User Authentication

Return to Glossary

User Authentication verifies the identity of a user attempting to gain access to a network or computing resource by authorizing a human-to-machine transfer of credentials during interactions on a network to confirm a user's authenticity. The term contrasts with Machine Authentication, which is an automated authentication method that does not require user input.

Authentication helps ensure only authorized users can gain access to a system by preventing unauthorized users from gaining access and potentially damaging systems, stealing information, or causing other problems. Almost all human-to-computer interactions – other than guest and automatically logged-in accounts – perform user authentication. It authorizes access on both wired and wireless networks to enable access to networked and internet-connected systems and resources.

A straightforward process, user authentication consists of three tasks:

1. Identification. Users have to prove who they are.
2. Authentication. Users have to prove they are who they say they are.
3. Authorization. Users have to prove they're allowed to do what they are trying to do.

User authentication can be as simple as requiring a user to type a unique identifier, such as a user ID, along with a Password to access a system. It can also be more complex, however – for example, requiring a user to provide information about physical objects or the environment or even take actions, such as placing a finger on a fingerprint reader.

Source: https://searchsecurity.techtarget.com/definition/user-authentication