Multi-factor authentication (MFA)

THE SINGLE BEST PROTECTION AGAINST RANSOMWARE

MFA can save your business from malicious ransomware and other cyber attacks

Small businesses are exposed

According to the department of Homeland Security approximately 50 - 75% of all ransomware breaches were against small businesses [1].

With the rise in successful ransomware breaches, the associated costs of a ransomware attack are increasing. The cost of a ransomware breach ballooned by 202% to $275K [2] in the last year.

Email compromises like phishing scams are the leading entry point for ransomware.

MFA can dramatically reduce the risk of a cyber criminal compromising your company and infecting your systems with ransomware by requiring additional ways to verify a user beyond their initial login.

What is Multi-factor authentication (MFA)?

One of the easiest and most effective ways to prevent ransomware attacks is MFA. MFA requires users to verify their identity at least twice when logging in to your applications, ensuring the user is who they say they are. And it's easy to implement.

How to implement MFA

Click here for instructions for Google Suite.
Note, Google refers to MFA as 2-step verification.
Be sure to require 2-step verification when setting up.

For how to activate MFA for Microsoft 365, click here.

For other services, you can use an MFA solutions provider such as Google Authenticator, Microsoft Authenticator, or Authy.

1 - *Statement from Homeland Security Secretary Alejandro Mayorkas on May 5 ,2021.*
2 - *NetDiligence 2020 Cyber Claims Study.*