Securing Sensitive Data Through the Use of Multifactor Authentication

by Travis Gatlin, Staff Associate II

Posted on October 8, 2024

How many times have you tried to set a password for something, only to run into requirement after requirement regarding how complex your password must be? Upper and lowercase letters, numbers, special symbols… long are the days when you could just use your cat's name and be done with it. It begins to reach the point where you struggle to remember your password, thus, how could a hijacker possibly figure it out and infiltrate your account? However, did you know that, for modern-day password-cracking software utilized by hackers, an 8-character password consisting of upper and lowercase letters, numbers, and symbols can be cracked in as little as just a few hours? This is where the importance of multifactor authentication comes into play.

What is Multifactor Authentication?

Multifactor authentication, more commonly known as MFA, is a security control that is an additional step in accessing your accounts and data. You can think of MFA as a "second password," that is continuously updating into a new, randomly generated code every time you attempt to access your account, as well as being only available to be viewed by yourself. Even if your account name and password are compromised, MFA controls can help prevent access to and maintain the security of your sensitive information to allow you an adequate window of time to change your login information.

What types of MFA are out there?

There are not only multiple providers of MFA controls out there, but there are also multiple different methods of MFA controls. The Microsoft Authenticator mobile application, which also features face identification-controlled access, is one of the most utilized forms of MFA protection, granting a new 6-digit login code every 30 seconds. For individuals who would rather not use their mobile phones, however, computer-based MFA controls in the form of one-time passwords "OTPs," which can be provided through email are also available. Finally, if you want to be really fancy, fingerprint and retina scanners are even available on modern computers today. With so many options available, there is no excuse to not utilize these controls to protect yourself or your business.

Who is trying to steal my information?

You may be asking yourself, why would anyone want my information? Anyone from large businesses to single individuals are targeted for hijacking, with a primary goal in mind: profit. The worst part is you may not even know that you are getting targeted until it is too late. If you work regularly with computers, at some point in your employment, you have likely had to complete security awareness training relating to information technology. Strange emails, suspicious attachments, unfamiliar links; you may think, "Who would ever fall for this?" but, you must keep in mind if these methods never worked, cybercriminals would not continue using them.

Suspicious links may prove to possess downloads for what is known as a "keylogger," a computer program that records every keystroke made by an individual, with that individual being completely unaware that everything they type is being recorded. While it's a bit of a messy situation, all is not lost with proper MFA controls in place, offering a random and constantly changing code that is useless to any keylogging threat, granting you improved safety until the threat can be eliminated from your computer.

As information continues to experience an ever-increasing shift from paper-based documentation to fully electronic files, it is ever more important to maintain awareness and caution over how accessible your data may be. While we may roll our eyes every time we get asked to authenticate using an additional code, it is important to maintain peace of mind and remain cognizant of the fact that, with MFA controls in place, your information is secure.