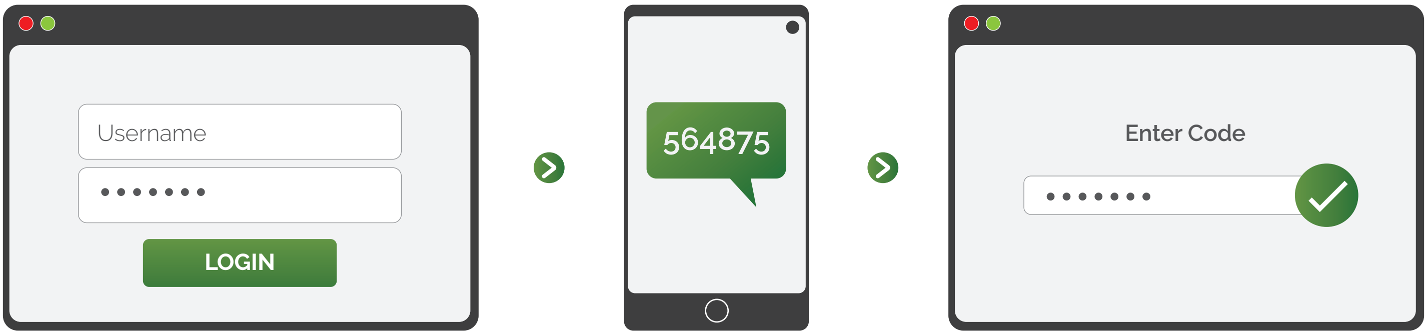
Beyond

Multi-factor authentication (MFA)

Hello everyone,

No matter what sector or field your organisation specialises in, information security is of the utmost priority when thinking of your organisation's livelihood, especially in today's day and age.
You know the importance of keeping sensitive data safe and the details to your work accounts protected through the use of strong passwords, but often times, we have come to find out that that isn't enough anymore.

Surfacing in the early 20th Century in the form of "security questions" and the like used by banks, **multi-factor authentication (MFA)** has been on a real rise in recent years in the form of a third-party authenticator app, or email/text message based, involving a randomly generated and constantly refreshing code which the user can use.



The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

What you might not have known is that some forms of MFA aren't as safe as you may initially think they are; there are pros and cons to each method to go about MFA and hopefully after this article, you will have a more informed idea of what route you'd like to take or just a better understanding as a whole!

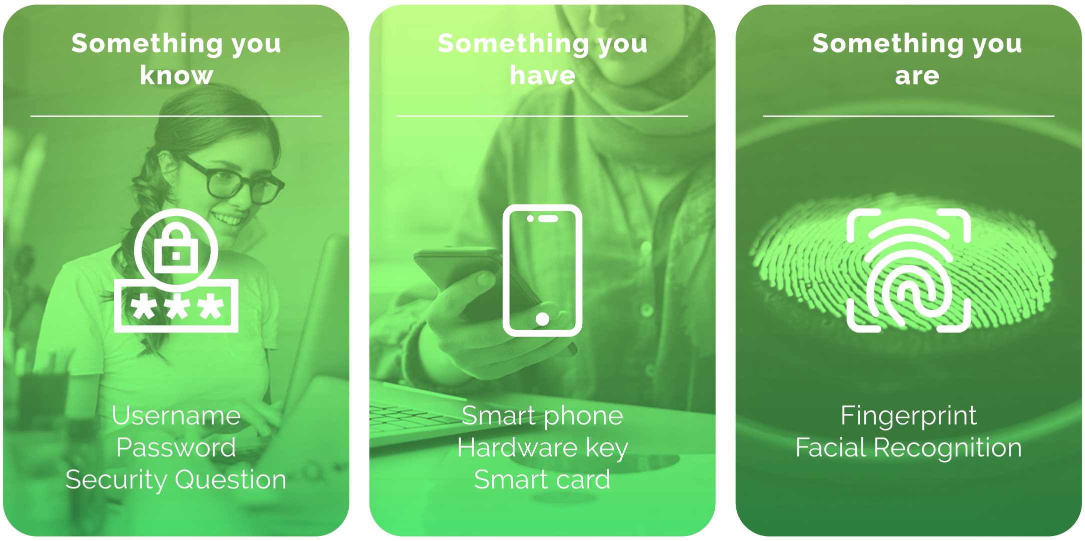
First and foremost, what is multi-factor authentication even really?
MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

Something you know, typically a password or a PIN.

Something you have, such as a key, card, or security token.

Something you are, most commonly as biometrics like fingerprint scan or face scan.

A good example of this that everyone can relate to is when you withdraw money at an ATM. To accomplish this, you need two things: your bank card and your PIN.



Something you know

Username
Password
Security Question

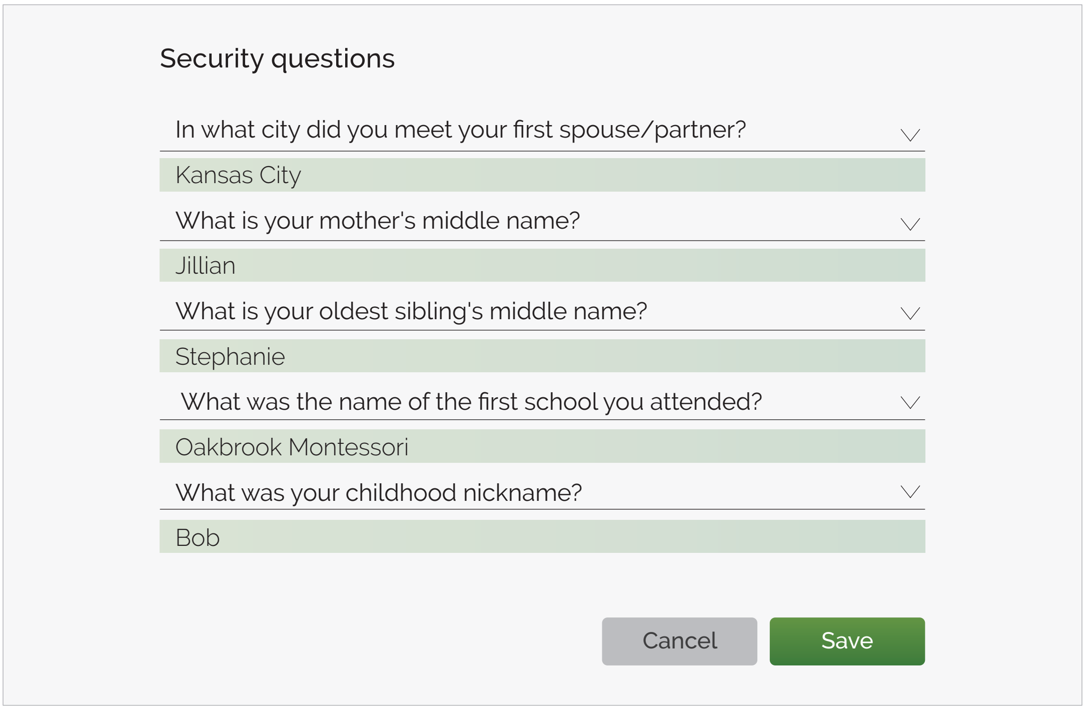
Something you have

Smart phone
Hardware key
Smart card

Something you are

Fingerprint
Facial Recognition

Historically, security questions were used as the most common form of MFA such as "Where were you born?". These have largely been phased out as they may be known to a wide group of people, or easily researched.



Security questions

In what city did you meet your first spouse/partner?

Kansas City

What is your mother's middle name?

Jillian

What is your oldest sibling's middle name?

Stephanie

What was the name of the first school you attended?

Oakbrook Montessori

What was your childhood nickname?

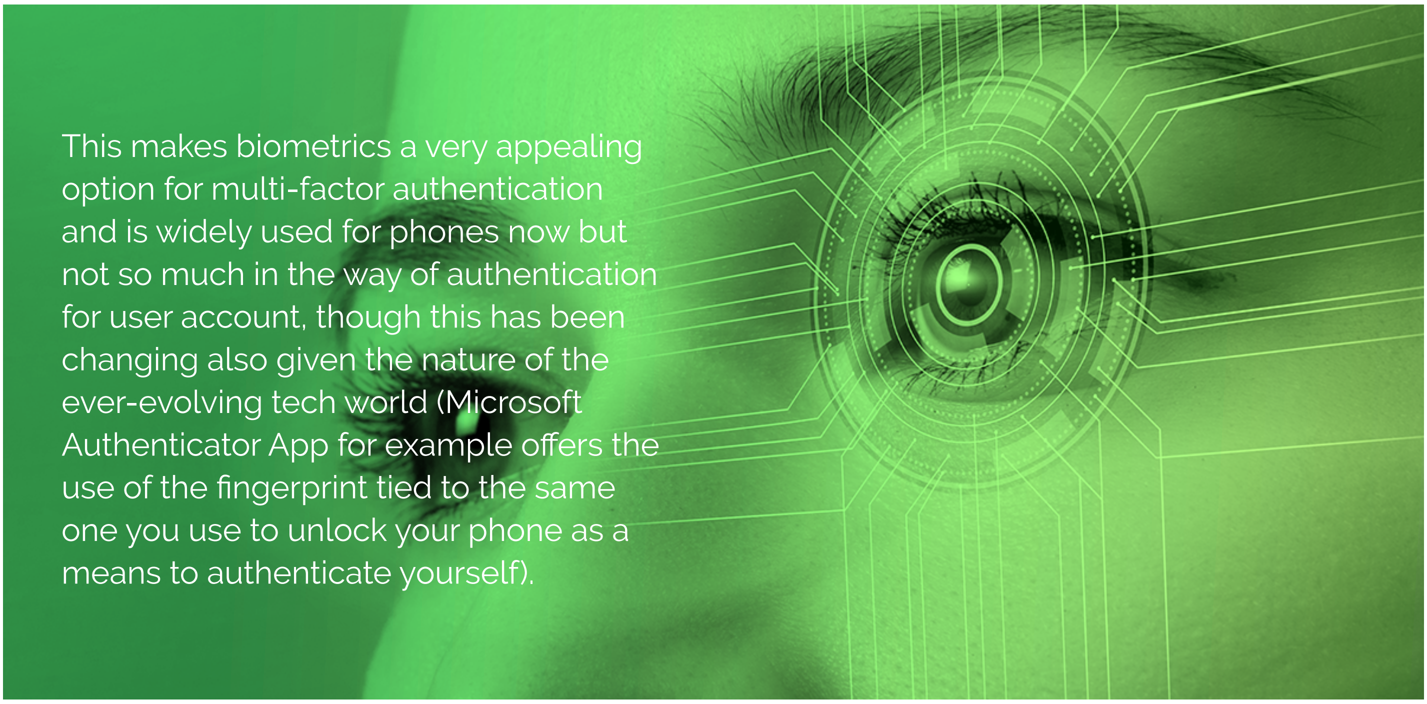
Bob

SMS verification came as a safer alternative to this shortly after, where users would use their PIN to unlock their phone on top of a one-time-valid, dynamically generated passcode. The advantage of this from a consumer standpoint is the convenience – everyone carries their phone around with them these days, so everyone has the opportunity to authenticate easily.

Unfortunately, SMS is a security risk more so than third-party authenticator apps as it can be easily breached by wiretapping or SIM cloning so it tends to be avoided these days.

Speaking of third-party authenticator apps, they are the most widely used variant of multi-factor authentication now, with apps like Microsoft Authenticator, Google Authenticator and Authy to name a few.
Similarly to SMS, these use a randomly generated and constantly refreshing code which the user can use. A benefit to these over SMS is that alongside being far more difficult to trace than SMS, they do not require mobile phone reception but also usually do not require an internet connection so they are very reliable and consistent.
However, considering all this, since this still requires the use of a mobile phone, there are cons to consider as if a mobile phone isn't available due to being lost, stolen, dead battery, or for any other reason not work, they cannot authenticate.

With "something you are", factors associated with the user like fingerprint/face/voice, they are a lot more robust as they are inherent to only the user and not something like a bank card. It's not like someone can just steal your fingers and use that to gain access to the device/account, and more often than not, it's tied to your phone so they would need both your phone and, well, **you.**



This makes biometrics a very appealing option for multi-factor authentication and is widely used for phones now but not so much in the way of authentication for user account, though this has been changing also given the nature of the ever-evolving tech world (Microsoft Authenticator App for example offers the use of the fingerprint tied to the same one you use to unlock your phone as a means to authenticate yourself).

Using the example of the ATM from before, "something you have" would involve something the user is in possession of such as a bank card, a key or a security token in the form of a USB drive. In my opinion, this is the weakest form of multi-factor authentication, which makes sense as it's the most primitive method, being around for centuries in the form of a lock and key.
The major drawback with "something you have" methods of authentication in general though is that the user must carry around the physical object essentially at all times – loss and theft are risks. Without your token, you can't access your information.

The future of MFA for mobile devices is bright and considers different methods that prove to not be a hindrance to the user but also far more robust. With advancements in mobile hardware technology such as GPS, microphone, and gyro/accelerometer, the ability to use them as a second factor of authentication is becoming increasingly appealing. For instance, one possibility could be recording the ambient noise of the user's surroundings from the mobile device and comparing it with the ambient noise from the computer in the same room in which the user Is trying to authenticate. If it matches, it is effectively a second factor of authentication, one that also reduces the amount of effort and time needed to complete the process aswell.

Regardless of which method appeals to you for your own use, I'm sure you can see that any form of multi-factor authentication is worth using over none at all and I hope that you enjoyed this post and learnt a thing or two about the different forms of authentication

If you need any help with deciding on security or even which method of MFA you'd like to use, we are here to assist you!

Visit us at https://www.beyondmigration.com/services

Author
Bilal Ali Ahmad
Junior Technical Delivery Engineer