Multi-Factor Authentication and your TCPS accounts
Who, What, When, Where, Why, and How

What is MFA and why do I need to know?

Multi-Factor Authentication, also known as "MFA", is a data security method that requires that a user have more than just a password to sign-in to an account. Currently, most MFA methods require only a "second factor" of authentication beyond a password, but it can include more than two factors.

The most common "second factor" currently in use is entering a code received as a text message to a mobile phone; however, downloadable "Authenticator Apps" are also available. Unless you intend to use an authenticator app for multiple services, the easiest way is to just receive the text message.

Using MFA is something you should strongly consider for both professional and personal accounts if you aren't already using it, especially for your personal financial accounts.

Who is required to set up MFA and when?

All adults with a district provided email account in Kentucky *must* have MFA enabled for their Microsoft 365 (M365) account before the end of the 2022-2023 school year. This is being done to prevent cyber actors from accessing your account following a compromised password. Password compromises have become commonplace due to successful phishing emails and breached databases of 3rd party vendors.

Setting up MFA will *help* protect your staff accounts and student information that your staff account may have access to.

All those who have a district issued computer must have a second device available to them for the MFA process to work. The recommendation is that you use a personal mobile phone. Regardless of the device you choose, you must have access to your second factor to sign in to your M365 account when off the school network.

Where/When will I have to use MFA?

Currently, MFA is only required for your district Microsoft 365 account. This means it is required to access your district email. Some staff members have additional district accounts, such as Google Workspace and Infinite Campus, tied to their M365 account. In these cases, you will also be prompted for the second factor.

You will only have to use the second factor of authentication on a device that is not connected to the school network. In other words, you will need to use the second factor on any personal devices that you use with your district accounts, as well as any district devices you use outside of the district (e.g. home or conference).

Additionally, you will have the option to have your internet browser "remember" your device for up to 30 days. This will prevent you from having to use the second factor for that length of time provided you use that browser on that device again and don't clear the browser's cache. More information on this can be found in the setup instructions.

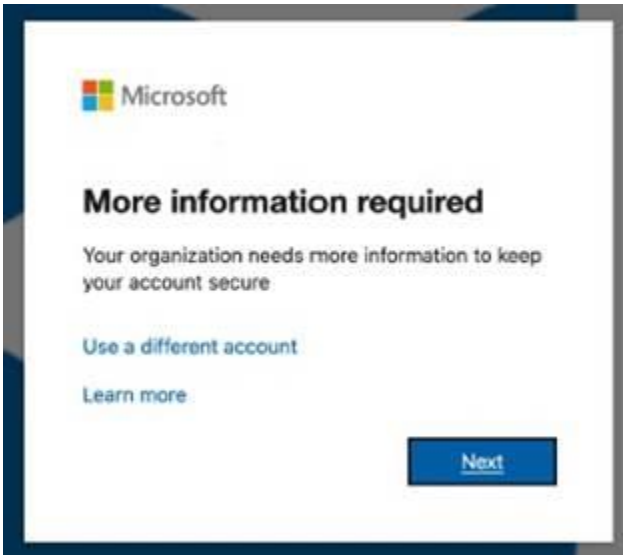
Why do I need to use MFA?

The Kentucky Department of Education is currently working to move ALL of the school districts and the Office of Education to be more in line with the federal security guidelines. This process started last year with the move to a fifteen (15) character passphrase, instead of an eight (8) character password and will continue with more enhanced security measures over the next few years. As a state, we are currently experiencing over 1 MILLION attempts to breach our networks and programs per month.

How *do I set up Multi-Factor Authentication (MFA) for my district account?*

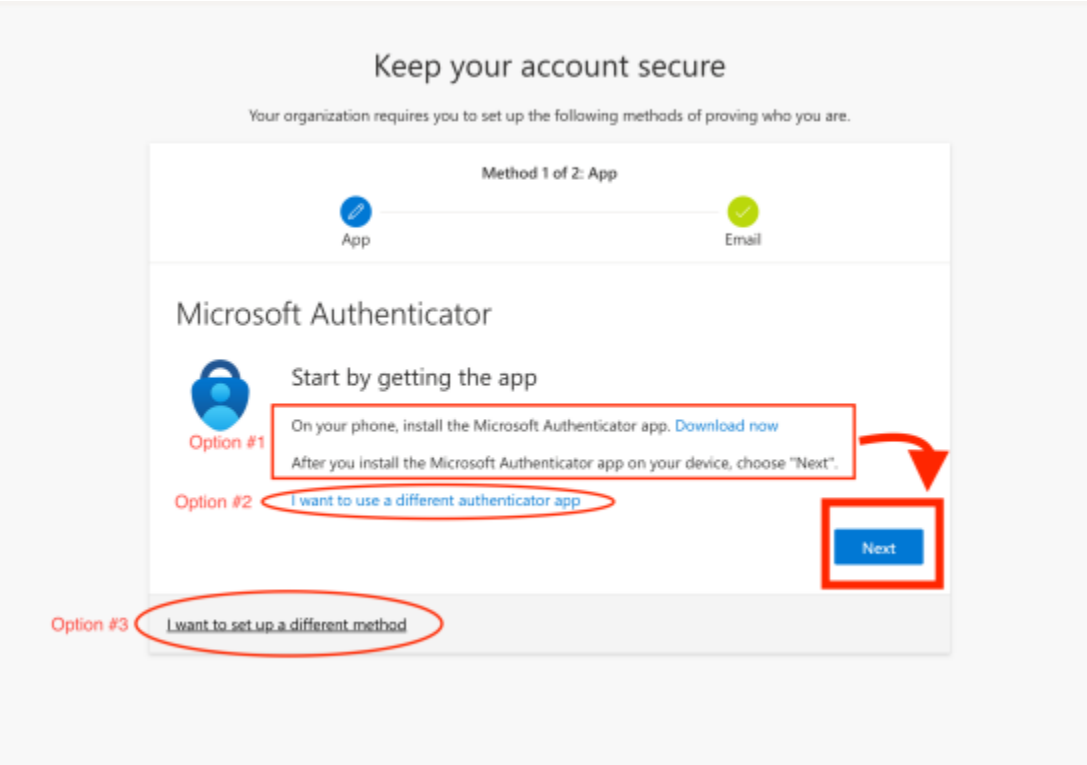
If you haven't already performed this as part of the Self-Service Password Reset instructions I sent a few weeks ago, please follow the steps below.

1. *Once the Technology Department enables MFA for your M365 account,* you will be prompted for "more information" the next time you attempt to access your Microsoft 365 account. Select "Next" to choose your MFA option



2. You may set up MFA to use a text message or to use an authenticator app. **We recommend you use a text message for simplicity. In the screenshot below, that is Option #3, *"I want to setup a different method."* Make sure you click that link instead of clicking on "NEXT".** If using this method, proceed to the next page for more specific instructions.

If you choose to use an authenticator app instead, select either Option #1 or Option #2 as shown in the screenshot below, click the Next button, then follow the instructions on your computer screen.



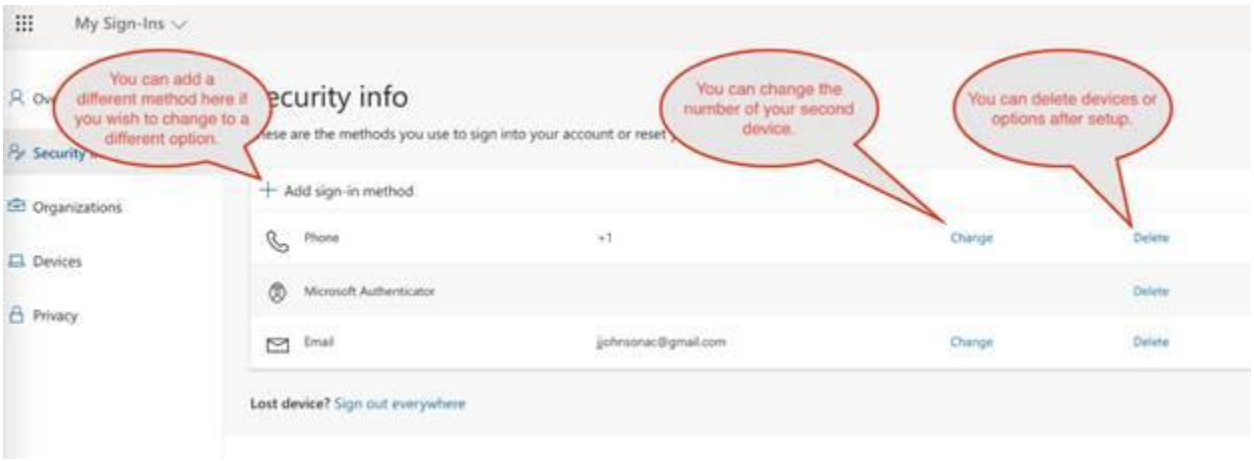
3. If you are using the recommended texting option, follow the below steps.
Authenticate using voice or text*

1. Click on the link "*I want to set up a different method*."
2. Expand the drop-down menu and select the "phone" option, then "Confirm."
3. Enter the phone number of your second device and click on "Next."
4. Enter the code sent to your mobile phone on the computer when prompted.

**The phone you use must be able to receive a text message in order to complete the setup process. However, once setup is completed, you will have the option to authenticate by way of receiving a phone call or a text message to that phone.*

You can change you MFA method anytime in the future by:

• Navigating to the following link:
https://aka.ms/mfasetup
• Navigating the following path once logged in to your Microsoft365 account:
[select name/avatar in upper-right corner] > View Account > Security Info


My Sign-Ins
You can add a different method here if you wish to change to a different option.
You can change the number of your second device.
You can delete devices or options after setup.
ecurity info
Organizations
Devices
Privacy
Add sign-in method
Phone
+1
Change
Delete
Microsoft Authenticator
Delete
Email
jjohnsonac@gmail.com
Change
Delete
Lost device? Sign out everywhere