volcorp
OCTOBER 2022

THE FRONTBURNER

Welcome to the October edition of ***The FrontBurner***! And, also, welcome to Fall weather! I'm so glad it is here. Too bad it comes and goes so quickly. This time of year is ideal for yard work, family activities outside, and, as we do A LOT of at our home, playing soccer. As far as I am concerned, there is no time like the present to get things done outside…especially when the weather is this awesome. Enjoy the weather…it will be cold way too fast!

If you keep reading, you will soon see there is no time like the present for getting other things done as well; namely protecting yourself and your organization from *bad actors*. In this month's edition of ***The FrontBurner***, we offer a little education on Multi-Factor Authentication (MFA). My 13-year-old has become quite a good soccer player, but I keep telling her there is always room to reinforce what you are already good at and to learn more to fine-tune your craft. Even if you are already savvy at MFA, I'd encourage you to read on…reinforce what you already know…and hopefully learn something more to fine-tune your ability to be that first line of defense.

With that, I hope you enjoy this month's edition of ***The FrontBurner***.

Jeff Merry, President/CEO

The Five Ws (and One H) of **Multi-Factor Authentication**

There are six basic questions (who, what, when, where, why and how) we were all taught as children to ask when learning something new or attempting to solve a problem. Let's ask those questions ourselves as we learn more about Multi-Factor Authentication, or MFA.

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is an authentication method using security technology that requires multiple means of identity verification from at least two or more of the different categories or "factors." The main factors of authentication are as follows:

- **Something You Know (Knowledge)** - ex: A password, passphrase, or PIN
- **Something You Have (Possession)** - ex: A security badge, smartcard, token, or smartphone
- **Something You Are (Inherence)** - ex: A biometric like a fingerprint, facial recognition, or voice recognition

Additionally, two newer factors include the following:

- **Somewhere You Are (Location) -** ex: At the office, or a trusted IP address (working from home)
- **Something You are Doing (Behavioral Analytics)** - ex: What time is it (regular business hours or after-hours), what device is being used to access (same device or new device), has this been accessed before (normal use or first-time use)

> "…54% of staff reuse the same passwords across multiple work accounts."

Why is MFA Important?

We all use passwords in our daily lives to gain access to email, social media, and countless other websites. We are typically forced to change these passwords periodically to try and stay a little safer online. However, this often is not the case, especially since around 70% of users reuse passwords across multiple sites, and 54% of staff reuse the same passwords across multiple work accounts. Stop for a moment and think about the websites that you use. Are you using a different username for each website where possible? Are all your passwords different for each website like security experts recommend? Are some passwords re-using parts of another password to try and make it easier to remember?

Continued…

The Five Ws (and One H) of Multi-Factor Authentication *(continued)*

volcorp

Now think about the total access someone would have on all those websites. Take your Google account, as an example. With a Google username and password, you have access to Email, Calendars, Google Documents, YouTube, and various other web applications. This interconnectedness can get even worse if you use the "Sign in with Google" option that several websites offer. Google is not the only platform that offers such features, with many websites allowing you to connect with your Apple ID, Facebook account, or Twitter account, just to name a few.

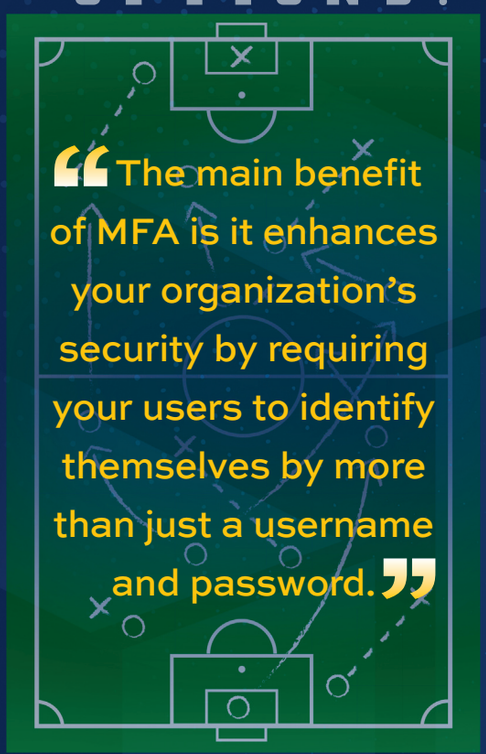
Now that you have an example of personal accounts and password usage, let's transition to think about your work accounts. What does that one username and password grant you access to? The thought of someone gaining control of your username and password, and all the access that they would then have the ability to use, can be frightening. Usernames and passwords are vulnerable to things like social engineering (phishing), brute force attacks, or exposure through data leaks, just to name a few. By leveraging MFA, we can further reduce the aforementioned risks leading to account compromise.

How does Multi-Factor Authentication Work?

The main benefit of MFA is it enhances your organization's security by requiring your users to identify themselves by more than just a username and password. Most websites and services support Two-Factor Authentication (2FA), which is a weaker subset of MFA, since you are limited to two factors. Those factors are usually a password and a One-Time Passcode (OTP) generated by email, text message, or through an app. While this is a good place to start, more websites are starting to add the option for multiple factors of authentication.

Let's walk through a typical use of multiple factors for accessing a system. First, you are prompted for a username and password *(something you know)*. Upon successfully logging in with the correct credentials, therefore passing the first factor of verification, you are then prompted for a second factor. In this instance, you are alerted on your smartphone to verify that you are indeed attempting to access the system *(something you have)*. You respond back and confirm that you are attempting access, therefore passing the second factor, and being prompted for a third factor. Your smartphone then prompts you for your fingerprint *(something you are)*. Upon verifying your fingerprint, you know have access to the system.

OPTIONS:



If any of those three factors in the example were to fail, your account would still be safe and secure. Keep in mind, you are not just limited to three factors. Depending on the system or data that you are protecting, you can add additional factors for verification before access is allowed.

Where can MFA be used?

While MFA usage was limited to just a few websites and services in the recent past, this has become an option or requirement for accounts. Remember that MFA is not just for websites anymore. It is used in other tools and systems as well, such as your work VPN, or even when you authenticate into your computer.

Who should implement Multi-Factor Authentication?

Everyone. It really is that simple. If a website, service, or system you use offers it, enable it with as many factors as you can.

When should I implement Multi-Factor Authentication?

There is a saying, *"There is no time like the present."* Based on the previously discuss topics such as password reuse, password breaches, and phishing scams, etc., having an additional layer that acts as a stop gap to these events is important to have in place. While hindsight might be 20/20, this is definitely not something you want to "wish" you had done earlier. Don't delay, start today.