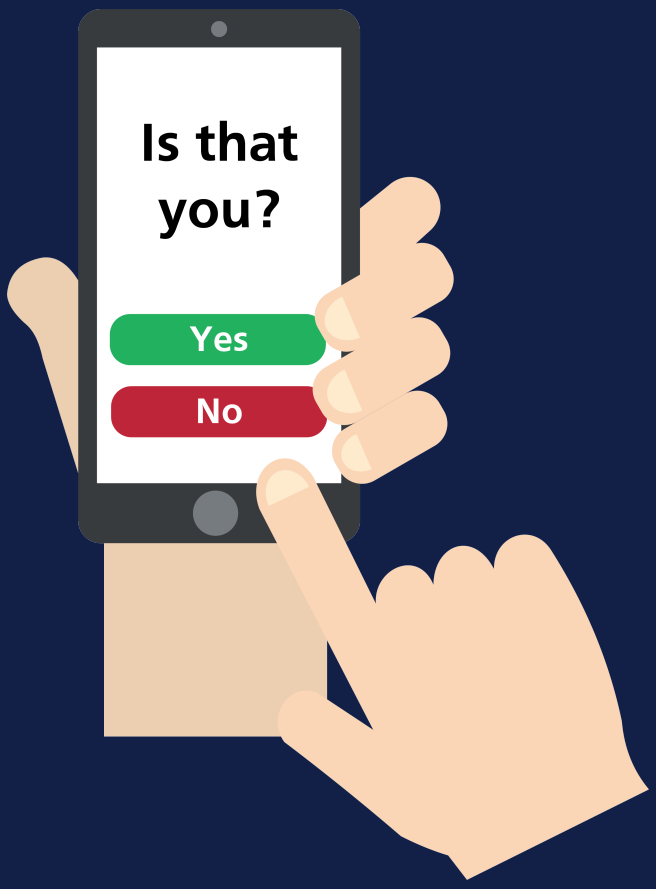


Multi-Factor Authentication (MFA)

Our guide to MFA

www.breakwaterit.co.uk

breakwater IT

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is an authentication method that requires two or more verification factors.

For example:

Entering a password and **an MFA app code:**

****

MFA can also go by the name Two Factor Authentication (2FA).

2FA = two authentication factors only.
MFA = two or more authentication factors.

Types of MFA

Something you **know**

Password

****

Pin

1 2 3 4

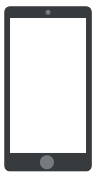
Combination

9V7$

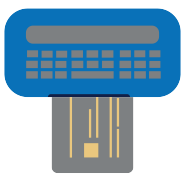
Something you **have**

Key

Smart Phone



Token Device



Something you **are**

Finger Print

Facial Recognition

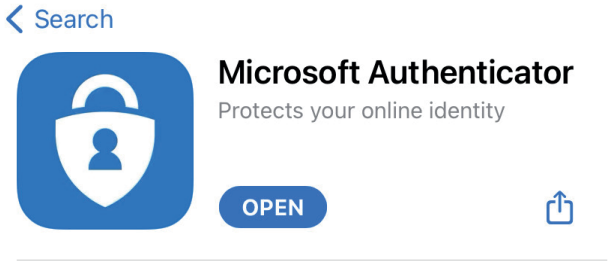
Voice

MFA Mobile Apps

MFA apps are the simplest way to secure your accounts. Once linked to your account, the app will generate random codes for you to enter after your password. These codes change regularly.

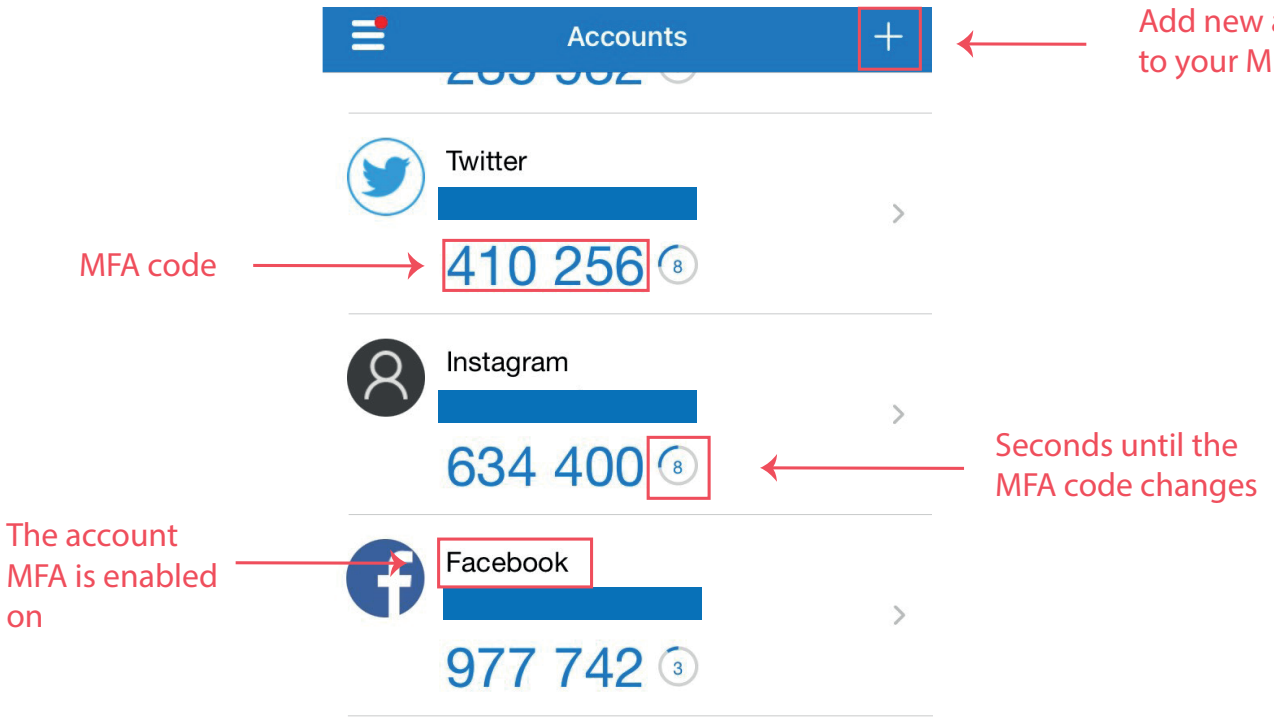
You can also enable sign-in notifications for certain accounts, including Office 365. This means that rather than entering a code, a notification will pop-up and you simply hit an approve or deny button.

To begin with MFA, visit your mobile app store and search for the Microsoft Authenticator app:

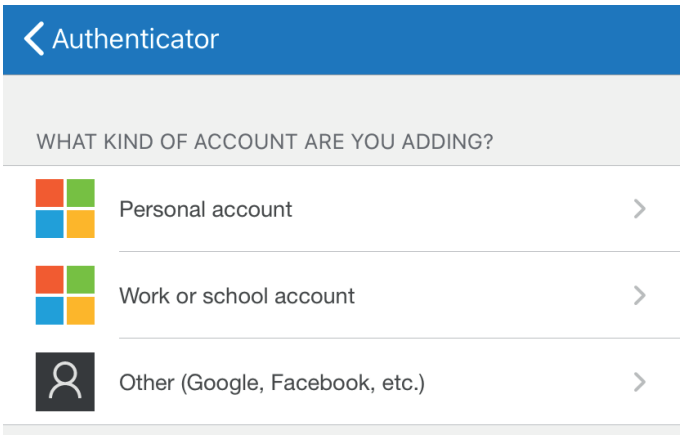


Download the app.

Once you've downloaded the app, it will look pretty empty. Below is an example of the app with MFA activated on some accounts:



If you click on the plus button in the top right to add new MFA accounts, you'll be given three options:



Personal account: this will cover a Windows account you use at home.

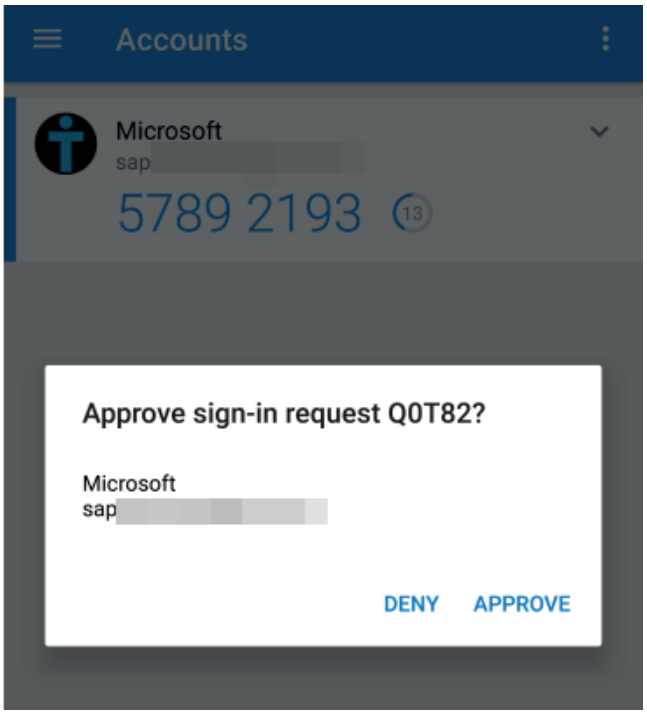
Work or school account: your work or school accounts can be added here.

Other: this will allow you to add any other accounts, such as other email accounts or social media accounts.

When you select one of the options, you'll then be asked to scan a QR code or you have the option to manually enter a code. Both the QR code and manual code will be on screen when setting up MFA on your account.

For some accounts, you may then be asked to enter the MFA code from the app to confirm setup.

When you click on an account in the MFA app, it will bring information about the setup. This can include the option to enable notification approval. If you enable this, an approve or deny option will appear when you sign into the account.



Remeber:

You can allow certain browsers or devices to be recognised, meaning you don't have to enter your authentication details every time you login. Here are some examples:

1. If you do this with your Microsoft 365 login, it will only ask you to provide an MFA code, or approve or deny notification, when you login to a new device, change your password or login at a new location.

2. If you use MFA on a password manager, you can set the password manager to recognise a browser.

3. If you setup MFA on social media and access it via mobile, you can recognise the device. You will only be asked to enter MFA if you then tried to login to the account using another device.

When using an MFA app, it's wise to place an authentication method on the app. This could be finger print or facial recognition.

For any additional help with setting up MFA, or anything else you need, get in touch:

Service Desk:
01603 709301 I servicedesk@breakwaterit.co.uk

Enquiries:
01603 709300 I enquiries@breakwaterit.co.uk