Multi-Factor Authentication

What is MFA and why does it matter?

Multi-factor authentication (MFA) is a security setting that requires users to provide more than one method of verification to gain access to websites or applications. Sometimes, it's referred to as two-factor authentication (2FA).

Implementing MFA at sensitive access points is a simple and highly effective way to protect against ransomware and other cyber attacks. Cyber criminals often breach systems with stolen usernames and passwords before deploying ransomware. MFA adds an additional layer of security and makes it more difficult for attackers to breach a system.

Security experts agree: MFA can block 99% of account compromise attacks.[1]

How At-Bay helps keep businesses secure

We conduct a sophisticated security scan of every business we quote and also ask whether or not they've implemented MFA at the time of quoting. If MFA is in place, we can typically extend full ransomware coverage for large, high-risk companies seeking larger limits.

We recommend implementing MFA at all sensitive access points.

This includes email, internal applications, remote network access, and any external-facing systems. The most common and safest verification method is an authenticator application, such as Google Authenticator, which is recommended over text messages or phone calls.

Implementing MFA is easy

We often hear concerns that implementing MFA may be disruptive to employees, but it doesn't have to be.

Businesses can set up MFA so employees are only required to enter an authenticator code during the setup process and whenever they use a new device. For businesses that outsource IT support, MFA implementation should not be a complicated or expensive task — and it's worth investing in now before it's too late.

[1] Microsoft: One simple action you can take to prevent 99.9 percent of attacks on your accounts