Passwordless Authentication

Reasons for adopting Passwordless authentication

Deploy passwordless strong authentication for all access points:

- Desktop or tablet web access
- Mobile access to Mobile apps or web applications

Strong authentication is meant to secure access to all your digital assets, not just one channel.

It may seem obvious, but securing only Desktop or PC access is simply not sufficient. Other channels need to be secured. Today, nearly 60% of all digital media is accessed through mobile channels - users often access their CRM, ERP or other applications from smartphones, too.

It is therefore crucial not only to deploy strong authentication on mobile as well as desktop channels, but to minimize user interactions during the authentication process to increase compliance.

The challenge is to improve security of all access points, while streamlining infrastructure and maximizing simplicity of use for end users.

That's where the Safewalk Fast Auth passwordless solution shines - as it provides:

- A unique platform to easily deploy multi-factor authentication on all channels
- Strong authentication in only a few clicks to access applications from any device
- A secure and streamlined on boarding process to install and register Fast Auth mobile
- A seamless, frustration free user experience
- A wide range of other methods that can be deployed from the same platform to meet the needs of other specific use cases where the passwordless method is less relevant

Why is passwordless strong authentication better than other methods?

1. Easy deployment of strong authentication for desktop & mobile access

   - Safewalk Fast Auth mobile passwordless strong authentication method can be easily deployed in most frequent use cases, such as access to applications or web portals from a desktop or smartphone. It enables access to all types of native or web access mobile apps

   - It provides secure access to consumer portals, with a large number of users, by providing the easiest authentication method in order to significantly reduce help desk involvement

2. Streamlined user experience
   - Users no longer have to devise and remember complex passwords or type them each time they log on
   - They no longer have to renew or change passwords
   - Access is straight forward, utilizing biometric recognition or pattern entry, providing a seamless and intuitive user experience
   - When accessing portals or mobile apps from a smartphone, strong authentication is done with two user clicks

3. Improved security

With the many credentials a typical user has to remember today, remembering usernames and/or passwords can be problematic and frustrating. This inevitably leads to passwords being reused and eventually security being compromised.

Obviously, users' passwords are vulnerable to many traditional attack vectors. But, with passwordless authentication, the users' authentication data is not stored within the system, as a password would be. This gives a Passwordless solution a significant security advantage, as it eliminates the existence of attack vectors that are inherent to traditional passwords.

4. IT cost reduction

- A passwordless method greatly reduces the associated costs of password management operations such as storage and protection.
- Help desks will no longer be clogged up with endless users' demands for changing or resetting forgotten passwords - this is particularly helpful for strong authentication of high user volumes.