Two-Factor Authentication (2FA)

Return to Glossary

Two-Factor Authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves. This process is done to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on Single-Factor Authentication (SFA), in which the user provides only one factor – typically, a Password or passcode. Two-factor authentication methods rely on a user providing a password, as well as a second factor, usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who have stolen a password database or used phishing campaigns to obtain user passwords.

See also: Smart Card

Source: https://searchsecurity.techtarget.com/definition/two-factor-authentication