What Is Phishing-Resistant MFA? The Authentication Bar That AI Cannot Defeat

Definitions / Last updated 2026-06-11 / https://www.scrambleid.com/learn/what-is-phishing-resistant-mfa

In one sentence: Phishing-resistant MFA is an authentication ceremony that cannot be replayed by a phishing site or relayed by a man-in-the-middle attacker, because the cryptographic assertion binds to the relying-party origin and the private key never leaves the user's hardware-protected key store.

TL;DR (canonical)

- **Definition:** Authentication that cannot be phished, relayed, or replayed, because the cryptographic ceremony binds to the relying-party origin and uses a hardware-bound private key.
- **What qualifies:** FIDO2/WebAuthn (passkeys, security keys) and PKI-based authenticators (PIV/CAC smart cards).
- **What doesn't:** SMS OTP, TOTP (Google Authenticator and similar), push notifications, knowledge-based questions, voice biometrics, magic links.
- **Why it matters:** MFA-fatigue and adversary-in-the-middle (AiTM) phishing have made non-phishing-resistant MFA increasingly easy to defeat. Multiple high-profile breaches (Twilio, Uber, Cisco, MGM) have started with non-phishing-resistant MFA being bypassed.
- **Who requires it:** OMB M-22-09 for federal; CISA as the canonical guidance; FedRAMP, CJIS, NYDFS, PCI DSS v4.0.1, and most regulated industries are converging on the same bar.

The formal definition

CISA's "Implementing Phishing-Resistant MFA" fact sheet is the canonical reference. The defining property: the authentication ceremony binds cryptographically to the relying-party origin (the website, application, or service the user is authenticating to), so an attacker who proxies the user's session through a phishing site cannot produce a valid assertion for the real origin.

NIST SP 800-63-4 describes this property as **verifier-impersonation resistance**: an authenticator that resists impersonation of the verifier (the relying party). Verifier-impersonation resistance plus hardware-bound key storage and bound-channel binding define the AAL3 authenticator properties.

In practice, "phishing-resistant" means the authentication ceremony has all of these properties:

1. **Origin binding.** The signed authentication assertion includes the origin (e.g., the URL of the relying party). A phishing site at a different origin cannot produce a valid assertion for the real origin.
2. **Hardware-bound key.** The private key is held in a hardware-protected key store (Secure Enclave on Apple, TPM on Windows, Android Keystore, hardware security key) and never leaves it.
3. **Replay resistance.** Each authentication assertion includes a fresh challenge. A captured assertion cannot be replayed.
4. **Adversary-in-the-middle resistance.** Even if an attacker proxies the user's session, the ceremony cannot be relayed because the user's authenticator only signs assertions for the origin it is challenged from.

What qualifies as phishing-resistant MFA

The two ceremonies CISA and OMB recognize:

FIDO2/WebAuthn (and passkeys)

FIDO2/WebAuthn is the W3C and FIDO Alliance specification for browser-based cryptographic authentication. The browser mediates the ceremony: the relying party sends a challenge, the browser scopes the challenge to the origin, the authenticator (platform authenticator like Touch ID/Windows Hello, or external security key) signs over the challenge plus the origin, and the assertion is returned.

Phishing-resistant by construction. A phishing site at a different origin cannot make the authenticator sign a valid challenge for the real origin.

Passkeys are an implementation of FIDO2/WebAuthn credentials with cross-device synchronization in some implementations. Synced passkeys preserve phishing-resistance; what differs is the recoverability and the credential lifecycle.

For deeper coverage, see What Is FIDO2? and What Are Passkeys?.

PKI-based authenticators (PIV, CAC, smart cards)

PIV (federal civilian) and CAC (DoD) cards built to FIPS 201-3 carry an X.509 certificate and a private key on the card. The authentication ceremony is a smart-card challenge-response: the relying party sends a challenge, the card signs over it with the private key, and the assertion is verified against the certificate.

Phishing-resistant by construction. The user does not enter a code that can be replayed; the cryptographic ceremony binds to the verifier.

Derived PIV (NIST SP 800-157) is a credential cryptographically derived from a PIV credential, issued in software or to a hardware key on a mobile device. Derived PIV preserves phishing-resistance for contexts where smart-card readers are impractical.

What does not qualify

Authenticator	Why it isn't phishing-resistant
Password	Trivially phishable; one-way knowledge factor with no origin binding
SMS OTP	SIM swap, SS7 interception, and AiTM relay all defeat it
Voice OTP	Same vulnerabilities as SMS plus audio capture
Email OTP	Email account compromise becomes the new attack surface; AiTM still relays the code
TOTP (Google Authenticator, Authy, 1Password OTP)	The shared seed can be phished; the user types the code into the phishing site, attacker replays
Push notifications (Duo Push, Microsoft Authenticator without number-matching)	MFA-fatigue and AiTM relay; the user's "Approve" action does not bind to origin
Push with number-matching and contextual approval	Better, but still not origin-bound. AiTM proxies that show the legitimate context can defeat it
Voice biometrics ("we recognize your voice")	Increasingly defeated by deepfake voice cloning
Knowledge-based questions (mother's maiden name, etc.)	All available to attackers via breaches
Magic links	Email account compromise and AiTM relay

The pattern: any authentication ceremony where the user transmits a code, types into a UI, or approves a prompt that does not cryptographically bind to the origin can be relayed.

Why it matters now

Three converging factors made phishing-resistant MFA the new bar:

1. AiTM phishing kits are commoditized. Tools like Evilginx, Modlishka, and Muraena let an attacker stand up a phishing proxy in minutes. The proxy captures username, password, and the user's MFA approval, then replays the session. Push notifications and TOTP are defeated as easily as passwords.

2. MFA fatigue works. Repeated push prompts overwhelm users. Multiple high-profile breaches (Uber, Cisco) have started with the user accepting one too many push prompts.

3. Voice deepfakes are cheap. Voice biometrics as the sole authenticator is increasingly defeated by AI-generated voice cloning. The contact-center authentication problem is real.

The response was the OMB M-22-09 directive (January 2022), CISA's phishing-resistant MFA guidance, and a wave of regulatory updates. NYDFS Part 500, PCI DSS v4.0.1, the FTC Safeguards Rule, FedRAMP baselines, and CJIS Security Policy have all moved.

Phishing-resistant MFA vs other MFA terminology

Term	What it means	Is it phishing-resistant?
MFA (Multi-Factor Authentication)	Two or more factors from different categories	Sometimes, depending on factors used
2FA (Two-Factor Authentication)	Exactly two factors	Sometimes, depending on factors used
Strong MFA	Marketing term, no formal definition	Varies by vendor
Adaptive MFA / Risk-based MFA	MFA prompted based on risk signals	Varies by factor used at the prompt
Passwordless MFA	MFA without a password factor	Sometimes; passwordless is independent of phishing-resistance
Phishing-resistant MFA	MFA that cannot be replayed or relayed	Yes, by definition
MFA at AAL2	NIST 800-63 AAL2 properties	Has resistance to phishing but not full verifier-impersonation resistance
MFA at AAL3	NIST 800-63 AAL3 properties	Yes; verifier-impersonation resistance is a defining AAL3 property

For the AAL framework, see What Are NIST AAL Levels?.

Who requires phishing-resistant MFA

Mandate / Framework	Requirement
OMB M-22-09	Federal staff, contractors, partners by FY24; phishing-resistant options on public-facing services
CISA Phishing-Resistant MFA Fact Sheet	Canonical federal guidance
FedRAMP (Moderate, High)	NIST 800-53 IA-2(8) impersonation resistance for privileged users
NYDFS 23 NYCRR Part 500 (as amended 2023)	MFA for any individual access; phishing-resistant increasingly the default for privileged
PCI DSS v4.0.1	Replay-resistant authentication factors; verify current version with QSA
FBI CJIS Security Policy	Advanced authentication for CJI access
FTC Safeguards Rule (amended 2023)	MFA for non-bank financial institutions
HIPAA Security Rule (proposed 2024 NPRM)	Moves toward explicit MFA for ePHI access

Mandate / Framework	Requirement
OMB M-24-15 (FedRAMP Modernization)	Reinforces M-22-09 direction for federal Cloud
Industry-specific: HITRUST, CMMC, IRS Pub 1075	Each layers additional requirements aligned with the federal direction

For deeper coverage on specific industries, see the industry guides for Financial Services, Healthcare, SaaS / Cloud, Retail / Hospitality, and Government / Public Sector.

Common misconceptions

"We have MFA, so we're phishing-resistant." Most enterprise MFA today is push or TOTP. Both can be defeated by AiTM phishing or MFA-fatigue. "MFA" without a phishing-resistant factor is not phishing-resistant.

"Number-matching push is phishing-resistant." Number-matching is an improvement (it defeats fatigue and basic AiTM). It still doesn't bind to origin, so a sophisticated AiTM proxy that shows the legitimate context can defeat it. CISA recognizes number-matching as a step up but not as phishing-resistant.

"FIDO U2F is the same as FIDO2." FIDO U2F is the predecessor specification. Both are phishing-resistant by construction. FIDO2/WebAuthn is the current standard.

"Hardware security keys are the only phishing-resistant option." Platform authenticators (Touch ID, Face ID, Windows Hello) using FIDO2/WebAuthn are also phishing-resistant. Hardware security keys (YubiKey, etc.) are one form factor among several.

"We just need phishing-resistant on web. Voice can stay on KBA." The fraud follows the path of least resistance. KBA at the contact center remains a primary attack surface in financial services and healthcare even after web-side phishing-resistance is in place.

How to roll out phishing-resistant MFA

A practical sequence for an enterprise that is not starting from zero:

1. **Inventory authentication paths.** Enumerate every place a user, contractor, partner, or service authenticates: web, mobile, desktop, voice, email-link, recovery, partner integration, M2M.
2. **Score each path.** Phishing-resistant today, capable of being phishing-resistant, or fundamentally not (KBA, SMS).
3. **Prioritize by blast radius.** Privileged access, high-risk transactions, customer-data export, and identity-proofing-bound credentials first.
4. **Pilot with a low-friction population.** Engineering, IT security, ops teams that can absorb deployment friction.

5. **Roll forward through workforce SSO.** Then partner integrations, then customer-facing if applicable.
6. **Address recovery and break-glass.** A phishing-resistant primary with an SMS-based recovery is not phishing-resistant. See Recovery and Fallback Playbook.
7. **Address the contact center.** This is the single most overlooked path in regulated industries.
8. **Address machine-to-machine.** Sender-constrained tokens (mTLS, DPoP), short-lived credentials, cloud workload identity.

The endpoint is a single phishing-resistant identity that travels across web, mobile, voice, in-person, and machine channels, with audit evidence at every authentication event.

Key Takeaway

Phishing-resistant MFA is an authentication ceremony that cannot be replayed by a phishing site or relayed by a man-in-the-middle attacker, because it binds cryptographically to the relying-party origin and uses a hardware-bound private key. FIDO2/WebAuthn (including passkeys and security keys) and PKI-based authenticators (PIV/CAC) qualify. SMS, TOTP, push notifications, voice biometrics, and KBA do not. CISA's phishing-resistant MFA fact sheet, OMB M-22-09, and a wave of regulatory updates (NYDFS Part 500, PCI DSS v4.0.1, FedRAMP, CJIS) have made phishing-resistant the new bar across federal, financial, healthcare, and SaaS contexts. The biggest deployment failure mode is recovering to a non-phishing-resistant path (SMS recovery, help-desk reset) that becomes the new attack surface.

FAQ

What is phishing-resistant MFA?

Phishing-resistant MFA is an authentication ceremony that cannot be replayed by a phishing site or relayed by a man-in-the-middle attacker. It typically achieves this by binding the authentication assertion cryptographically to the relying-party origin and by using a private key that never leaves the user's hardware-protected key store. CISA's canonical fact sheet identifies FIDO2/WebAuthn and PKI-based authenticators (PIV, CAC) as meeting the bar.

Why isn't push-OTP MFA phishing-resistant?

Push-OTP is vulnerable to two attack patterns. MFA-fatigue: the attacker repeatedly triggers push prompts until the user approves out of frustration or by mistake. Adversary-in-the-middle (AiTM): the attacker proxies the user's session through a phishing site, captures the user's password, prompts the user to approve the push, and steals the resulting session. Both attacks succeed because the user's approval action does not bind to the relying-party origin.

Are passkeys phishing-resistant?

Yes. Passkeys are an implementation of FIDO2/WebAuthn credentials, which are phishing-resistant by construction: the cryptographic ceremony binds to the relying-party origin, and the private key remains in the user's hardware-protected key store. A phishing site that proxies the legitimate site cannot make the user's authenticator sign a valid challenge for the real origin. See What Are Passkeys?.

Is SMS-based MFA phishing-resistant?

No. SMS is vulnerable to SIM-swap attacks (the attacker takes over the phone number with the carrier), SS7 attacks (interception in the carrier signaling layer), and AiTM phishing (the user types the SMS code into the phishing site). NIST SP 800-63B has discouraged SMS for higher-assurance contexts since 2017.

Does the government require phishing-resistant MFA?

OMB M-22-09 (January 2022) requires phishing-resistant MFA for federal staff, contractors, and partners, and requires phishing-resistant MFA options for public-facing federal services. CISA's phishing-resistant MFA fact sheet is the canonical guidance. State and local programs, FedRAMP, CJIS, and federal grant programs increasingly align with the same direction.

What's the difference between phishing-resistant MFA and passwordless?

These are different properties. Phishing-resistant means the authentication ceremony cannot be replayed by a phishing site or relayed by a man-in-the-middle. Passwordless means there is no shared secret (no password). Most modern phishing-resistant methods (FIDO2/WebAuthn, passkeys) are also passwordless, but the two terms describe different security properties. Passkeys, for example, are both passwordless and phishing-resistant.

References (public)

- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- OMB M-22-09: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- W3C WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/
- FIDO Alliance, Passkeys: https://fidoalliance.org/passkeys/
- NIST SP 800-63-4: https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST FIPS 201-3 (PIV): https://csrc.nist.gov/pubs/fips/201-3/final
- NIST SP 800-157 (Derived PIV): https://csrc.nist.gov/pubs/sp/800-157/final

---

Related reading

- What Is FIDO2?
- What Are Passkeys?
- What Are NIST AAL Levels?
- Phishing-Resistant Web Authentication
- Compliance Mapping: NIST and CISA
- Recovery and Fallback Playbook
- Enterprise Passwordless Vendors Compared