CYBER READINESS
INSTITUTE

Multi-Factor Authentication Guide

The Cyber Readiness Institute (CRI) recently conducted a global survey to gauge the awareness and implementation of multi-factor authentication (MFA) among small and medium-sized businesses. We discovered that 55% of small and medium-sized businesses (SMBs) are not aware of MFA and its security benefits. With this updated guide, we seek to raise MFA awareness among SMBs by providing easily digestible and actionable information that you can implement today to protect your organization from most cyber-attacks.

Cybercriminals want to compromise login credentials and will use a variety of techniques, including impersonating your financial institution or business partners to fraudulently obtain them. However, requiring your employees to use MFA will protect your business information and data while protecting theirs as well. With MFA, the employee's password is no longer your company's only line of cyber defense. Hackers seeking to steal your company data will not be able to simply guess or break an employee's password. Instead, MFA will shield your employees and your company from these attacks.

If you are searching for the most effective way to enhance your cybersecurity today, then you should immediately implement MFA across your organization. While this guide is written for SMBs, this guidance applies to organizations of all sizes. According to Microsoft, 99.9% of account compromise attacks can be blocked simply by using MFA. The following guidance will help you become familiar with MFA and help you understand how to implement this capability to improve cybersecurity for you and your organization.

info@cyberreadinessinstitute.com

What is multi-factor authentication?

Multi-factor authentication, sometimes known as two-factor authentication (2FA), is an electronic authentication process that requires users to verify their identity in two or more ways before granting access to online accounts. MFA usually falls into three categories: something you know, something you have, or something you are. Some examples of MFA you might be familiar with include:

1. **SMS or Email Authentication: You receive and use a unique code via text on your mobile phone or on email to prove your identity.**
2. **Software Authentication: You download and use a mobile app on your phone to prove your identity**
3. **Biometric Authentication: You use a fingerprint or face scan to prove your identity.**
4. **Push notification: Your phone will prompt you to allow or block a login attempt.**

Should my Company be using MFA?

Yes, you and everybody in your company should use MFA across all accounts that connect to your business operations. For example, you should use MFA on email, accounting, and human resources accounts to protect your customer, partner, and employee data. In fact, if some of the software or services you use do not have MFA, you should consider switching to an alternative that does.

If a cybercriminal gets access to your business accounts, they can steal your money and information. They can shut down your business for days, weeks or longer. MFA is an important way to keep your system secure from bad actors.

Who in my company should be required to use MFA?

Everybody. MFA should be mandatory on all company devices and services, especially email and file sharing.

Does using MFA change our need for using strong passwords?

Strong passwords are one form of authentication, and MFA builds on that with other forms (i.e., one-time passcode, fingerprint, etc.). Whether you are accessing work emails, retrieving files from a shared drive or logging into any online services, the password with another form of authentication comprises MFA.

What do I need to consider when selecting an MFA solution for my company?

It is important to consider a few key factors when selecting the appropriate MFA solution for your business:

1. **Is the solution accessible to all employees whether they're working onsite or from a remote location?**
2. **How easy is it to use?**
3. **Are training resources available to introduce my employees to the solution?**
4. **Does the provider offer 24-hour support?**

How do I implement an MFA policy at my company?

First, the CEO should designate a lead to manage the MFA implementation process, which will include a messaging campaign and training sessions for employees. It's important to designate someone in your organization who accepts the responsibility for cyber readiness to help employees troubleshoot as they begin using MFA.

Then, work with the lead to prioritize what systems and data need to be protected, decide what MFA technology is best for those specific needs, and finally assess the impact on employees.

It is important to remember that delivering MFA across an entire organization may create challenges, but clear communication will allow successful implementation. Holding workforce information sessions and training where you communicate your MFA policies, expectations, and explain how easy the process is for employees will assist in effective implementation.

How do I communicate the importance of MFA with my employees?

Create a campaign to inform employees of the benefits of using MFA, and the risk of not. You can use physical posters or banner ads in your buildings to explain why you are making the transition to MFA. Focus on informing your users and explaining why you are making this change—making it clear to employees that MFA is there to support them and protect their accounts, not as a nuisance or workplace tracking policy.

Is one type of MFA more secure than others?

There are a variety of MFA options available for your business, but what is most important to remember is that any of these options is better than none. Consider the size of your business and number of employees when selecting an MFA option that is secure but not overly burdensome for employees.

Where can I learn more?

Now that you have a basic understanding of MFA's importance to your business and how you can implement it, you can explore additional cyber readiness resources and practices at BeCyberReady.com. Also, check out CISA's free information for additional insights on MFA **here.**

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized businesses (SMBs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit **www.BeCyberReady.com**.