# MULTI-FACTOR AUTHENTICATION
FACTSHEET

When you log in to most University applications, you invariably just use a simple 'username and password' combination. The University recommends adding another layer of security called Multi-factor Authentication (MFA).

WHAT IS MFA?

MFA provides a second layer of security that verifies you really are the person you are claiming to be. This becomes a second step in the authentication process, where in addition to submitting something you know, a password, you also use something you have e.g. a mobile phone.

WHY DO I NEED MFA?

It is proven that MFA is the most secure and seamless way to prove your identity. MFA can also protect you should your password be stolen. Without access to the second factor, your username and password are useless to an attacker.

Are you trying to log in to XYZ?

YES   NO

Your username

Your password

CODE   123456
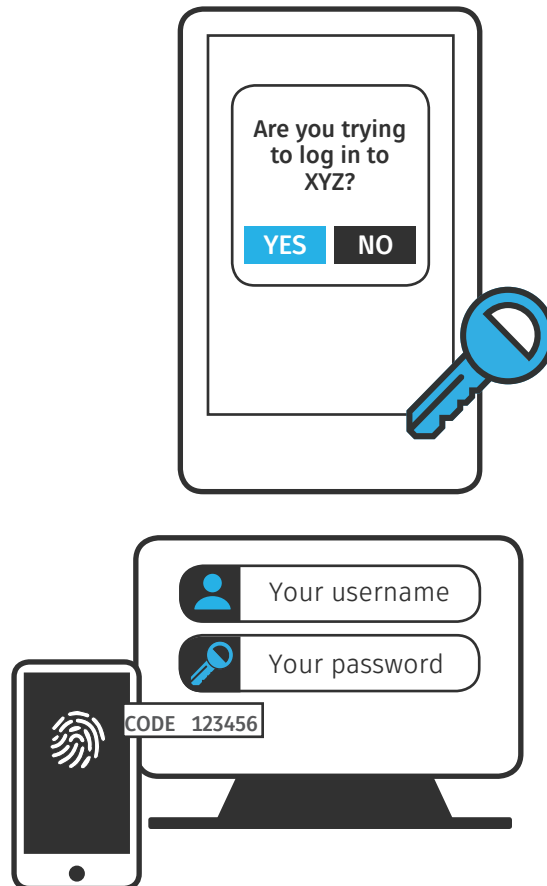
HOW IT WORKS

After you have used your password to log in, you will be asked to use a second factor such as the Okta Verify app on your phone to confirm your identity. This is similar to how you may access online banking. As the system learns the locations and devices you typically use, it will prompt you less often for a second factor.

HOW TO TURN IT ON?

You can opt in to MFA by **submitting this form**.

For more information on MFA please see this Knowledge Base article on serviceUON.