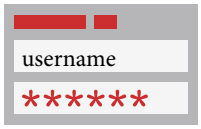
TRAVELERS

Multi-Factor Authentication (MFA)

What is MFA?

Multi-Factor Authentication (MFA) is the use of two or more authentication factors. MFA is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identity ***prior*** to granting access.



1. SOMETHING YOU KNOW

A password or passphrase is something you know.

2. SOMETHING YOU HAVE

A token or smart card is something you have.

3. SOMETHING YOU ARE

Biometric identification through a fingerprint or retina scan establishes something you are.

There is flexibility regarding which authenticators are used by a business to validate a user's identity without undue inconvenience.

Why is MFA critical?

99.9%

of account compromise attacks can be blocked by MFA[1]

94%

of ransomware victims investigated did not use MFA[2]

MFA helps protect a business by adding an additional layer of security, making it more difficult for cyber criminals to access a business' systems. Credentials like user IDs and passwords can be the weakest link in a business' cybersecurity, as they are frequently compromised and posted on the dark web. And passwords are growing more insecure. As users connect to more systems that require a user ID and password, they tend to get lazy. They create simple, easy-to-guess passwords, use the same password for different sites, share them and sometimes inadvertently give them to the attacker.

What should be protected with MFA?

Remote Network Access

MFA for remote network access is an important security control that can help reduce the potential for a network compromise caused by lost or stolen passwords. Without this control, an intruder can gain access to a business network in a similar manner to an authorized user.

Privileged/Administrative Access

MFA for both remote and internal access to administrative accounts helps to prevent intruders that have compromised an internal system from elevating privileges and obtaining broader access to a compromised network. This can prevent an intruder from gaining the level of access necessary to successfully deploy ransomware across the network, erase activity logs, create bogus user accounts or even turn off anti-malware protection.

Remote Access to Email

When accessing email through a website or cloud-based service on noncorporate devices, MFA can help reduce an intruder's ability to gain access to a user's corporate email account. Threat actors often use email access to perpetrate various cyber crime schemes against businesses, as well as the businesses' clients and customers.

[1] Source: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[2] Source: Arete Presentation "Ransomware Cards" 7-31-2020

To learn more, talk to your broker or visit travelerscanada.ca/cyber.

TRAVELERS