Passwordless Authentication vs MFA: Three Independent Axes That Most Teams Conflate

Fundamentals / Last updated 2026-03-05 / https://www.scrambleid.com/learn/passwordless-authentication-vs-mfa

In one sentence: Passwordless authentication removes the password; MFA requires multiple factors. They are different axes, and the strongest enterprise posture is phishing-resistant passwordless MFA, where no password is involved AND the ceremony cannot be phished.

TL;DR (canonical)

- **Passwordless** = no reusable password in the login ceremony. It says nothing about how many factors are required or whether the method is phishing-resistant.
- **MFA** = two or more authentication factors (something you know, have, or are). It says nothing about whether a password is one of those factors.
- **Passwordless MFA** = multiple factors, none of which is a password. Example: FIDO2 passkey (device possession) + biometric or PIN (user verification).
- **Phishing-resistant passwordless MFA** = passwordless MFA where the authentication ceremony cannot be relayed or proxied. FIDO2/WebAuthn is the primary example: origin binding prevents phishing, device binding prevents theft, and no shared secret crosses the network.
- Not all passwordless is MFA. Not all MFA is passwordless. Not all of either is phishing-resistant. The terms are independent, and conflating them creates dangerous gaps in policy.

Why does this distinction matter?

Because "go passwordless" and "deploy MFA" are not interchangeable security directives, and treating them as equivalent leads to real gaps.

Consider these four scenarios:

Scenario	Passwordless?	MFA?	Phishing-resistant?
Password + SMS OTP	No	Yes	No
Magic link (email)	Yes	No (single factor)	No

Scenario	Passwordless?	MFA?	Phishing-resistant?
Password + FIDO security key	No	Yes	Partially (key is PR, but password is still phishable)
FIDO2 passkey with biometric UV	Yes	Yes	Yes

Only the last row is the target state. The first three each have at least one critical weakness, and all three are commonly described as either "passwordless" or "MFA" in vendor marketing.

What exactly is passwordless authentication?

Passwordless authentication is any method that verifies identity without the user entering a reusable password. The password is removed from the ceremony.

Methods that qualify as passwordless:

- FIDO2/WebAuthn passkeys (strongest)
- Platform authenticators, Windows Hello, Touch ID, Face ID (when using WebAuthn)
- Magic links sent to email
- SMS or email OTP (the code replaces the password)
- Push notification with approve/deny

The critical point: passwordless describes what is absent (the password), not what is present. A magic link is passwordless, but it is single-factor and not phishing-resistant. Removing the password is necessary but not sufficient for strong authentication.

What exactly is MFA?

Multi-factor authentication requires the user to present two or more distinct authentication factors from different categories:

- **Something you know**, password, PIN, security question answer
- **Something you have**, phone, security key, smart card
- **Something you are**, fingerprint, face, voice

MFA does not care whether a password is involved. Password + OTP is MFA. Password + fingerprint is MFA. Security key + PIN is MFA. The requirement is factor diversity, not password absence.

NIST SP 800-63B defines authenticator assurance levels (AAL) based on the number and type of factors. AAL1 allows single-factor. AAL2 requires multi-factor. AAL3 requires multi-factor with a hardware-bound authenticator.

Where do they overlap?

Passwordless MFA is the intersection: multiple factors, none of which is a password.

The cleanest example is a FIDO2/WebAuthn passkey with user verification enabled:

- **Factor 1 (something you have):** The device holding the private key.
- **Factor 2 (something you are / know):** The biometric or PIN that unlocks the credential locally.

No password is entered. Two factors are present. And because WebAuthn validates the relying party origin before signing, the ceremony is also phishing-resistant as defined by CISA.

This is why FIDO2 passkeys carry the strongest assurance posture: they simultaneously solve three problems that are usually addressed separately (password elimination, multi-factor assurance, and phishing resistance).

What does "phishing-resistant" add to the picture?

Phishing resistance is a third independent axis. It means the authentication ceremony cannot be successfully proxied, relayed, or replayed through a fake verifier.

Method	Passwordless	MFA	Phishing-resistant
Password only	No	No	No
Password + SMS OTP	No	Yes	No
Password + push (approve/deny)	No	Yes	No (MFA fatigue, approval relay)
Password + push (number matching)	No	Yes	Partial (harder to relay, but not cryptographically bound)
Magic link	Yes	No	No
SMS OTP (no password)	Yes	No	No
Password + FIDO security key	No	Yes	Partial (key is PR, but password can still be phished separately)
FIDO2 passkey + biometric UV	Yes	Yes	Yes
PIV/CAC smart card + PIN	Optional (depends on setup)	Yes	Yes

The only methods that check all three boxes are FIDO2 passkeys with user verification and hardware-bound smart cards (PIV/CAC). Everything else compromises on at least one axis.

What should enterprises actually deploy?

The target is phishing-resistant passwordless MFA. The path depends on where you are today:

If you have passwords only (no MFA): Deploy phishing-resistant MFA immediately. FIDO2/passkeys are ideal because they eliminate the password and add phishing-resistant MFA in one step. If passkey rollout takes time, use push MFA with number matching as a transitional control, but understand it is not fully phishing-resistant.

If you have password + OTP MFA: Upgrade to FIDO2/passkeys. This replaces both the password and the phishable OTP in one move. Keep OTP as a monitored break-glass fallback, not as the default ceremony.

If you have passwordless but single-factor (magic links, SMS OTP): You have removed the password but weakened your factor count. Add a second factor or migrate to passkeys, which are inherently multi-factor.

If you have FIDO2 passkeys on web: Extend the same cryptographic identity to other channels, voice, desktop, in-person, M2M. Web-only passwordless MFA leaves the other channels as the weakest link.

Key Takeaway

Passwordless authentication and MFA are independent concepts. Passwordless means no reusable password is used. MFA means two or more factors are required. Passwordless MFA, specifically FIDO2/WebAuthn passkeys with user verification, is the strongest enterprise pattern because it eliminates the shared secret, requires multi-factor assurance, and is cryptographically phishing-resistant. Not all passwordless methods are MFA (magic links are single-factor), and not all MFA is passwordless (password + OTP is the most common MFA pattern). NIST SP 800-63B and CISA both distinguish phishing-resistant methods from weaker alternatives.

FAQ

What is the difference between passwordless authentication and MFA?

Passwordless authentication removes the password from the login ceremony. MFA requires two or more authentication factors, which may or may not include a password. They solve different problems: passwordless eliminates the shared secret, while MFA adds defense in depth. The strongest approach combines both, phishing-resistant passwordless MFA, where the user authenticates with a device-bound credential and local biometric, with no password involved.

Is passwordless authentication the same as MFA?

No. Passwordless means no password is used. MFA means multiple factors are required. A user who logs in with only a magic link is passwordless but single-factor. A user who logs in with a password plus an OTP is MFA but not passwordless. A user who logs in with a FIDO2 passkey (device possession + biometric unlock) is both passwordless and MFA.

What is phishing-resistant passwordless MFA?

Phishing-resistant passwordless MFA is authentication that uses no password, requires two or more factors, and cannot be bypassed by phishing or real-time credential relay. FIDO2/WebAuthn passkeys are the primary example: the device provides the possession factor, the biometric or PIN provides the user-verification factor, the origin binding prevents phishing, and no shared secret crosses the network.

Can MFA be phishing-resistant without being passwordless?

In theory, yes, certificate-based authentication (PIV/CAC) with a hardware token and PIN is phishing-resistant MFA that could coexist with passwords. In practice, most phishing-resistant MFA methods are also passwordless because the underlying protocol (WebAuthn, client-authenticated TLS) does not use a password at all.

Should enterprises deploy passwordless or MFA first?

If you have neither, deploy phishing-resistant MFA first, it provides immediate security improvement. If you already have OTP-based MFA, upgrade to phishing-resistant passwordless MFA (FIDO2/passkeys) because it simultaneously eliminates the password, adds phishing resistance, and reduces user friction. Deploying passwordless without multi-factor strength (e.g., magic links alone) weakens your posture.

Does passwordless MFA work beyond web login?

Most passwordless MFA solutions focus on browser-based login. For enterprises where authentication risk spans the call center, desktop workstations, in-person transactions, and machine-to-machine APIs, the same cryptographic identity needs to extend across all channels. A passwordless MFA ceremony that only works in the browser leaves the other channels relying on weaker methods.

References (public)

- W3C WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/
- FIDO Alliance, Passkeys: https://fidoalliance.org/passkeys/

- NIST SP 800-63B (Authentication and Lifecycle Management): https://csrc.nist.gov/pubs/sp/800/63b/4/final
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- NIST SP 800-63-4 (Digital Identity Guidelines): https://csrc.nist.gov/pubs/sp/800/63/4/final

---

Related reading

- What Is Passwordless Authentication?
- Phishing-Resistant Web Authentication
- XFactor Step-Up
- Compliance Mapping: NIST and CISA