Introducing Multi-Factor Authentication (MFA)

CHALLENGE

Technology plays a central role in the operation and management of all types of business. That makes cybersecurity a top priority for any organization, particularly as more and more employees expect to work remotely, on the move, or on client sites. The heightened risk of cybersecurity breaches means that cyber insurance policy requirements are being tightened. Many insurers now stipulate that multi-factor authentication (MFA) must be implemented to enhance security and prevent unauthorized access to business assets.

MFA is a security technology that requires users to enter two or more verification 'factors' to gain access to a system. These factors can include a password, a code sent to another device, answers to 'secret' questions, and biometric evidence.

SOLUTION

LastPass is an award-winning password-management solution, which includes the option to introduce MFA for some or all business users accessing your systems. MFA can be introduced at any entry point that could potentially allow unauthorized or malicious access to your data.

Consider the example of an employee who is offsite, either travelling or working remotely. This employee will need to connect to your corporate network via VPN, to gain access to your customer relationship management (CRM) system – or other work tools. This process requires access to be granted at various points, all of which could be secured using MFA.

Initially, when the employee logs in to their laptop, MFA could be used to grant access. Once authenticated, the employee will need to establish a VPN connection, which could also be protected by an MFA process.

The user will then need to access their LastPass password vault, once again using MFA to verify their identity. Finally, they will access the CRM system – or other business tools – using single sign-on (SSO), which can include MFA as part of the authentication sequence.

In this example, LastPass gives your business four opportunities to verify the authenticity of the user at different points in their journey. It does so via a single application, providing a common user experience at every stage.

OUTCOME

LastPass represents an affordable, robust and easy-to-implement password-management solution that will tighten up security across your workforce, wherever they are working. MFA helps to ensure that only genuine, authorized business users can gain access to your data and systems.

By giving employees fast, frictionless and secure access to tools and applications, LastPass helps to boost productivity and minimize time wasted on IT access problems or password resetting. By incorporating MFA and SSO, LastPass not only enhances your IT security but also helps to reduce your cyber insurance premiums.

Please contact your MSP to find out how LastPass can safeguard your IT systems and data, reduce business risks and boost productivity.