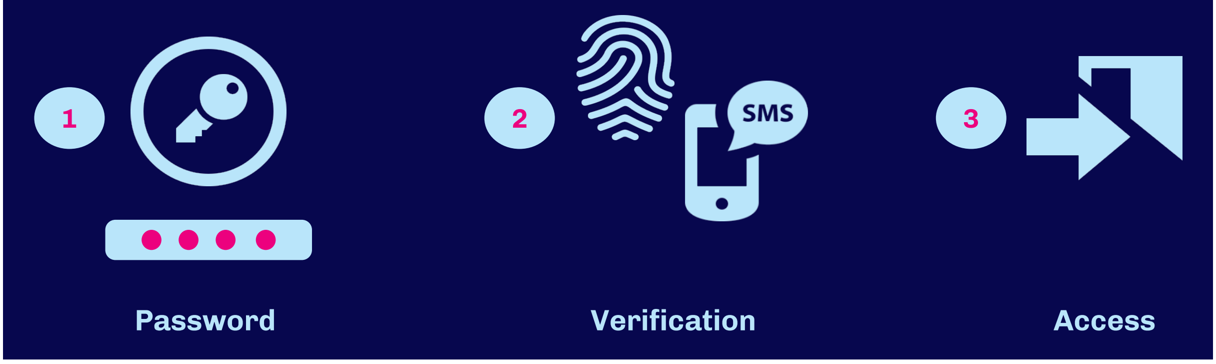
Multi Factor Authentication and Single Sign-On

A Short Guide by ***Spector***

Multi-Factor authentication (MFA) is the method of a user proving his/her identity by providing a minimum of two instances of authentication – something they **have**, something they **know** or something they **are**. This could mean a device (phone, tablet), your physical attributes (fingerprint, iris, face) or a secret question. It will consist on a new layer of protection and your password alone will not be enough to access your data.

How does it work?



1 Password

2 Verification

3 Access

Benefits

Strengthens Security: The main benefit of Multi-Factor authentication is the extra security provided by adding multiple layers of protection. The more layers a company has in place, the less risk it has of an intruder gaining access to their network and resources.

A Step towards Compliance: Some of the most common compliance standards specify that organizations need to implement MFA for certain situations. This is especially true when it comes to protecting sensitive data or financial details.

Single Sign-On

Single sign-on works by validating the user through MFA during the login process. Once the user is authenticated, they are logged into their single sign-on portal. From there they have access to all their productivity apps and tools without the need to log in for each separately. This means the user does not need to remember or even know the passwords to be able to work.

Simplification of Login

This scenario gives practicality to MFA implementation, as one of the challenges of implementing it is login fatigue. Combined with single sign-on, a single MFA instance would cover all apps needed by the user.