

Microsoft Multi-Factor Authentication (MFA)

A brief introduction

The KCMO Cyber Security Team will be enabling MFA for all Microsoft Office 365 accounts. Multi-Factor Authentication is one of the most effective and least-intrusive methods of ensuring the everyday user is secure in an ever-growing security landscape. Multi-Factor authentication (or MFA) is a secondary form of logging into a service. There are multiple options for MFA:

- Email
- Phone call
- Text
- Security Questions
- Mobile App

What does this mean for you?

It is strongly recommended that you setup MFA as soon as possible. You can only setup MFA from within the City Network and from a City Computer. Any attempts to setup MFA outside of the City network will result in a denial of permissions or an error. When setting up MFA you do not have to go with the default option of using the Microsoft Authenticator App.

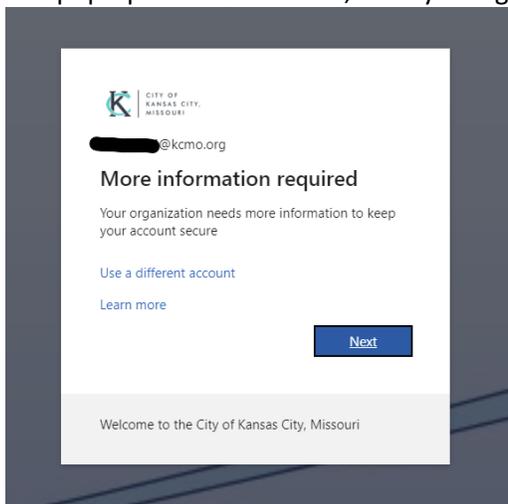
To setup MFA use the following link:

<https://aka.ms/MFASetup>

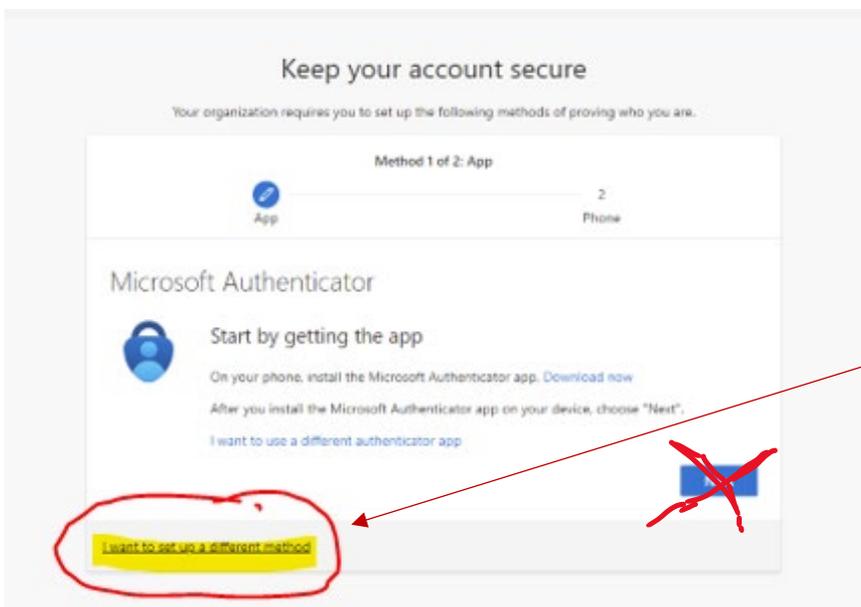
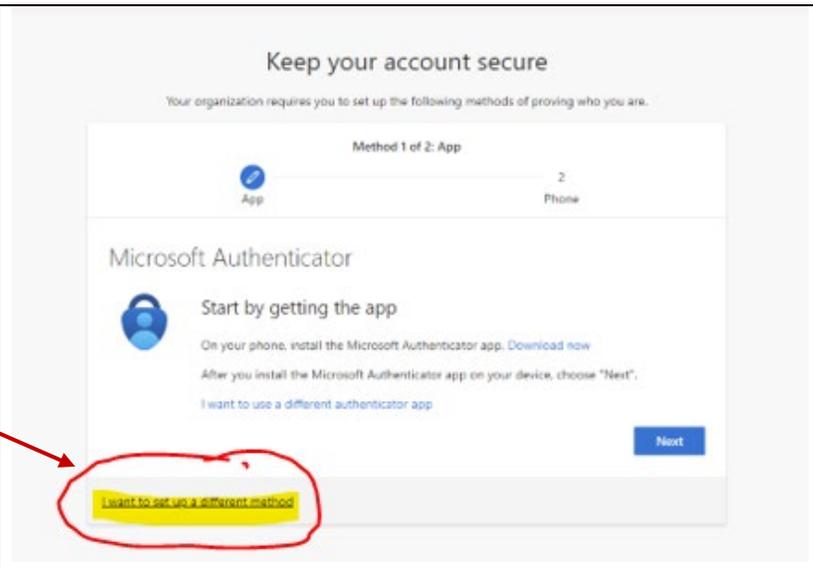
- **Follow the instructions on pages 2 & 3 of this guide**

Once MFA is enabled for the Fire Department, you will be forced to set it up. A pop-up screen will come up when you log into your computer and open a cloud app like Microsoft Outlook Web, Sharepoint Online, or another Microsoft web-app.

The pop-up will look like this, after you login with your email and password (click next):



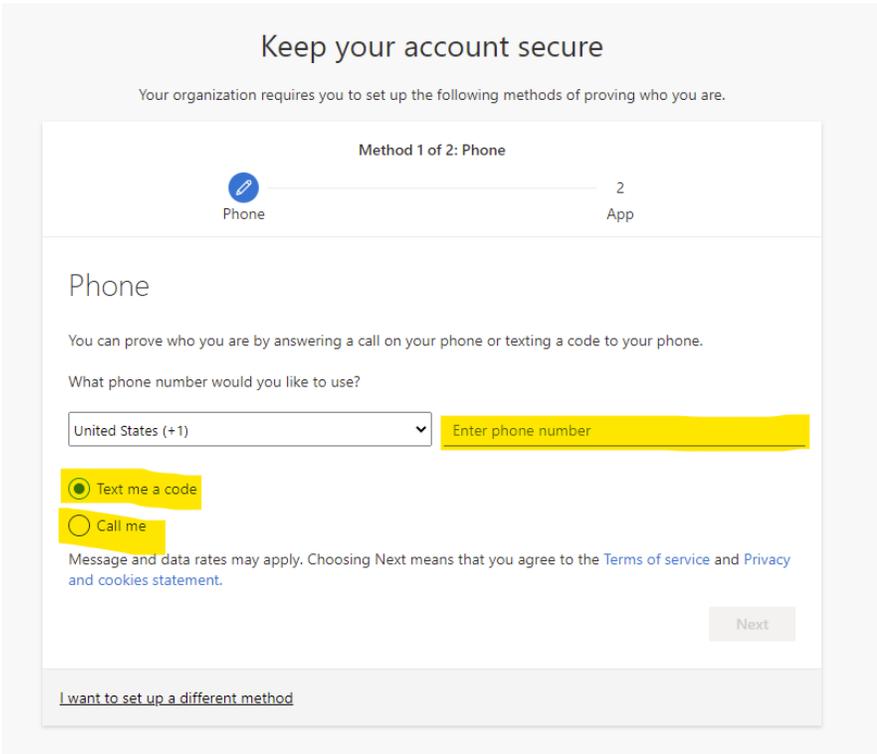
When setting up MFA, you will be prompted to setup a method of verifying who you are. You can select SMS text, phone call, email, or security questions. The default option set to the Microsoft Authenticator App, however, we recommend selecting one of the other options by selecting **“I want to setup a different method”** link.



You do not have to use the Microsoft Authenticator App. To use your cell phone or other options select the **“I want to setup a different method”** link.

If you wish to find out more information about your desired method of multi-factor authentication, see the methods below:

- SMS Text: [CyberSecurity - MFA Setup - SMS Text](#)
- Email: [CyberSecurity - MFA Setup - Email](#)
- Phone Call: [CyberSecurity - MFA Setup - Phone Call](#)



After you setup the first method the system will have you setup a secondary method of authentication.

As a reminder, this must be performed from a computer on the city network. To add a secondary method, make sure that you can access the secondary resource. The secondary resource includes:

- Your cell phone
- Your personal email account (outside of your work email)
- Your desk or home phone
- Security Questions

What happens if I don't set it up?

If MFA is not set up, then the ability to log into typical resources will be denied. Cyber Security is looking into making MFA a strict requirement to ensure the security of our users. Access to workplace resources will remain denied until MFA is set up.

Should any problems arise, please contact firesupport@kcmo.org or cyber.security@kcmo.org.

If you wish to set up your multi-factor authentication now, you can always visit the following link here: <https://aka.ms/MFASetup>