Multi-Factor Authentication

By Locknet® Managed IT

Security

Systems that use two or more different factors are typically considered stronger than those that use only one factor.

Compliance

Some regulations specify that organizations must use two or multi-factor under certain circumstances, accessing particular types of data or connecting from certain locations.

Flexibility & Productivity

Modern, efficient, and affordable security that's scalable and easy to use.

Using a single set of credentials is no longer secure

Today, more people are living their lives online and as our digital world expands, so do the risks. Consequently, there are more attackers ready to steal our identities, deplete our bank accounts and sabotage our businesses by stealing and using our usernames and passwords or tricking us into giving them away. While staying aware and practicing good password security is still a must, it's no longer enough. We need an additional and stronger layer of security to safeguard our keys to the digital world.

Securing your access

Locknet's Multi-Factor Authentication (MFA) is a vital barrier that provides a second layer of security to the authentication process after a username and password are entered to verify an identity, making it harder for attackers to gain unauthorized access to our digital world. Although MFA has been around for some time to control access to sensitive data and systems, today more businesses are electing to use MFA to protect their users' credentials from hackers who have stolen a password database or used phishing campaigns to obtain them.

How multi-factor authentication works

By using an authentication app, users can log into an application with their primary credentials, it will prompt them with a push notification, email or one-time password to complete the secondary authentication by approving the request. This method is more difficult for an attacker to intercept and offers a convenient way for users to log in by using their smartphone or other device.

Multi-factor authentication benefits

- Easy and secure
- Single sign-on (SSO)
- Supports work applications such as VPN, Multicloud, Microsoft O365 and Azure
- Users can self-enroll in a few easy steps, using flexible authentication options (mobile push, U2F, soft token, phone call, and SMS)
- Users authenticate in seconds; no codes to enter
- Verify trust for any device and limit access to compliant devices
- Supports iOS and Android
- Meets compliance requirements (FFIEC, HIPPAA, GDPR, DEA EPCS, NIST, PCI-DSS)

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com » 844-365-4968