THE RISE AND STALL OF PASSWORD-BASED MFA:

5 Common MFA Weak Links and Why They're a Risk to Your Company Today

Few things are worse than a false sense of security.

That feeling when you've done all you can to protect your organization, employees, and even customers — only to discover that it fell short.

You ask employees to reset their passwords regularly. You plead with them not to reuse passwords across websites. Still, they open themselves up to credential stuffing, password reuse, and phishing attacks.

Worse yet, new attack vectors emerge that actually prey on *stored* credentials, making all your access management and security layers insufficient.

Passwords have given businesses and organizations a false sense of security even with the addition of multi-factor authentication (MFA) alongside traditional passwords. That's where authentication has been stuck for the last two decades: password-based MFA.

The Rise and Stall of Password-Based MFA

Also known as two-factor authentication (2FA), MFA is a method of verifying a user, application, or device by requiring them to present an additional identifier to supplement a password. MFA is meant to provide an extra layer of security beyond single-factor authentication or passwords.

In its most familiar use, password-based MFA requires the user of an application to register a selection of identifiers or "factors" from two of these three categories:

Something you are:

your fingerprint, face scan, or other biometric recognition.

Something you have:

your smartphone, which acts as a physical FIDO token, similar to a security key or smart card.

Something you know:

a password or PIN.

Additional factors come in different forms including hardware keys, alphanumeric PINs, mobile SMS codes, and biometrics. For example, after typing in your username and password, some applications and websites will send a one-time passcode (OTP) to your phone that also must be entered.

For years, MFA has been the gold standard in securing digital identity, and for good reason. It provides additional security above authentication reliant on a single factor.

However, in recent years millions of passwords have been stolen and published online. Gartner now observes that most MFA tools are only one-factor authentication by "adding a single extra factor to a legacy password."

While MFA has gained some traction, its adoption has slowed. A 2021 report by Twitter found that only 2.3% of its active accounts use multi-factor authentication and Microsoft revealed a paltry 11% MFA adoption rate among its enterprise cloud users.

While MFA has been mandated in many places, businesses still have a difficult time enforcing its adoption by customers and employees. In a survey of security professionals and IT decision makers, 74% of respondents said they receive complaints about MFA from their users — and 9% went so far as to say they "hate it."

1. The Need for Secure Remote Access

Remote work has reignited urgency for multi-factor security by exposing adoption gaps across desktop login and remote access. Yet, adoption of MFA, even among remote workers, is lagging. In a 2020 study on remote work conducted by G2, researchers found that just one in four remote workers use MFA to access business information. The study also notes that while remote work has increased by 160%, MFA usage has increased by a mere 26%.

2. Password-Based MFA Is No Longer Enough

So, why are businesses and organizations retreating from MFA? For one, MFA protects accounts and data far less than IT and security professionals had hoped.

Today's sophisticated cybercriminals and hackers can bypass MFA by simply exploiting account-recovery systems or intercepting access codes. Hardware keys or cards are easily lost or stolen. A mobile account profile can be transferred from one SIM card to another (SIM swapping) resulting in OTP messages being delivered to an unauthorized device.

In fact, many recent large-scale attacks have employed MFA bypass. Even major MFA providers such as Microsoft have experienced significant attacks, with hackers bypassing MFA by exploiting IMAP protocols.

The lesson: Password-based MFA was once an effective solution. However, it's viability as a security measure has changed in today's threat landscape. Password-based MFA is actively exploited and an insecure method for protecting user accounts against phishing and account takeover (ATO) fraud.

3. The Friction Factor Derails MFA Adoption

As MFA rose in popularity, technology companies flocked to create a myriad of MFA options. Now, users have a number of ways to log in on top of passwords. The selection of authenticator apps has grown dramatically.

Businesses have more MFA options than ever before and yet there are still gaps in user adoption. It's human nature: Any additional step creates inertia and kills usability. Ask people if they enjoy their login experience and you might hear complaints about password complexity, and a sense of reduced productivity.

Another facet of human nature? People are good at finding and exploiting workarounds. People seek the path of least resistance. Despite the fact that many enterprises are forcing their employees to jump through authentication hoops, employees find ways around MFA. For example:

- The employee who writes every password on a sticky note and leaves it on their computer monitor.
- The design team that shares a hardware OTP token taped to the whiteboard.
- The contractor who leaves a security key constantly plugged into their laptop.

These scenarios pose a security nightmare for all IT departments and access management professionals.

4. Push Attacks Are Rising

Push-based authentication is currently the industry standard in MFA. The process is simple: a user types in their password, receives a notification that is "pushed" to their smartphone, they respond and the system or application approves the access.

But what happens when a user is busy or distracted? What is likely to happen when they receive a notification on their phone? Will they actually read the notification or impulsively approve the request?

The reality is they are likely to approve a push notification without inspecting it. People hastily approve push notifications not knowing or understanding the repercussions. In 2018, malicious actors exploited "push fatigue" in concert with phishing tools to target politicians involved in the economic and military sanctions against Iran.

The last year has seen a sharp increase in attacks on systems using legacy and password-based MFA. The 2021 State of Passwordless Security report found that 90% of survey respondents experienced phishing attacks against their organizations. Of those attacks, credential stuffing was the most popular form (29%), followed by Remote Desktop Protocol attacks (14%). Push or push fatigue attacks — previously rare — had a stronger than anticipated showing of 9%.

Once praised as the method that took MFA mainstream, push notifications are now a weapon for malicious actors.

5. MFA Fatigue Is a Pain Point

With more ways to authenticate their identity, users find themselves in a chaotic soup of MFA solutions. Over and over, throughout their day, people must exhaustively prove that they are who they say they are — via username, password and then another authentication factor — on multiple platforms and applications. This leads to “MFA fatigue.”

It’s unsurprising, then, that people reuse credentials and passwords as just one of their many policy workarounds.

For IT professionals overseeing access management, MFA fatigue among users brings its own set of stubborn pain points. These include productivity loss, helpdesk strain, poor password hygiene and vulnerability to MFA attacks.

User account lockouts and loss of productivity

Password resets and helpdesk strain

Credential reuse and poor password hygiene

MFA bypass and MITM attacks

The Next Evolution: Passwordless MFA

From usability to cost efficiency to security, legacy and password-based MFA is significantly flawed.

This is where HYPR's True Passwordless™ MFA comes in.

True Passwordless MFA removes centralized passwords and shared secrets from the equation entirely. It enables users to authenticate their identity on their mobile device's native biometrics (e.g. Face ID), decentralized PIN, security keys, and platform authenticators built into existing devices such as Windows Hello and Touch ID.

By combining public-key encryption with user-initiated authentication, HYPR brings secure, fast, passwordless login to workstations and applications across the enterprise.

> “ Password lockouts generate service desk calls and lost user productivity. The adoption of HYPR passwordless is the rare cyber investment that returns immediate and measurable bottom line benefit.
>
> **- Karl Mattson, CISO** ”

The Impact of True Passwordless™ MFA

Eliminate risks associated with password use and reuse

Legacy and password-based MFA leaves companies and users exposed. Deploying passwordless MFA removes that threat.

Save on operational time and costs

Reduce the day-to-day impact of security risks on technical and helpdesk teams, and slash employee downtime caused by password friction.

Deliver a seamless and frictionless user experience

Elevate security without layering on additional points of frustration for workers and customers.

Secure, frictionless authentication can be realized by looking at it from a different angle — not by adding layers of shared secrets but by eliminating them altogether. By reimagining identity security you change the economics of an attack, strengthen your security posture, and improve the login experience.

ELIMINATE THE TARGET

www.HYPR.com

1001 Ave of the Americas, 10th Floor
New York, NY 10018
1-866-GET-HYPR