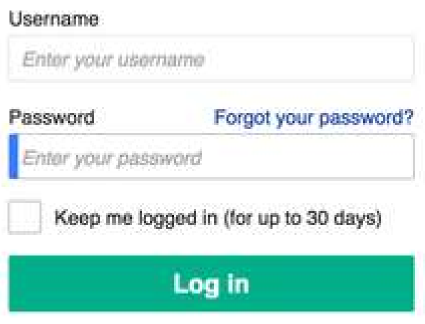
WIKIPEDIA
The Free Encyclopedia

Password

A **password**, sometimes called a **passcode** (for example in Apple devices), is secret data, typically a string of characters, usually used to confirm a user's identity. Traditionally, passwords were expected to be memorized,[1] but the large number of password-protected services that a typical individual accesses can make memorization of unique passwords for each service impractical.[2] Using the terminology of the NIST Digital Identity Guidelines,[3] 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,[4] the verifier is able to infer the claimant's identity.



A password field in a sign in form

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.[5]

History

Passwords have been used since ancient times. Sentries would challenge those wishing to enter an area to supply a password or *watchword*, and would only allow a person or group to pass if they knew the password. Polybius describes the system for the distribution of watchwords in the Roman military as follows:

> The way in which they secure the passing round of the watchword for the night is as follows: from the tenth maniple of each class of infantry and cavalry, the maniple which is encamped at the lower end of the street, a man is chosen who is relieved from guard duty, and he attends every day at sunset at the tent of the tribune, and receiving from him the watchword—that is a wooden tablet with the word inscribed on it – takes his leave, and on returning to his quarters passes on the watchword and tablet before witnesses to the commander of the next maniple, who in turn passes it to the one next to him. All do the same until it reaches the first maniples, those encamped near the tents of the tribunes. These latter are obliged to deliver the tablet to the tribunes before dark. So that if all those issued are returned, the tribune knows that the watchword has been given to all the maniples, and has passed through all on its way back to him. If any one of them is missing,

> he makes inquiry at once, as he knows by the marks from what quarter the tablet has not returned, and whoever is responsible for the stoppage meets with the punishment he merits.[6]

Passwords in military use evolved to include not just a password, but a password and a counterpassword; for example in the opening days of the Battle of Normandy, paratroopers of the U.S. 101st Airborne Division used a password—*flash*—which was presented as a challenge, and answered with the correct response—*thunder*. The challenge and response were changed every three days. American paratroopers also famously used a device known as a "cricket" on D-Day in place of a password system as a temporarily unique method of identification; one metallic click given by the device in lieu of a password was to be met by two clicks in reply.[7]

Passwords have been used with computers since the earliest days of computing. The Compatible Time-Sharing System (CTSS), an operating system introduced at MIT in 1961, was the first computer system to implement password login.[8][9] CTSS had a LOGIN command that requested a user password. "After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy."[10] In the early 1970s, Robert Morris developed a system of storing login passwords in a hashed form as part of the Unix operating system. The system was based on a simulated Hagelin rotor crypto machine, and first appeared in 6th Edition Unix in 1974. A later version of his algorithm, known as crypt(3), used a 12-bit salt and invoked a modified form of the DES algorithm 25 times to reduce the risk of pre-computed dictionary attacks.[11]

In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online.

Choosing a secure and memorable password

The easier a password is for the owner to remember generally means it will be easier for an attacker to guess.[12] However, passwords that are difficult to remember may also reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password across different accounts. Similarly, the more stringent the password requirements, such as "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system.[13] Others argue longer passwords provide more security (e.g., entropy) than shorter passwords with a wide variety of characters.[14]

In *The Memorability and Security of Passwords*,[15] Jeff Yan et al. examine the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords.

Combining two or more unrelated words and altering some of the letters to special characters or numbers is another good method,[16] but a single dictionary word is not. Having a personally designed algorithm for generating obscure passwords is another good method.[17]