emudhra
Trust Delivered

Why Multi-Factor Authentication Must Be Phishing-Resistant

emudhra
Trust Delivered

Attackers Don’t Break In, They Log In

- Most breaches start with valid credentials
- Phishing supplies attackers with real user access
- MFA authentication is meant to stop this, but often doesn’t
- The problem is not MFA adoption, but MFA quality

MFA Was Built for a Different Threat Model

Traditional MFA:

- Designed to protect passwords, not stop real-time phishing
- Assumes users can reliably detect fraud
- Relies on shared secrets and one-time codes
- Fails when attackers proxy authentication in real time

This Is Where eMudhra's MFA Delivers

- Phishing-resistant MFA using certificate-based authentication
- Device-bound private keys secured in hardware
- No OTPs, no prompts, no replayable credentials

eMudhra replaces fragile MFA with cryptographic identity assurance.

emudhra
Trust Delivered

The MFA Fatigue Trap

- Repeated push prompts condition users to approve
- Social engineering accelerates approvals
- Helpdesk-driven MFA resets weaken defenses
- MFA authentication becomes a human vulnerability

emudhra
Trust Delivered

When “Multi-Factor” Is Still Phishable

- OTPs can be captured and replayed
- Push approvals can be proxied
- Session tokens can be hijacked
- MFA authentication fails when credentials remain reusable

emudhra
Trust Delivered

The Shift to Cryptographic Proof, Not Prompts

- **Phishing-resistant MFA removes reusable secrets**
- **Authentication is bound to:**
  - Device
  - Application
  - Cryptographic keys
- **Identity becomes something attackers cannot copy**

emudhra
Trust Delivered

What Phishing-Resistant MFA Actually Looks Like

- Certificate-based authentication
- Hardware-backed credentials
- Device-bound identity
- Biometric unlock of cryptographic keys

No codes. No prompts. No replay.

emudhra
Trust Delivered

Zero Trust Starts at Authentication

- **Every access request must be verified**
- **Every session must be defensible**
- **MFA authentication must:**
  - Prove identity cryptographically
  - Validate device trust
  - Enforce least privilege

Zero Trust fails without phishing-resistant MFA

emudhra
Trust Delivered

Security Outcomes That Actually Change

- Account takeover becomes impractical
- Credential phishing loses value
- Reduced incident response cycles
- Stronger audit and compliance posture

This is what effective MFA authentication delivers

emudhra
Trust Delivered

Replace Fragile MFA with Cryptographic Identity

- Phishing-resistant MFA authentication that cannot be replayed or proxied
- Certificate-based, PKI-driven identity bound to users and devices
- Eliminates OTPs, push fatigue, and shared secrets
- Built for regulated, high-risk enterprise environments

Modern MFA starts with cryptographic proof, not user prompts

emudhra
Trust Delivered

Power Passwordless Zero Trust with eMudhra

- PKI-native identity and authentication platform
- Supports passwordless and Zero Trust architectures at scale
- Discover how leading enterprises secure their identities with eMudhra.

Visit: www.eMudhra.com