What is Multi-Factor Authentication and Why is it Important?

What is multi-factor authentication?

Multi-factor authentication is essentially a means of identifying that you are who you say you are by using more than one method of verification.

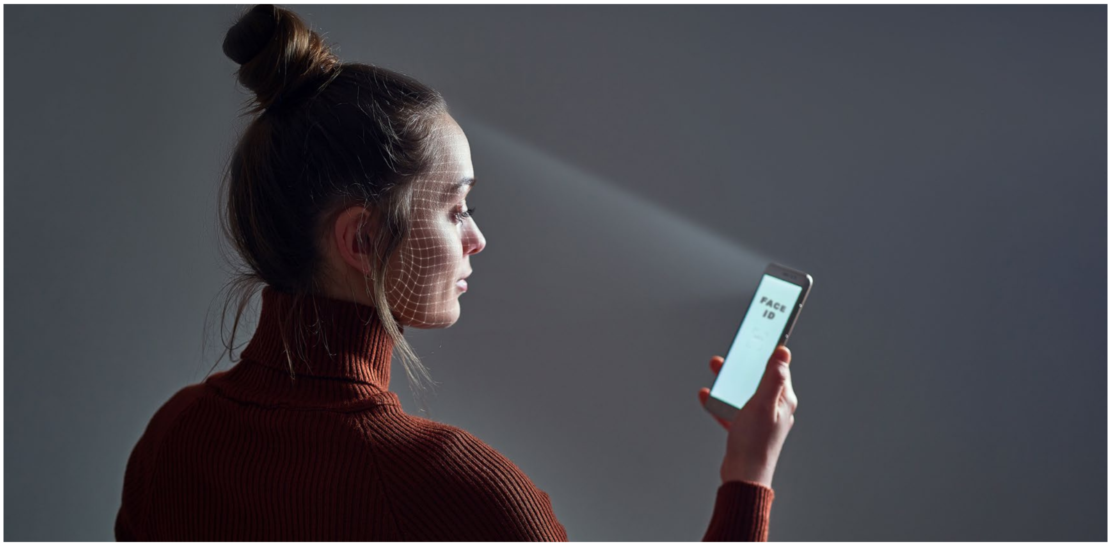
You might have heard it called 2-factor authentication – where you need to present two pieces of evidence – but ‘multi-factor’ is the umbrella term for any login that requires more than one set of credentials.

When logging into an account that requires multi-factor authentication – for example, your bank – you’ll typically type in your username and password as usual. You might then need to enter a second code that gets sent to your phone or even your face ID.

Having one password that you use across several accounts leaves each of them vulnerable to attack. If a hacker cracks one password, they very quickly have access to each of those other accounts. Yet, surprisingly enough, 54% of consumers use five or fewer passwords across their entire online life according to **research from Telesign.**

It goes without saying, then, that unique passwords are absolutely vital to protect your information. But another hacker-proof way to do just that is by using the wonder that is multi-factor authentication.

It’s simpler than it might sound – let’s dive in!



Examples of multi-factor authentication (MFA)

The factors used in MFA can include:

- Something only you know, like a PIN or answer to a question like 'what was the name of your first pet?'
- Something you possess, like a security key within a USB, a Google Authenticator app, etc
- A registered device or approved IP address
- A biological factor, like a fingerprint, eye scan, or face scan
- Logging in within a specific timeframe

Each of these factors has their own advantages and disadvantages. For example, while a PIN is easy for the consumer to remember, it is (as a result) easier to crack, especially if it's a 4-digit combination.

Device authentication is a hugely popular method because of the speed and ease with which you can retrieve a code. However, if you don't have the device nearby or it has run out of battery, what was easy can become a hassle.

As a result, if you're setting up multi-factor authentication within your business, you will need to weigh up which means of authentication is right for you — what will cause the least disruption to your staff but provide the most protection?

Why is MFA so important?

While it's easy to hack a single password using brute force, MFA adds an extra layer of security — and the more combinations of factors there are, the harder it is for the wrong people to access your accounts.

MFA is hugely important both on an individual and organisational level. On your personal devices at home, you'll want to protect your accounts, money, and data. When it comes to business, MFA is all the more significant because you're not only responsible for your own accounts.

Multi-factor authentication is needed across the entire organisation in order to better protect the data of your business, your employees, and your consumers. It can protect against many types of attack, including brute force, phishing, and more.

As such, it is a crucial part of your overarching cybersecurity strategy — without it, you could be risking an expensive attack and losing your customers' trust.

Getting set up with MFA

If you're not sure where to start when it comes to multi-factor authentication or cybersecurity, we are here to help.

We offer **managed IT support for businesses** that don't have the time or internal resources to manage IT issues like security or provide technical support. Particularly in this new age of hybrid working, cybersecurity is a challenge not to be faced alone.