INTELLIGENT TECHNICAL SOLUTIONS

Everything You Need to Know about Multi-Factor Authentication (MFA)

TABLE OF CONTENTS

I. **Introduction**: Understanding Multi-Factor Authentication

II. **Chapter 1**: Forms of Authentication

III. **Chapter 2**: Common Authentication Methods Used in MFA

IV. **Chapter 3**: Reasons to Implement Multi-Factor Authentication

V. **Chapter 4**: Steps to Implement MFA for Your Business

Introduction: Understanding Multi-Factor Authentication

Usernames and passwords can no longer adequately protect accounts and assets. Though they persist and will continue for years, sole dependence on these login credentials often leads to disaster. Businesses fall victim to cybercrimes and are impaired by their effects.

Multi-factor authentication (MFA) was made to counter the looming threats brought by the increasing vulnerability of passwords. As the name suggests, it requires users to go through multiple (at least two) authentication steps before gaining access to data, accounts, or systems. MFA is different from two-factor authentication (2FA), which requires only two types of authentication.

An example of MFA is being prompted to input a PIN sent to your mobile device or asked to scan your fingerprint when accessing your bank account. **These extra steps act as additional security layers that cybercriminals need to pass to launch an attack**.

At best, these authentication factors make it impossible for attackers to succeed. At worst, it makes the infiltration process long and laborious, giving you more time to react and prepare for whatever's to come.

Intelligent Technical Solutions (ITS) is a managed security services prover (MSSP) with over 20 years of experience helping organizations with their cybersecurity. We know that there's much to learn about MFA, including its different authentication forms and types, benefits, and proper implementation. We discuss all of that in this eBook, which compiles everything you need to know about the subject. After going through this, you should fully grasp MFA and its importance to your business.

Chapter 1: Forms of Authentication

You've undoubtedly heard and even used common authentication examples, such as one-time passwords and email codes. We'll dive deeper into those in a later chapter. For now, we'll discuss the different authentication categories that these examples fall into, and they are:

1. **Knowledge-based authentication (KBA)**. This uses things you know, such as login credentials, security questions, and personal identification numbers (PINs).
2. **Possession-based authentication**. As the name suggests, it uses things you have, like a physical USB key, token, badge, or subscriber identity module (SIM) card.
3. **Inherence-based authentication**. This pertains to biological traits or the things you are and includes fingerprints, facial recognition, and voice authentication.

The three mentioned above are common MFA forms that are widely used by businesses today. The following two forms are rarely applied, but we'll include them as they may grow in popularity:

4. **Location-based authentication**. This authentication type is possible through smartphones and other devices with a global positioning system (GPS).
5. **Time-based authentication.** This is a complicated form that detects a user's presence at a scheduled time of day or between a specified time interval while in a distinct location.

Chapter 2: Common Authentication Methods Used in MFA

Let's examine the most common authentication methods used in MFA applications. These are used in addition to your login credentials and other initial identity verification methods

1. Email Codes

Email codes are among the most popular authentication methods today. Their popularity is mainly due to their convenience.

With email codes, you only need an existing email account and internet connection. Once you attempt to log in to an MFA-enabled system or device, a code (usually a combination of numbers and letters) will be sent to said email. You can then use this to verify your identity and gain access.

But be warned: their popularity comes with a trade-off. Email codes pose a significant risk, especially now when email compromise is one of the top cybercrimes. Malicious actors can easily hack your accounts and bypass any authentication methods that utilize your email. So, convenient as they are, they aren't the most secure.

2. One-time Passwords (OTPs)

One-time passwords are **similar to email codes but sent as texts or calls.** They're equally popular and convenient since almost everyone nowadays has a cellphone.

However, they have **two significant drawbacks**: 1) They're **vulnerable to attacks like sim cloning or swapping**, and 2) they **have a time limit**. The codes expire in a short time, usually a few minutes, so if you have poor reception or aren't near your device, you may be unable to authenticate in time. There's the option of resending an OTP, but even that has a cooldown period.

As such, we don't recommend using SMS for multi-factor authentication, at least not as the primary and only option.

3 . Security Questions

Security questions pertain to a user's personal life and are used to verify their identity. There are two types: **static knowledge-based authentication** and **dynamic knowledge-based authentication**.

Static KBA allows users to pick the questions and answers. Sample questions may include "What's the name of your childhood pet?" or "What's your mother's maiden name?" The selected questions and answers are then stored and used by companies for verification.

Users won't have trouble remembering answers to static KBAs because they're relevant to their lives. However, the advent of social media has made personal information readily accessible. **Malicious actors can easily browse profiles and find the answers to these security questions.**

On the other hand, **dynamic KBA questions are based on a user's credit history or public records.** You could be asked about the kind of car registered to your name in 2009 or the address of your alma mater. These pieces of information are more complex to fish online and difficult to remember, so dynamic KBA is typically applied to systems requiring higher cybersecurity.

4 . Hardware Tokens

Hardware tokens are **physical keys that hold unique codes and interact with a device to verify your identity**. Imagine a flash drive that you plug into a computer to log in or a card that you tap into a turnstile for entry.

These tokens are considered one of the most secure authentication methods. The only way for tokens to be compromised is if the keys are misplaced, lost, or stolen. It cannot be compromised online.

As always, there is a catch; in this case, it's cost. **Applying hardware token authentication can be challenging for businesses with budget limitations.** They could use it for a limited number of users – preferably the highest-value ones – but securing all team members this way would be difficult.

5 . Software Tokens

Software tokens are often **used in authentication applications (or authenticators) installed on mobile devices**. Companies like Microsoft and Apple offer these third-party solutions to their users for increased safety.

These authenticators verify your identity in two ways:

- Sending a unique and expiring code through the app that you must input into the account
- Sending you a notification or login request, which you must approve or deny

We highly recommend enabling this authentication option whenever available because it provides convenience and security without much vulnerability. If there's anything to criticize, it's that **businesses rarely support this method of authentication**.

6 . Biometric Verification

Biometric verification **uses physical characteristics**, such as fingerprints, to verify your identity. It is commonly implemented on smartphones, mobile apps, and physical offices.

Since users have unique physical features, this **offers high security**. It's also convenient because you don't have to input anything physically. After registering your biometrics, you must only have your fingers or face scanned for verification.

Again, there is a disadvantage. Once biometric information is compromised, it is lost forever. **You cannot reset it like a password**. Because of this, biometrics is often used as a supplementary authentication form.

Chapter 3: Benefits of Multi-Factor Authentication

It's time to answer the lingering questions on your mind, like: "What's the point? Why does my business need MFA?"

There are many reasons to implement MFA. Much of it is about security, but it affects other business aspects, too. Here are the benefits of proper MFA implementation:

1 . Protection against password attacks

There's been an alarming rise in password attacks in recent years, with records stating that 941 attempts happen every second. Malicious actors are continuously growing smarter and discovering new ways to compromise passwords. It also doesn't help that businesses have poor password creation and management practices. With MFA, you add an additional (and needed) layer of defense against such attacks.

2 . Remote work security

Ideally, **your remote and hybrid workers should work on secure devices and connections managed by your IT team**. But you can't always guarantee that. Personal devices will come into play either through necessity or disobedience, which will put your network at risk. In such cases, MFA can ease your worries because it **makes it harder for cybercriminals to exploit unsecure networks, devices, and accounts.**

3 . Risk mitigation

MFA protects you from threats outside password attacks and remote work vulnerabilities. It'll keep you safe from any cyber threats that depend on unauthorized access. Not only will it tire malicious actors in some cases, but it will also make entry into your system impossible. We say "in some cases" because MFA alone won't make for a foolproof cybersecurity strategy, but it is a necessary component.

4. Regulatory compliance

Businesses that handle sensitive data must comply with strict security regulations that dictate the adoption of MFA. The Health Insurance Portability and Accountability Act (HIPAA) is an example of such regulation. Similar laws exist, and **compliance is necessary to maintain operations.**

5 . Cost savings

MFA adoption incurs significant costs, especially during initial setup, when you may be required to purchase hardware or software and conduct member training. You also need to hire experts to oversee and ensure proper implementation. Yes, it's expensive, but **the cost of investing in your defenses is peanuts compared to the average cost of data breaches.**

6 . Client trust and reputation building

Stakeholders want nothing more than to work with a trustworthy business. Cybersecurity initiatives such as MFA show your commitment to protecting your assets and their data. Such actions help boost business reputation and build client/consumer trust, ultimately **leading to stronger and longer-lasting relationships.**

7 . Futureproofing

Much like technology, cyber threats are ever-evolving. Malicious actors grow smarter by the day and continue to discover new ways of infiltrating networks and compromising data. The **best way to prepare your business for incoming threats, new or old, is to adhere to effective security practices,** including MFA.

8 . Peace of mind

Cyber threats are like intrusive thoughts that pop up in your mind every now and then and give you anxiety. Their existence makes you constantly fear getting attacked, affecting productivity and efficiency. Implement robust security measures to nip this problem in the bud and give yourself and your team members peace of mind.

Chapter 4: 9 Tips for Effective MFA Implementation

In the previous section, we enumerated the benefits of proper MFA implementation. Now, we'll give you tips on ensuring your MFA strategy is effective and convenient.

1. **Educate your users** about the value of MFA and its impact on their experience.
2. **Open communication lines** where members can send in their worries and inquiries.
3. **Implement MFA wherever possible** to guarantee absolute effectiveness.
4. **Deploy strategies and steps** and train your users on MFA to avoid pushback.
5. **Choose the right factors** that provide adequate protection and consider user availability and accessibility.
6. **Give users options** that fit their capabilities and yours as well.
7. **Ensure convenience**, especially when accessing systems or accounts that are used regularly.
8. **Regularly monitor and improve** your strategies based on risk mitigation impacts and user feedback.
9. Remember that **MFA is only one part of a robust cybersecurity strategy**.

Ensure Proper MFA Implementation with ITS

MFA boosts your business' defenses against the majority of today's cybercrimes. The risk of falling victim to cyberattacks is significantly lowered when MFA is enabled, and every member of your organization cooperates fully. This level of security allows you to focus on pushing your business forward and achieving your goals.

However, keep in mind that you only get its benefits when properly implemented and partnered with other cybersecurity strategies. If you need help with MFA adoption or strengthening your IT defenses in other ways, ITS is always ready to help.

We've been in the managed services market for 20 years and have worked with several businesses to fortify their cybersecurity approach. MFA is but one part of our services. We can offer much more—a full suite of cybersecurity services—to ensure that you are protected on all fronts.

Learn how we can help solve your cybersecurity and tech problems by meeting with one of our consultants today.

Intelligent Technical Solutions
(885) 204-8823
www.itsasap.com