# Multi-Factor Authentication FAQs

## What is multi-factor authentication?

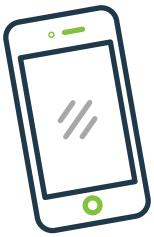
You know how you need to enter a password to log in? Multi-factor authentication (MFA) is the technical name for when you have to enter more than a password – like when you also have to enter a code sent to your smartphone. MFA is sometimes known as two-factor authentication (2FA) or strong authentication.

The purpose of authentication is to prove to a system that you are who you say you are (the person with authorized access). The more "factors" included in the authentication process, the more secure the system is.

## What is a factor?

A factor is a type of credential. There are three categories of factors:

**Something you know, like your password or PIN**



**Something you have, like your smartphone or an access card**

**Something you are, like a fingerprint or face scan**

## Why should I care about (and use) MFA?

Unfortunately, passwords are generally easy to guess, steal, and crack. For example, more than 613,000,000 passwords have been publicly exposed.

If a cybercriminal gets access to your account, they can steal your money and information, plant ransomware on your device, and impersonate you online to cause all types of harm. To keep your computers, phones, social media, finances, and personal information safe, you need to use more than just a password to secure your accounts — you need MFA.

## How do I get started using MFA?

Many websites and accounts allow you to turn on MFA. Check with the companies that provide your services, like your bank, entertainment providers, email provider, and others and sign up for their MFA solutions.

While any system can be hacked by a determined cybercriminal, **using MFA significantly protects your accounts.**