Multifactor Authentication (MFA)

Return to Glossary

Multifactor Authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows, such as a Password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

The goal of MFA is to create a layered defense that makes it more difficult for an unauthorized person to access a target, such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one or more barriers to breach before successfully breaking into the target.

MFA is has the following factors:

- Knowledge Factor
- Possession Factor
- Inherence Factor
- Location Factor
- Time Factor

Source: https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA