# What Is MFA, and Why MFA Matters

LastPass •••|

Get LastPass Free

With 85% of cyber breaches due to a human element, such as phishing or reused passwords, adding multi-factor authentication (MFA) has become a priority for companies and SaaS services alike.

Multi-factor authentication is the process of adding identification authentication factors to verify a user's identity before approving access to systems, networks, programs, and services. IT teams and administrators can set authentication protocols and policies that increase security while streamlining the user experience, adding to improved productivity and efficiencies.
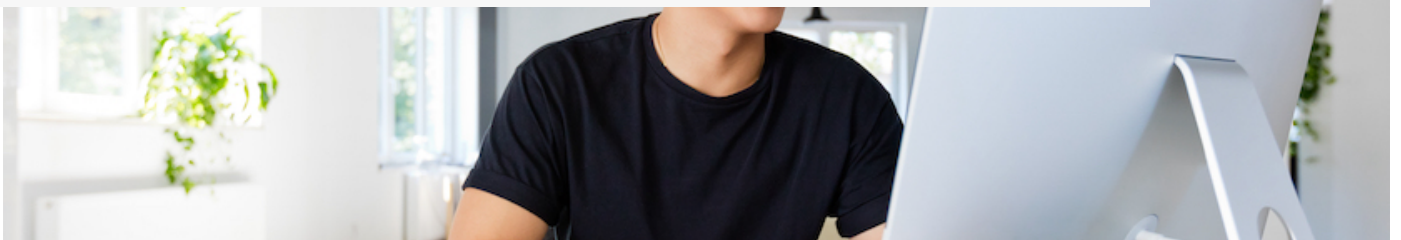
# Features of multi-factor authentication

**Greater peace of mind**

**Reduced data risk**

**Stronger password hygiene**

# The importance of multi-factor authentication

**Why MFA matters**

MFA improves security, reducing the risk of cyber attacks, phishing success, and even unauthorized access to sensitive data within your business. MFA also blocks against a tactic known as "credential stuffing," where hackers use programs and codes to push through credentials in attempts to hack systems. MFA blocks access by requiring next-level access authentication.

With MFA, you select the requirements for authentication and what level of security you need for your users, customized to your business. Then, you also choose what access the users have, protecting productivity and data alike.

# Multi-factor authentication advantages

### Adaptive authentication
Prove a user's identity with a combination of factors that adapts to users and scenarios.

### Passwordless user experience
Access work across all devices – mobile devices to desktop – without requiring a password.

### Secure every access point
Apply MFA authentication methods to cloud apps, VPNs, workstations, identity providers, and more.

### Customizable to your business
Create and apply unique MFA factors at the user or group level to ensure all-around security.

# Examples of MFA

Multi-factor authentication can be as simple or robust as your business or service needs to protect sensitive data and entry points. Some examples of MFA include:

- Question or token validation – often used in two-factor authentication (2FA) an additional step of answering a security question or confirming the inclusion of an image token selected at registration.

- Single-use codes or passwords – a secondary password authentication process sent via email or text to enter.

- Push notifications – codes or actions sent to mobile devices that require action before access is granted.

- Voice recognition – requiring vocal confirmation that digitally matches the voice sample set at registration.

- Biometric verification – using facial recognition sign-on, fingerprints, or retinal scans to authenticate identity.
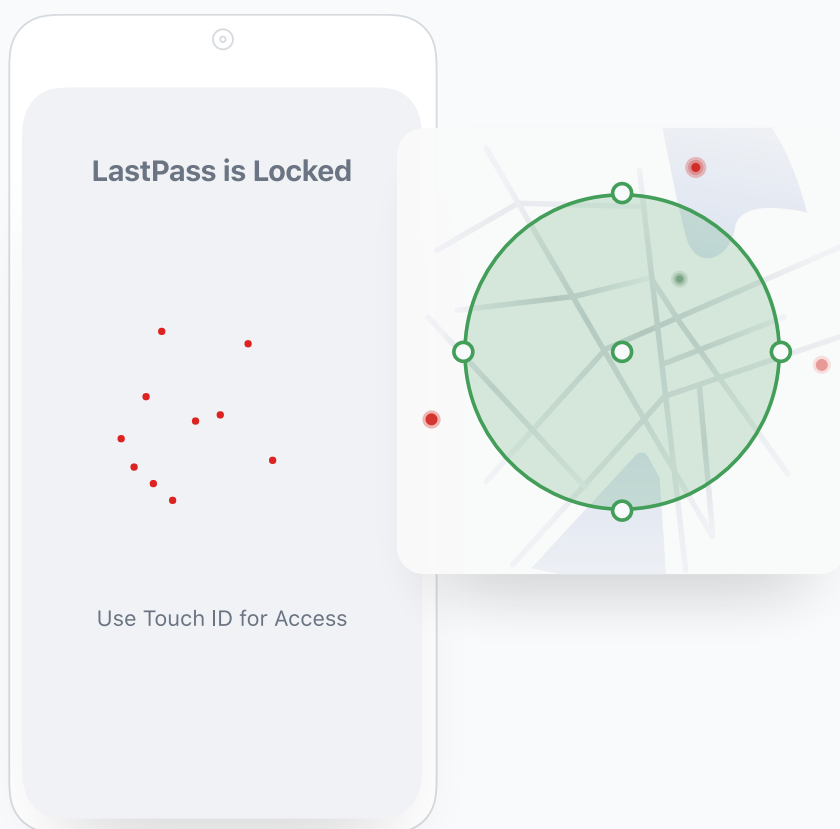


# LastPass MFA is a smarter way to authenticate

While these extra steps may seem cumbersome, they exponentially increase security levels. They can also be combined or implemented with single sign-on

(SSO) and passwordless login options to reduce the effort of users, while also increasing the efficiency and management of users and business.

Leverage biometric and contextual factors to better protect your business while securing the employee login experience with LastPass MFA.

# Learn More

## LastPass for Business

Improve security, reduce the risk of data breaches, maintain convenience.

**Explore LastPass Business ❯**

## Request a Demo

See how password management can secure your business.

**Request a Demo ❯**

## LastPass Blog

Get updates, insights, news and tips from the LastPass team blog.

**Stay Up to Date ❯**

**LastPass Resource Center**

All you need to improve security in one password management solution.

Go to Resource Center ›

# Get started with LastPass Business

**Start Your Free Trial Today**

Follow us on:

LASTPASS ➕

FEATURES ➕

FOR BUSINESS ➕

RESOURCES ➕

COMPANY ➕

PRODUCTS ➕

GET LASTPASS ➕

Available on the App Store   GET IT ON Google play

🌐 English ⌃