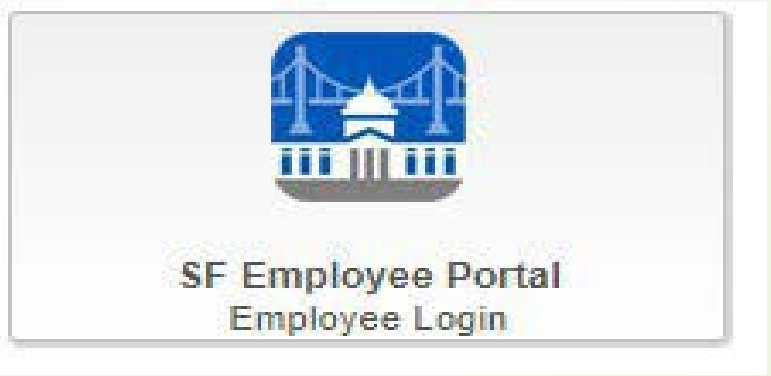
How to Access the SF Employee Learning Portal

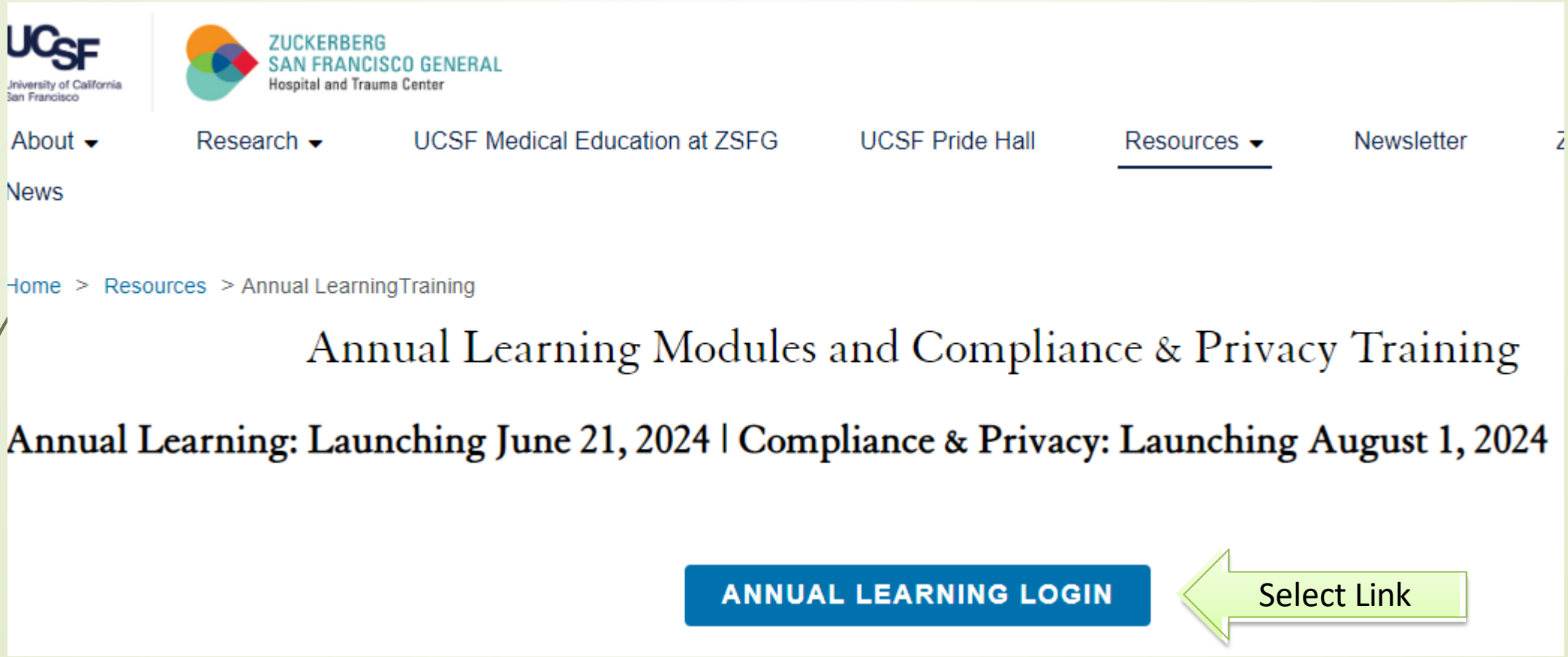
A Quick Guide for UCSF Faculty, Staff, andTrainees at ZSFG



Reminders	- Use Firefox, Microsoft Edge, or Chrome - Turn Off Pop-Up Blockers

Step 1

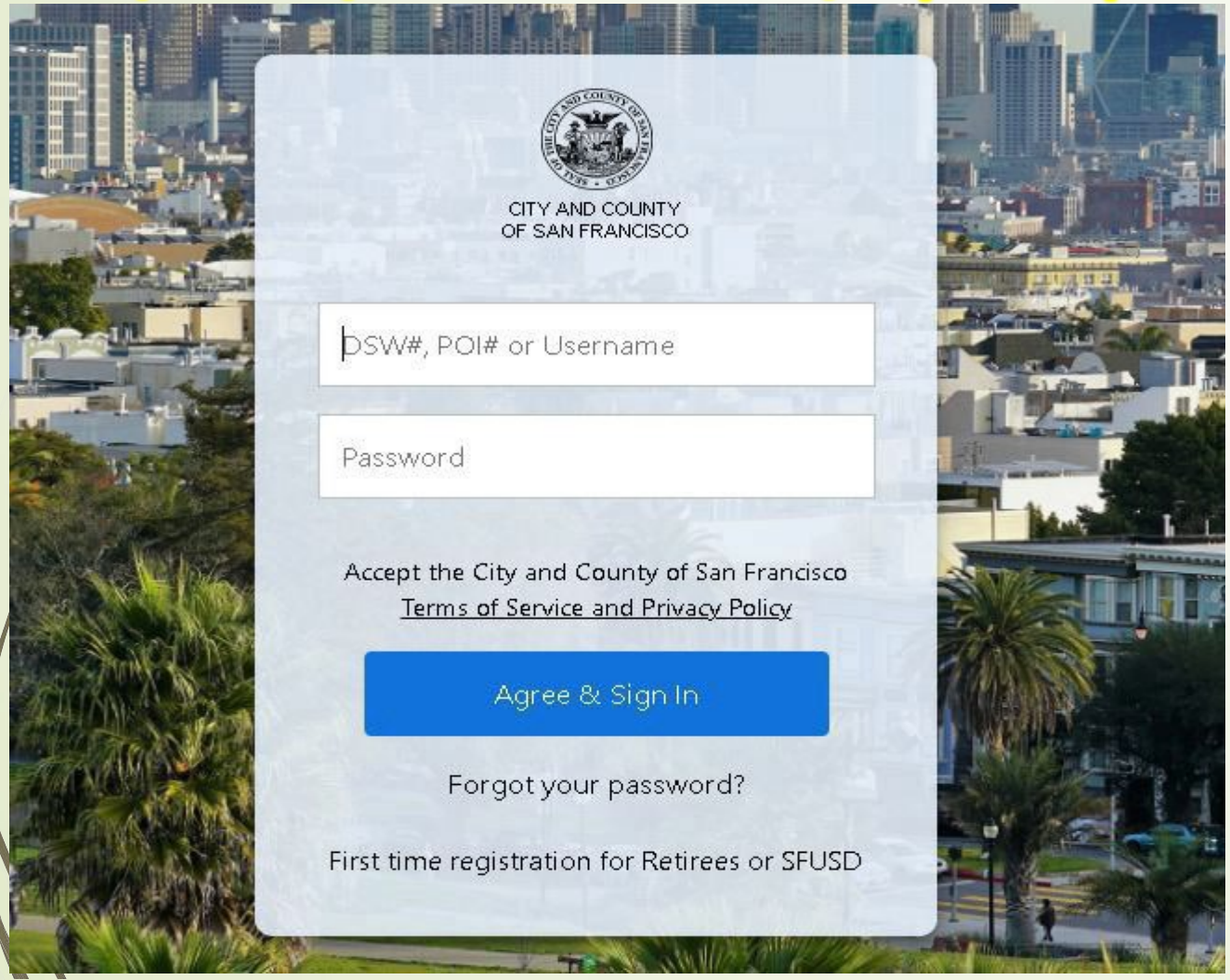
Visit: https://zsfg.ucsf.edu/sflearn



Step 2

CCSF Login Page

If you know your POI# and Password, skip to Step6



- Enter UCSF POI#

Contact: Department Manager/ Champion or Trainee Administrator for Assistance

- Enter Password

First Time User?

Contact DPH IT for temporary password,628-206-7378

Previous User and Forgot Password?

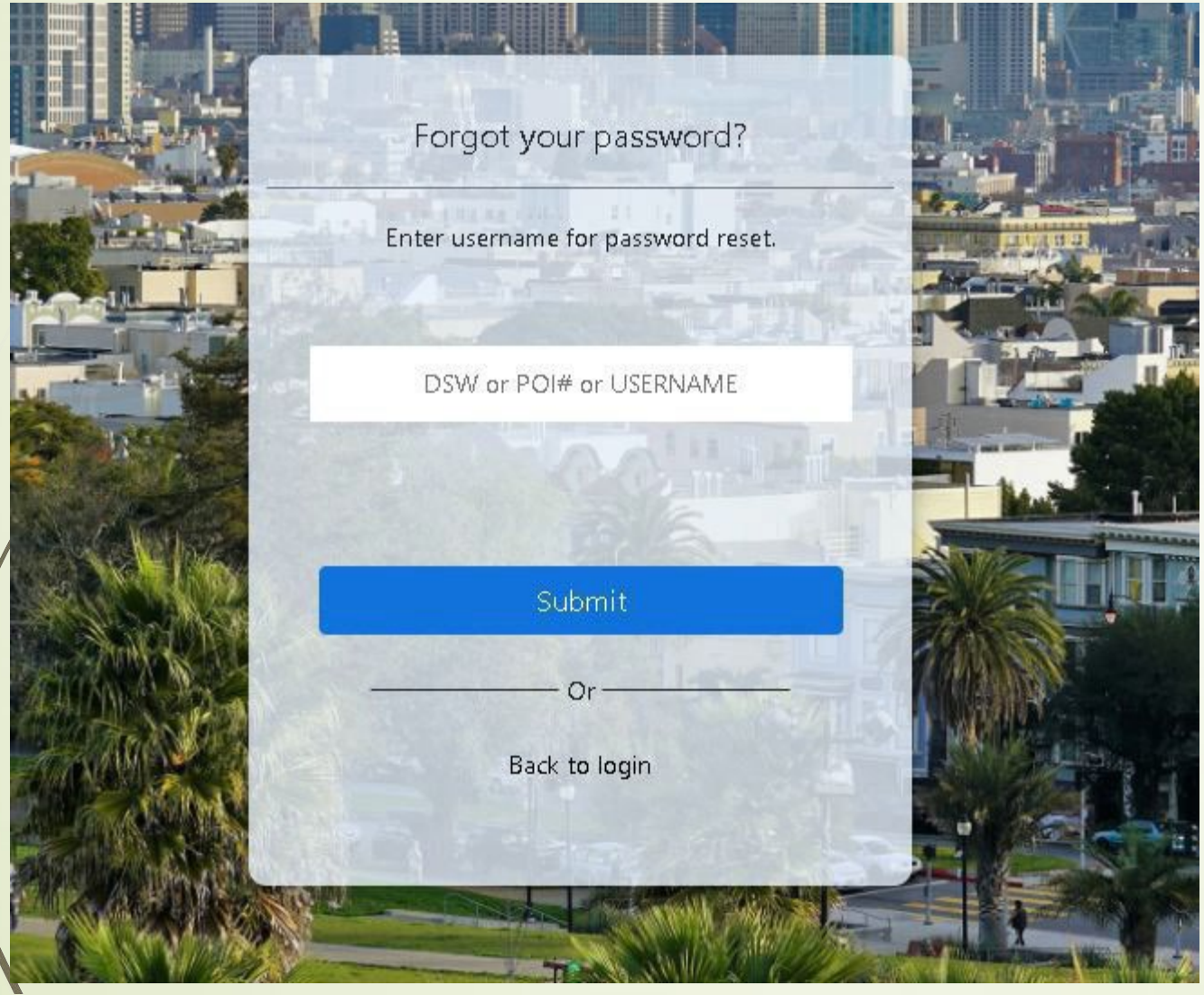
Select 'Forgot your password?' link

- Select 'Agree & Sign In'

IF you entered both POI# and Password

Step 3

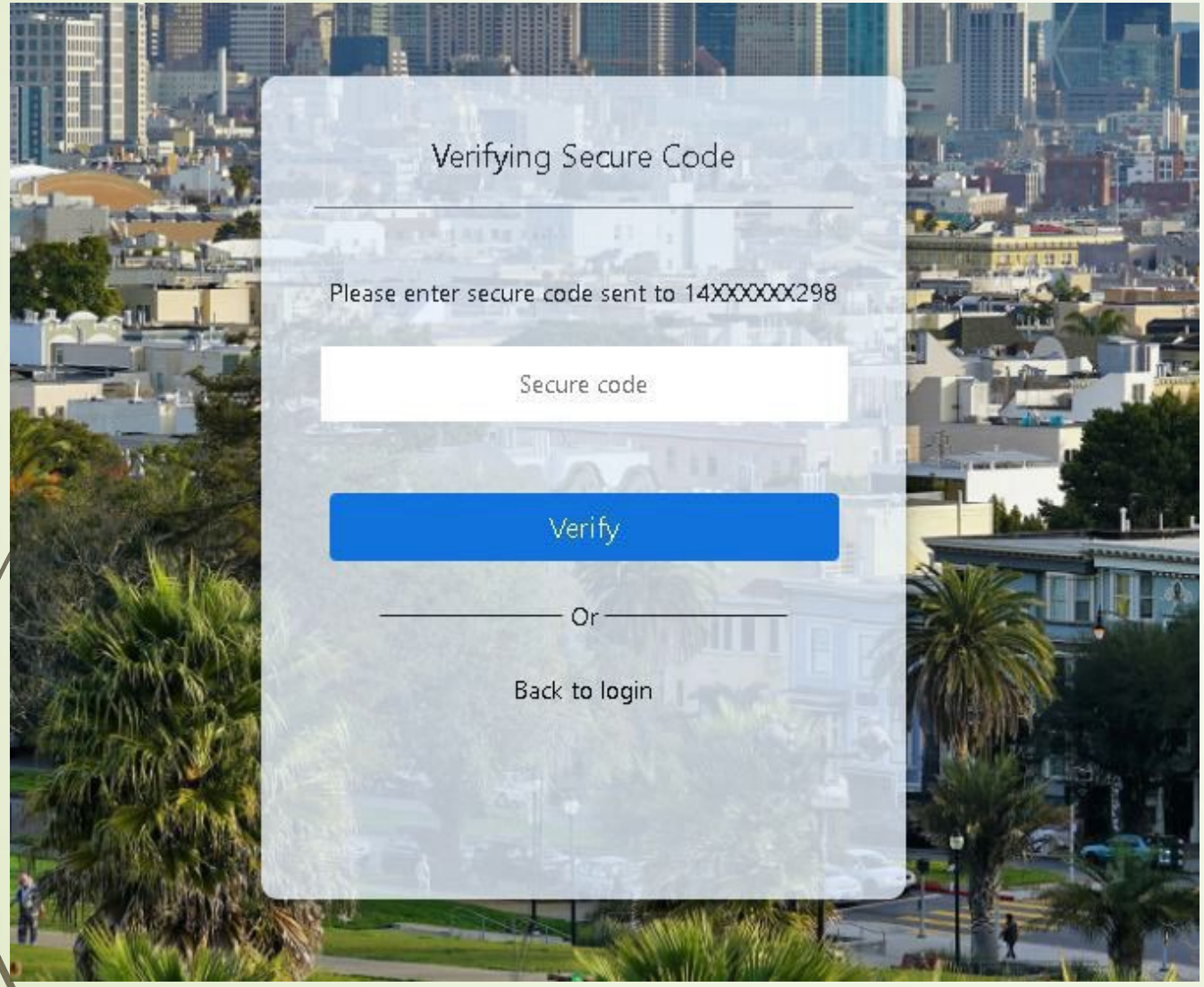
Forgot your password? Page



- Enter your UCSF POI#
- Select ‘Submit’

Step 4

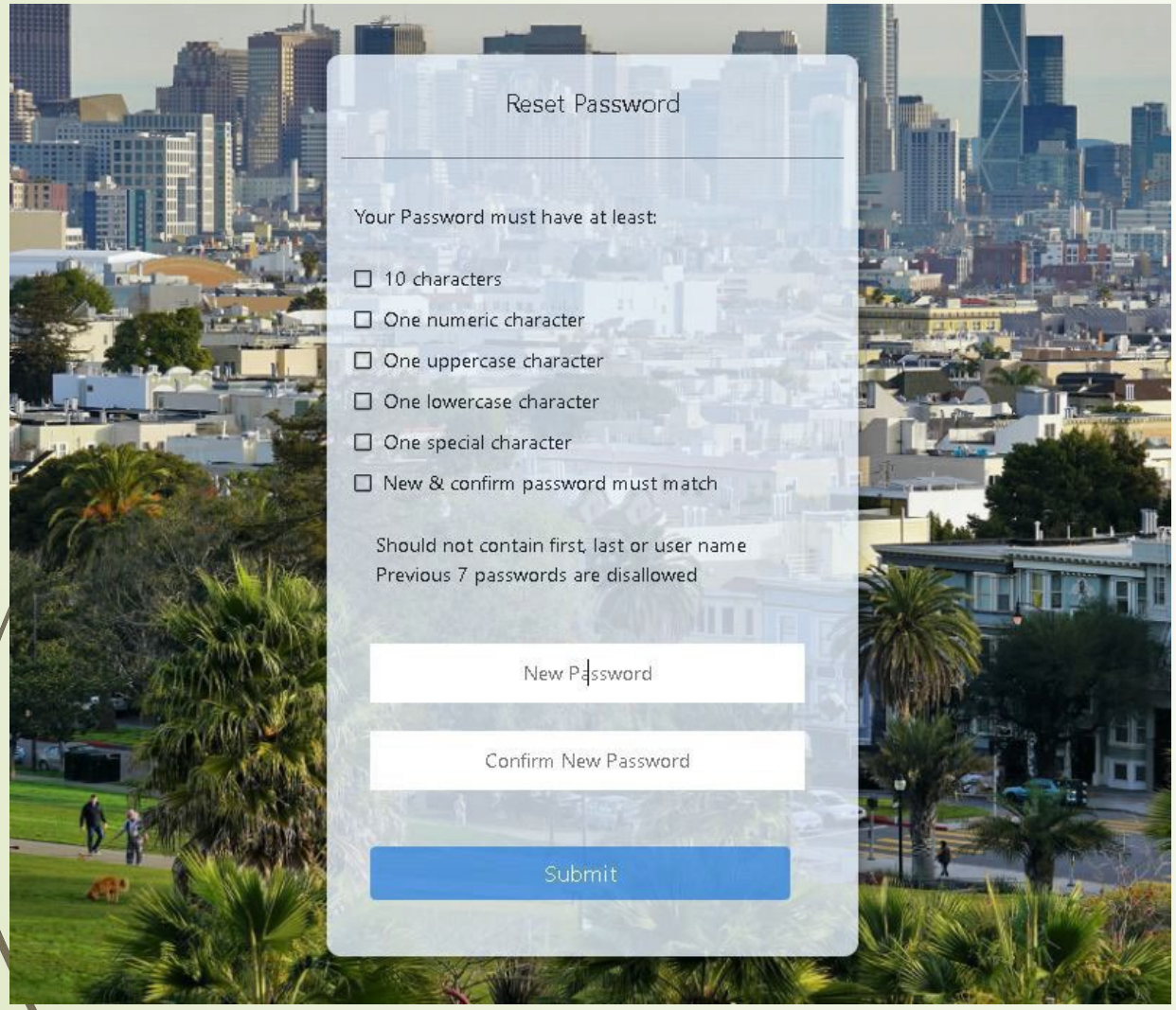
Verifying Secure Code Page



- Enter Secure Code from Phone
- Select ‘Verify’

Step 5

Reset Password Page



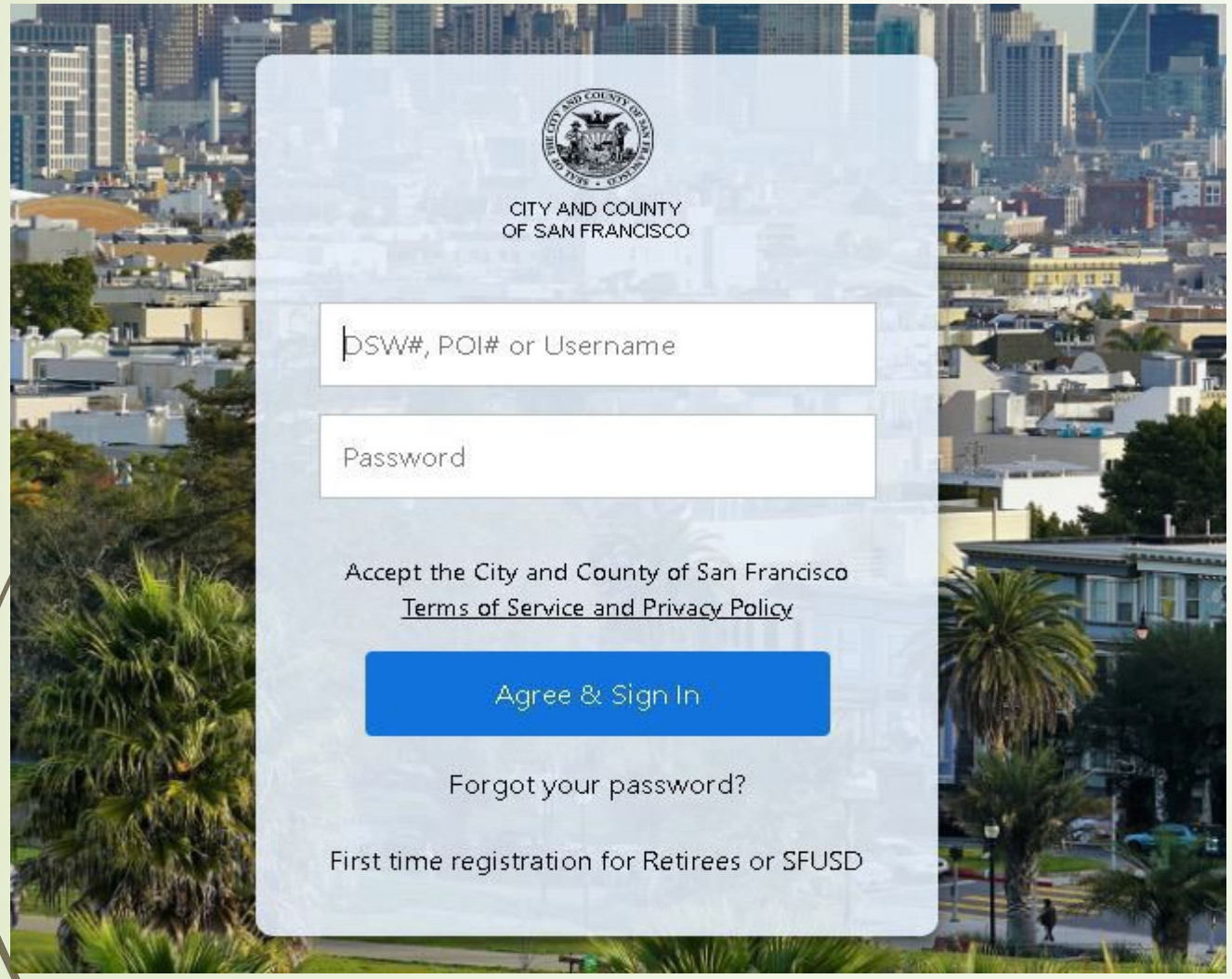
New Password Guidelines:

- 10 characters
- One numeric character
- One uppercase character
- One lowercase character
- One special character
- New & confirm password mustmatch

Select “Submit’

Step 6

CCSF Login Page



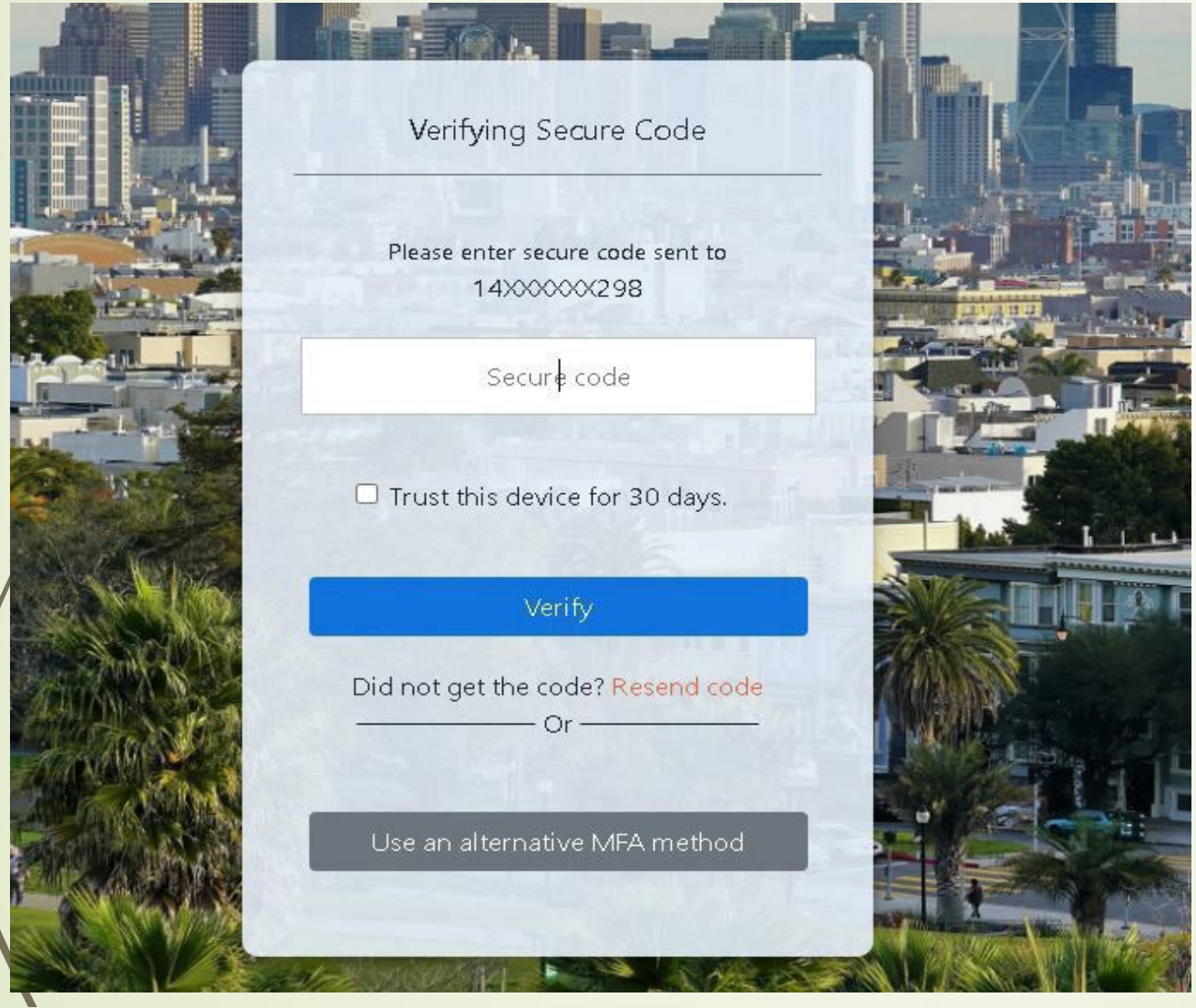
- Enter UCSF POI#

- Enter Password

- Select ‘Agree & Sign In’

Step 7

Verifying Secure Code



- Enter Secure Code from Phone

- Select ‘Trust this device for 30 days’

- Select ‘Verify’

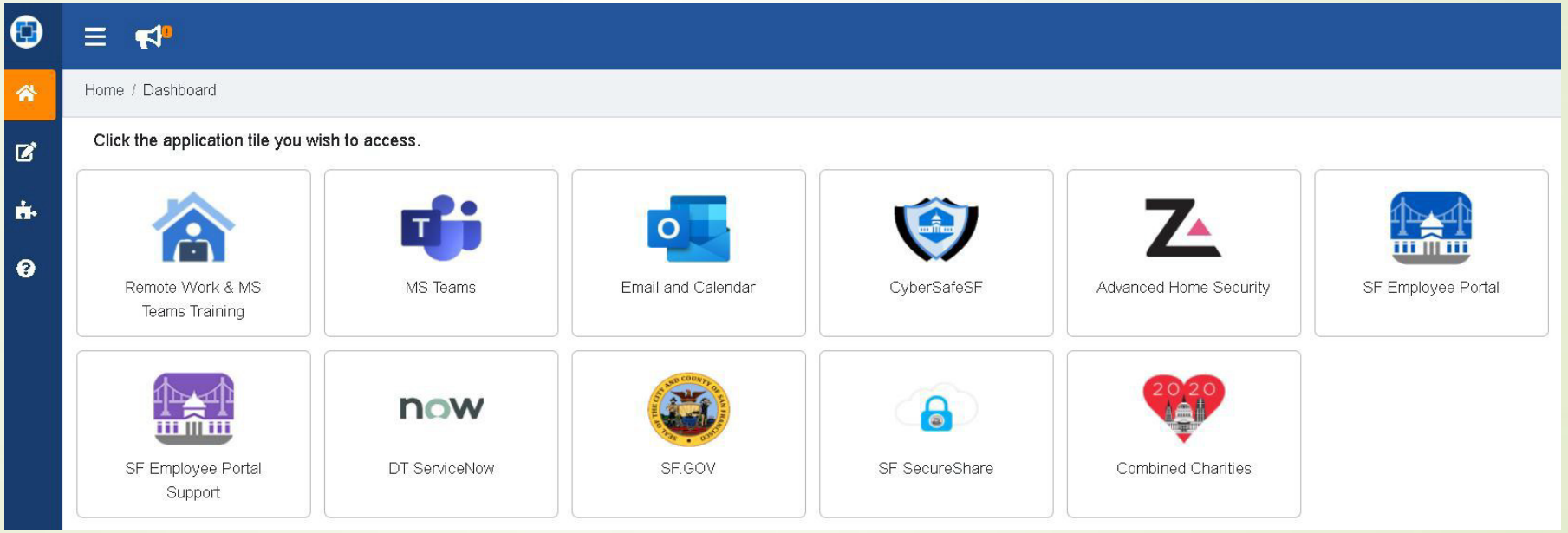
Step 8

CCSF Dashboard Page

If you have logged onto this site previously, you may be directed to Step 22

Select 'Multi-Factor'

(To Add Additional Layer of Security)



Step 9

Multi-Factor Page

User Guide: Register Multi-Factor Authentication (MFA)

The MyApps Portal requires users to set up at least two multi-factor authentication (MFA) methods after validating their login credentials to access their account.

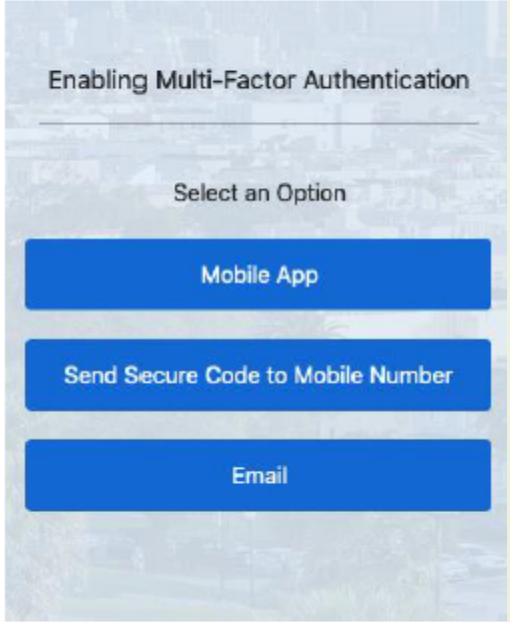
1. **Enroll first MFA factor**

   Go to https://myapps.sfgov.org/.

   Enter username:
   (Employees use DSW number,
   POIs use POI number,
   Contractors use loginID,
   Suppliers use supplierID number)
   and password.

   Click "Agree & Sign in".

   After validating login credentials, the user will see a window that asks to enroll in at least one MFA factor such as Mobile App, SMS to Mobile Number and Email.

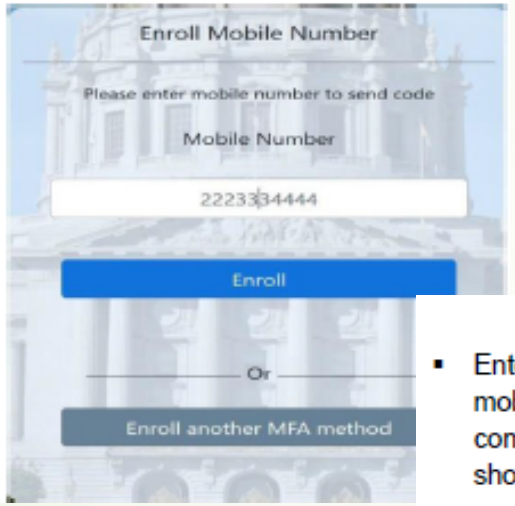


Step 10

Multi-Factor Page (continued)

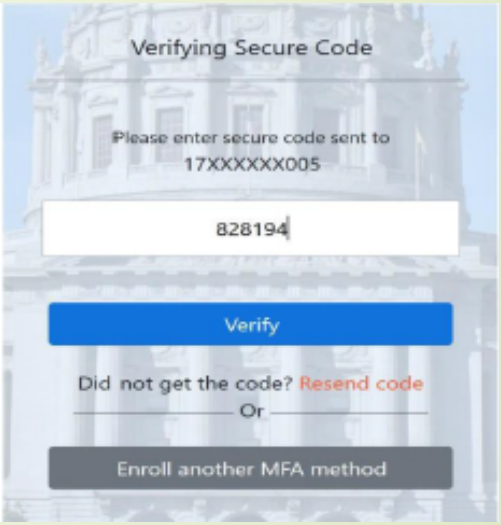
1.1 Enroll Mobile Number

- Click "**Send Secure Code to Mobile Number**" button.



- Then, it will open a new window where a user must **enter** a mobile number and click "**Enroll**" button to receive a mobile message with a secure code.

- Enter the secure code that you received on your mobile number and click the "**Verify**" button to complete the enrollment of mobile number as shown in the image:



- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup others such as email or mobile app.

Step 11

Multi-Factor Page (continued)

1.2 Enroll Mobile App

- Click the "**Mobile App Notification**" button.

  Note: Download the Oracle Authentication Mobile App from the iOS App Store or Google Play Store.

- After clicking "mobile app notification", a user will see a screen with **QR code to scan** as shown:

- Once the app is installed on your phone, open the camera from the Oracle Authenticator app and **scan** or hover the camera over the QR code as showing in the below image.

- After the QR code has been scanned, you will be asked to add a new device or overwrite an existing one. If this is your first time setting up the app, please select add a new device.

- After the mobile application has been installed and configured on your mobile device, you will see the following screen on your computer:

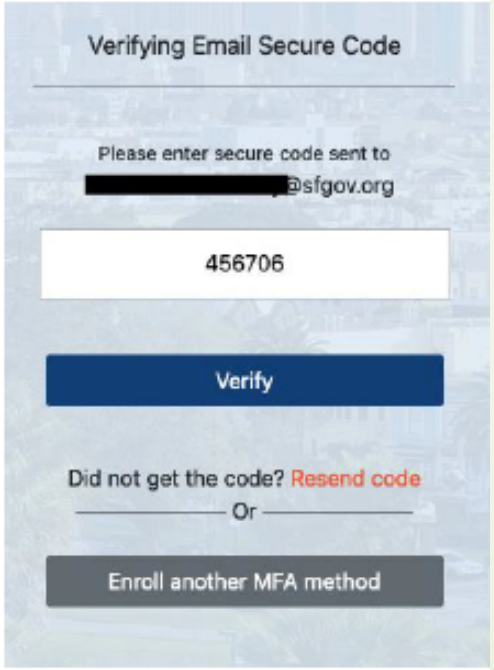
- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup email or a mobile phone.

Step 12

Multi-Factor Page (continued)

1.3 Enroll Email

- Click "**Email**" button.
- A new window opens and asks the user to enter the One Time Passcode (OTP) sent to their email.
- Enter the One Time Passcode (OTP) that you received on your email and click the "**Verify**" button to complete the enrollment of email as shown in the image.
- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup others such as email or mobile app.



Step 13

Multi-Factor Page (continued)

2. Enroll second MFA factor

Users are allowed to add multiple Mobile App, SMS, and FIDO authentication factors; however, they can add only one email factor.

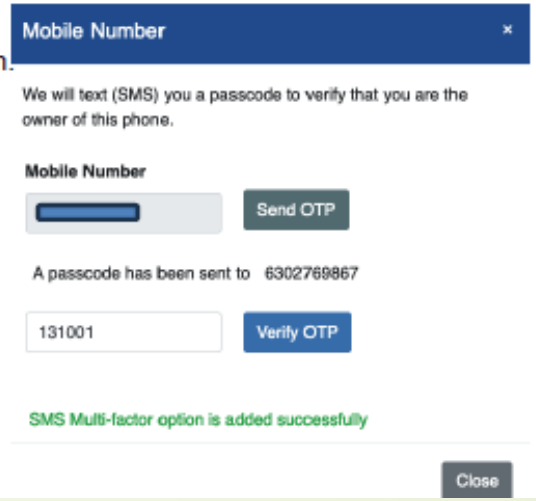
To add a new MFA factor, click "Configure" on the tile or click the arrow on the MFA menu  and choose one of 'Add FIDO Authenticator', 'Add Mobile App', 'Add Mobile Number'.

2.1 Enroll Mobile Number

To add a new Mobile Number (SMS Factor)

- Click 'Configure' on the Mobile Number tile or click 'Add Mobile Number' menu from the MFA menu (burger)
- On the pop-up window enter the mobile number you wish to enroll, then click **Send** OTP button.

- On the next page, enter the One Time Passcode received on your mobile and click **Verify** OTP button. The message "SMS Multi-factor option is added successfully" will be displayed.



Step 14

Multi-Factor Page (continued)

2.3 Enroll Mobile App

- Click 'Configure' on the Mobile App tile or click 'Add Mobile App' from the MFA menu (burger)
- Note: Users can download the Oracle Authentication mobile app from the mobile iOS App Store or Google Play Store.

- A pop-up box will appear in the middle of the screen as shown below:
- Once the app is installed on their phone, users can open the camera from the Oracle Authenticator app and scan or hover the camera over the QR code (shown in the image below).

- Once users scan the QR code, a pop-up box will appear on their mobile screen, asking them to add a new device or overwrite the existing one. If using the authenticator app for the first time, users should select "add new." Otherwise, users can select "overwrite."
- Once the QR code has been canned in the authenticator app and configuration is done, select "close" to see the enrolled device info in the mobile app section.

Step 15

3. Authenticate using MFA to access the MyApps Portal

After enrolling in MFA users will need to authenticate using MFA to gain access to the MyApps Portal.

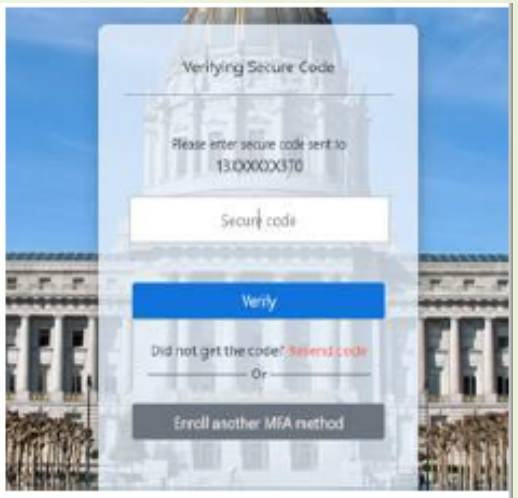
- If a user has set **email** authentication as their default, they will see the following screen.

- The user should follow the instructions on screen to enter the secure passcode received by email.

- Click the "**Verify**" button. The user will be redirected to the MyApps Portal dashboard.

Step 16

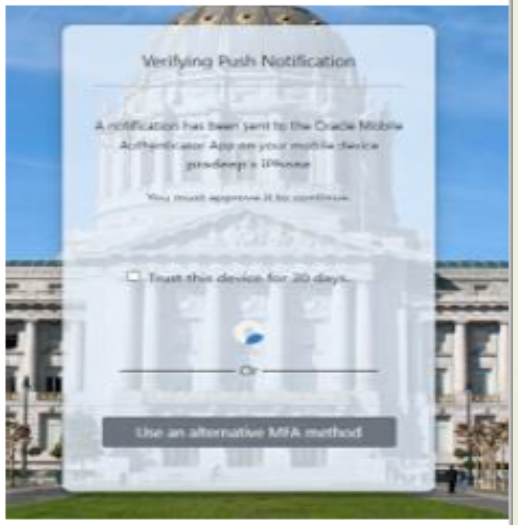
- If a user has set **mobile number** authentication as their default, they will see the following screen.



- The user should follow the instructions on screen to enter the secure passcode received by their mobile device.

- Click the "**Verify**" button. The user will be redirected to the MyApps Portal dashboard.

- If a user has set **mobile app** authentication as their default, they will see the following screen.

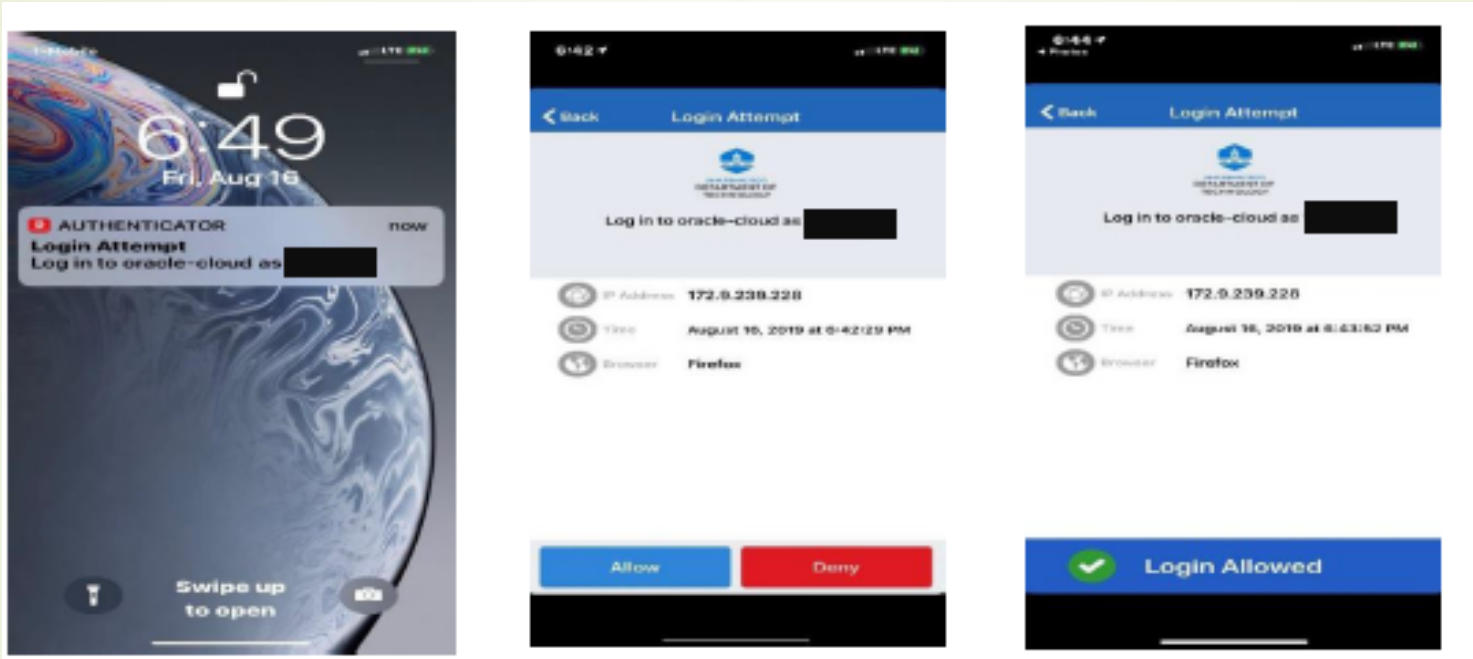


- The user should follow the instructions on screen to approve the push notification received by their mobile device.

- Open the push notification in the "**Oracle Authentication App**" on the user's mobile device.

- Tap the "Allow" button on the mobile device. After few seconds, the user will be redirected to the MyApps Portal dashboard.

Step 17



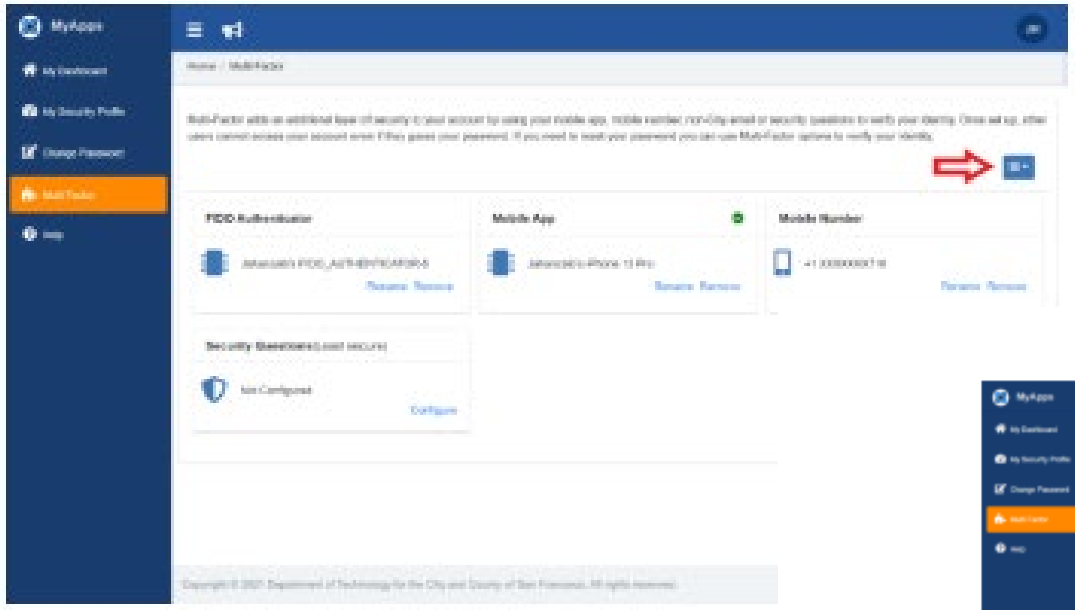
- A user can also check the box **"Trust this device for 30 days"** to prevent MFA verification each time a user access MyApps portal.

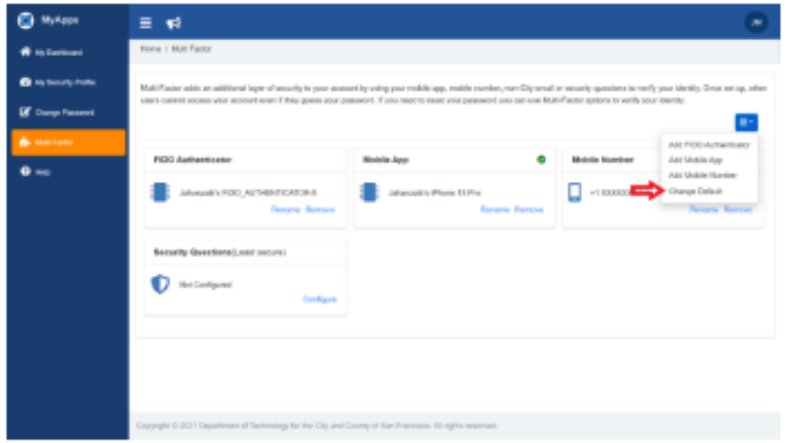
UCSF University of California San Francisco

ZUCKERBERG SAN FRANCISCO GENERAL Hospital and Trauma Center

Step 18

4. Set default MFA Factors

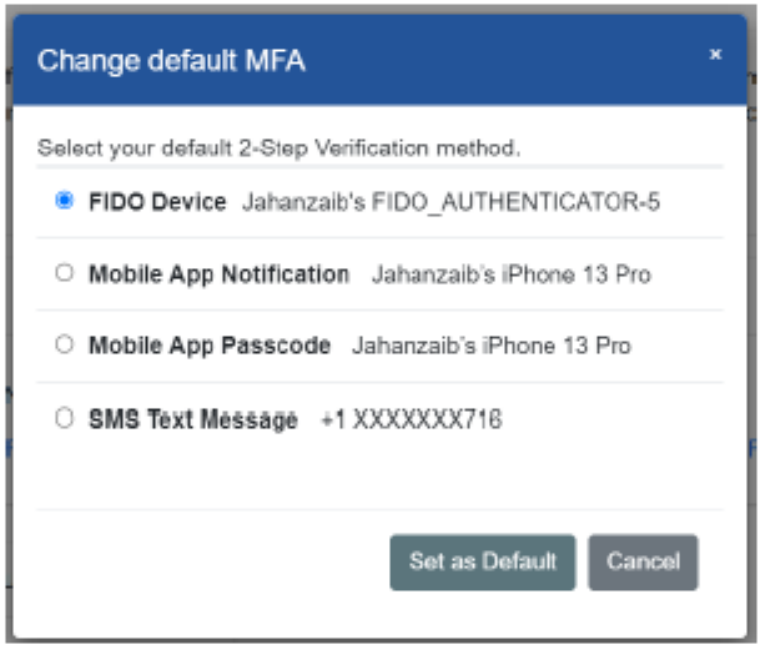




- This feature helps a user to choose which MFA factor they want to use for authentication when accessing the MyApps Portal from an external network.
- Click the "**Change Default**" button.

Step 19

- After clicking the "Change Default" button, a new pop-up screen will appear as shown:

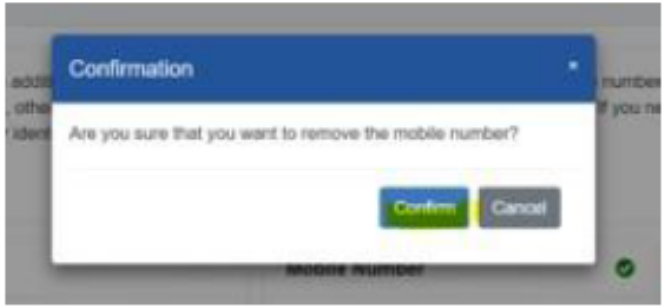


- Users can select an MFA factor such as Email, Mobile Number, Mobile App or FIDO Device by choosing a radio button from the list.
- Once a radio button is selected, click the "**Set as Default**" button.

Step 20

5. Remove MFA Factors such as Security Questions, Mobile Number and Mobile App

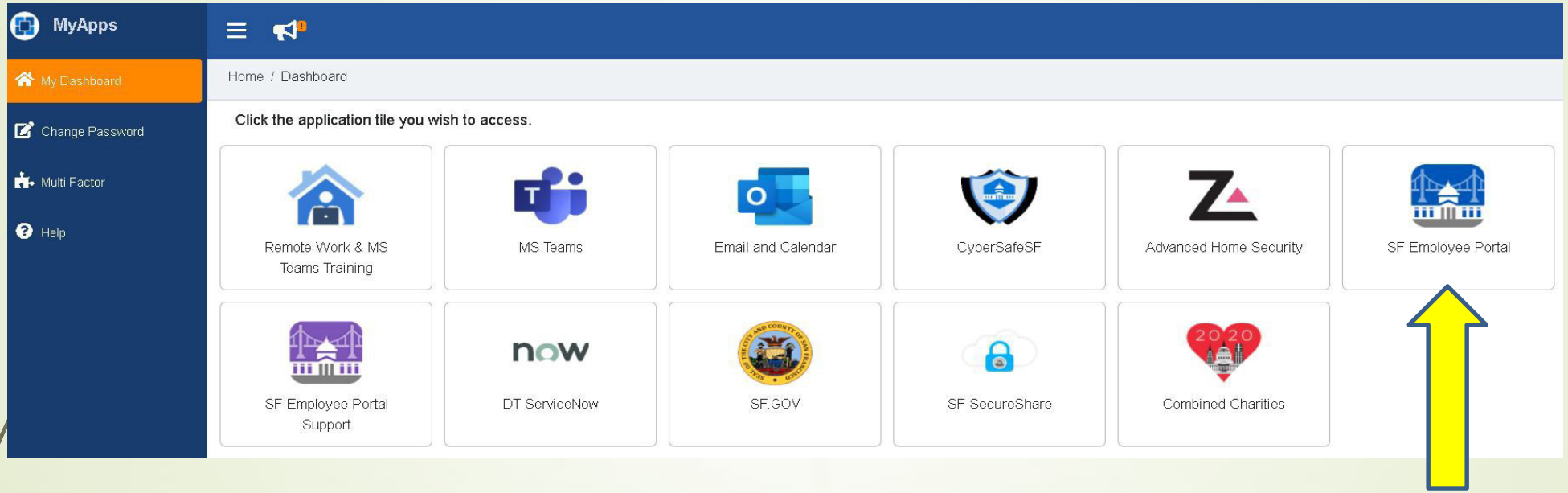
- Users should select the MFA factor they want to remove such as Email, Mobile Number or Mobile App. For example, if they want to remove an email MFA factor, they can go to the email section and click the **"Remove"** button on the right side of the pane as shown in the image.



- After clicking "remove", you will see a pop-up box that will ask you to confirm your selection again.

Step 21

CCSF Dashboard Page



Choose '*SF Employee Portal*'

Step 22

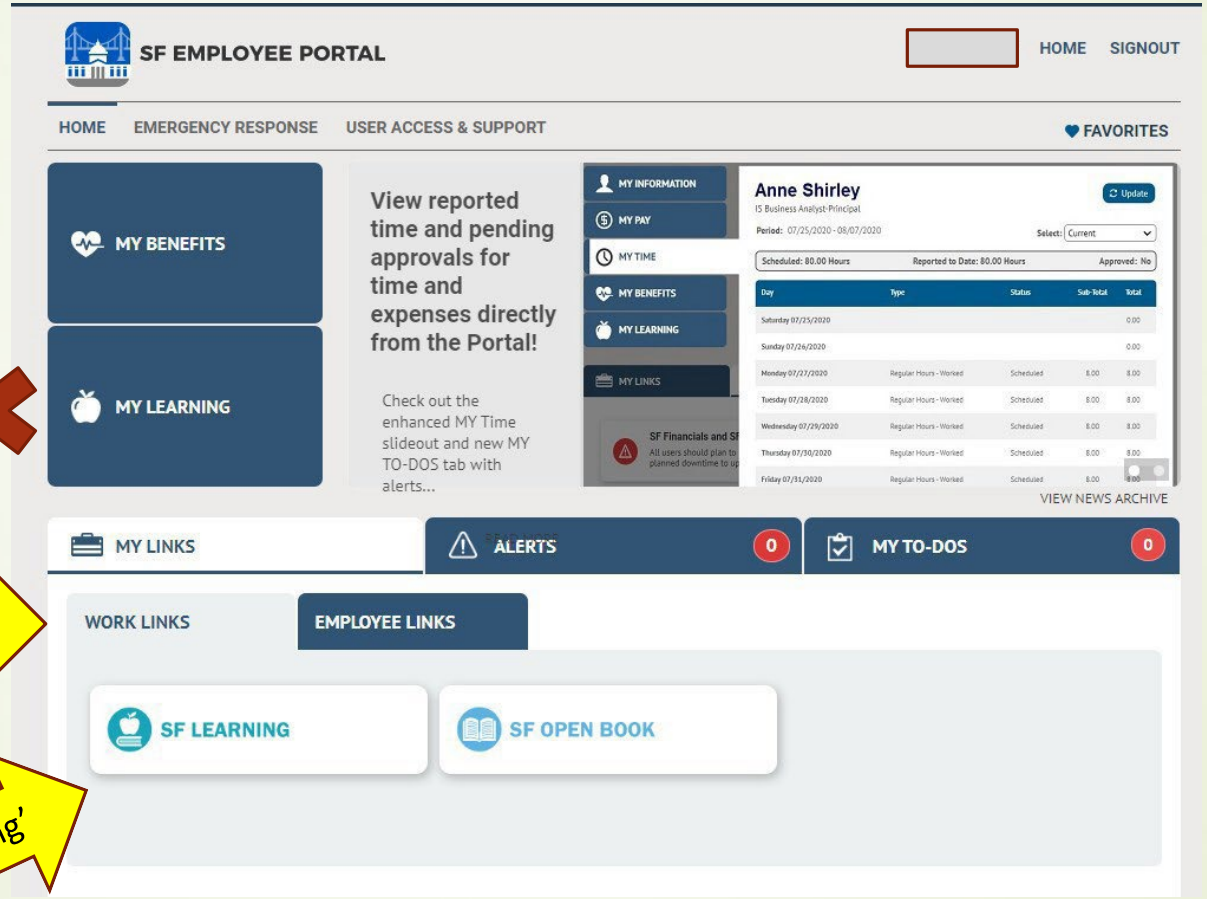
SF Employee Portal

DO NOT Select ‘My Learning’ option

Select ‘WorkLinks’

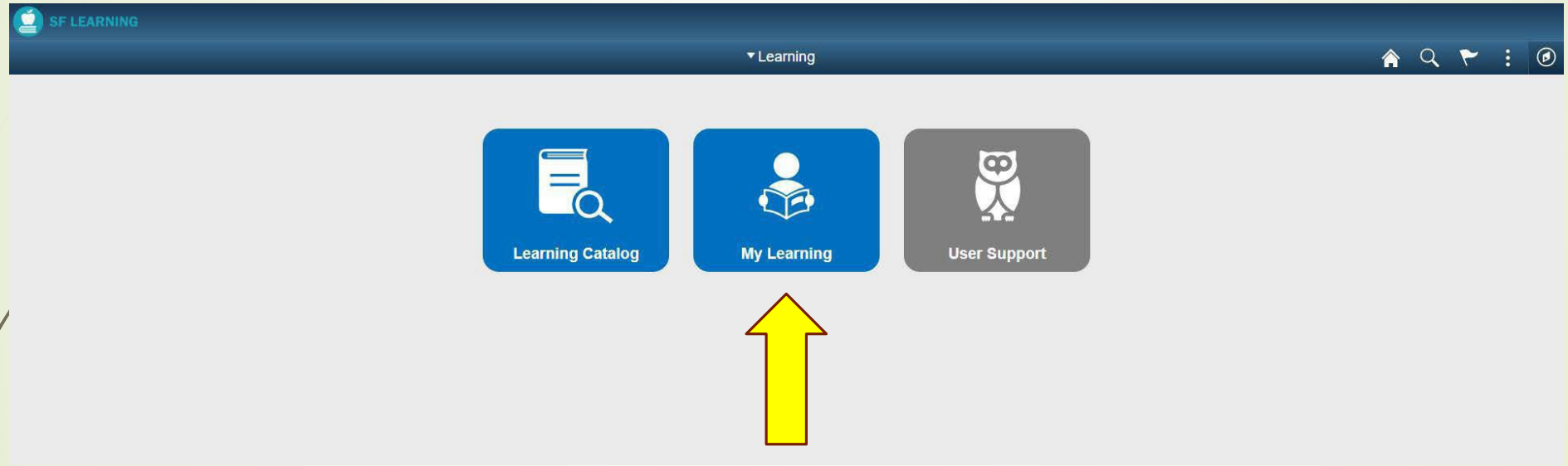
then

Select ‘SF Learning’



Step 23

SF Learning Platform Page



Select ‘My Learning’

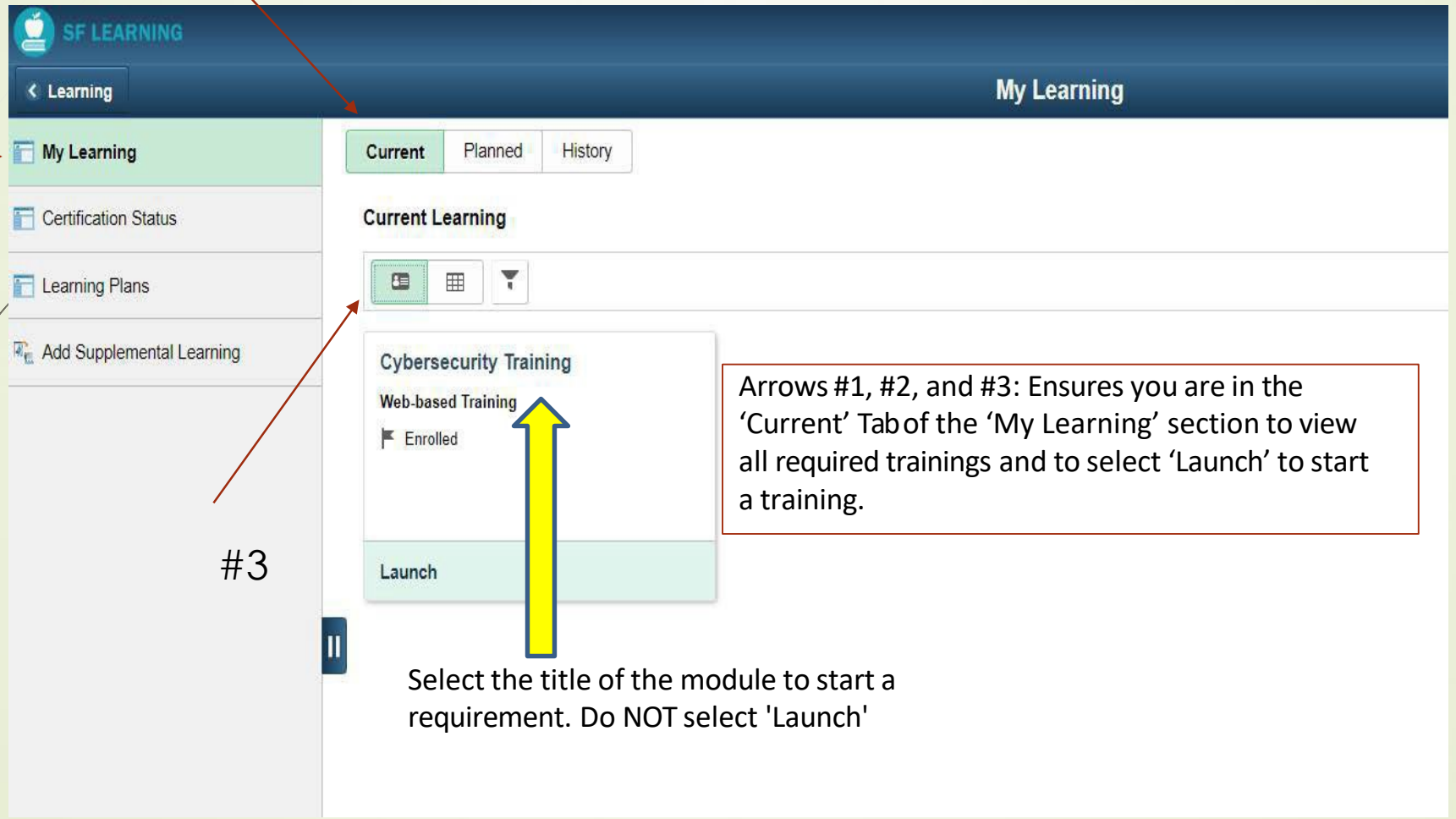
Step 24

My Learning Requirements Portal: **Current**

#1

#2

#3

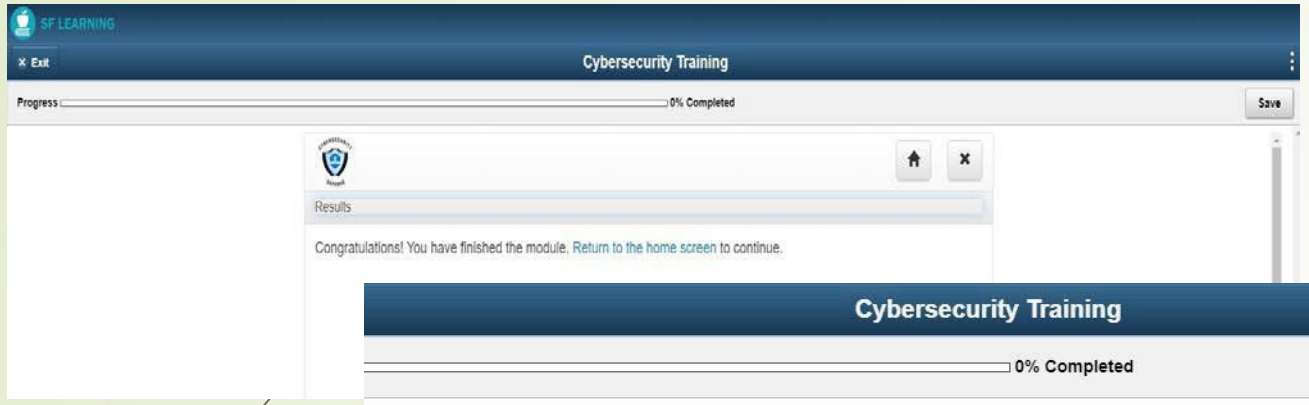


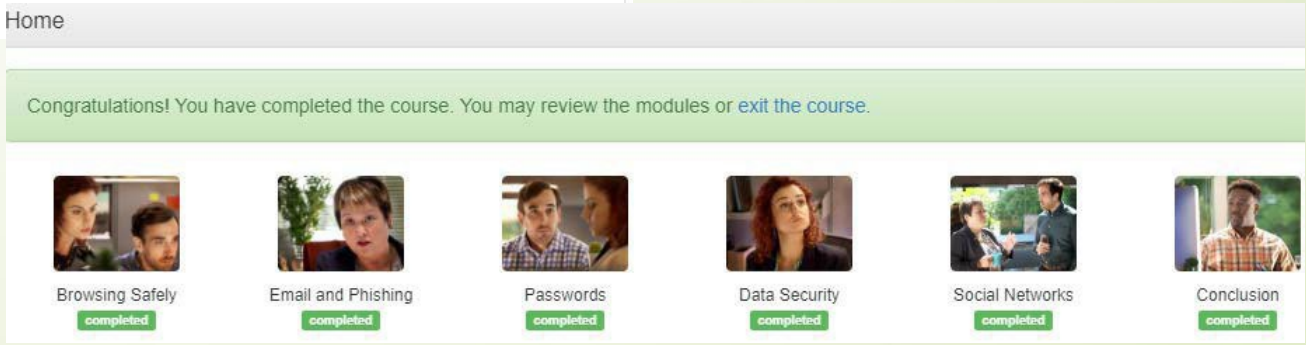
Arrows #1, #2, and #3: Ensures you are in the 'Current' Tab of the 'My Learning' section to view all required trainings and to select 'Launch' to start a training.

Select the title of the module to start a requirement. Do NOT select 'Launch'

Step 25

Recommended: Take Screenshots

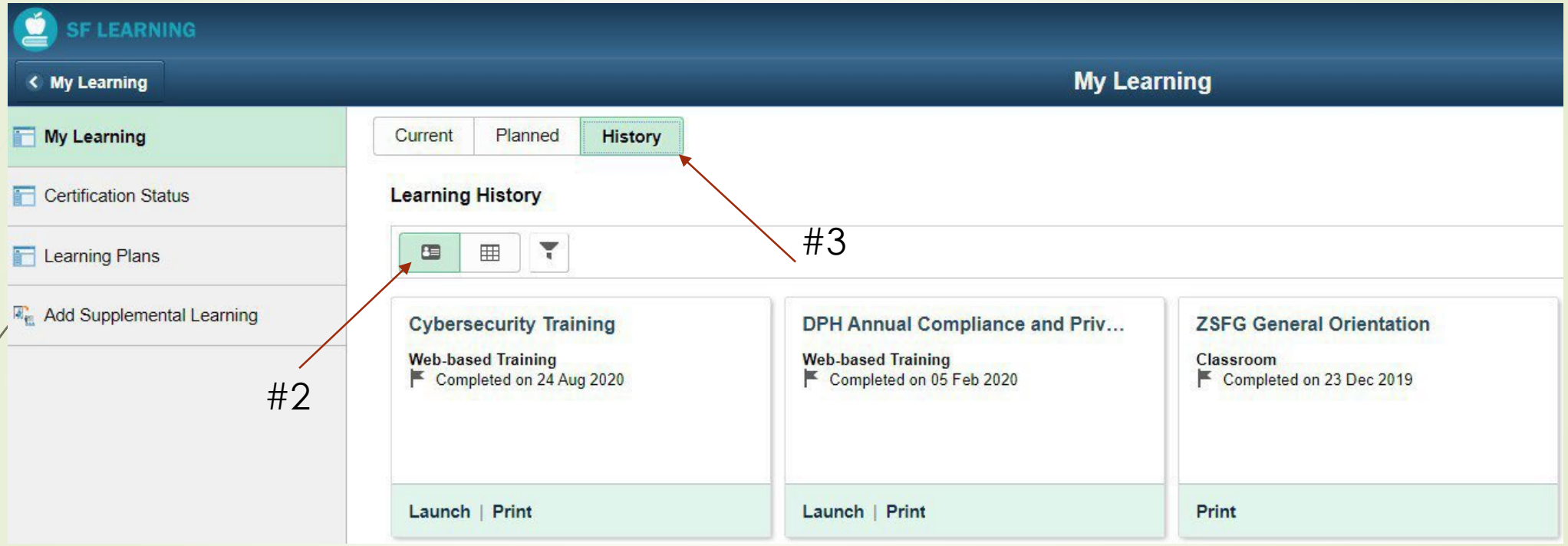




Helpful Tip:
Take screenshots when completing a module& requirement, in case the system does not automatically record completion.

Step 26

My Learning Requirements Portal: **History**



Arrows #1, #2, and #3: Ensures you are in the 'History' Tab of the 'My Learning' section to verity the system recognizes completion of the Cybersecurity Training.

Congratulations!

You have successfully logged into the SF Employee Portal, launched the My Learning application, and completed the Annual Cybersecurity training!

UCSF University of California San Francisco

ZUCKERBERG SAN FRANCISCO GENERAL Hospital and Trauma Center

THANK YOU!