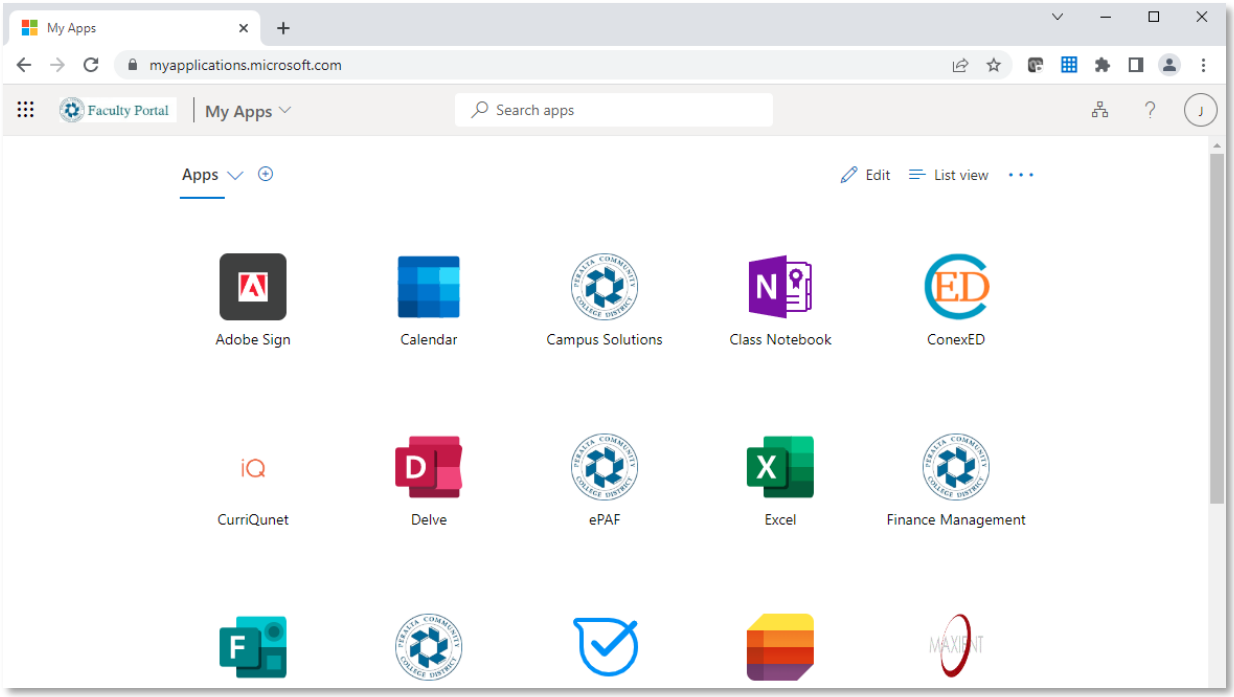
SET UP SECURITY INFORMATION FOR MULTI-FACTOR AUTHENTICATION USING PHONE METHODS

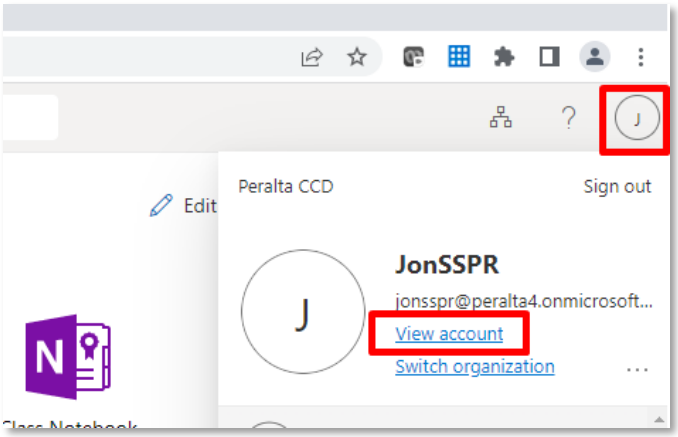
As of November 2022, all staff accounts are required to use multi-factor authentication to access Peralta systems. Multi-factor authentication ("MFA") means that when you log in to your Peralta account with your username and password, a secondary validation method is also required, such as a text code sent to your mobile phone.

This document explains how to register one or more *authentication methods* for use with MFA.

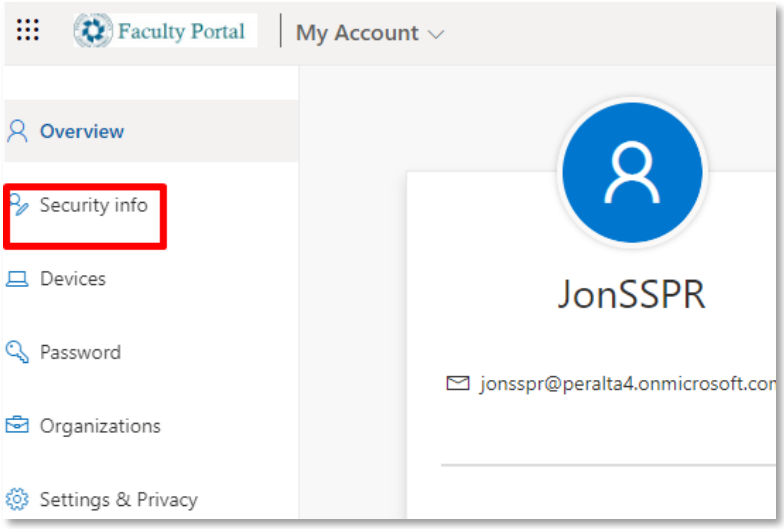
1. Log into the Web Portal at https://myapplications.microsoft.com



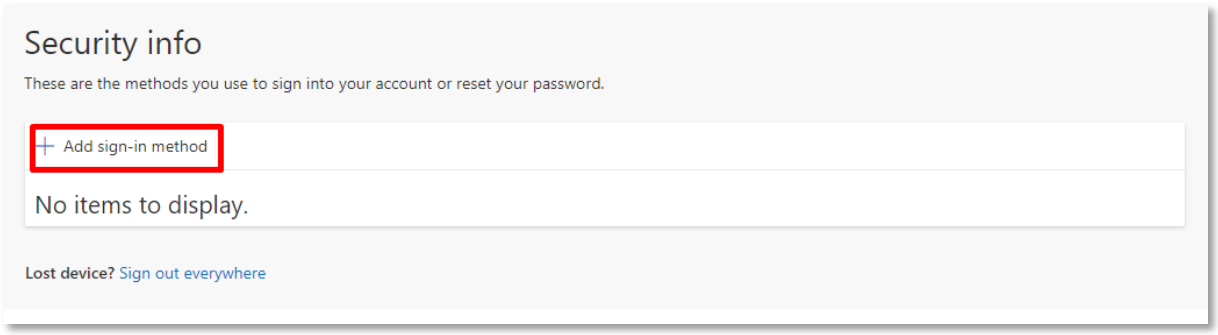
2. Click on your **account icon** in the upper-right hand corner. A menu appears. Click on **View Account**.



3. On the left navigation, click on **Security Info**.



4. Click on **Add sign-in method.**



5. You must register either a phone or the Microsoft Authenticator mobile app. The phone(s) you register can include your cellular, home and work phones. You can register multiple methods.

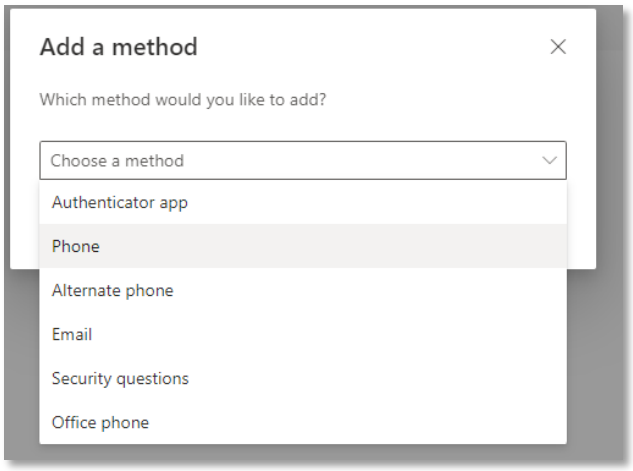
   For most, cell phone will be the most straightforward option, however, if you have a land line at home, it also recommended to register it as a backup in the event your cell phone is lost or stolen.

   Descriptions of each method are provided below:

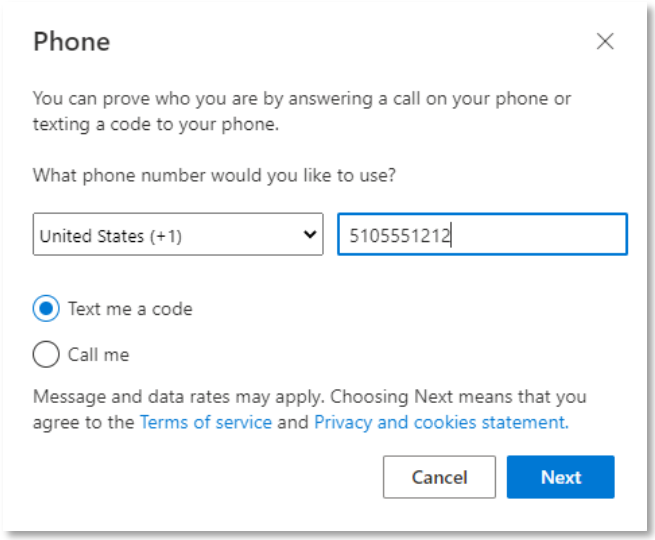
   - **Phone:** Select this option to register your cell phone. This is the simplest and most convenient method for most. You can select voice or text as the verification method. Note, if you frequently work in cellular “dead zones”, we strongly encourage you to set up a second or third method as a backup.
   - **Office Phone:** Use this option to register the phone you use at work. Note that a confirmation call will be sent to this phone, so you must be present in the office to register it.

- **Alternate Phone:** Use this option to register the phone you use at home (i.e. a "landline"). Note that a confirmation phone call will be sent to this phone, so you must be at home to register it. This is a good option for those who frequently work from home and also have poor cellular service.
- **Microsoft Authenticator:** This is an optional method. It requires an Android or iOS/Apple mobile app that can installed on your phone or tablet. The Authenticator is a good choice if you work in areas with poor cell phone coverage since it also works over regular WIFI and LAN connections. There are some additional steps to set it up (See instructions in the attached document).
- **Email:** This method will allow you to reset your password if you forget it, but it **will not** work with MFA.
- **Security Questions:** This method will allow you to reset your password if you forget it, but it **will not** work with MFA.

6. Select Phone from the dropdown.

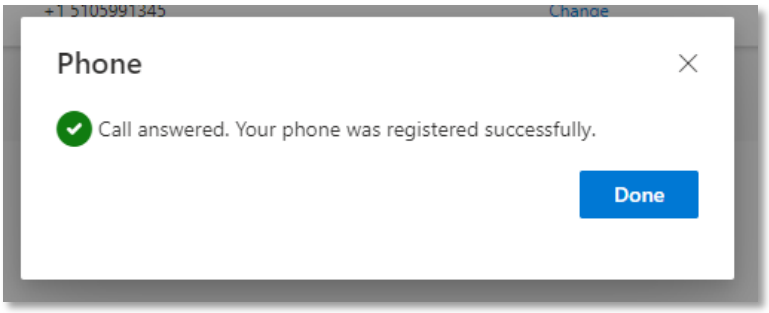


7. Enter your **area code + phone number**. (Dashes and parentheses are not required.) Select whether you wish to receive a **call** or **text message**, then click **Next.**



If you select the text method, a code will be sent to you. Input the code to complete the registration.

If you select the phone method, you'll receive an automated call from Microsoft and it will instruct you to press the pound (#) key to complete verification. Once you do this, you will receive the following message on your computer.



You have now met the minimum requirements for multi-factor authentication (MFA).

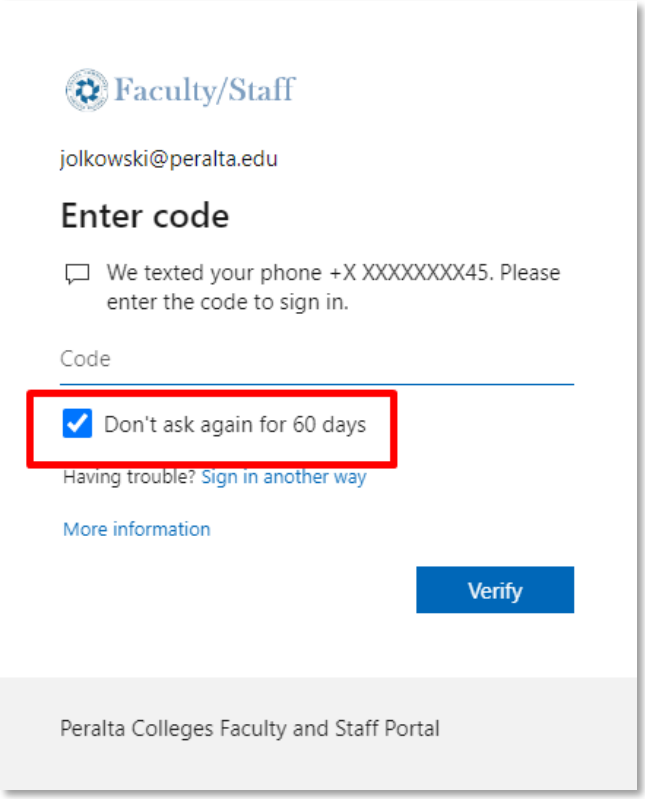
MORE INFORMATION

When I go to my security methods, my phone is already registered.

For some staff, the phone number was pre-registered based on information submitted at the time of employment onboarding. For others, if you previously enrolled in self-service password reset (SSPR), your phone can be used for both MFA and resetting your password. In either case, if the phone number is correct, no further action is required from you. However, we encourage you to set up at least one additional phone (home or work) as a backup in case your phone is lost or stolen.

Will I need to use MFA every time I log in?

No. You must use MFA whenever logging in with a new device. Once you complete the login, you can check the box which says, **Don't ask again for 60 days**. Once you check this box, you will not need to perform the MFA login on that device for the next 60 days. For example, if you have a cell phone and laptop computer, you will be required to perform MFA on both, and re-validate every 60 days.



Should I use Microsoft Authenticator in addition to phone or instead of phone?

Microsoft Authenticator is the most secure method but requires installing the App on your Android or iOS mobile phone or tablet, which may be challenging for some.

In addition to being more secure, it can be used over home or work WIFI when cellular service is unavailable (cellular dead zone). If you work remotely from a location that has poor cellular reception, we recommend using this option in addition to cell or home phone.

If you wish to use Authenticator, please see the instructions attached to this email.

I'm having trouble setting up my security options.

Contact your campus IT Support staff or the District Helpdesk for further assistance:

Berkeley City College – bcchelpdesk@peralta.edu

College of Alameda – coahelpdesk@peralta.edu

Laney College – laneyhelpdesk@peralta.edu

Merritt College – merritthelpdesk@peralta.edu

District Administrative Center – helpdesk@peralta.edu