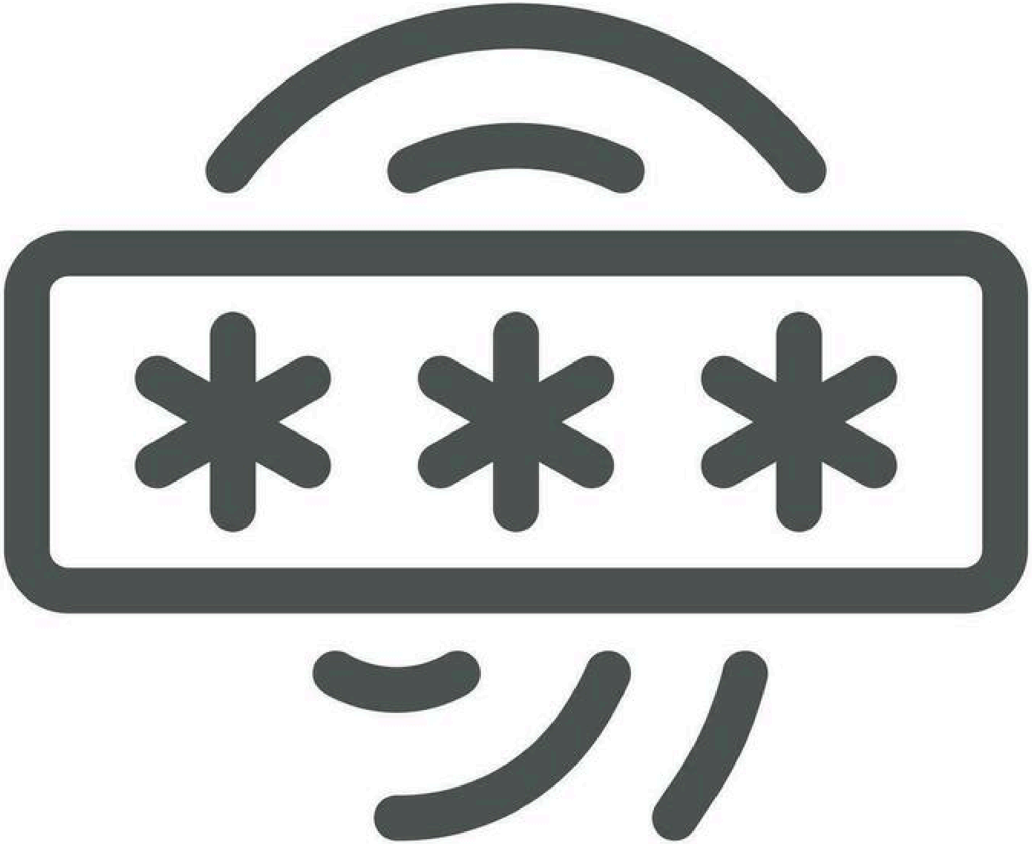
User Authentication Methods

User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User A only has access to relevant information and cannot see the sensitive information of User B. Cybercriminals can gain access to a system and steal information when user authentication is not secure

1. Passwords

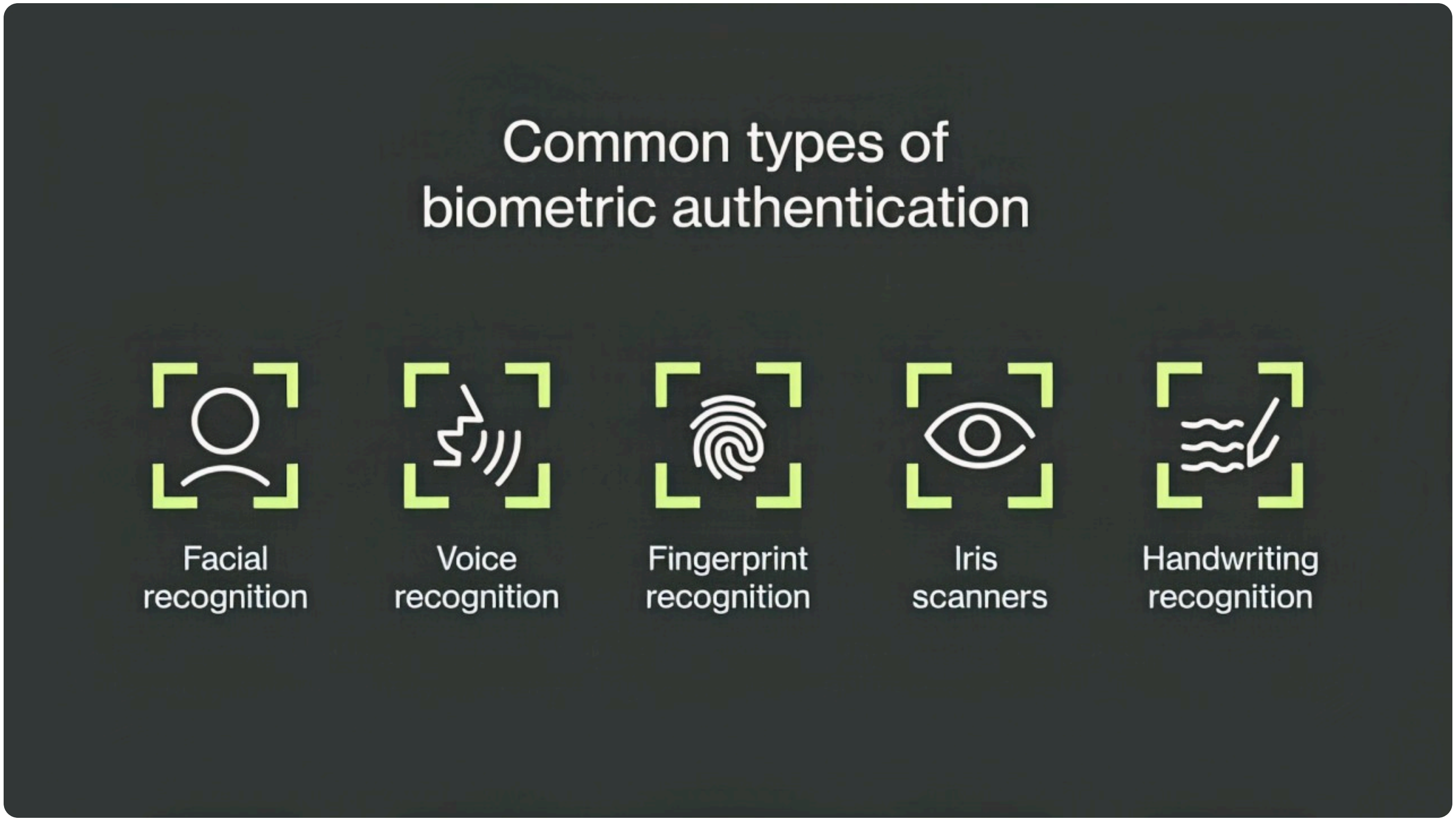


The most common method of authentication. Users enter a username and password to access their account In terms of security, the longer and more complex a user's password is, the better. It's recommended that you enforce good practice behaviours when forming a new password. There should be certain minimum requirements for the users however, there also needs to be a happy medium with the requirements and how complex they are. To enforce a strong password, here are some rules you should consider for your users: Minimum of 8 characters At least one uppercase letter At least one number At least one special character .

2. Two-Factor Authentication (2FA)

This method requires users to provide two forms of verification: something they know (password) and something they have (code sent to their phone). The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. .

3. Biometric Authentication



Utilizes physical characteristics of the user, such as fingerprints or facial recognition, to verify their identity some examples are: Chemical biometric devices Visual biometric devices behavioral biometrics Auditory biometric devices .

4. Social Media Authentication

Users can log in using their social media accounts (such as Facebook or Google), simplifying the registration and login process. Social login (also known as social sign-on or social SSO) is an authentication method that enables users to log in to apps using their existing social network accounts to confirm their identity. For example, they'll click "Sign in with Facebook" on an app's login page, grant Facebook permission to share their identity details with the app, and voila. It lets users access your app or website without having to create a new set of credentials from scratch—or remember yet another password.

5. Token-Based Authentication

Users receive an access token after logging in, which is used to authenticate future requests without needing to re-enter credentials.