What Is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA) is an authentication method that requires users to prove their identities with at least two different verification methods so that they can gain access to mobile applications, websites, or other online resources.

If one factor is broken or compromised, an attacker still has to at least one more barrier to get through before they can gain access to a target account.

The majority of multi-factor authentication implementations use at least two authentication factors.

The most common authentication factors are entering your password, and then entering your code sent to either your mobile device or email address to verify that you are in fact the account owner.

How Multi-Factor Authentication Works

MFA is a process where multiple technologies are used to verify a user's identity. Single-factor authentication uses a single technology such as a password to prove authenticity.

Multi-factor authentication requires users to combine verification technologies from at least two groups or authentication factors.

Adaptive authentication is an important part of MFA. The idea is that users circumstances are constantly changing and authentication rules need to constantly adjust to keep up.

Good adaptive authentication methods will set risk-based policies across multiple dimensions, including:

- By user or user group
- By authentication method
- By application
- By network information
- By geographic location

Authentication Factors

Something You Know – Knowledge Factor

This is generally a PIN, passphrase, pattern, password, or security questions, and their corresponding answers.

To satisfy this technology, the user has to enter the information that the backend can then match against what has been previously set up.

Something You Have – Possession Factor

For the introduction of smartphones, users carried around smart cards or tokens.

Those devices would generate a one-time passcode (OTP) that could be entered into the back-end system.

The majority of users today rely on their smartphones with an authenticator app as the device to generate the codes.

Something You Are – Inherence Factor

This includes retina scans, facial recognition, fingerprints, voice recognition, or

even a user's behavior (for instance, how fast they type or swipe on a screen) to be used to verify a user.

To achieve MFA, at least two different technologies from at least two different technology groups have to be used for the authentication process.

As a result, using a PIN and a password is not considered multi-factor authentication.

However, using a pin with facial recognition as a second factor is. It is also okay to use more than two forms of authentication.

However, the majority of users want frictionless authentication or the ability to be verified without needing to perform verification.

Time Factor

This verifies a user by challenging the time of an access attempt. This is based on the idea that certain behaviors should occur within predictable time frangers.

If someone attempts to access the platform outside of that usual time range, the attempt can be terminated or challenged until a user can verify their identity.

Location Factor

This verifies a user based on their location in the world.

For instance, if a user registered an account in the United States, and then attempted to log in from another country, location factors could force the user to verify their identity.

Many location factors are based on the original user's IP address, and compare the IP of the original with the new attempt to access information.

Using a virtual private network, or VPN, may trigger location factor authentication.

Two-Factor vs. Multi-Factor Authentication

Two-factor authentication (2FA) requires the user to present two authentication factors such as what you know and what you have.

Multi-factor authentication is broader and requires organizations to use at least two factors in the authentication process.

A common type of 2FA is the time-based one-time password (TOTP) that generates a key locally on the device the user is attempting to access.

The key is entered into the website or application to gain access.

The keys expire after a certain period of time, with a new one generated the next time a user logs in.

Benefits of MFA

MFA provides several benefits to companies that use it as part of their security strategy.

Better Security

Using MFA provides increased security against cybercriminals compared to static passwords and single-factor authentication processes.

Improved Productivity and Flexibility

Removing the reliance on passwords helps to improve the customer experience.

By providing low-friction authentication challenges, companies can potentially increase security while also improving the overall user experience.

Achieve Industry and Regulatory Compliance

MFA can help companies comply with any industry regulations.

MFA is necessary to satisfy the strong authentication requirement of PSD2.

financial institutions are required to comply with PSD2.

Types of MFA Technologies

Hardware Tokens

These are small and easy to use hardware devices that an owner carries with them to authorize access to a small network.

Supporting a strong authentication with one time passwords, Hardware tokens provide The Possession factor for multi-factor authentication while enabling enhanced security for banks and application providers who need to secure multiple applications using a single device.

Soft Tokens

Software or app-based tokens generate a one-time-use login pin.

Generally, the tokens used for multi-factor authentication possession factor. The device, usually a smartphone, facilitates the token.

SMS Text Message and Voice 2FA

SMS text message and voice 2FA provide one time passwords to the user for authentication.

The password is delivered to the user through either an SMS text message to the user’s mobile device or a voice message.

Push Notification

Push notifications send the authentication code or one-time password through to a user’s mobile device with a push notification.

Instead of receiving a text message, the notification appears on the lock screen of the device.

Visual Cryptogram

This MFA technology uses a visual challenge contained in a graphical cryptogram made with a matrix of Color Dots.

The customer uses the camera on their mobile device to take a photo of the cryptogram and then decrypt the transaction details inside it.

Mobile Authentication

Mobile authentication is the process of verifying a user with their phone or verifying the device itself.

It allows users to log into secure locations and access resources from anywhere.

Biometric Authentication

Biometric authentication leverages face recognition or a fingerprint scan to accurately and securely authenticate users even on mobile devices.

Biometric authentication also includes behavioral authentication to provide an invisible layer of security that continuously authenticates the end-user by the unique ways they interact with their mobile device or computer with a swipe pattern, a mouse movement, keystroke, and more.

Why You Need MFA

Authentication methods that rely on more than a single factor are more difficult to compromise.

Properly designed and implemented are more reliable and a stronger deterrent for cyber crimes than simply relying on username and password authentication alone.

The username-password authentication is much more difficult to defend against security breaches that compromise data security.

The data breaches may result in serious damage to the organization or the consumer with sewing data, phishing attacks, identity theft, brute force attacks,

and more.

MFA requires users to prove their identities with two or more verification methods before they can access information.

If one factor is compromised, the attacker still has at least one more barrier to get through before being able to access anything.

Where You Can Use MFA

MFA needs to be used when accessing any kind of sensitive data; for instance:

- When you visit your Facebook, Google, or Microsoft accounts from a new location or device, you use MFA with the knowledge factor (the password) and possession factor (your mobile phone) to approve before you can log-in.
- When you access your bank account at an ATM, you use multi-factor authentication by having something you know (the PIN) along with something you have (your ATM card.) Some banks, like Wells Fargo, are now allowing you to use your mobile device in place of an ATM card to conduct ATM transactions. This approach still uses the knowledge and possession factors, but changes the possession from your ATM card to your smartphone.
- When you use your mobile phone, you use MFA by something you have (your phone) and something you are (your facial scan or fingerprint) or other biometric information (such as a pattern on the lock screen) on the device. Instead of something you are, you may also use something you know (a PIN) to unlock your device.
- Good multi-factor authentication allows for security while providing the ability to seamlessly do so when accessing the features and functions of a service provider.

What’s your goal today?

1. Use PLANERGY to manage purchasing and accounts

payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide "Preparing Your AP Department For The Future"

Download a free copy of our guide to future proofing your accounts payable department. You'll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts