# INTRODUCTION TO MULTI-FACTOR AUTHENTICATION

# WHAT IS MULTI-FACTOR AUTHENTICATION?

**What is Multi-Factor Authentication (MFA)?**

MFA is a security layer that makes it more difficult for hackers to gain access and take control of computing accounts, and online information. MFA verifies your identity through a two-step process before granting you access to the associated online application(s). You may already be using MFA to protect access to online services such as your banking or credit card accounts.

The two verification methods that are usually required to prove your identity are information you know, almost always your username and password AND a unique item you have, typically your cell phone.

**What two-factors will CVUSD be using?**

CVUSD will be using a combination of:

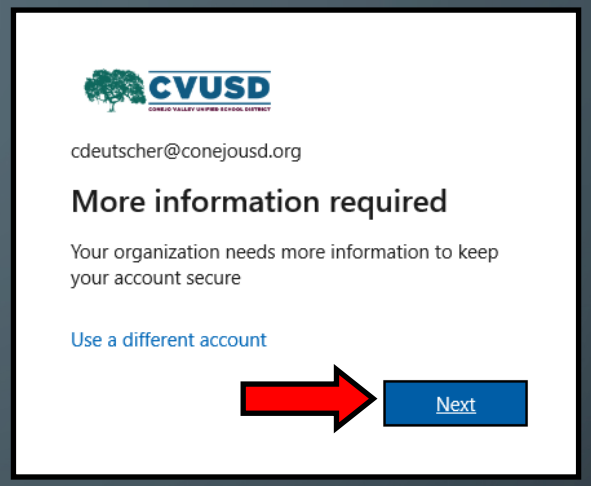
1. Your CVUSD username / password and
2. A code sent via text message OR a code generated by an authenticator mobile application. *You choose the option you prefer!*

**Why are we implementing Multi-Factor Authentication?**

Risk reduction is critical for organizations! MFA does not stop all types of attacks, and it does not guarantee security, but it does reduce the risk of technology and data compromises by making cyberattacks more difficult, even if your password is compromised.

# HOW TO SETUP YOUR MFA

- Getting started is easy!
- To setup MFA, simply click this link: https://www.office.com/login and login using your CVUSD username and password; *this is the same account you use to login to your computer*
- You will be greeted by the "More Information Required" pop-up
- Select the "Next" button to start setting up your MFA




There are 2 options for MFA:

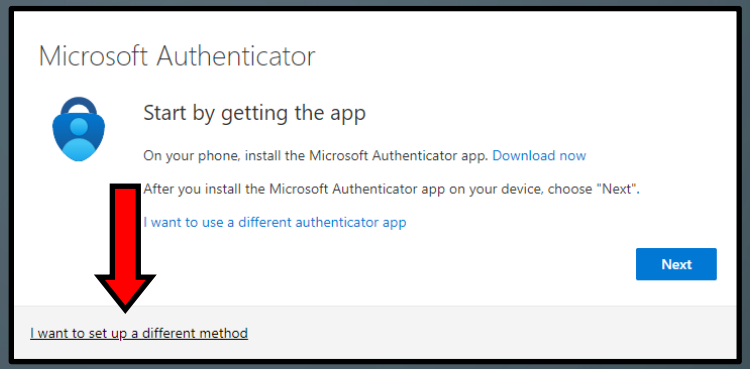
- Option A is to receive your MFA code via text to your cell phone (**Pgs. 4 - 5**)
- Option B is to receive your MFA code via an authenticator mobile app (**Pgs. 6 - 7**)

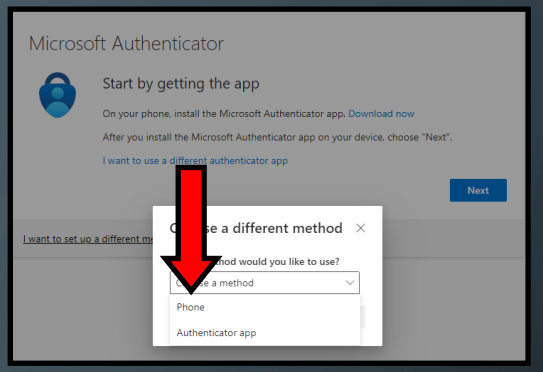
Please proceed to the appropriate page for your setup instructions.

# OPTION 1: MFA USING TEXT MESSAGE

**Step 1:**

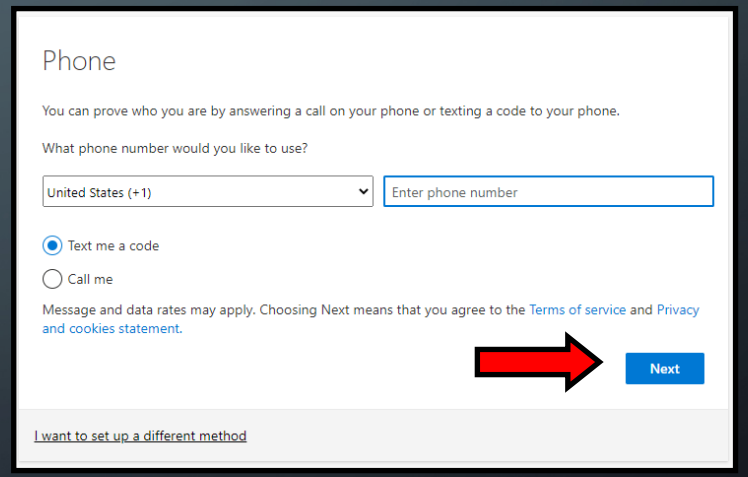
- On the Microsoft Authenticator screen, click on the "I want to setup a different method" link
- Select "Phone" from the drop-down list
- Press the "Confirm" button and then "Next"




**Step 2:**

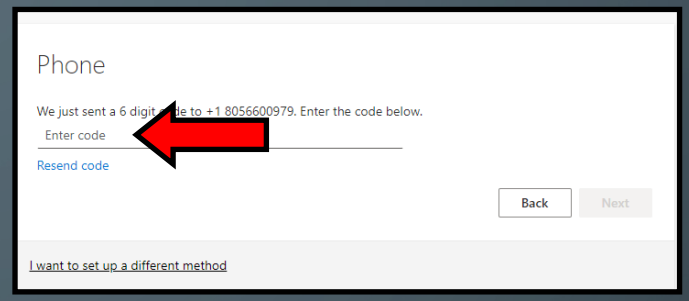
- Enter your phone number in the available box then press "Next"
- **Please note:** This is the phone number that will receive your MFA codes



# OPTION 1: MFA USING TEXT MESSAGE

**Step 3:**

- A code will be text to the phone number you entered in the previous step
- Enter that code into the box and click “Next”

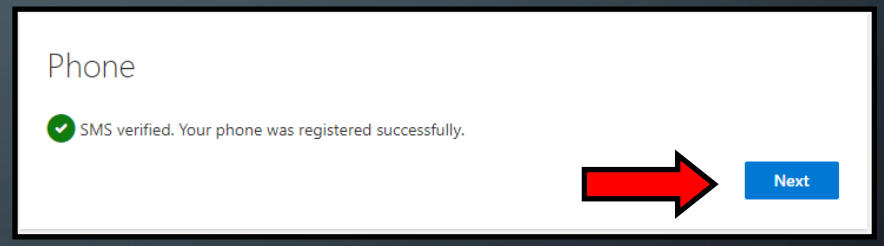



**Step 4:**

- Success! You have setup your MFA!

Click “Next” to finish

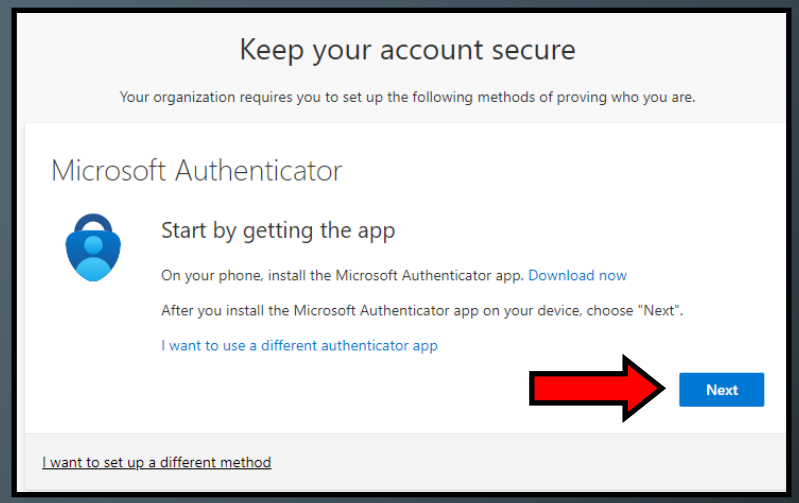
- Please Proceed to the FAQ’s on pg. 9



# OPTION 2: MFA USING A MOBILE APP

**Step 1:**

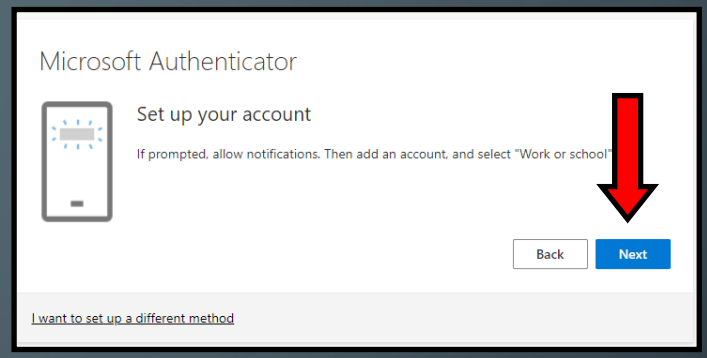
- At the “Microsoft Authenticator” screen, you will be asked if you have an authenticator app on your phone.
- If you do not have Microsoft Authenticator installed on your phone, click “Download now” or scan one of the QR codes below to install the app
- Once installed click “Next”



# OPTION 2: MFA USING A MOBILE APP

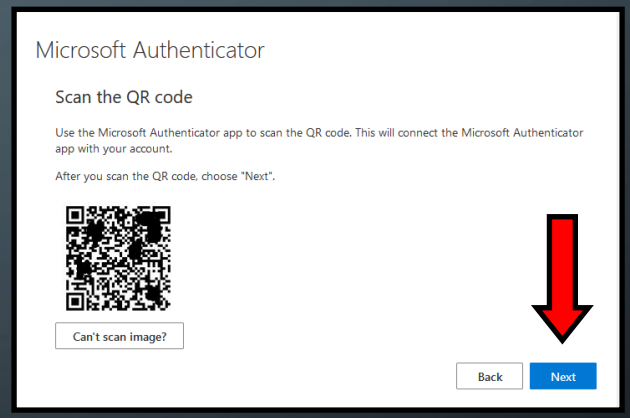
**Step 2:**

- **On your mobile device**: Once Microsoft Authenticator is installed, select "Add account" (*image not shown*)
- **On your mobile device**: Select "Work or School account" followed by the "Scan QR Code" option when prompted (*image not shown*)
- Click "Next" on the computer prompt




**Step 3:**

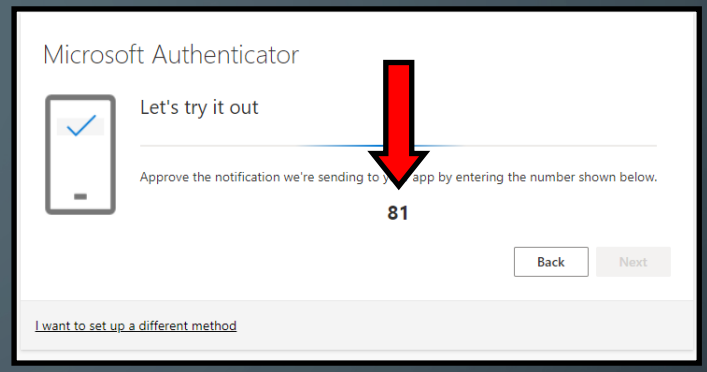
- Scan the QR code on the computer screen and select "Next"



# OPTION 2: MFA USING A MOBILE APP

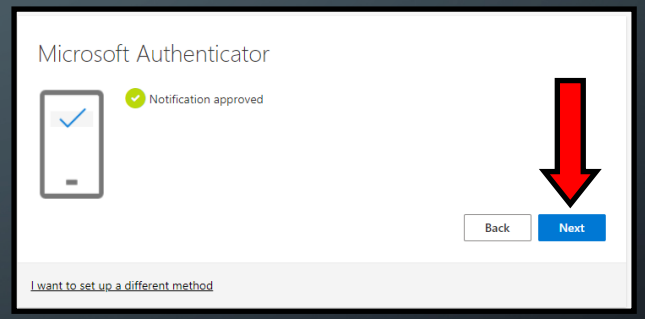
**Step 4:**

- A prompt will appear on your phone and ask you to enter the number that appears on the computer screen.




**Step 5:**

- Success! Press the "Next" button to complete your MFA Setup



# FREQUENTLY ASKED QUESTIONS

**Will I need to use MFA every time I use my computer?**

**No.** You will not be prompted for MFA when logging into your District computer.

You will be prompted for an MFA code in the following scenarios:

- When you first establish MFA for your account
- When first accessing Frontline (https://login.frontlineeducation.com/sso/conejousd) and every 90 days thereafter
- When first accessing your email remotely via Outlook Web Login (http://outlook.office.com/) and every 90 days thereafter
- When first accessing your email on your mobile device and every 90 days thereafter
- Anytime our system does not recognize the device you are logging in from

**Can MFA be used to see data on my phone or track the location of my phone?**

No. There is no connection between MFA and device data or location.

**What happens if I lose my cell phone or phone number?**

Open a ticket by visiting http://helpdesk.conejousd.org or contact your Site Technician

**Will this impact how I login to Google, Escape or Q?**

No. This process does not impact or change how you login to Google, Escape, or Q.

**What if I want to change my authentication method?**

Visit http://mysignins.microsoft.com security-info to add or remove devices and MFA methods

Or for assistance, open a ticket by visiting http://helpdesk.conejousd.org or contact your Site Technician