



## Multi-factor Authentication

Multi-factor Authentication (MFA) strengthens access security by requiring two methods to verify your identity. These factors can include something you know - like a username and password - plus something you have - like a smartphone app - to approve login authentication requests. MFA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

Due to an increased volume in businesses and organizations working remotely, heightened security is more important than ever before. Right Click Solutions recommends creating a layered defense to your logins by using MFA software, making it more difficult for an unauthorized person to access your information.

Right Click Solutions has partnered with a reputable MFA service provider that offers a fast and easy way to log in securely with a user-friendly interface. Users of MFA software can quickly verify their identity by approving push notifications, which are sent via text message or email, before accessing applications. It is just as quick to deny an unfamiliar login attempt, so users can easily stop fraudulent attempts to access applications or company data.

By using MFA you are significantly reducing the risk of a credential compromise. According to Melanie Maynes from Microsoft Security, *“By providing an extra barrier and layer of security that makes it incredibly difficult for attackers to get past, MFA can block over 99.9 percent of account compromise attacks. With MFA, knowing or cracking the password won’t be enough to gain access.”*

**For more information, call Right Click Solutions.**

