FEITIAN

WE BUILD SECIRITY

DIFFERENT TYPES OF MFA & WHAT YOU NEED TO KNOW

QUICK RECAP ON MFA

Authentication typically works with a few factors:

Something You Know	Something You Have	Something You Are
Password, Security Questions, PINs	Things In The Users' Possession, E.G., Smartphones, Hardware Tokens	Usually Biometric Factors (Fingerprint, Iris, Face ID, Etc)

Multi-factor authentication means that whatever application or service you're logging in to is double-checking that the request is really coming from you and not a hacker, by confirming the login with you through a separate venue, or factor.

MFA plays a pivotal role in bolstering digital security as it effectively neutralizes the risks posed by compromised passwords. Shockingly, over two-thirds of individuals still employ the same passwords across multiple accounts. In the event of a password being hacked, guessed, or phished, it no longer grants intruders access without approval at the second factor. Moreover, MFA goes beyond passwords, contributing to establishing a user's identity in a highly secure manner, making identity proofing a foundational element in the Zero Trust architecture.

DIFFERENT TYPES OF MFA

PHONE CALLBACKS

Phone callbacks are one of the less popular versions of MFA, but they're an effective – if time-consuming – way to implement a second factor. In a phone callback setup, once a user logs in, they receive an automated phone call that prompts them to approve or deny the access request

SMS BASED OTP

Usually consists of a short string of numbers sent to a smartphone. Passcodes definitely count as MFA. Since they rely on phone lines, however – which can be compromised – they represent the least secure method. Passcodes aren't a real hit with users, either: each code must be manually entered, which can be a nuisance.

ONE TIME PASSCODE (OTP) TOKENS

Many web security teams opt to arm their users with tokens. These typically are small keychain fobs that generate codes for users to enter as their second factor. Tokens are more secure than cellular delivered passcodes, as they don't rely on phone lines, but they don't address the annoyance of entering codes. Tokens are attractive because they are affordable and don't require system administrators to collect phone numbers — but they're battery-operated, and batteries die. Using tokens will mean dealing with the headache of timing replacements to avoid users losing access to crucial systems.

MOBILE AUTHENTICATOR APPS

Authenticator apps are exactly what they sound like: smartphone apps that handle the second-factor approval process as standard notifications. Authenticator apps require internet connectivity to deliver login approval requests, which is more secure than using phone lines.

MOBILE AUTHENTICATOR APP VARIANTS

Mobile Authenticator Apps come in various forms, offering convenience and improved user experience. The first variant is OTP-based, functioning similarly to OTP tokens programmed via QR codes.

The second variant is platform-based, with each platform like Microsoft, Duo, or Okta having its own authenticator that may utilize device biometric protection for added security. Users can verify their biometric (facial or fingerprint) before confirming authentication with a simple tap or push.

Lastly, the new FIDO variant involves a synced passkey, backed up and synchronized to the platform provider's infrastructure (e.g., Apple's iCloud, Google's, Microsoft's). While these authenticator apps offer enhanced UX, it's essential to remain cautious about compromising security levels.

PKI / X.509 /Smart Card

This type of MFA, popularized by PIV/CAC, remains a widely used authentication method, albeit with some administrative overhead. FIDO security keys have emerged as an evolution of PKI keys, offering improved user experience and streamlined authentication processes. While both approaches are effective in providing secure access, FIDO security keys present a more user-friendly and convenient option for users, enhancing overall MFA adoption and usability.

CONCLUSION

Multi-factor authentication (MFA) is a vital component of digital security, neutralizing the risks associated with compromised passwords. Different types of MFA, such as phone callbacks, SMS-based OTP, OTP tokens, and mobile authenticator apps, offer varying levels of security and convenience. As organizations continue to prioritize cybersecurity, adopting the most suitable MFA solution becomes paramount to safeguarding critical systems and sensitive data.

Explore FEITIAN's cutting-edge MFA solutions to enhance your organization's security posture and stay ahead in the ever-evolving digital landscape.