TIP SHEET:

MULTI-FACTOR AUTHENTICATION (MFA)

Overview & Best Practices

LMG SECURITY

WHAT IS MULTI-FACTOR AUTHENTICATION?

Authentication is the process of verifying a user's identity. Typically, this is done using any of the following factors:

- ✓ **SOMETHING YOU KNOW**
  such as a username or password
- ✓ **SOMETHING YOU HAVE**
  a physical token or authenticator app for example
- ✓ **SOMETHING YOU ARE**
  such as a fingerprint or retinal scan

Multi-factor authentication, or MFA, combines two or more factors to add extra layers of protection to your account. That way, if an attacker steals your password or your phone, you still have another layer of protection. LMG recommends that organizations enable MFA on any compatible internal and internet-facing applications, services, and accounts.

WHY DO YOU NEED MFA?

The 2022 Verizon Data Breach Investigation Report found that 82% of breaches involved a human element – e.g. social engineering – and over 60% of those attacks were a result of phishing. As organizations continue to grow their cloud portfolios, share credentials, and build trust relationships between platforms, criminals will increase their focus on compromising emails to gain access to your organization, on-premises systems, cloud environments, and even partner ecosystems.

Let's look at one recent example.

> A finance clerk fell victim to a phishing attack and typed her email password into a criminal's website by mistake. Since the organization did not require multi-factor authentication, the criminal easily accessed and searched the clerk's emails and identified the organization's payroll vendor. The criminal then entered the clerk's email password into the payroll login screen (unfortunately, the clerk used the same password for multiple accounts) and successfully accessed the company's payroll cloud platform. The lucky criminal used the access to divert the paychecks of multiple employees into the criminal's own bank account—which the criminal then emptied and closed after the next pay period—walking away with a hefty payday.

Implementing MFA is one of the most inexpensive ways to reduce your risk of fraud and data breaches.

BEST PRACTICES FOR IMPLEMENTING MFA

- ✓ Enable MFA on every compatible application, service, and account. Prioritize high-risk services such as Internet-facing accounts and cloud platforms.

- ✓ Whenever possible, used strong MFA such as a smartphone application or a hardware token. Simple SMS messages are more easily intercepted and misused by criminals. Consider implementing one of the following as your primary MFA solution:

  Authenticator apps. Authenticator apps are designed to encrypt sensitive authentication tokens, authenticate endpoints, and resist attacks.

  Hardware fobs. These small devices, such as Yubikey and Titan Security Key, are small enough to attach to your keychain. These options are either directly connected to your computer or are scanned using a protocol like Near Field Communication (NFC). This eliminates the risk from lost cell phones or SIM swapping attacks.

  Biometric authentication. Go passwordless! You can use fingerprints, palm scans, facial recognition, or other options.

- ✓ If you must use SMS authentication (which is less secure and subject to SIM jacking / SIM swapping):

  Contact your telecommunications provider and add a PIN or passphrase to your cellular accounts. This makes it much harder for a criminal to take over your phone number and have your texts sent to their phone. All major U.S. carriers support this option.

- ✓ Check the fallback options! Often, victims get hacked because a criminal forces the MFA system to use a backup method such as SMS. Make sure you understand what fallback options are enabled in your MFA system and disable any that don't fit your security model.

- ✓ Check that your cloud providers support strong authentication (not just SMS) before you sign up. If you're already using a platform that does not support strong authentication, urge your vendor to roll out support, and carefully evaluate whether the risk is worth the benefit of that service.

HOW TO CHOOSE AN MFA SOLUTION

You have multiple options for MFA solutions. But our first caveat is that no matter which solution you choose, HOW you configure and implement any of these solutions impacts their performance.

Three of the most common and most supported options are Duo, Microsoft Authenticator, and Google Authenticator. Here's a quick overview of what sets them apart:

Microsoft Authenticator. It's free with your Office 365 or Azure AD subscription! It supports all Microsoft services and can be used manually to sign into any traditional TOTP MFA integration. As an added bonus: the Microsoft Authenticator can also act as a password manager with direct mobile integration and available apps for both Google Chrome and Microsoft Edge.

Google Authenticator: It's free! The authenticator is a code generator and is supported by a large number of vendors and services right out of the box. While it shares many features in common with Microsoft and Duo, it lacks many of the management, response, and more sophisticated options. Google Authenticator is especially appropriate for individual and small business usage.

Duo. Requires a fee (although it is relatively inexpensive) for more than 10 seats, but it's a full-featured and robust solution with the following benefits:

- Supports a variety of authentication methods
- Facilitates push notifications
- Works natively with a large variety of services (out of the box support for Slack, Akamai, Atlassian, etc.)
- Includes strong logging and monitoring features
- Enables self-enrollment for a user's personal or work devices
- Integrates directly with Identity Providers like Azure AD to facilitate Single Sign-on (SSO) services

Any MFA is better than no MFA, but some solutions provide more features and are easier to manage. Implementing the right solution for your needs can quickly and easily provide your organization with a much stronger security posture.

Want LMG to implement or manage MFA for you? **Contact us**. We offer MFA as a managed service or handle the implementation for you to take the burden off your team.