QUICK READ

MULTI-FACTOR AUTHENTICATION

Cyber security awareness Series | 23F17
Exclusively for members of ARIA by Sanjay Kadel, Infosec Partner

MFA or Multi-factor Authentication is a mechanism of authenticating a user for any system (including any application or device) through two or more pieces of evidence (factors).
In simple terms, MFA means requiring multiple credentials for access.

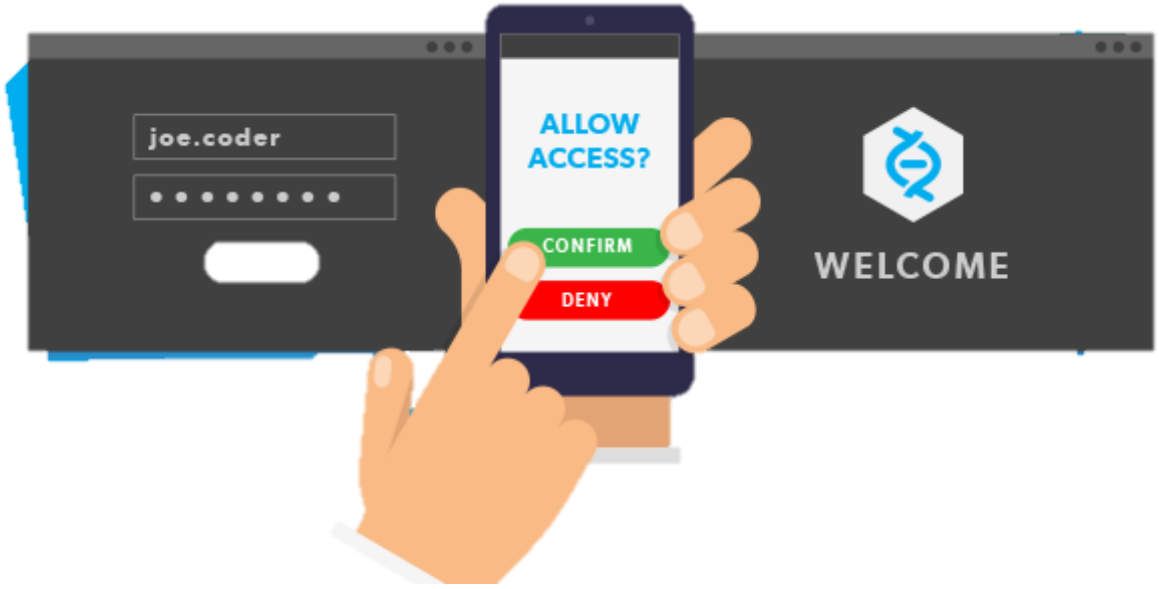
Traditionally only passwords were the way to authenticate, but with growing need for secured access, multi-factor authentication has become an utmost necessity.

Enabling MFA can block around 99.9% of automated attacks, 99% of bulk phishing attacks and 90% of targeted attacks.

Let's understand the concept of MFA in little more detail (what), know it's significance (why) and also know, ways to implement it (how) in our Daily digital life journey – DDLJ :)

I. Passwords are not enough

*While strong password practices is crucial, implementing or enabling multi-factor authentication (MFA) builds **an extra layer** of security by requiring **multiple credentials for access**. MFA significantly reduces the risk of unauthorized access, even if passwords are compromised or by-passed.*



Multi-factor authentication uses following categories of multiple ***authentication factors (i.e. credentials to gain and retain access)***.

These can be used to authenticate your access and retain the access until your usage session is complete.

1. Knowledge Factors

These are the factors related to – ***what you know***.

For instance,

- Password or Passcode
- Personal Identification Number (popularly called as PIN)
- Secret Questions & Answers
- Personal Authentication message

2. Possession Factors

These are the factors related to – ***what you have***.

For instance,

- Smart phone or Smart device (like tablet & laptop) – generate OTP / push Notification / Call / IVR authentication

- User's device – like IP address, Mac address
- User's location – like device geolocation
- Authenticator app
- OTP sent via Email / SMS / Instant messaging
- Physical Access badge – for display
- Remote Access badge – like Smart card
- Physical key
- Remote key – like Key fob
- Hardware token – like RSA SecurID token, Digital Signature Certificate (DSC) as token, USB devices
- Software token, Digital Signature Certificate (DSC) as file

3. Inherence Factors

These are the factors related to – ***what you are***.

For instance,

- Your biometric features – like your fingerprints, thumbprints, palm or handprints, voice, face, eyes retina or iris
- Your behavior – like your actions undertaken / responses provided to gain access to the system, pattern lock on mobile phones, way of walking, your location of activity, the network you use

II. Why is MFA Essential for Cybersecurity?

Now that we know, what is MFA and various categories and examples of MFA – knowledge factors, possession factors and inherence factors – ***the significance of adopting such MFA is further emphasized below.***

1. Adopt Zero Trust approach

'Zero Trust' approach is driven by the principle of "never trust, always check", as it aims to protect modern digital environments.
Multifactor authentication (MFA) is an important step, towards achieving Zero Trust. MFA adds a layer of security to access a network, application or database by requiring additional factors to prove the identity of users.

2. Stronger defence against password attacks

Password-based authentication is susceptible to various attacks, including password guessing, brute force attacks, and credential stuffing. MFA mitigates these risks by introducing an additional layer of authentication.
Even if an attacker manages to obtain or guess a password, they would still need access to the additional authentication factor to gain entry.

3. Protection against phishing and social engineering

Phishing attacks, where cybercriminals trick individuals into divulging their passwords, remain a significant threat. MFA provides an effective defence against such attacks as, even if a user falls victim to a phishing attempt and shares their password, the attacker would still require the additional factor to access the account.

4. Safeguard against credential theft

With the increasing frequency of data breaches, passwords are often exposed to cybercriminals. Many people reuse passwords across multiple accounts, making them vulnerable to credential stuffing attacks. MFA prevents unauthorized access even if passwords are compromised, as the attacker would still need the additional factor to gain entry.

5. Improved security for remote access

While working remotely, securing the remote access has become a top priority. MFA ensures that even if an employee's password is compromised, remote access to corporate networks and sensitive data remains protected, preventing unauthorized entry from external threats.

III. Implementing / Enabling MFA Best-practices

Lack of strong defence is understandable as an excuse for becoming victim of cyber security breaches / attacks but not using the available defence is not excusable.
So, please implement or enable MFA as much as possible.

1. Enable MFA on all Accounts

Whenever possible, enable MFA ***on all your online accounts***, including ***email***, ***social media***, ***banking***, and ***cloud services***. Most popular platforms and online accounts, offer MFA options.

2. Use App-Based Authentication

Instead of relying solely on SMS-based codes, consider using authenticator apps like Google Authenticator, Authy, or Microsoft Authenticator. These apps generate time-based codes, providing an extra layer of security.

3. Biometric MFA

Whenever available, leverage biometric authentication factors such as fingerprints or facial recognition for added convenience and security. Biometric data is unique to each individual and difficult to replicate, making it a robust form of authentication.

4. Adoption due to regulations

Several ***industry regulations*** now require or strongly recommend the use of MFA. For example, the Payment Card Industry Data Security Standard (PCI DSS) mandates the use of MFA for remote access to cardholder data.

Other ***legal regulations***, such as the GDPR in EU and HIPAA in USA encourage implementation of MFA as part of a comprehensive security strategy. In India, RBI has insisted on 'compulsory MFA' for the Banks and Fin-tech service providers like Wallets, UPI applications and payment gateways for financial transactions including online transfers, UPI payments and Credit card / Debit card transactions.

Even securities transactions could require OTPs sent on the mobile / email to authenticate the execution of such transaction / related activity.

Aadhaar based OTPs and use of DSC tokens, in many regulatory compliances like Income-tax, MCA, GSTIN, CKYC, and others have become the norm.

5. Keep backup methods

Ensure you have alternative MFA methods set up in case your primary authentication factor becomes unavailable. This prevents being locked out of your accounts if, for example, your smartphone is lost or damaged.

6. Avoid accounts / service providers not having MFA

Try to minimize and if possible, avoid accounts and service providers which do not offer MFA features.

7. Priority to cyber security over convenience

While MFA implementation may sound technical enablement of such tech-facility, it could also be deliberately avoided by many of us, to prioritize convenience additional authentication troubles. Well, I guess all the trouble is good! to avoid that one-moment of world crashing-down if wrongful access is gained by unauthorised hacker / attacker.

Multi-Factor Authentication (MFA) is an essential tool in today's cybersecurity landscape. By implementing MFA, you fortify your defences against password-related attacks, phishing attempts, and credential theft. ***Its simplicity and effectiveness make it a vital component of a comprehensive cybersecurity strategy.***

Embrace MFA to add an extra layer of protection to your digital identity and safeguard your valuable information in an increasingly interconnected world.

Let's save the day! by using MFA *— Sanjay Kadel*

Caveat – The design of controls and extent of cyber security best practices, to be adopted for the organization / user, should be based on business requirements (nature and size), risk assessment and feasibility (technical, financial, and operational), and compliance requirements! Arising from policies, contractual obligations, legal & regulatory mandates.
