MULTI-FACTOR AUTHENTICATION: WHY YOU SHOULD RACE TO EMBRACE IT

When you add layers of authentication, you add layers of security to your accounts, data, and systems

Authentication, in a security context, is about verifying your identity. And you authenticate on a regular basis: When you log into accounts and systems, the information you provide is intended to confirm your status as an authorized user. The problem with single-point authentication—think passwords and PINs—is that it's also a single point of failure. If a password is the only safeguard in place, and that password is compromised … well, everything is compromised.

Multi-factor authentication (MFA)—also commonly referred to as two-factor authentication (2FA)—has gained steam over the past several years. Technology advancements have made it relatively simple to implement MFA for key accounts, data repositories, and cloud-based systems. But there is another driving force behind MFA adoption: Password theft and successful credential compromise attacks have skyrocketed.

> "ALWAYS TAKE ADVANTAGE OF MFA WHEN IT'S OFFERED."

MFA enhances security by requiring two or more pieces of information—that is, multiple factors—during the authentication process. There are three key factors in MFA:

1. **Something you know,** like a password, PIN, or passphrase
2. **Something you have,** like a real-time, unique verification code. These authentication codes are usually generated by a mobile app or security token, or they are delivered to you via a text message.
3. **Something you are,** at a biometric level, like a fingerprint, iris scan, or voice pattern.

When It's an Option, Always Opt for MFA

In some cases, MFA isn't optional. Organizations often require employees to provide multiple forms of authentication for assets like virtual private networks (VPNs) and cloud-based systems.

But in other cases, the choice is yours. Many websites and applications have implemented MFA—but it's up to you to enable it. Here are three reasons you should always take advantage of MFA when it's offered:

1. **It's easy to add –** Yes, you must take an action to enable MFA for your logins. But the process isn't difficult. Sites and applications generally provide simple, step-by-step instructions and clearly explain when to expect an MFA prompt, and how to complete a login.
2. **It's easy to use –** As noted, there are multiple ways an organization might implement MFA. But regardless of the technology behind the additional authentication factor(s), MFA adds just a few seconds to your login process. (And the extra seconds are worth it.)
3. **It's far more secure than a password alone –** Cybercriminals have access to billions of stolen usernames and passwords on underground forums. So … what if the only thing standing between a criminal and your data, finances, and files is a compromised password? MFA helps to limit the damage that can be done if a threat actor steals (or buys) account credentials.