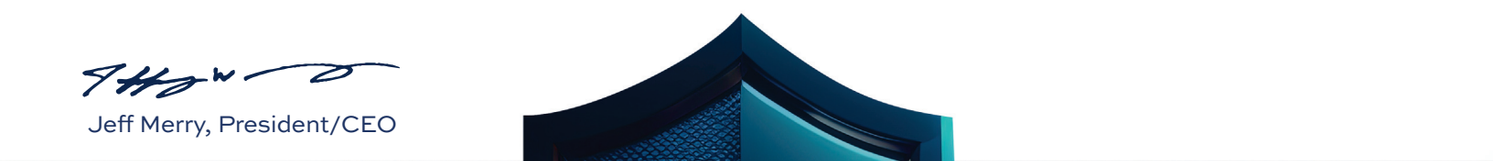
volcorp
APRIL 2023

THE FRONTBURNER

On a nearly monthly basis, we provide ***The FrontBurner*** to talk about a topic that should be top of mind for us all at that given time. I always provide a little commentary about life and then segway that into the content of the article. This week, I received the request to provide my narrative and was told the content of the article was going to be about how MFA "can help to protect you and your organization, what risks MFA can help mitigate, as well as what the future has in store for MFA." As I think about life, protecting ourselves, mitigating risks, and the uncertainty of the future, all I can think about is the senseless school shooting that just occurred here in Nashville. I don't want to write about it, but I can't stop the quivery chin and the sickening thought of how close it was to home.

So, instead of writing something fun and airy, I want to introduce this month's topic by just honoring those precious lives who were lost in this incident and to thank the police officers who rushed into the building and mitigated the situation to keep it from being even worse. Three beautiful children and three school workers whose names and pictures have been all over the news were lost. I hope we can all band together to lift their families and friends up in prayer. May they find strength and courage to endure the heartache of this new life without their loved ones and may those beautiful souls rest in peace.

Jeff Merry, President/CEO



Multi-Factor Authentication – A Deeper Dive

In October of 2022, we released a FrontBurner article titled, "The Five W's (and One H) of Multi-Factor Authentication," which introduced you to the who, what, when, where, why, and how of Multi-Factor Authentication (MFA). If you haven't had a chance to read it yet, we highly recommend reviewing it as a primer for this month's ***FrontBurner*** article. This month we delve even deeper into how MFA can help to protect you and your organization, what risks MFA can help mitigate, as well as what the future has in store for MFA.

Data breaches are one of the biggest issues in corporate security today, but we sometimes believe they only happen to other businesses. Consider not only the financial loss that could occur as a result of a data breach, but also the reputational damage your credit union could suffer. Regaining your current (and future) members' trust could take years to reestablish. Cybercriminals employ various techniques to gain unauthorized access to personal or corporate data, using phishing attacks, social engineering, credential stuffing, and brute-force attacks. One effective way to prevent these attacks is by requiring multiple factors for authentication.

MFA is a security mechanism that requires users to provide two or more different types of authentication credentials to gain access a system, application, or sensitive data, while making it more difficult for unauthorized users to gain access. Even if a bad actor manages to steal or guess one of the factors, they still need to provide additional authentication factors in order to gain access.

MFA can help prevent various types of attacks, including the following:

- **Social Engineering Attacks** - Social engineering attacks rely on tricking users into revealing their credentials. This includes more commonly known tactics such as Phishing.
- **Credential Stuffing Attacks** - Credential stuffing attacks involve using automated tools to try previously stolen usernames and passwords on various websites.
- **Password Guessing** - Password guessing involves using various techniques to guess a user's password to gain unauthorized access to a system or application. This is often based off open-source intelligence (OSINT) on your website, or various social media platforms.
- **Man-in-the-Middle Attacks** - In a man-in-the-middle (MITM) attack, an attacker intercepts communications between two parties to obtain sensitive information or modify the communication.
- **Physical Theft** - Physical theft involves stealing a user's authentication credentials, such as a security token or mobile device.

Continued...

Now that we have covered a few of the threats that most people think about when thinking of security, let's talk about what other ways MFA can help mitigate risks:

- **Increased Security** - MFA helps to increase security by adding an extra layer of protection against unauthorized access to various systems, such as your financial transaction platform.
- **Reduced Risk of Data Breaches** - MFA can reduce the risk of data breaches by making it more difficult for attackers to gain access to sensitive information, such as member Gramm-Leach-Bliley Act (GLBA) or Personal Identifiable Information (PII).
- **Compliance** - Many regulations and standards, such as PCI DSS, HIPAA, and GDPR, require the use of MFA to protect sensitive data. By implementing MFA, organizations can demonstrate compliance with these regulations and standards, reducing the risk of fines and penalties.
- **User Accountability** - MFA can also help to increase user accountability by providing an audit trail of authentication attempts. If a security breach occurs, the audit trail can help to identify the source of the breach and the steps taken to prevent it.
- **Flexibility** - MFA can be implemented in a variety of ways, such as hardware tokens, software tokens, biometrics, or mobile apps. This flexibility allows organizations to choose the most appropriate method of authentication for their specific needs, reducing the risk of compatibility issues.
- **Scalability** - MFA can be easily scaled to accommodate changes in an organization's needs, such as the addition of new users or the expansion of systems and applications. This scalability helps to ensure that security measures keep pace with organizational growth and development.

MFA is certainly not anything new. It has been around for many years, and the Federal Financial Institutions Examination Council (FFIEC) issued guidance[1] for the adoption of MFA by financial institutions in 2005. As adoption has grown, the industry has figured out what does and doesn't work, with the National Institute of Standards and Technology (NIST) putting out a special publication[2] in 2017 recommending the avoidance of any authentication solution that relies on your phone or phone number as part of the authentication. This includes all SMS text-based or voice call-based MFA factors.

More recently, President Biden signed the Zero Trust Executive Order[3] to push civilian agencies to further adopt MFA and phish resistant MFA practices. To clarify, this order states that you should stop using any MFA solution that is overly susceptible to phishing. This includes the previously mentioned SMS text-based and voice call-based factors, as well as one-time passwords (OTP) and push notifications.

> "The Zero Trust Executive Order...states that you should stop using any MFA solution that is overly susceptible to phishing. This includes the previously mentioned SMS text-based and voice call-based factors, as well as one-time passwords (OTP) and push notifications."

Does that mean that you can no longer use certain technologies for MFA, such as "push notifications" to a specialized app or SMS text-based passcodes? Not at all. The recommendation is to begin to transition away from these less secure methods of MFA as soon as possible or avoid them entirely as you begin to adopt the use of MFA in your environment. If you are currently using or planning on using one of the less phishing resistant MFA options, make sure to employ additional security layers to those factors. One example would be adding number matching[4] to push notifications as an additional layer of security that makes push notifications more phishing resistant.

As the requirement to adopt and implement MFA grows, as well as the need to keep MFA phishing resistant, we can expect to evolve in the following ways:

- **Biometric MFA** - The use of biometric factors, such as facial recognition, fingerprint scans, or voice recognition, is likely to increase as they are becoming more reliable and user-friendly. Biometric MFA provides a high level of security and is more convenient than traditional MFA.

Continued...

- **Risk-Based/Contextual MFA** - This type of MFA analyzes contextual factors, such as location, time, device, and behavior, to verify a user's identity. For example, if a user tries to log in from an unusual location or device, risk-based or contextual MFA may require additional authentication methods.

- **Passwordless MFA** - Passwordless MFA is a type of authentication that eliminates the need for passwords. It uses a combination of biometrics and other authentication factors, such as security tokens or smart cards, to authenticate users. Passwordless MFA provides a secure and convenient way to authenticate users without the need for passwords.

- **Windows Hello** - Windows Hello is a WebAuthn supported biometric authentication technology built into Windows 10 and Windows 11. It supports facial recognition, fingerprint recognition, and PIN authentication. Windows Hello provides a secure and convenient way to authenticate users without requiring passwords.

- **Apple FaceID** - Apple FaceID is a WebAuthn supported facial recognition technology built into newer iPhones and iPads. It uses a front-facing camera to scan a user's face and authenticate them. Apple FaceID provides a secure and convenient way to authenticate users without requiring passwords.

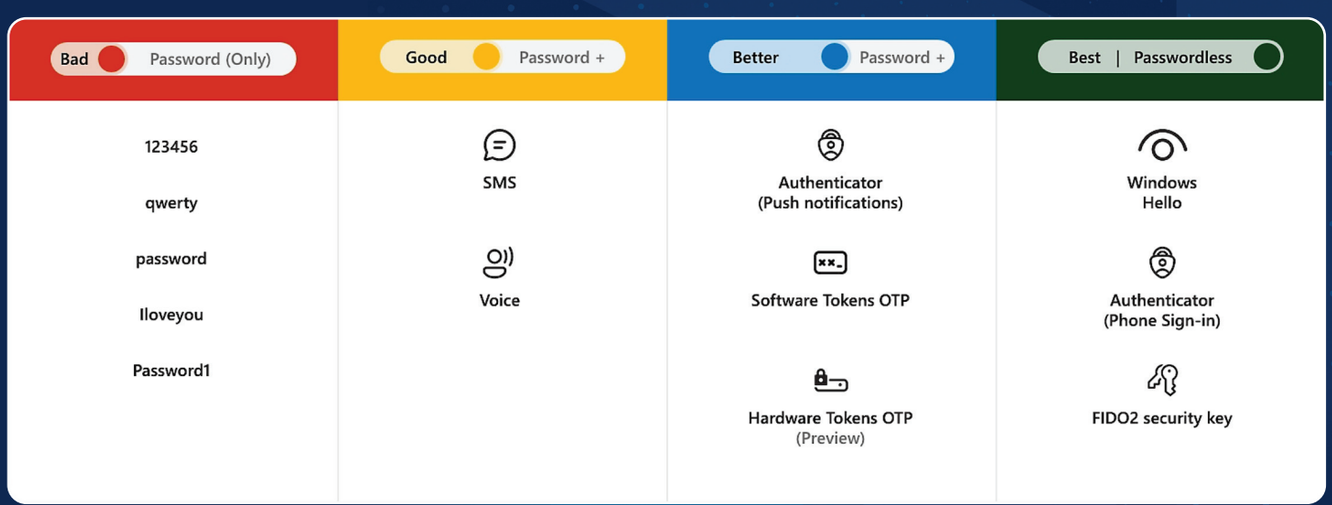


***Chart from** Microsoft.com

In addition, the MFA industry is moving towards more advanced and secure authentication methods that provide a higher level of security and convenience for users by leveraging technologies that we use daily to help assist with the adoption of MFA. Such technologies include the following:

- **FIDO2** - FIDO2 is an open authentication standard that supports the WebAuthn passwordless authentication standard. It uses public-key cryptography to authenticate users and provides strong security without requiring passwords. FIDO2 is supported by major browsers, including Chrome, Firefox, and Edge.

Overall, the future of MFA is likely to involve a combination of these different types of MFA and technologies to help provide a high level of security and user convenience. As technology continues to evolve, new authentication methods may emerge, and MFA will continue to adapt to meet the changing needs of organizations and its users.

(1) – FFIEC Releases Guidance on Authentication in Internet Banking Environment

(2) – NIST Special Publication 800-63-3, Part B

(3) – Zero Trust Executive Order

(4) – Implementing Number Matching in MFA Applications