CYBER READINESS
INSTITUTE

Multi-Factor Authentication Guide

Follow these guidelines to understand and implement multi-factor authentication in your organization

Small and medium-sized businesses searching for practical ways to enhance their cybersecurity should implement multi-factor authentication (MFA) across their organization. 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 (also known as 2-factor authentication "2FA") and help you understand how to implement this capability to improve cybersecurity for you and your organization.

What is MFA?

MFA requires users to present more than one piece of evidence (credential) whenever the user logs in to a business account (ex. company email, payroll, human resources, etc.). MFA usually falls into three categories: **something the user knows** (a 15-character password), **something the user has** (fingerprint), or **something the user receives** (a code sent to the user's phone or email account).

info@cyberreadinessinstitute.com

Why does MFA matter?

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, empowering your employees to use MFA will protect your business information and data while protecting theirs as well.

Using strong 15-character passwords is one critical step, but **MFA offers a human-centered technical solution**. 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**.

How do I implement MFA?

Implementing MFA does not require hardware changes to your company computers, mobile devices, or printers. Instead, there are numerous free and low-cost software-based tools that users can download to their company and personal devices. For example, it's likely that your email provider offers (and encourages) MFA. Therefore, it can be as easy as clicking an option in your settings to turn on MFA.

Still, you might be wondering about the best way to implement MFA across your workforce. First, you should **update your policies and procedures with specific explanations of your expectations**. For example, all employees should implement MFA on their company email account. Next, you should **hold workforce information sessions and training** where you communicate your MFA policies, expectations, and explain how easy the process is for employees. Finally, you should **designate someone in your organization who accepts the responsibility for cyber readiness to help employees troubleshoot** as they begin using MFA.

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**.

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**.