brute force attack.

Users often choose words that make sense to keep them in mind. However, there is usually no need for brute force, i.e. trying all potential character combinations one by one. Dictionary attacks can find passwords in less time and with fewer attempts. Dictionary attacks also try meaningful words. A brute force attack is the most commonly used method to obtain valid passwords for servers or personal devices. That's why passwords shouldn't be simple [22]. Especially servers with open ssh service have serious problems in this regard. Password attacks are carried out by malware-infected devices rather than directly by individuals.

The crudest method that a hacker trying to crack a password can resort to is to try all possibilities one by one. Therefore, the greater the number of possible passwords, the more difficult the hackers' job. When subscribing to a website, the system may not accept the password that it describes as weak and may direct the user to set a stronger password. For example, it may require that the password contain at least one uppercase letter, one number, and one punctuation mark. Such requirements are implemented to improve user security and complicate the password-cracking process of hackers. As the variety of characters used to create a password increases, the number of possible password combinations also increases [23].

Brute force attacks can be categorized into several types, each employing different strategies to gain unauthorized access to systems or accounts. One of the most basic forms is the *simple brute force attack,* where an attacker systematically attempts every possible combination of characters from a specified character set. This method relies solely on computational power to eventually find the correct password or encryption key, making it time-consuming, especially as the length and complexity of the password increase. While guaranteed to succeed eventually, this approach is often impractical due to the vast number of combinations that must be tested.

A more refined method is the *dictionary attack,* which utilizes a predefined list of words or phrases, known as a "dictionary." Instead of attempting every possible combination, the attacker tries each entry in the dictionary, targeting likely candidates based on common user behavior. The dictionary often includes common passwords, variations, and phrases that users are likely to select. This method is significantly more efficient than a simple brute force attack, as it focuses on probable passwords rather than all potential combinations.

The *hybrid brute force attack* combines elements of both dictionary and simple brute force attacks. In this approach, attackers take words from a dictionary and apply variations, such as adding numbers, and symbols, or changing letter cases. For instance, they might attempt passwords like "password," "Password1," and "P@ssw0rd." This method effectively targets users who modify simple words slightly to meet complexity requirements, increasing the chances of successful exploitation.

Another type is the *reverse brute force attack,* where the attacker starts with a known password and attempts to find the corresponding usernames or accounts associated with that password. This approach is particularly effective if the attacker knows or suspects that a specific password is commonly used. By leveraging previously compromised data or widely used passwords, attackers can quickly identify valid accounts, making this method a potential threat.

Credential stuffing is another common brute force attack method, where attackers use previously leaked username-password pairs from data breaches to gain unauthorized access to accounts on different websites. This method exploits users' tendency to reuse passwords across multiple platforms. Once the attacker possesses a valid pair, they can access the target account quickly and efficiently, often without requiring sophisticated techniques.

In a *distributed brute force attack,* attackers utilize multiple machines or a botnet to increase their computational power for guessing passwords. By distributing the workload across

many devices, attackers can attempt a significantly larger number of combinations in a shorter time frame. This method enhances the effectiveness of brute force attacks and makes detection more challenging, as the attempts may come from numerous sources simultaneously.

Online brute force attacks involve directly attempting to log into an account on a target system or website by submitting password attempts in real-time. This method carries a higher risk for attackers, as it may trigger security mechanisms such as account lockouts or CAPTCHA challenges after a certain number of failed login attempts. In contrast, *offline brute force attacks* target hashed passwords stored in databases. Attackers obtain a database of hashed passwords (often through data breaches) and attempt to crack them by guessing the original passwords at their own pace without triggering immediate security responses.

To defend against brute force attacks, organizations and individuals should implement various security measures. Enforcing strong password policies that require complex passwords can significantly reduce the likelihood of successful attacks. Additionally, account lockout mechanisms that temporarily disable accounts after a specified number of failed login attempts can thwart attackers' efforts. Implementing multi-factor authentication (MFA) adds another layer of security by requiring additional verification methods beyond just passwords. Monitoring systems that can detect and alert administrators to suspicious login attempts are also essential. By employing these strategies, the effectiveness of brute force attacks can be significantly diminished, safeguarding sensitive information and maintaining secure systems.

Dictionary attack is a type of cyber-attack in which an attacker attempts to gain unauthorized access to a system by systematically trying a list of common words or phrases, typically stored in a "dictionary" file. Unlike brute force attacks, which try all possible character combinations, dictionary attacks rely on pre-compiled lists of likely passwords such as common words, names, and common phrases. These lists often include variations with numbers, symbols, and capitalization, making the attack more efficient. The effectiveness of dictionary attacks stems from the fact that many users choose weak or predictable passwords based on common words, making their accounts vulnerable to such attacks. Hackers often use dictionary attacks in combination with data from previous breaches, where they may refine the word lists to include passwords commonly used by people [24].

There are several types of dictionary attacks, each employing different techniques to exploit weak passwords. The most basic form is the *standard dictionary attack,* where attackers use a predefined list of common words, phrases, or known passwords in an attempt to guess a

user's password. This list typically includes dictionary words, names, or easily guessed passwords like "password123" or "qwerty." The attacker systematically tries each word or phrase until they find a match, making it an effective method against users who rely on simple, predictable passwords.

A more advanced variation is the *hybrid dictionary attack,* which combines elements of both dictionary and brute force methods. In this approach, the attackers take the words from a dictionary and applies variations such as adding numbers, special characters, or changing capitalization such as "Password123!". This technique accounts for users who slightly modify simple words to meet password requirements, thus increasing the chances of success.

The *reverse dictionary attack* targets hashed passwords. In this method, attackers compute hash values for every word in their dictionary and compare them to the hash of the target's password. If the hash values match, the original password is discovered. This attack is particularly effective against systems that use weak or unsalted hashing algorithms, as it allows attackers to reverse-engineer the password from its hash.

A *rainbow table attack* is a specialized form of dictionary attack that uses precomputed tables of hash values for common passwords. By leveraging these tables, attackers can compare hash values to plaintext passwords more efficiently, significantly reducing the time needed to crack weakly protected systems. Rainbow tables are particularly effective against systems that use predictable or weak password hashing mechanisms.

Another variation is the *phonetic dictionary attack*, which focuses on passwords derived from how words sound rather than their exact spelling. Attackers generate phonetic variations of dictionary words, anticipating that users may create passwords based on the pronunciation of words such as "Luv" for "Love". This method exploits the tendency of users to rely on familiar, easy-to-remember passwords.

In a *targeted dictionary attack*, the attacker customizes the dictionary based on the victim's personal information. By using words related to the victim's interests, names of family members, birth dates, or other personal details, attackers can increase the likelihood of success. These attacks often rely on social engineering to gather relevant personal information, creating a tailored word list specific to the victim.

Finally, a *distributed dictionary attack* involves multiple computers or bots working together to distribute the computational load of a dictionary attack across several machines. This significantly speeds up the process of trying password combinations and reduces the

likelihood of detection. Distributed attacks are often conducted using botnets, allowing attackers to perform large-scale attacks with greater efficiency.

To counter these attacks, users and organizations must employ a variety of security measures. Password complexity requirements, such as using a mix of letters, numbers, and special characters, can reduce the effectiveness of dictionary attacks. Salting passwords - adding random data to passwords before hashing - also helps by preventing precomputed attacks like rainbow tables. Additionally, implementing account lockout policies can block repeated login attempts after a set number of failures, thwarting dictionary and brute force attempts. Finally, multi-factor authentication (MFA) adds another layer of security beyond just a password, and using password managers encourages the creation and storage of complex, unique passwords that are difficult to guess.

Password cracking software can create and test combinations of letters and numbers in a certain order, as well as use words in dictionaries of hundreds of thousands of words given to them. That's why passwords that are easy to remember are usually easy to obtain. The fact that the password or passwords of a user are in the hands of second parties does not only create a security vulnerability for that user. Sometimes, other points on the network can be accessed through the password or password in question. Even if only one user creates an information security vulnerability, it can unwittingly cause damage to the network or all users using the system. Brutus, RainbowCrack, Wfuzz, Cain & Abel, and John The Ripper are prominent tools used for password cracking through brute force and dictionary attack methods.

4 SECURE PASSWORD GENERATION METHODS

Secure password policies should be established to prevent passwords in network systems from falling into the hands of attackers. Network users should be encouraged to use passwords that are difficult to guess or crack, and if necessary, they should be enforced. It should be known that passwords with different characters and numbers are more secure because they will take years to crack.

4.1 Secure Password Generator Software

To better protect systems and data, it's important to understand what a strong password is and how to store it securely. One of the main problems with password security is that users use the same password on multiple platforms. This increases security risks and compromises all accounts of users in the event of a possible attack. However, thanks to password generation

and management software, it is possible to store and manage all passwords securely [25]. Secure password generation software is essential for creating strong, unique passwords that enhance security against unauthorized access. These tools utilize complex algorithms and various character sets to produce passwords that are difficult to guess or crack. Here are some popular options:

LastPass is a widely used password manager that includes a built-in password generator. Users can customize password length and complexity, ensuring that passwords meet specific security requirements. Its integration with the LastPass vault allows for easy storage and retrieval [15].

Dashlane offers a comprehensive password management solution with a secure password generator. Users can create complex passwords and save them directly within the Dashlane vault. The tool also features a password strength assessment and is compatible with both web and mobile platforms [26].

Bitwarden is an open-source password manager that provides a robust password generator. Users can generate secure passwords that are stored in an encrypted vault. The tool includes a password strength meter and offers customizable options for password length and character types [14].

KeePass is an another open-source password manager that allows for secure password generation and credential management in an encrypted database. It supports various plugins and offers customizable settings for generating strong passwords. Notably, it works offline, providing users with secure access without an internet connection [27].

Random.org provides a simple online password generator that uses true randomness based on atmospheric noise. Users can specify the length and character types for password creation, making it a straightforward option without requiring software installation [28].

Online tools for generating strong passwords are user-friendly and efficient. They allow users to customize password length and character sets for instant, secure results, often without requiring an account. Passphrase generators create long, memorable phrases by combining multiple words, offering a balance of security and ease of recall.

Password-management software takes security further by generating and securely storing complex passwords. Users only need to remember a master password to access their encrypted password database. These lightweight programs, often portable, streamline password organization and usage. While initial setup may take some effort, the enhanced security and convenience make it worthwhile.

4.2 Setting a Password by Security Level

The purpose of creating a strong password is to make it difficult for cyber attackers to crack and guess. The strength of passwords is directly proportional to the complexity of the characters they contain. Some of the prominent problems are insufficient password length, low password complexity, and guessability of passwords.

The length and complexity of a password are crucial factors in determining how long it would take for a computer program to crack. Let's calculate the number of possible combinations a password cracker would need to try, assuming the password is composed only of lowercase English letters. For each character in a password, there are 26 possible choices (since there are 26 lowercase letters).

Password Length: 3

Calculation: $26^3 = 26 * 26 * 26$ =17.576 (Number of possibilities)

Password Length: 5

Calculation: 26^5 = 11.881.376

Password Length: 7

Calculation: 26^7 = 8.031.810.176

Password Length: 9

Calculation: 26^9 = 5.429.503.678.976

Now, if we expand the character set to include both digits and uppercase letters (increasing the total number of possible characters to 62), the number of variations increases dramatically:

Password Length: 3

Calculation: 62^3 = 238.328 (Number of possibilities)

Password Length: 5

Calculation: 62^5 = 916.132.832

Password Length: 7

Calculation: 62^7 = 3.521.614.606.208

Password Length: 9

Calculation: 62^9 = 13.537.086.546.263.552

Password cracking speed, a critical factor in assessing the security of a password, refers to the time it takes for a given method or tool to guess a password. To calculate password cracking speed, we can use the following formula:

$$Time\ to\ Crack = \frac{Total\ possible\ combinations}{Attempts\ per\ second} \quad (1)$$

To estimate the total possible combinations, we can use:

$$Total\ Possible\ \text{Combinations} = Character\ Set\ Size^{Password\ Length} \quad (2)$$

Assuming a modern PC processes 100.000 password attempts per second, we can estimate the time required to crack a password based on the number of possible combinations and the character set used (26 for lowercase letters, 36 for letters and digits, 52 for mixed-case letters, and 68 for letters, digits, symbols, and punctuation). Table 1 shows the results.

Table 1. The time required to crack a password depends on its length

Password Length	26 Characters	36 Characters	52 Characters	68 Characters
3	0.18 seconds	0.47 seconds	1.41 seconds	3.14 seconds
4	4.57 seconds	16.8 seconds	1.22 minutes	3.56 minutes
5	1.98 minutes	10.1 minutes	1.06 hours	4.04 hours
6	51.5 minutes	6.05 hours	13.7 days	2.26 months
7	22.3 hours	9.07 days	3.91 months	2.13 years
8	24.2 days	10.7 months	17.0 years	1.45 centuries
9	1.72 years	32.2 years	8.82 centuries	9.86 millennia
10	44.8 years	1.16 millennia	45.8 millennia	670 millennia
11	11.6 centuries	41.7 millennia	2.384 millennia	45.582 millennia
12	30.3 millennia	1.503 millennia	123.946 millennia	3.099.562 millennia

Based on these figures, a random password of at least 8 characters, using lowercase letters and digits, offers substantial protection. If the password is only 5 characters long, it could easily be cracked. Therefore, longer and more complex passwords are highly recommended to ensure better security.

It has been observed that simple passwords such as 12345, 123456, abcdef, password, abc123, 123456, abcdef, 000000, 20172017, ahmet2003, 5551234567, qwerty, asdf1234, 1970, 12345, abcd, 123abc are widely available in the databases of tools used for password cracking. Although they seem complicated passwords, even if they are so long, as long as they are meaningful, passwords like Firefox3beta5, 1453istanbul, murat124, a4tech, mplayer, bukadaruzunolsabileanlamlıolduğusürecetehlikevar, ubuntuwindowsudöver, 1919-05-19, komikinsanınkomikşifresi, forumpassword, debian4etch are insecure passwords.

High security does not necessarily mean that all passwords contain complex character sets. It is possible to group and simplify these passwords by determining the security levels of passwords according to their areas of use. For example, it is acceptable for passwords created for frequent use to be less complex than passwords created for accounts that require higher security. In this context, users should design their passwords considering the security needs of a particular system. Since systems requiring high security usually include access to sensitive information such as financial information, personal data or confidential documents, it is important for such passwords to be complex and strong. On the other hand, simpler passwords can be used for less critical accounts. Determining the security levels of passwords can both improve the user experience and make password management more effective. This approach increases the security of users and also supports the memorability of passwords. A three-level security approach is given below as an example.

Security Level - 1 (Insignificant)

Accounts such as forum sites, temporary accounts, and guest sessions can be included in the group with a low level of security. These types of accounts can be managed with a simple and single password, as they are usually designed for everyday use and do not cause serious problems when lost. By setting a short and easy-to-remember password for these accounts, users can speed up their transactions and provide ease of use. However, the use of such passwords on other accounts can increase security risks. Therefore, within the framework of basic security awareness, it is important to distinguish the passwords set for such accounts from the passwords created for more critical systems.

- Example 1: c*9080 (Containing all characters)
- Example 2: cy9080 (Containing only letters and numbers)
- Example 3: 909080 (Containing digits only)

Security Level - 2 (Important)

Systems that contain personal or sensitive information, such as computer logins, email accounts, and social media, are among the accounts with medium security requirements. It is recommended to create separate passwords for such accounts. Passwords must be between 6 and 8 characters (the length can be increased depending on user preferences) and may contain the user's individual information. For example, unique references such as "ba" for the province of Batman and "72" for the license plate can be used. This method both increases the memorability of passwords and strengthens security. However, such passwords mustn't be used on other accounts, as this can lead to security vulnerabilities.

- Example 1: b72*a73 (Containing all characters)
- Example 2: ba72ab6 (Containing only letters and numbers)
- Example 3: 72742024 (Containing only numbers)

Security Level - 3 (Very Important)

Systems that contain monetary or critical information, such as electronic cash registers and Internet banking, are among the accounts that require high security. It is recommended to create separate passwords for such accounts. Passwords must be at least 8 characters long and contain no meaningful phrases.

Users should choose complex passwords that use a combination of letters, numbers, and special characters. Although some systems require only numerical input, it increases security if passwords contain complex and meaningless phrases and are as long as possible. In addition, the use of both lowercase and uppercase letters will significantly improve the security of passwords. The fact that passwords are case-sensitive strengthens security even more. Therefore, it is necessary to pay attention to the methods of creating secure passwords for such accounts.

- Example 1: 3bd*35A=09 (Containing all characters)
- Example 2: mu44AZ8090 (Containing only letters and numbers)
- Example 3: 4490121444 (Containing only numbers)

Passwords are often forgotten or hard to recall, especially when managing many or unused for long periods. To mitigate this, users may write down passwords and store them

securely, such as in wallets, safes, or other private spaces. However, this method carries risks of loss, theft, or unauthorized access, requiring carefully safeguarding storage locations. Writing down passwords or storing them digitally can also be vulnerable to threats like keyloggers. To enhance security, users should avoid sharing passwords, refrain from using browser password-saving features, and update passwords regularly. Protecting passwords is as crucial as creating strong ones.

4.3 Setting Highly Secure Passwords

Strong passwords are essential for maintaining security and must meet four key requirements, prioritized by importance. Firstly, the password should be easily memorable for the user to ensure it can be easily recalled. Secondly, it should be challenging for others to guess, preventing unauthorized access. Thirdly, it must be resistant to automated guessing methods employed by programs, which often utilize dictionary attacks or brute force techniques. Finally, a strong password should exhibit complexity by incorporating a combination of numbers, symbols, uppercase, and lowercase letters. This multifaceted approach to password creation significantly enhances security and reduces the risk of unauthorized access [29].

Among the requirements for a strong password, the first - being easily memorable for the user - emerges as the most crucial. If a password can not be recalled, its effectiveness is undermined, regardless of its complexity or resistance to guessing. For instance:

#4ssFrX^-aartPOknx25_70!xAdk<d! exemplifies a strong password as it meets the criteria of being hard to guess by others or programs due to its complexity, which includes a mix of numbers, symbols, and both uppercase and lowercase letters. However, the intricate nature of this password renders it exceedingly difficult for an individual to remember. Thus, while complexity is essential, the ability to recall the password easily is paramount for ensuring consistent and secure access to accounts.

Using a mix of uppercase letters, numbers, and symbols is a basic method as it will make it more difficult for attackers to guess the generated password. Passwords such as A+214!, *+At13, 17!+A@k are examples of trusted passwords. M&y2ş<G7, b1/2d8Y{Oö, v^4+U?n8ç are examples of very reliable passwords. However, these passwords should be meaningful to the owner, as in the example below. So, it is more secure to use a passphrase rather than a password created with classical methods.

Arabamı severim. (passphrase)

Ar@b@mıs3verIm. (password)

a→@ , e→3, i→I (character change)

A simple security password can also be created by taking the initials of a randomly generated song phrase. "Armudun iyisini ayılar yerler." (aiay) This phrase is secure because it is not in the dictionary. To make this even safer, first letter can be capitalized and put a dot at the end (Aiay.)

The security of passwords depends on the variety of the character set used. A password is entered into the system via the keyboard and the keyboard characters are first decoded with ASCII codes. Today's standard keyboards usually contain 102 keys, which corresponds to approximately 102 ASCII codes. However, when shift keys such as SHIFT and ALT are used, this character set expands. While pressing the SHIFT key activates an additional 102 characters, the ALT key allows some special characters to be typed. In this case, the combination of normal characters with the SHIFT and ALTGR keys allows complex and strong passwords to be created. For example, a password such as "Ah*?3$" is created with such a combination and offers a high level of security. Therefore, the use of character variety and combinations when creating a password significantly increases security. In this context, the use of passphrases becomes inevitable for a password that is both easy to remember and difficult to crack.

4.4 Passphrases

Table 2 shows examples of passwords created as Normal, Good, and Best [21]. If the created passwords are not created according to a certain algorithm or structure, it may cause situations that are difficult to control for end users. Today, the use of passwords is used in many web applications such as e-government, education, health, and bank transactions. Various methods have been developed for the management of so many passwords, such as writing them on paper, using the same password everywhere, and using password management applications. However, it is known that these methods also contain security vulnerabilities. Although creating strong passwords is no longer a problem for conscious users thanks to awareness studies, remembering these passwords continues to be a problem. To solve this problem, the passphrase method, which is frequently used by people working in the field of Information Technologies (IT) but is not aware of by end users, is a permanent solution.

Table 2. Normal, Good, Best password examples [21]

Normal	Good	Best
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
Ilikemyschool	ILikeMySchool	!Lik3MySch001
Hightidenow	HighTideNow	H1gh7id3Now

Creating secure and memorable passwords plays a critical role in ensuring digital security. The only exception to the rule that a strong password should be meaningless but easy to remember is long meaningful sentences. For example, individuals can choose a meaningful proverb or idiom and use the first letters of each word of this phrase. Such an approach increases the complexity of the password while also increasing its memorability. In addition, a number that the user can easily remember, such as the year of birth, can be placed between these letters. To further strengthen the password, it would be useful to add a special character at the end. To concretize this method, we can take the example of the proverb " Rüzgar eken fırtına biçer ". The first letters of each word of this phrase are taken and a string is obtained in the form of "Refb". Then, the number 1983, the user's year of birth, is placed between these letters: "R1e9f8b3". Finally, adding a special character to the password will increase its security. For example, if a hash (#) sign is added, the result will be a password that is both strong and easy to remember, such as "R1e9f8b3#".

One effective way to create strong and memorable passwords is to use the first letters and numerical values of meaningful sentences. This method makes complex passwords easier to remember and harder to guess. For example, the phrase " Her sabah kahvemi iki şekerli içerim " can be used to create a password like "Hsk2şi". Similarly, personal information can be used by coding it into a regular structure. For example, the phrase " Kardeşim Ahmed 12 Nisan 2004 yılında doğdu " can be used to create a strong password like "KA12.N.2004yd"

A strong password should contain at least one uppercase letter, lowercase letter, number, and special character. It can sometimes be difficult to create and remember these passwords. For this, password phrases, which are password creation methods that are frequently used by employees in the IT sector but not known to end users, should be used. If the sentence " Benim annem bir melektir." is used as an example of creating a password with a password phrase, if the first two characters of each phrase are taken, the password "Bean1me." is obtained [21]. It

doesn't matter if the password is meaningless. The important thing is not to forget the password phrase. The password to be created should not be shared and the sentence should not be forgotten. The password should not be a dictionary word. It is more reliable to use a passphrase than a password created by classical methods.

A strong password should be personalized and meaningful to the user. It should be at least 8-20 characters long, incorporating a mix of uppercase and lowercase letters, numbers, and special characters. Interchanging these elements enhances complexity and makes the password difficult to guess. Additionally, the inclusion of at least one punctuation mark further strengthens its security. Different methods can be preferred to create an easy-to-remember passphrase. Passphrase examples created with different methods are presented below.

Passphrase: benim iki oğlum var [21]
Change: l→!, b→6, a→@, i→1, o→0, ğ→9, e→3, iki→2, var→V
Coded Password Phrase: 63n1m209!umV

Password phrase: Sivas1960Zara
Change: 9→g, i→1, 0→(), a→@, 1→!, Z→7
Coded Password Phrase: S1v@s!g6()7@r@

Password phrase: Hiç çekmediğin şutları yüzde 100 her zaman kaçıracaksın.
Changes: Write the first letters of the words in the passphrase with ending dot and also yüzde→%
Coded Password Phrase: Hçş%100hzk.

Password Phrase: Ayda 1 yetimleri ziyaret etmek için sevgi evine gider misin?
Changes: Write the first letters of the words and the rest is the same.
Coded Password Phrase: A1yzeisegm?

5 RESULT AND RECOMMENDATIONS

The importance of privacy in cyber security environment is a critical factor that directs individuals to create stronger and more secure passwords. End users feeling safe in the digital world is directly related to their ability to create strong passwords. Knowing how to make a password effective and strong is one of the cornerstones of this security process. The most important element that ensures the security of information is not legal regulations but the will

and awareness of individuals. Considering that every piece of information shared in the network environment leaves permanent traces, it is understood that individuals will need various tools, the skills to use these tools, and behavioral changes to protect themselves, their information, and their digital systems.

Teaching reliable password creation methods starting from secondary school is important for individuals to acquire a digital security culture at an early age. It should be emphasized that unique and complex passwords should be used, especially for important accounts such as e-mail and online banking. It is equally important to store passwords securely; these passwords should be kept in a secret area that belongs only to the owner and should be protected in a way that cannot be accessed by others. Critical account passwords in particular should be secret. Indeed, the principle of "what two people know is not a secret" constitutes the essence of security at this point.

In cases such as forgotten passwords or account lockouts, recovery methods come into play to provide access to accounts. Many platforms send a verification e-mail for password resets, and therefore it is of great importance that the recovery e-mail address is up-to-date and accessible. In addition, adding a phone number to profile information to increase account security makes it possible to receive a verification code via text message during password reset. Using a mobile phone number is a more reliable verification method compared to other recovery options because the device is physically in the individual's possession, making it a more secure identification tool than a secondary e-mail address or security questions. As a result, promoting effective password-generation techniques, and fostering a cyber security culture are critically important for maintaining security in the digital world.

Conflict of Interest Statement

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics.

Artificial Intelligence (AI) Contribution Statement

This manuscript was entirely written, edited, analyzed, and prepared without the assistance of any artificial intelligence (AI) tools. All content, including text, data analysis, and figures, was solely generated by the authors.

Contributions of the Authors

İbrahim AYAZ : resources, software, writing original draft, writing-review and editing.

M. Zekeriya GÜNDÜZ : resources, supervision, methodology, writing original draft, writing-review and editing.

REFERENCES

[1] C. Online, "Şifre güvenliği ve hack." https://www.chip.com.tr/haber/sifre-guvenligi-ve-hack_17955.html (accessed Oct. 11, 2024).

[2] M. Dell'Amico, P. Michiardi, and Y. Roudier, "Password strength: An empirical analysis," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5461951.

[3] U. Bodkhe, J. Chaklasiya, P. Shah, S. Tanwar, and M. Vora, "Markov model for password attack prevention," in *Proc. 1st Int. Conf. Computing, Communications, and Cyber-Security (IC4S 2019)*, P. K. Singh, W. Pawłowski, S. Tanwar, N. Kumar, J. J. P. C. Rodrigues, and M. S. Obaidat, Eds. Singapore: Springer, 2020, pp. 831–843, doi: 10.1007/978-981-15-3369-3_61.

[4] A. Nosenko, Y. Cheng, and H. Chen, "Password and passphrase guessing with recurrent neural networks," *Inf. Syst. Front.*, vol. 25, no. 2, pp. 549–565, Apr. 2023, doi: 10.1007/s10796-022-10325-x.

[5] M. Jin, J. Ye, R. Shen, and H. Lu, "Search-based ordered password generation of autoregressive neural networks," Mar. 15, 2024, *arXiv*:2403.09954, doi: 10.48550/arXiv.2403.09954.

[6] Y. Li, H. Wang, and K. Sun, "Personal information in passwords and its security implications," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 10, pp. 2320–2333, Oct. 2017, doi: 10.1109/TIFS.2017.2705627.

[7] Y. Guo, Z. Zhang, Y. Guo, and X. Guo, "Nudging personalized password policies by understanding users' personality," *Comput. Secur.*, vol. 94, p. 101801, Jul. 2020, doi: 10.1016/j.cose.2020.101801.

[8] M. Siponen, P. Puhakainen, and A. Vance, "Can individuals' neutralization techniques be overcome? A field experiment on password policy," *Comput. Secur.*, vol. 88, p. 101617, Jan. 2020, doi: 10.1016/j.cose.2019.101617.

[9] N. Huaman, S. Klivan, M. Oltrogge, Y. Acar, and S. Fahl, "They would do better if they worked together: The case of interaction problems between password managers and websites," in *Proc. IEEE Symp. Security and Privacy (SP)*, May 2021, pp. 1367–1381, doi: 10.1109/SP40001.2021.00094.

[10] I. Mannuela, J. Putri, Michael, and M. S. Anggreainy, "Level of password vulnerability," in *Proc. 1st Int. Conf. Computer Science and Artificial Intelligence (ICCSAI)*, Oct. 2021, pp. 351–354, doi: 10.1109/ICCSAI53272.2021.9609778.

[11] "How secure is my password?" https://howsecureismypassword.net/ (accessed Dec. 03, 2024).

[12] "Kaspersky: Secure password check." https://password.kaspersky.com (accessed Dec. 03, 2024).

[13] "Securely store, manage & autofill passwords," NordPass. https://nordpass.com/ (accessed Dec. 03, 2024).

[14] "Password tester | Test your password strength," Bitwarden. https://bitwarden.com/password-strength/ (accessed Dec. 03, 2024).

[15] "Password manager - For everyone, everywhere - LastPass." https://www.lastpass.com/password-manager (accessed Dec. 03, 2024).

[16] "Have I been pwned: Pwned passwords." https://haveibeenpwned.com/passwords (accessed Dec. 03, 2024).

[17] F. Yu and H. Yin, "A security analysis of the authentication mechanism of password managers," in *Proc. IEEE 21st Int. Conf. Communication Technology (ICCT)*, Oct. 2021, pp. 865–869, doi: 10.1109/ICCT52962.2021.9657969.

[18] S. Furnell, "Assessing website password practices – Unchanged after fifteen years?," *Comput. Secur.*, vol. 120, p. 102790, Sep. 2022, doi: 10.1016/j.cose.2022.102790.

[19] K. H. Hong and B. M. Lee, "A deep learning-based password security evaluation model," *Appl. Sci.*, vol. 12, no. 5, Art. no. 5, Jan. 2022, doi: 10.3390/app12052404.

[20] M. Z. Gündüz and R. Daş, "Sosyal mühendislik: Yaygın ataklar ve güvenlik önlemleri," presented at the *9th Int. Conf. Information Security and Cryptology*, 2016.

[21] M. Z. Gündüz and R. Daş, "Kişisel siber güvenlik yaklaşımlarının değerlendirilmesi," *DUJE*, vol. 13, no. 3, Art. no. 3, Sep. 2022, doi: 10.24012/dumf.1122997.

[22] A. A. Hamza and J. S. Al-Janabi, "Detecting brute force attacks on SSH and FTP protocol using machine learning: A survey," *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 16, no. 1, Art. no. 1, Mar. 2024, doi: 10.29304/jqcsm.2024.16.11432.

[23] H. Hussain, "Password security: Best practices and management strategies," *Social Science Research Network*, Rochester, NY, Jun. 14, 2022, doi: 10.2139/ssrn.4136333.

[24] C. W. Munyendo, Y. Acar, and A. J. Aviv, "In eighty percent of the cases, I select the password for them: Security and privacy challenges, advice, and opportunities at cybercafes in Kenya," in *Proc. IEEE Symp. Security and Privacy (SP)*, May 2023, pp. 570–587, doi: 10.1109/SP46215.2023.10179410.

[25] A. P. Umejiaku, P. Dhakal, and V. S. Sheng, "Balancing password security and user convenience: Exploring the potential of prompt models for password generation," *Electronics*, vol. 12, no. 10, Art. no. 10, Jan. 2023, doi: 10.3390/electronics12102159.

[26] "Dashlane password manager," Dashlane. https://ripleyprd.wpengine.com/ (accessed Dec. 03, 2024).

[27] D. Reichl, "KeePass password safe." https://keepass.info/ (accessed Dec. 03, 2024).

[28] "Random.org - Password generator." https://www.random.org/passwords/ (accessed Dec. 03, 2024).

[29] N. Lykousas and C. Patsakis, "Decoding developer password patterns: A comparative analysis of password extraction and selection practices," *Comput. Secur.*, vol. 145, p. 103974, Oct. 2024, doi: 10.1016/j.cose.2024.103974.