CS

CYBER SECURITY & YOU

OCTOBER 2021

LASERS & MULTIFACTOR AUTHENTICATION

What is Multifactor Authentication?

Multifactor authentication (MFA) is a security control used to verify user identity by prompting two or more authentication factors prior to logging into your applications and accounts. MFA uses two different types of authentication - something you know (a password) and something you have (your cell phone). At its simplest, it is an extra layer of security.

Mobile applications, tokens, text codes, and phone calls are all ways that you may be familiar with when verifying your identity using MFA. Have you ever been asked to enter a code that has been emailed or texted to you after entering your login credentials in your banking app? That's multifactor authentication hard at work.

Why does LASERS use MFA?

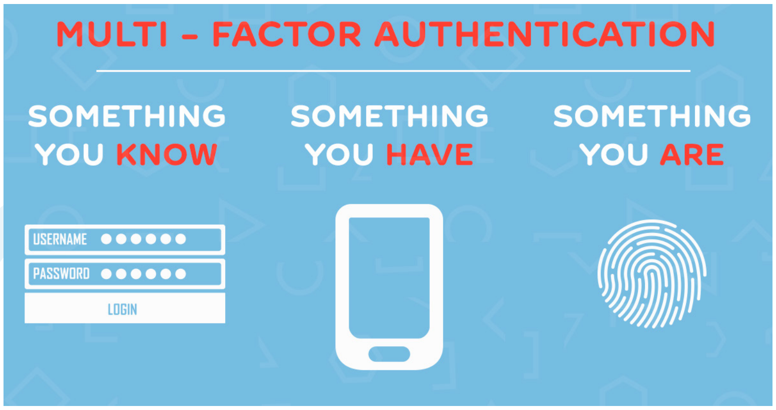
It is becoming increasingly difficult to keep usernames and passwords out of the hands of malicious actors, and phishing continues to be a top method that attackers use to obtain private information. Hackers can remain undetected in computer networks for months gathering important data, which can cost huge sums of money to fix. Loss of professional credibility and trust is another risk factor with long-term consequences. MFA helps remediate these risk threats. Another reason to implement MFA is that it is now considered a minimum requirement by insurance companies in order to obtain or renew a cyber insurance policy. They see multifactor authentication as a critical method of protection, and so do we at LASERS.

What are the Benefits of MFA?

Multifactor authentication is not complex. In fact, it is extremely easy to implement and requires minimal ongoing management and administration. It can also be implemented with simple user controls that will lessen the impact on the end user. For example, you can whitelist your corporate network, so employees are only prompted for two-factor authentication when they are working remotely.

What Next?

LASERS currently uses MFA in the myLASERS system and remote VPN access. In the near future, we will expand MFA to the new Employer Self-Service system (ESS) for agencies. We will also add MFA to certain IT Administration functions to better improve security. CMA Technology Solutions Director of Security, Adam Arceneaux, writes, "Implementing MFA is the one change you can make in your organization that will have the single biggest impact on your security posture. With MFA in place on all your external access points, the majority of attacks against your end users and their credentials will be stopped dead in their tracks. With the adoption of cloud-enabled access and remote working, managing remote access and protecting those accounts has become the new security perimeter." ■



LASERS IT
Making Digital Retirement a Reality