THE POWER OF

MULTI-FACTOR AUTHENTICATION

Passwords aren't enough.

What is Multi Factor Authentication? (MFA)

Multi-factor authentication (MFA) is a security measure that requires two or more forms of identification to access an account. This involves a combination of:

SOMETHING **YOU KNOW**

Typically a username or password

SOMETHING **YOU HAVE**

A unique code sent to the user's cell phone via text or authenticator app

SOMETHING **YOU ARE**

A fingerprint or retina scan

What should my business protect with MFA?

Any account with access to critical data, applications, and systems within your business should be protected. Here are some critical areas to address:

- Remote network access
- Privileged/administrative account access
- Business email
- Customer relationship management (CRM) system

MFA can **block** over

99.9%

of account compromise attacks*

MFA and Cyber Insurance

Enabling MFA is a strong indicator of proactive risk management practices. This, along with other measures can have a significant impact on the availability and affordability of coverage. Due to rising claims frequency, MFA is becoming a more common condition to qualify for coverage. MFA has the potential to prevent claims, which over the long term can result in preferential pricing and coverage terms.

How to Implement MFA

The vast majority of MFA is free and several common platforms (Gmail, Outlook, Dropbox) offer it internally. For 3rd party platforms, there are also several apps available that allow you to set up MFA free of charge.

It's best to engage with your IT department or IT vendor to set up an implementation plan that not only establishes MFA but educates your employees on using the feature and explains the purpose and need for added security.

Additional Resources:

MFA Explained in Under 2 minutes | How to implement Multi Factor Authentication (Microsoft*)

Enable MFA in Outlook | Enable MFA in Gmail | Enable MFA for Apple ID

Morris & Garritano | www.morrisgarritano.com | 805.543.6887 | License #0305584