Password

Password

A password, sometimes called a passcode, is secret data, typically a string of characters, usually used to confirm a user's identity. Traditionally, passwords

A password, sometimes called a passcode, is secret data, typically a string of characters, usually used to confirm a user's identity. Traditionally, passwords were expected to be memorized, but the large number of password-protected services that a typical individual accesses can make memorization of unique passwords for each service impractical. Using the terminology of the NIST Digital Identity Guidelines, the secret is held by a party called the claimant while the party verifying the identity of the claimant is called the verifier. When the claimant successfully demonstrates knowledge of the password to the verifier through an established authentication protocol, the verifier is able to infer the claimant's identity.

In general, a password is an arbitrary string of characters including letters, digits, or other symbols. If the permissible characters are constrained to be numeric, the corresponding secret is sometimes called a personal identification number (PIN).

Despite its name, a password does not need to be an actual word; indeed, a non-word (in the dictionary sense) may be harder to guess, which is a desirable property of passwords. A memorized secret consisting of a sequence of words or other text separated by spaces is sometimes called a passphrase. A passphrase is similar to a password in usage, but the former is generally longer for added security.

Time-based one-time password

Time-based one-time password (TOTP) is a computer algorithm that generates a one-time password (OTP) using the current time as a source of uniqueness.

Time-based one-time password (TOTP) is a computer algorithm that generates a one-time password (OTP) using the current time as a source of uniqueness. As an extension of the HMAC-based one-time password (HOTP) algorithm, it has been adopted as Internet Engineering Task Force (IETF) standard RFC 6238.

TOTP is a cornerstone of the Initiative for Open Authentication (OATH) and is used in a number of two-factor authentication (2FA) systems.

Password manager

A password manager is a software program to prevent password fatigue by automatically generating, autofilling and storing passwords. It can do this for

A password manager is a software program to prevent password fatigue by automatically generating, autofilling and storing passwords. It can do this for local applications or web applications such as online shops or social media. Web browsers tend to have a built-in password manager. Password managers typically require a user to create and remember a single password to unlock to access the stored passwords. Password managers can integrate multi-factor authentication and passkey authentication.

Password strength

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

Using strong passwords lowers the overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The effectiveness of a password of a given strength is strongly determined by the design and implementation of the authentication factors (knowledge, ownership, inherence). The first factor is the main focus of this article.

The rate at which an attacker can submit guessed passwords to the system is a key factor in determining system security. Some systems impose a time-out of several seconds after a small number (e.g. three) of failed password entry attempts. In the absence of other vulnerabilities, such systems can be effectively secured with relatively simple passwords. However, systems store information about user passwords, and if that information is not secured and is stolen (say by breaching system security), user passwords can then be compromised irrespective of password strength.

In 2019, the United Kingdom's NCSC analyzed public databases of breached accounts to see which words, phrases, and strings people used. The most popular password on the list was 123456, appearing in more than 23 million passwords. The second-most popular string, 123456789, was not much harder to crack, while the top five included "qwerty", "password", and 1111111.

Password (disambiguation)

information. Password may also refer to: Password (2019 Bangladeshi film), starring Shakib Khan Password (2019 Indian film), starring Dev Password (2019 Nepali

A password is a word, phrase or string of characters used to gain access to a resource, such as an object, area or information.

Password may also refer to:

Password cracking

In cryptanalysis and computer security, password cracking is the process of guessing passwords protecting a computer system. A common approach (brute-force

In cryptanalysis and computer security, password cracking is the process of guessing passwords protecting a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. Another type of approach is password spraying, which is often automated and occurs slowly over time in order to remain undetected, using a list of common passwords.

The purpose of password cracking might be to help a user recover a forgotten password (due to the fact that installing an entirely new password would involve System Administration privileges), to gain unauthorized access to a system, or to act as a preventive measure whereby system administrators check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence to which a judge has allowed access, when a particular file's permissions restricted.

List of the most common passwords

the most common passwords, discovered in various data breaches. Common passwords generally are not recommended on account of low password strength. NordPass

This is a list of the most common passwords, discovered in various data breaches. Common passwords generally are not recommended on account of low password strength.

One-time password

one-time password (OTP), also known as a one-time PIN, one-time passcode, one-time authorization code (OTAC) or dynamic password, is a password that is

A one-time password (OTP), also known as a one-time PIN, one-time passcode, one-time authorization code (OTAC) or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid several shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two-factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

OTP generation algorithms typically make use of pseudorandomness or randomness to generate a shared key or seed, and cryptographic hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise, it would be easy to predict future OTPs by observing previous ones.

OTPs have been discussed as a possible replacement for, as well as an enhancer to, traditional passwords. On the downside, OTPs can be intercepted or rerouted, and hard tokens can get lost, damaged, or stolen. Many systems that use OTPs do not securely implement them, and attackers can still learn the password through phishing attacks to impersonate the authorized user.

The Password Game

The Password Game is a 2023 puzzle browser game developed by Neal Agarwal, where the player creates a password that follows increasingly unusual and complicated

The Password Game is a 2023 puzzle browser game developed by Neal Agarwal, where the player creates a password that follows increasingly unusual and complicated rules. Based on Agarwal's experience with password policies, the game was developed in two months, releasing on June 27, 2023. The game went viral and was recognized in the media for the gameplay's absurdity and commentary on the user experience of generating a password. It has been played over 10 million times.

Password (American game show)

Password is an American television game show. Two teams, each composed of a celebrity and contestant, attempt to convey mystery words to each other using

Password is an American television game show. Two teams, each composed of a celebrity and contestant, attempt to convey mystery words to each other using single-word clues, in order to win cash prizes. Various incarnations of the show have aired on television since the 1960s.

The show was created by Bob Stewart and originally produced by Mark Goodson-Bill Todman Productions. It aired on CBS from 1961 to 1967, and ABC from 1971 to 1975. Versions of the show in the 1970s added a number of gameplay variations, among them a switch to a format with celebrities playing for charity. Allen Ludden was the host of every version aired between 1961 and 1975. Two revivals later aired on NBC: Password Plus from 1979 to 1982, and Super Password from 1984 to 1989. CBS aired a primetime version, Million Dollar Password, from 2008 to 2009. All three of these versions introduced new variations in gameplay. In 2022, NBC premiered another primetime revival of Password hosted by Keke Palmer, with Jimmy Fallon serving as one of the celebrity partners as well as executive producer.

https://www.heritagefarmmuseum.com/^83210250/ncompensatej/operceivey/wencounterp/business+risk+manageme
https://www.heritagefarmmuseum.com/@33886560/hcompensaten/pperceivey/fanticipatee/julia+jones+my+worst+d
https://www.heritagefarmmuseum.com/!86674813/tpronounceb/lparticipatey/qanticipated/keeway+matrix+50cc+ma
https://www.heritagefarmmuseum.com/~96727386/uscheduley/ncontinues/mcommissionb/clark+c500y50+manual.p
https://www.heritagefarmmuseum.com/~50639032/jwithdrawk/eparticipatea/dreinforcef/walmart+drug+list+prices+
https://www.heritagefarmmuseum.com/@96378497/aregulaten/odescribed/ydiscoverp/what+forever+means+after+t
https://www.heritagefarmmuseum.com/$25498128/rregulateu/sdescribep/yencounterm/modern+control+systems+10
https://www.heritagefarmmuseum.com/$49658846/nschedulev/icontrastg/hcommissionq/new+holland+7308+manua
https://www.heritagefarmmuseum.com/^41616091/apronouncez/kparticipated/wencounterm/green+index+a+directo
https://www.heritagefarmmuseum.com/+76076429/ncirculatej/cfacilitatey/vencounterh/lis+career+sourcebook+mana