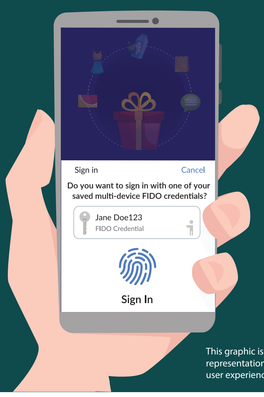
Introducing Multi-device FIDO Credentials

Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins



This graphic is a genericized representation of what the user experience may be.

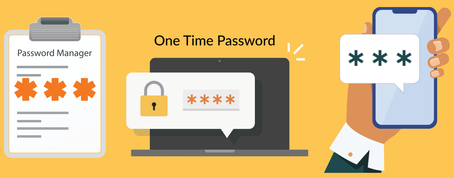
Passwords are a problem.

Knowledge-based | Hassle to use and remember | Easy to phish, harvest, replay

89% of organizations experienced a phishing attack in the past year.*

*HYPR, 2022 State of Passwordless Security Report

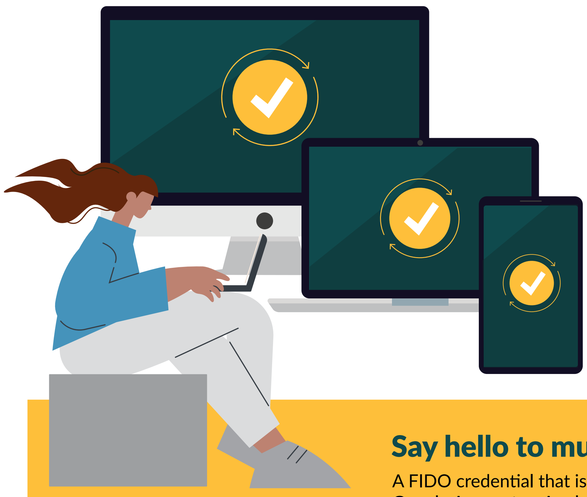
Common legacy authentication solutions don't address the security problem and/or are not usable enough to change consumer behavior.



FIDO AUTHENTICATION IS THE WORLD'S ANSWER TO THE PASSWORD PROBLEM.

FIDO Authentication provides a simpler user experience with phishing-resistant security.

WHAT IS FIDO? | HOW FIDO WORKS | FIDO SPECIFICATIONS



Improving access and usability for FIDO Authentication

With the introduction of multi-device FIDO credentials (referred to by some as a "passkey"), there's a new option for users to access their FIDO sign-in credentials on many of their devices, even new ones, without having to re-enroll every device on every account.

Say hello to multi-device FIDO credentials!

A FIDO credential that is backed up (usually to the user's platform account; e.g., Google Account or AppleID), allowing users to restore the credential to, and use it from, another device. From a user experience standpoint, this will be very similar to how one interacts with a password manager today to help them securely enroll and sign into websites – only it will be far more secure. For service providers, this expands the range of options for deploying modern, phishing-resistant authentication.

Here's what this means for...

User Experience

The user experience of signing in will become consistent across many of the user's devices – a simple verification of their fingerprint or face, or a device PIN, the same simple action that consumers take multiple times each day to unlock their devices.

Security

Multi-device credentials are based on FIDO Authentication, which is proven to be resistant to threats of phishing, credential stuffing and other remote attacks. Also, service providers can offer FIDO credentials without needing passwords as an alternative sign-in or account recovery method.

Scalability

Until now, users were required to enroll their FIDO credentials for each service on each new device, typically with a password for that first sign-in. With multi-device FIDO credentials, the credentials are available to users whenever they need them—even if they replace their device.

fido™ ALLIANCE | simpler stronger authentication

Learn more @ fidoalliance.org