One of the first mentions of using a password dates back to the Roman Empire. Those who wanted to enter a certain closed area had to tell the guard the password. Passwords have become more common with the invention of computers and software development. The Collaborative Time Sharing System (CTSS) was the first operating system to use a password for login (1961). In the early 1970s, Robert Morris developed a system for storing login passwords in hashed form. Such a scheme is currently the most widespread. For modern people, using passwords has become a daily routine. Logins and passwords are used to enter the operating system of a computer, mobile phone, to connect to the wireless Internet, access personal accounts, etc.

It seems that creating a password is easy, but at the same time, many users create easy-to-crack passwords that affect their personal data or the data of the companies they work for. Thus, such large companies as eBay, LinkedIn and Facebook have already been affected by this. According to Digital Shadows Photon Research, 24.6 billion complete sets of usernames and passwords were stolen in 2022 [1]. According to Verizon, 80% of data breaches involve passwords [2].

Despite the relative security of passwords, they are affected by the human element – 85% of data breaches involved a human element such as phishing, stolen credentials, and human error [2]. For some people, the convenience of using a password is in the first place, so they make mistakes when creating them. This applies to the use of both simple popular passwords and hackable patterns. The most popular passwords for 2022 are presented below (table 1).
Most popular passwords for 2022

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Time to crack</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>password</td>
<td>&lt; 1 Second</td>
<td>4,929,113</td>
</tr>
<tr>
<td>2</td>
<td>123456</td>
<td>&lt; 1 Second</td>
<td>1,523,537</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>&lt; 1 Second</td>
<td>413,056</td>
</tr>
<tr>
<td>4</td>
<td>guest</td>
<td>10 Seconds</td>
<td>376,417</td>
</tr>
<tr>
<td>5</td>
<td>qwerty</td>
<td>&lt; 1 Second</td>
<td>309,679</td>
</tr>
<tr>
<td>6</td>
<td>12345678</td>
<td>&lt; 1 Second</td>
<td>284,946</td>
</tr>
<tr>
<td>7</td>
<td>111111</td>
<td>&lt; 1 Second</td>
<td>229,047</td>
</tr>
<tr>
<td>8</td>
<td>12345</td>
<td>&lt; 1 Second</td>
<td>188,602</td>
</tr>
<tr>
<td>9</td>
<td>col123456</td>
<td>11 Seconds</td>
<td>140,505</td>
</tr>
<tr>
<td>10</td>
<td>123123</td>
<td>&lt; 1 Second</td>
<td>127,762</td>
</tr>
</tbody>
</table>

taken from the NordPass website [3]

The following are statistics that illustrate how the human element affects the creation of passwords and, as a result, their security. Passwords often contain information that can be found in the public domain:
- 15% of people use their own first name in their password [4];
- 21% of passwords include the user's birth year [4];
- 18% of passwords include the name of the user's pet [4];
- 37% of respondents have used their employer's name in a work-related password [5].

Also, problems may arise not with the password itself, but with its reuse and rare change:
- 62.9% of online users change their passwords only when prompted [6];
- Even though 92% of people know that using a variation of the same password is a risk, 65% always or mostly use the same password or a variation [7];
- Employees reuse a password an average of 13 times [8];
- 45% of survey respondents did not change their passwords in the past year even after a breach had occurred [7].

The password provides access to private data, so only the account owner should know the password, but statistically 49% of IT security professionals and 51% of individuals share passwords with colleagues to access business accounts [9].

At the same time, according to the rules, passwords must be long enough (from 12, and preferably 16 characters)[10], include characters of different types and impossible to guess based on public information about the user.

Adherence to the rules of password construction help protect against some types of attacks, such as:
- Brute force attack;
- Dictionary attack.

Below is information on how quickly it is possible to brute force passwords of different lengths and with different types of characters (table 2).
There are attacks that do not depend on the content of the password:
- Shoulder surfing;
- Key Logging;
- Phishing;
- Replay attack (reflection attack).

Statistics show that the percentage of easy-to-crack passwords is significant. So, the question arises: "Are passwords still the best method of authentication?"

To answer this question, alternative authentication methods should be considered. These include:
- Certificate-based authentication;
- Biometric authentication;
- Single sign-on (SSO).

Certificate-based authentication technology uses certificate files. A certificate is an electronic document that identifies the user and is provided by a third party (certification center). The certificate contains information for user identification – the public key, the name of the digital signature algorithm, the name of the certification center and the validity period. For certificate-based authentication, the user must provide his certificate, then identity verification is performed using a private key. This authentication method uses long keys that provide a sufficient level of protection. From the user’s point of view, it requires the creation of a certificate file and its constant updating when it expires.

Biometric authentication works by comparing the provided data with verified user information stored in a database. There are two types of biometrics: conventional (DNA, fingerprints, retina) and behavioral (touchscreen use, typing.
dynamics, mouse activity). Behavioral biometrics reflect the user's behavioral habits when using devices. Biometric authentication is more secure than passwords because biometric data cannot be found in the public domain. At the same time, hackers can use a presentation attack – make silicone fingerprints, use photos to create a 3D mask, or record user activity.

Single sign-on uses a third party for authentication. It can be a social network like Google, Facebook, etc. When using this authentication method, the verification of the user's identity is performed by a third party. This is convenient for the user because he does not need to create a separate password for a new account. On the other hand, if an attacker gets access to this account, then all the records for which SSO is used will be at risk.

At the same time, with the advent of alternative authentication methods, password authentication is also improving. All of them are based on multi-factor authentication. Most often, it consists of two stages (two-factor authentication). Examples of the second stage are:
- SMS or email code;
- Token;
- Transaction.

SMS or email code is the most common option for the second stage of authentication. A notification with a generated one-time code comes to the phone or email. Phone or e-mail is indicated during registration.

Token is another option. It can be a disk, flash drive or card. In this case, an interface for reading data from this medium should be provided. Other types of tokens involve the use of additional devices or applications on mobile devices.

The transactional authentication method compares the user's characteristics with what it knows about the user and looks for discrepancies. Thus, it always casts doubt on whether the user actually owns the account. If discrepancies appear, this triggers additional verification steps. For example, this applies to a new IP address for the account.

Therefore, taking into account the peculiarities of alternative authentication methods, they either require preliminary preparations, additional equipment, or are dependent on other accounts. Their use makes sense, but despite the weaknesses of passwords, there are currently no alternatives that can completely replace them. It should also be noted that passwords do not require additional hardware, so their implementation is simple and convenient for developers. It follows that multi-factor authentication is currently the most relevant method of authentication. It is both simple to create and quite safe. Using multi-factor authentication makes account 99.9% less likely to be compromised [12].

**Conclusion.** In this article, we substantiated the importance of creating a good password, a mistake in its creation can cost the user personal and work data. In addition, we considered modern methods of password cracking, provided relevant statistics. We have come to the conclusion that the password is still a valid method of authentication, but it has some problems. As a solution to the fact that in some situations a password does not protect against data leakage, we provide alternative authentication methods. The combined use of these methods and a password makes the protection of user data from attackers more reliable.
References:


