CHUBB®

Multi-Factor Authentication (MFA)

Many cyber attacks requires a hacker to have access to your corporate network or e-mail. With a traditional user login and password access, known as Single-Factor Authentication (SFA), it can be easy for criminals to get access to a company's IT system.

MFA helps shut cyber criminals out

Once an attacker has access to your e-mail, they may impersonate you and send out fake e-mails or, in case of access to your network, scout your environment, increase their privileges, delete back-ups and deploy ransomware.

This type of hacking can happen in several ways:

- **Brute force** or using a password cracking tool to automatically try many common passwords.
- **Credential harvesting** or exploiting the fact that many people use the same ID and password combinations across multiple accounts.
- **Phishing** or sending a fake email request for password reset, thereby harvesting that employee's business email information.

One of the most effective method to keep bad actors out of your systems is perhaps Multi-Factor Authentication (MFA), which essentially offers a second layer of authentication/defence.

What is MFA?

MFA requires two or more authenticating factors, or proofs of identity, to ensure that those seeking access to company email and other key company assets are actually who they say they are.

For example, three layers of authentication could be:

1.

Something you know
(typically a password or verification code)

2.

Something you have
(a trusted device that is not easily duplicated, like a phone or security key)

3.

Something you are
(biometrics)

> *Compromising two or more authentication factors presents a significant challenge for attackers – substantially reducing the risk of compromise.*

Why is MFA important?

The idea behind MFA is that, although cyber criminals may steal what legitimate users know, it is much less likely that they'll also have what those users possess. In the case of an email account, what users possess is the soft token or device that generates or receives a unique, short-lived code.

Implementing MFA

Enabling MFA can be one of the quickest and most impactful ways to protect user identities. Many, if not most, popular web services offer MFA – although it is often deactivated by default.

Get expert advice to implement the MFA that best fits your company