Two-Factor Authentication

mother technologies

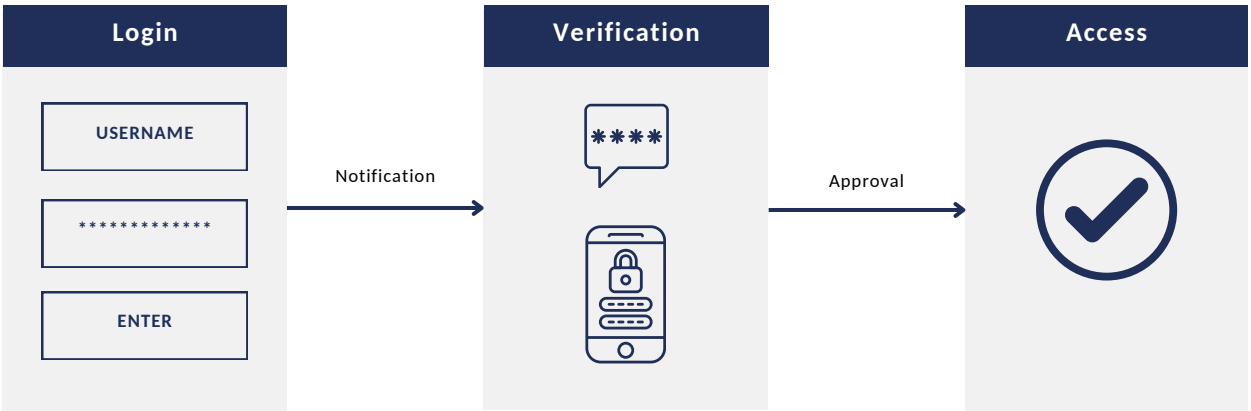
Secure your business with Two-Factor Authentication (2FA) to verify user identities and safeguard your systems and data. Without 2FA, your business faces heightened risks of cyberattacks.

Trusted Users	Trusted Devices	Secure Applications

Protecting your business from cyber threats is crucial. A cyberattack can have devastating effects, such as losing customer trust, disrupting operations, and damaging your brand's reputation. So, investing in strong cybersecurity is essential to keep your business safe and successful in today's world.

What is 2FA?

Passwords are vital for safeguarding sensitive accounts, but they're vulnerable to various threats like phishing and malware. These risks make relying solely on passwords insufficient for security. That's where 2FA steps in, adding another layer of defence. It boosts security, making it harder for cybercriminals to breach your data and systems. While some may initially hesitate due to perceived inconvenience of 2FA, implementing it is not merely an option, it is an essential in today's digital landscape.



Types of 2FA

For safer 2FA authentication, opt for authenticator apps or SMS over email due to their higher security, and consider using external off-net devices like mobile phones for enhanced safety.

Authenticator App

2FA authenticator apps provide a convenient and effective way to bolster the security by requiring both something the user knows (password) and something that's generated dynamically (authenticator app) for authentication.

Code sent to Mobile via SMS

SMS two-factor authentication validates the identity of a user by texting a One-Time Password (OTP) to their mobile device. It is the most common and simplest form of 2FA implementation.

Code sent to email

The system sends an OTP or verification link to the user's email address for 2nd layer authentication. This is as effective as sending a code via SMS but, since email platforms have known vulnerabilities and are more readily compromised, it is safer to use SMS or an Authenticator App.

Implementing 2FA

You may already have eligibility for 2FA within your existing 365 license subscription. If not, you can upgrade your subscription or reach for a 3rd party solution such as Cisco's 2FA solution, Duo. Duo has extensive customisable security features and is very easy to use.

Many businesses don't want to enable 2FA because it complicates their logins. Unfortunately, today's landscape is so cyber-crime abound that you must. Think of it this way, "If it's easy for you, it's easy for them." Whatever your preferred product, switch it on!

Benefits of 2FA

Stronger Authentication

The key advantage of 2FA is the extra layer of security it offers. Even if hackers acquire a user's login details, they're unable to access the data without a second form of authentication. This makes it challenging for criminals to breach sensitive information and shields it from unauthorised access.

Meets Compliance Requirements

Many regulatory standards and industry guidelines, such as GDPR, mandate the use of multi-factor authentication to protect sensitive data. Implementing 2FA can help company's meet these compliance requirements and avoid potential penalties or fines.

Secure Remote Access

Especially important for remote work scenarios, 2FA adds an extra layer of security when accessing sensitive company systems or data from outside the corporate network, reducing the risk of unauthorised access.

Adaptability and Flexibility

2FA solutions offer various methods for the second factor, including SMS codes or authenticator apps. This flexibility allows organisations to choose the most suitable authentication methods based on their security needs and user preferences.

Removes Risk of Password-Based Attacks

Consumers often reuse passwords or create easily compromised ones due to the burden of managing multiple accounts. This increases vulnerability to hacking. 2FA mitigates this risk. It prevents cybercriminals from exploiting simple or repeated passwords.