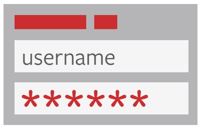
TRAVELERS

# Multifactor Authentication (MFA) Best Practices for Travelers CyberRisk Policyholders

## What is MFA?

Multifactor 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 smartcard 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 e-mail through a website or cloud-based service on non-corporate 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 cybercrime schemes against businesses, as well as the businesses' clients and customers.

## How does a business start to implement MFA?

An extra layer of security in the form of multifactor authentication is important but the options can vary from one solution to the next. To learn how a business can start to implement MFA and increase their cyber defenses, Travelers offers its CyberRisk policyholders access to a one-hour consultation with a Symantec™ Security Coach who can provide much-needed expertise and help pave the way for a stronger cybersecurity program. This confidential service is available Monday through Friday (9 a.m. - 5 p.m.) at no additional cost.

**For direct access to the Symantec Security Coach please contact Glen Carl at 844.211.4552 or via email at sed.cicsecuritycoach@broadcom.com.**

Travelers CyberRisk policyholders may also access many other pre-breach services and risk management resources by logging onto Travelers' eRiskHub portal, powered by NetDiligence®.

[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

TRAVELERS

travelers.com

Travelers Casualty and Surety Company of America and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material is for general informational purposes only. It is not intended as, nor does it constitute legal or professional advice, not nor is it an endorsement of any source cited or information provided. This information does not amend, or otherwise affect, the terms, conditions or coverages of any insurance policy issued by Travelers Casualty and Surety Company of America and its property casualty affiliates ("Travelers"). Participants should consult source material for more detail.

Certain services referenced herein may be provided to you by Symantec and in using them you must agree to Symantec's terms of use & privacy policy. Travelers makes no warranty, guarantee, or representation as to the accuracy or sufficiency of any such services. The use of the services and the implementation of any product or practices suggested by Symantec is at your sole discretion. Travelers disclaims all warranties, express or implied. In no event will Travelers be liable in contract or in tort for any loss arising out of the use of the services or Symantec's products.