

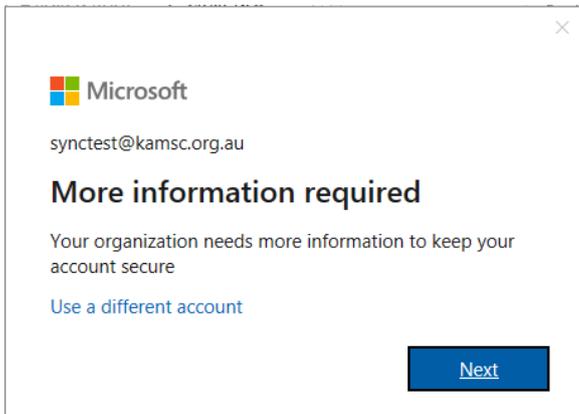
## What is Multifactor Authentication?

Multifactor Authentication (MFA, or 2FA – two factor authentication) is a form of authentication that requires more than just a password, or one form of authentication, to verify an account. Most people will have encountered some form of MFA nowadays, e.g. receiving an SMS code from your bank to verify your account during online banking.

Multifactor Authentication is integral to protecting our intellectual property – it assists by preventing unauthorized access to your accounts, even if somebody guesses or hacks your password, they will likely be prevented accessing your information as they will not have access to the second form of verification.

## Setting up MFA

After MFA is enabled for your 365/email account, you will receive a message like this when next logging into your account:



Click “Next” and use the following guidelines in the image to configure MFA for your account.



## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

**Step 1: How should we contact you**

Authentication phone

Australia (+61)

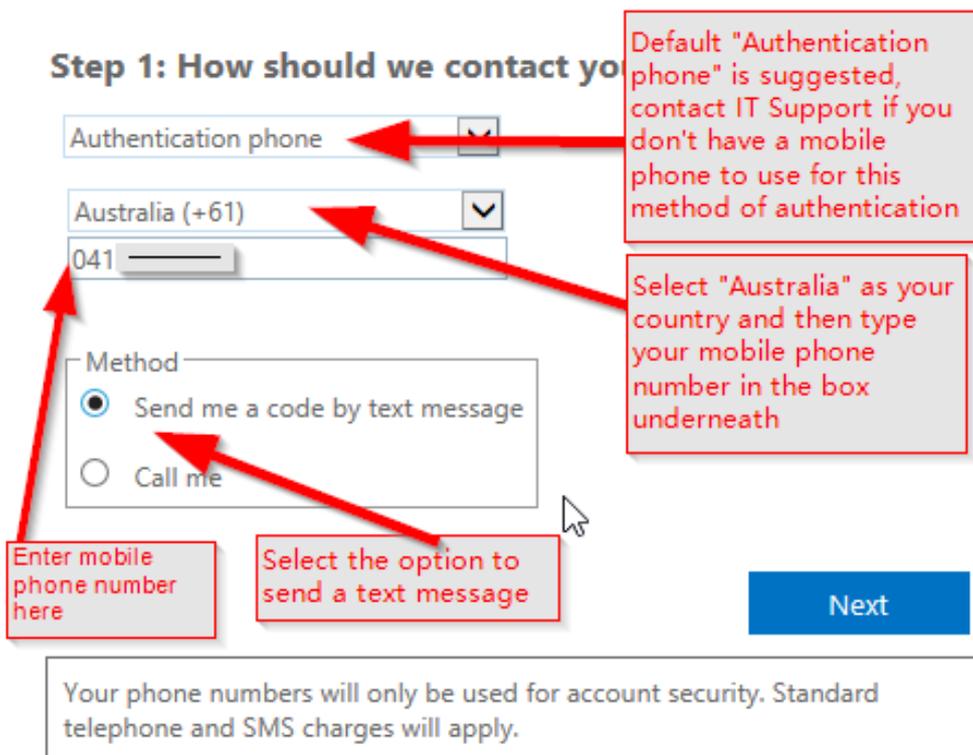
041

Method

Send me a code by text message

Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.



Default "Authentication phone" is suggested, contact IT Support if you don't have a mobile phone to use for this method of authentication

Select "Australia" as your country and then type your mobile phone number in the box underneath

Enter mobile phone number here

Select the option to send a text message

Click "Next" and when you receive the SMS code enter in the following screen

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

**Step 2: We've sent a text message to your phone at**

When you receive the verification code, enter it here

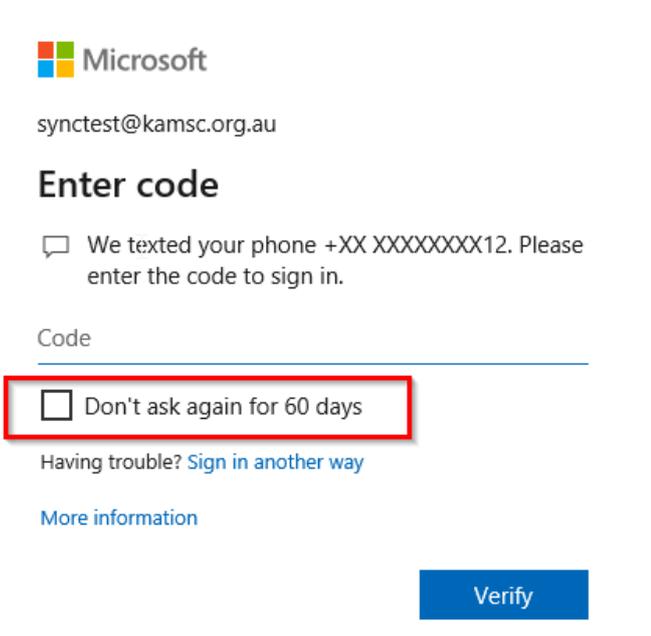
This concludes setting up MFA for your account – if you are prompted to copy or asked about app passwords you can safely ignore/continue/click "Done"

## FREQUENTLY ASKED QUESTIONS

### Q) Will I receive an SMS every time I login to my account?

A) Applications like Microsoft Outlook, Microsoft Teams, Onedrive should all only require the MFA verification once – sometimes after a password reset or change to account, these applications may ask again – but they should not require SMS verification code *every* time you use them. If this is happening please raise a ticket with ICT Helpdesk (email [itsupport@kamsc.org.au](mailto:itsupport@kamsc.org.au))

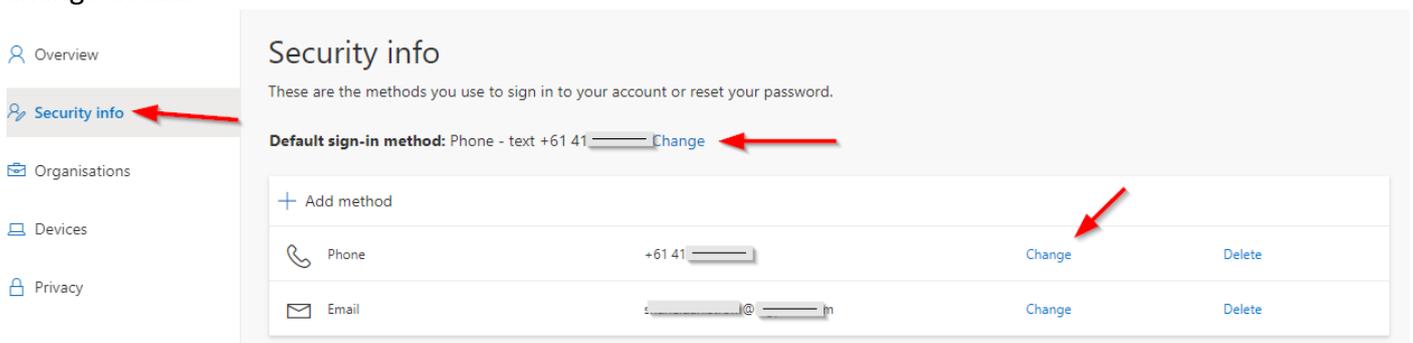
If you use a browser (Chrome/Edge/Firefox) to access your 365 account, then yes you will be prompted to verify each time – however – there is an option to trust a device for 60 days. When you are logging on via a browser, after entering the SMS code, tick the “Don’t ask again for 60 days” checkbox to save verifying each time



The screenshot shows the Microsoft login verification interface. At the top is the Microsoft logo and the email address 'synctest@kamsc.org.au'. Below this is the heading 'Enter code'. A message states: 'We texted your phone +XX XXXXXXXX12. Please enter the code to sign in.' There is a text input field labeled 'Code'. Below the input field is a checkbox labeled 'Don't ask again for 60 days', which is highlighted with a red box. Below the checkbox are links for 'Having trouble? Sign in another way' and 'More information'. At the bottom right is a blue 'Verify' button.

### Q) What if I change phone numbers/lose my phone/move to a different position?

A) You can change details yourself, by logging into <https://portal.office.com>, click your profile initials/picture in top right corner, and select “View Account” – then click “security info” for options to change details



The screenshot shows the 'Security info' page in a Microsoft account portal. On the left is a navigation menu with 'Security info' selected and highlighted by a red arrow. The main content area shows 'Default sign-in method: Phone - text +61 41 [redacted] Change', with a red arrow pointing to the 'Change' link. Below this is a table of sign-in methods:

+ Add method			
Phone	+61 41 [redacted]	Change	Delete
Email	[redacted]@ [redacted].in	Change	Delete

Red arrows point to the 'Change' links for both the phone and email methods.

Alternatively, ICT Helpdesk can reset MFA so that it asks to re-verify the details (including the phone number). Send an email to [itsupport@kamsc.org.au](mailto:itsupport@kamsc.org.au) asking to “reset MFA contact methods”.