Enable Legacy Applications with Phishing-Resistant Multifactor Authentication (MFA)

⚠ The Challenge

As cyber threats escalate, traditional network authentication, usernames, and passwords are no longer enough

Contractors, partners, and customers accessing your application and data externally demand stronger identity assurance

- ✓ Push notifications?
- ✓ SMS codes?
- ✗ These methods are vulnerable to phishing attacks and push bombing

Mandates Driving Change

New guidance and mandates require Phishing-resistant MFA at the individual application level:

- OMB (Office of Management & Budget)
- CISA (Cybersecurity & Infrastructure Security Agency)
- DOD (Department of Defense)
- NIST (National Institute of Standards & Technology)

Your organization must stay ahead to protect data and comply with evolving regulations.

Why Now?

Cybersecurity threats are rising. Requirements are tightening. Your legacy applications can't afford weak links.

- 🔐 Stop phishing attacks
- ⚡ Modernize legacy apps securely
- 📈 Meet federal & industry mandates
- 👤 Protect your workforce, partners & customers

What is Phishing-Resistant MFA?

Phishing-resistant MFA uses cryptographic credentials that cannot be intercepted or reused by attackers.

- No shared secrets like passwords or SMS codes
- No dependency on vulnerable mobile push notifications
- Secure tokens bind authentication to the legitimate application

➡ Stronger security at the application level for staff, contractors, partners — and an option for customers

XTEC

Let's Get Started

Enable phishing-resistant MFA for your applications today.

👉 Contact: sales@xtec.com | www.xtec.com

XTec's Phishing-Resistant MFA: Key Benefits

Enable Legacy Systems — No Rip & Replace

- Integrate with existing applications
- Add phishing-resistant MFA without major redevelopment

Cloud-Delivered & Scalable

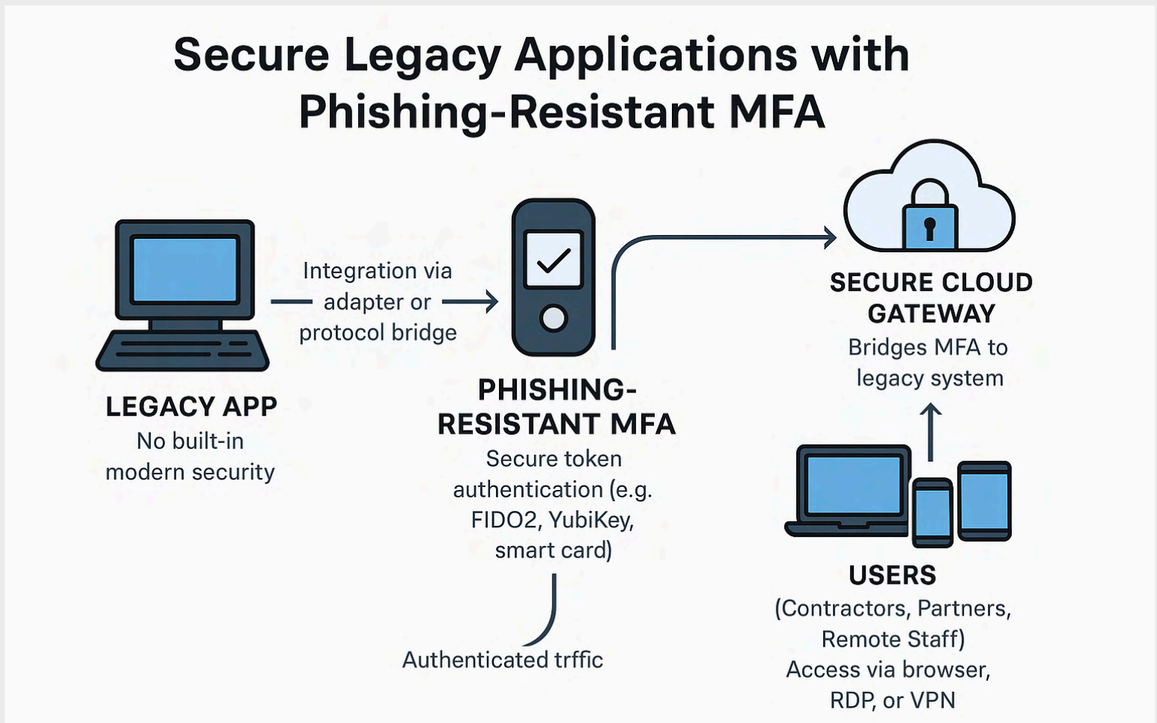
- Cloud-Delivered & Scalable
- SaaS delivery for simplified management
- High-assurance authorization at FedRAMP High

Proven Federal Expertise

- Over two decades of supporting mission-critical operations
- Solutions trusted by civilian and defense agencies

Flexible Token Options

- PKI-based tokens- Same security as the federal government without bureaucracy
- Derived PIV/CAC credentials
- FIDO2-compliant hardware tokens
- Mobile cryptographic credentials



Benefit to Customers

- Enhance Security — Defend against phishing and credential theft
- Simplify Management — Easy token management and user experience
- Ensure Compliance — Meet federal mandates With the same technical security used by all federal agencies
- Future-Proof — Build security resilience as threats evolve

About XTec

- 25+ years securing federal missions — XTec has delivered trusted identity and credentialing solutions for agencies for over two decades.
- Proven cryptographic identity management — We provide PKI-based identity solutions with FIPS-validated cryptography to ensure secure authentication and authorization.
- Comprehensive authentication, validation, and authorization — XTec enables secure, seamless integration across physical and logical access systems.
- Cloud-enabled services at FedRAMP High — Our identity solutions are hosted in FedRAMP High environments for maximum security and compliance..
- Trusted by federal civilian agencies and the DoD — Millions of credentials are secured by XTec for civilian and defense missions.
- Value-added identity management — XTec simplifies and strengthens credential lifecycle management through cryptographic automation