Steps to Configure Your Account in the New Environment For HCBS Explorer and other UMass-hosted applications

Table of Contents

Step-By-Step Instructions to Set Up Your Account and Launch HCBS/Explorer

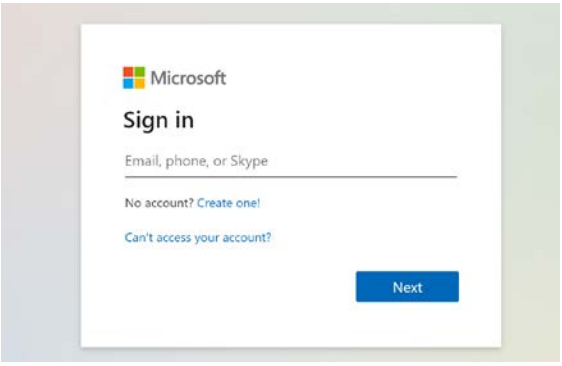
NOTE FOR USERS WHO ACCESS OTHER MICROSOFT ENVIRONMENTS

*The new environment for **HCBS Explorer** and other UMass-hosted applications is a Microsoft-hosted environment. Some users – but not all – may also be using Microsoft-hosted environments to run other applications, which may include Microsoft Office 365 applications like email.*

*If this is the case for you, we recommend that you attempt to access each of your Microsoft environments via a separate web browser (for example, make connections to E-Invoicing from a Chrome browser, and make connections to Microsoft email from an Edge browser). **We recommend Chrome and Firefox as browsers for accessing UMass applications.** Another approach would be to completely log out from one Microsoft environment before launching a connection to the new environment for UMass-hosted applications. Step 3 below contains additional information on Microsoft connections.*

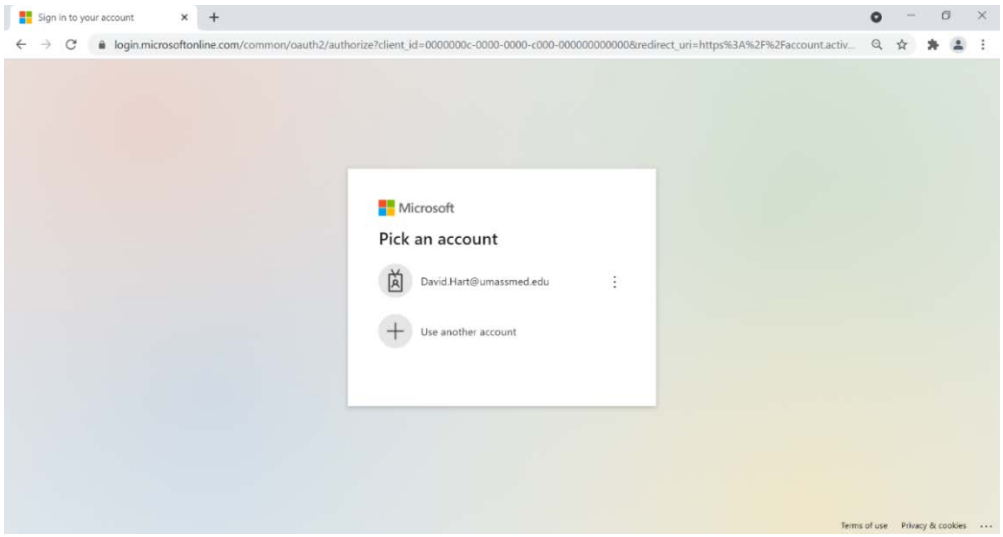
1. Access https://myapps.microsoft.com from your web browser (Chrome or Firefox recommended).

2. Next, a Microsoft log in page with title "Sign In" is displayed. Enter your User ID as it appears in the "User ID" field of the email you received with Subject line **Your new EOEA Online Account for HCBSExplorer**.

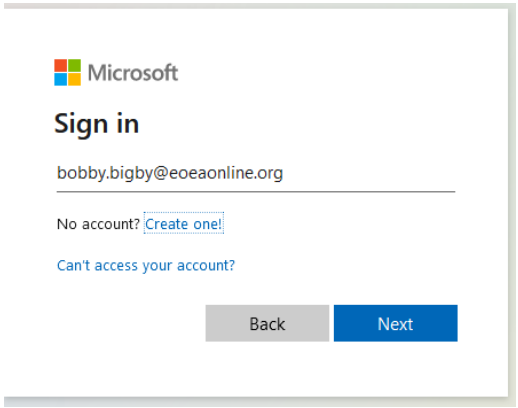


3. If you have previously accessed other Microsoft environments from the same browser on the same computer, you may automatically be logged into an account from a different Microsoft environment, or, you may see “Pick an account” with account names associated with your previous activity (see screen image below). If you are logged into a different Microsoft environment, please launch another browser application (Chrome and Firefox are recommended) to initiate your connection to HCBSExplorer via https://myapps.microsoft.com.

   If you don’t see an account in the “Pick an account” list that looks like your *firstname.lastname* followed by *@eoeaonline.org*, (e.g., robert.young@eoeaonline.org), click the plus sign (+) adjacent to “Use another account” (image below).

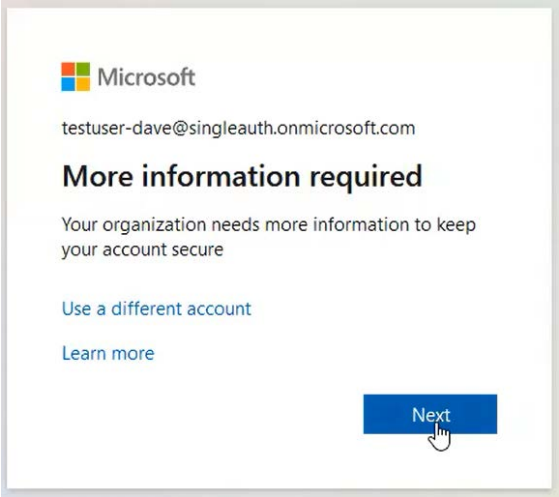


4. If you clicked the **+** next to “Use another account”, a Sign in prompt will be displayed as shown here:



After specifying your username,
click **Next** and you’ll be prompted for your password.

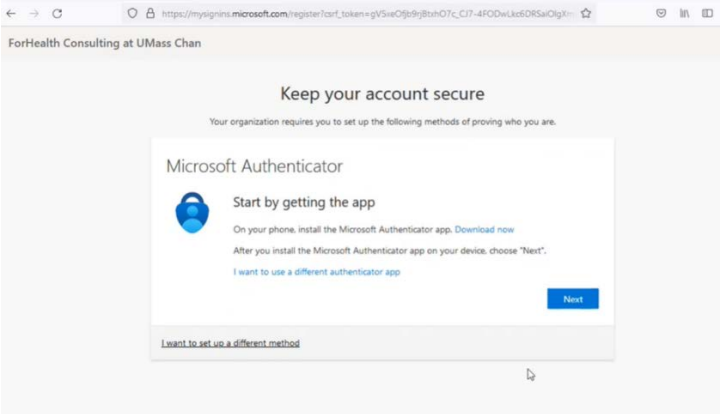
5. Next, you will be guided through a sequence of screens in which you will configure your account and security settings. The first of these screens is shown on the next page. Click **Next** in this screen.



6. Next, the system will guide you through steps to configure security functionality including multifactor authentication (MFA) in the new environment. The first of these configuration screens is displayed below. The default and recommended security method is the Microsoft Authenticator mobile app. The steps to configure Microsoft Authenticator are depicted directly below. There is also an option to configure another security method such as Phone/Text (refer to section **"I want to setup a different method" MFA Workflow** on page 6)

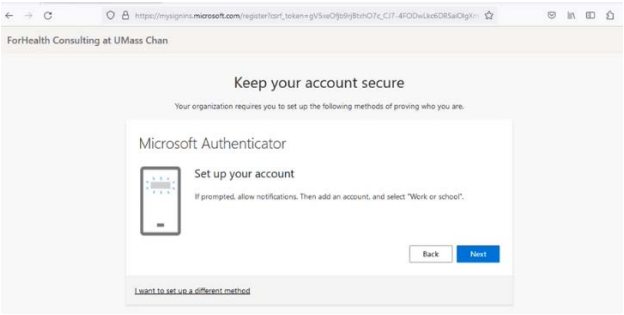
   NOTE: If you're going to set up the Microsoft Authenticator security option, please install Microsoft Authenticator on your mobile phone before you begin the Authenticator security setup on your computer. Please visit either the Apple or Android App Store to download Microsoft Authenticator. When you have Microsoft Authenticator installed on your phone, continue with the workflow on your computer by clicking "**Next**" on the Keep your Account Secure screen (image below).

AUTHENTICATOR SETUP MFA WORKFLOW

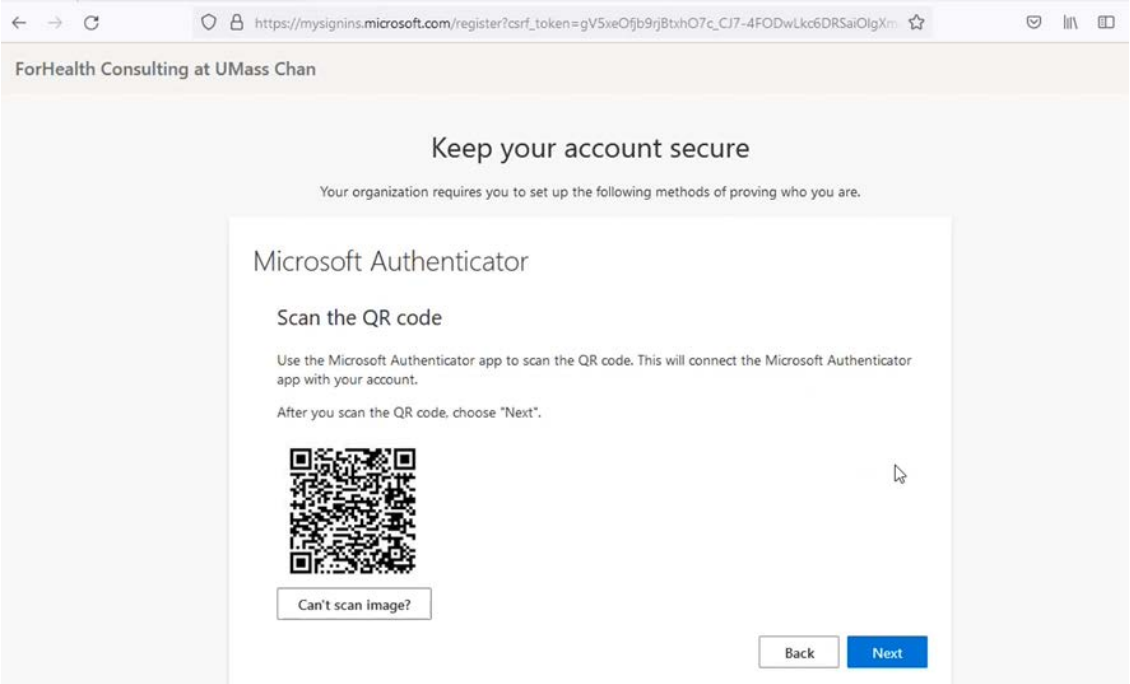


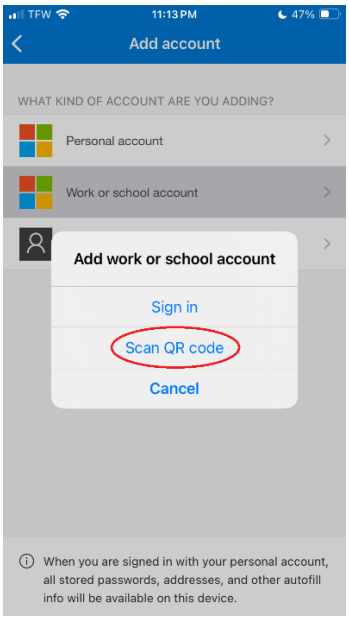
7. In the Microsoft Authenticator app ***on your phone***, click “Add account”, and then select “Work or school account”.

8. In the next setup screen ***on your computer*** (shown below), click “**Next**.”



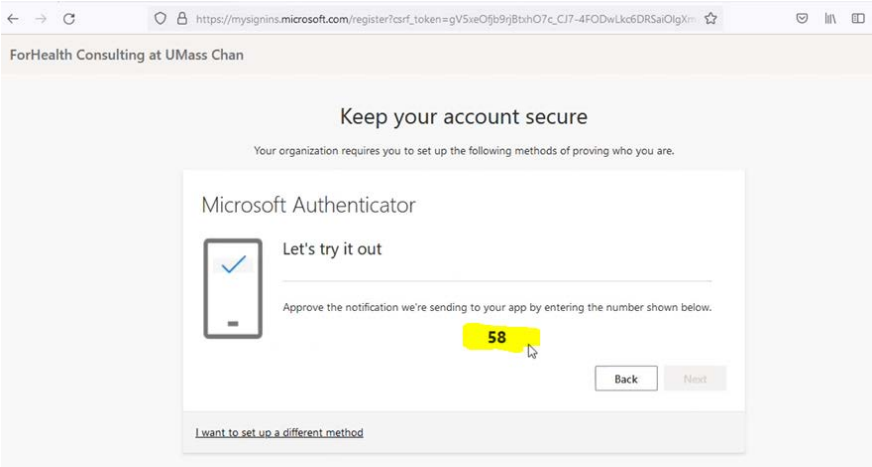
9. The next screen displayed ***on your computer*** (image below) prompts you to scan a QR code with your phone to establish the connection between the Authenticator app and your account. ***On your phone***, select “Scan QR code” (see image further below), then use your phone to scan the QR code on your computer screen.



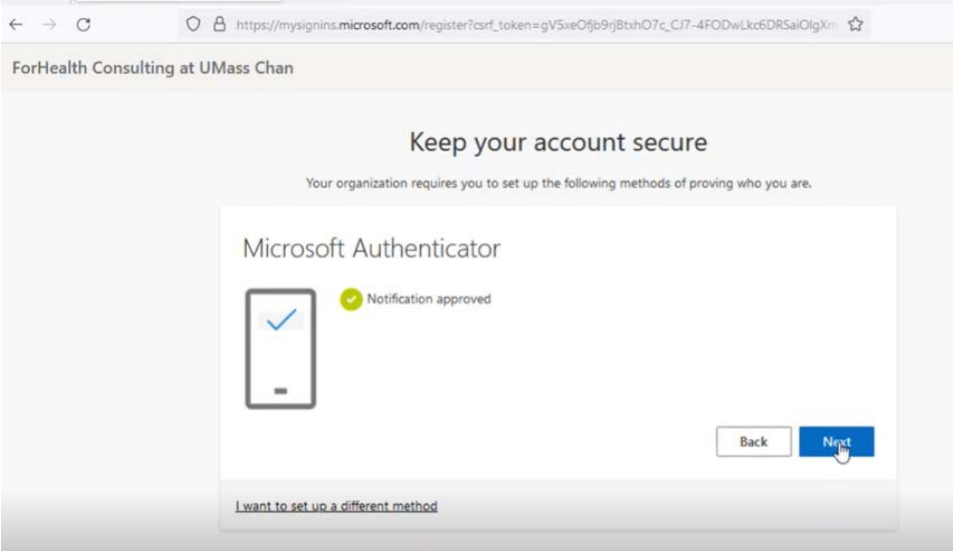


After you scan the QR code, the Authenticator app on your phone will display an entry for your account. Press “Next” on the setup screen on your computer.

10. Next, the setup workflow ***on your computer*** (image below) displays a two-digit code, highlighted below, that you must enter into Microsoft Authenticator. Enter this code on your phone.



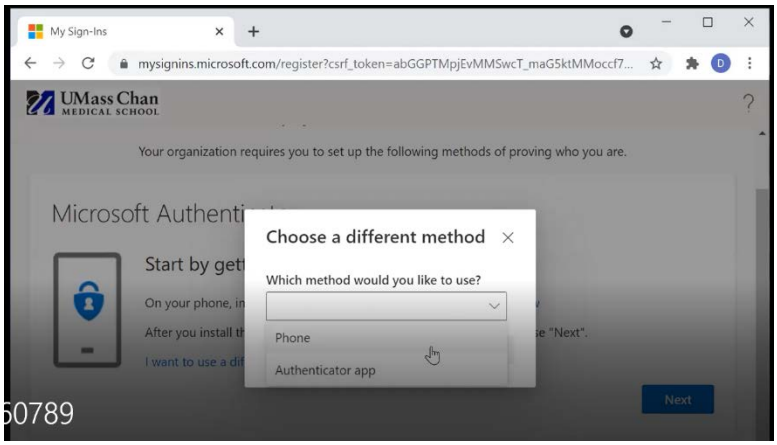
11. The next screen displayed ***on your computer*** (shown below) confirms that the Authenticator app configuration was successful.



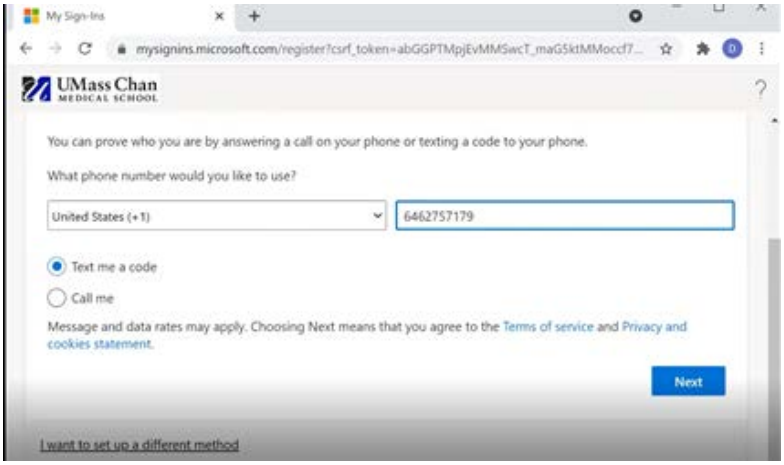
"I want to set up a different method" MFA WORKFLOW

If Microsoft Authenticator isn't a practical option for your situation, you may select "I want to set up a different method" in the lower-left of the "Keep your account secure" screen. The steps below depict the setup workflow for a user who selects to use a different method and configures to receive SMS text messages for MFA. Please note: Microsoft has indicated an intention to retire the SMS text method to maximize the security provided in its environment.

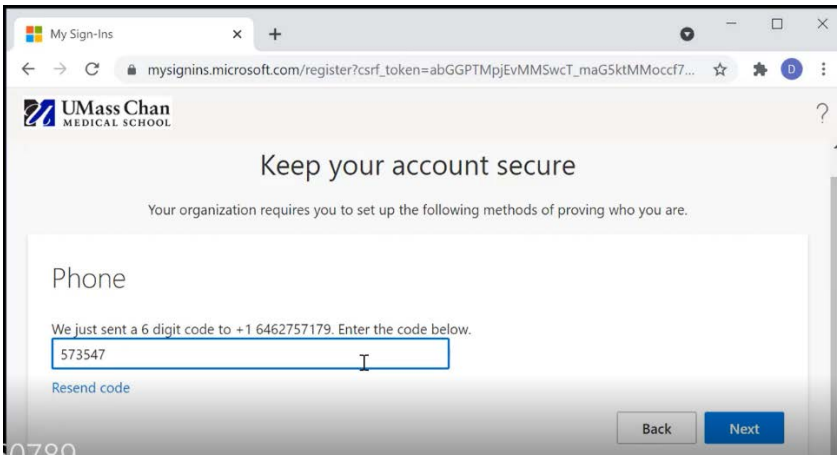
12. After you click to use another method, a dropdown displays, showing the available methods (see screen image below). Select **Phone** from the dropdown, then click the Confirm button.



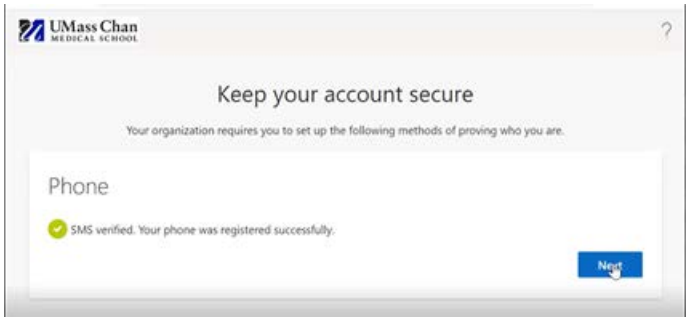
13. Next, a screen displays for you to configure the phone number which would receive a call or text message when you have forgotten your password and need to reset it. You may configure either to receive a text message or a phone call as part of the reset process. The screen image on the next page shows the scenario where the user wants to receive a text message. After you provide your phone number and select Text or Call, press **Next**.



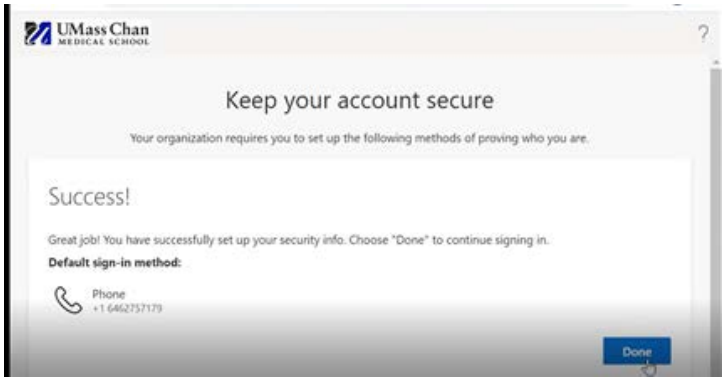
14. After pressing "Next", you will receive either a phone call or text message, depending on your selection. In the case of a text, enter the six-digit code from the text message (see screen image below). In the case of a phone call, respond to the prompt in the call. Then, press **Next**.



Next, a status screen displays (image below), indicating you have successfully registered your Phone security method, which will be used to confirm your identity when you click "I forgot my password" in future sessions. Press **Next** on this screen.

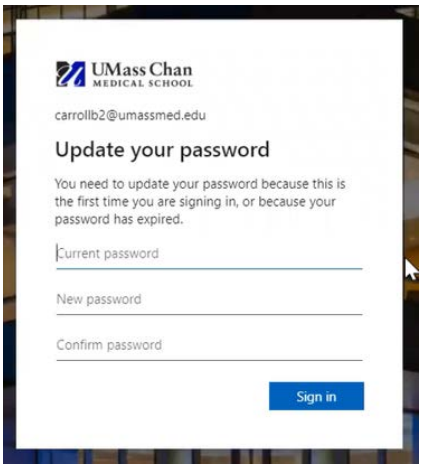


15. An additional screen displays, confirming the successful setup of your account's security information. Click **Done** on this screen.

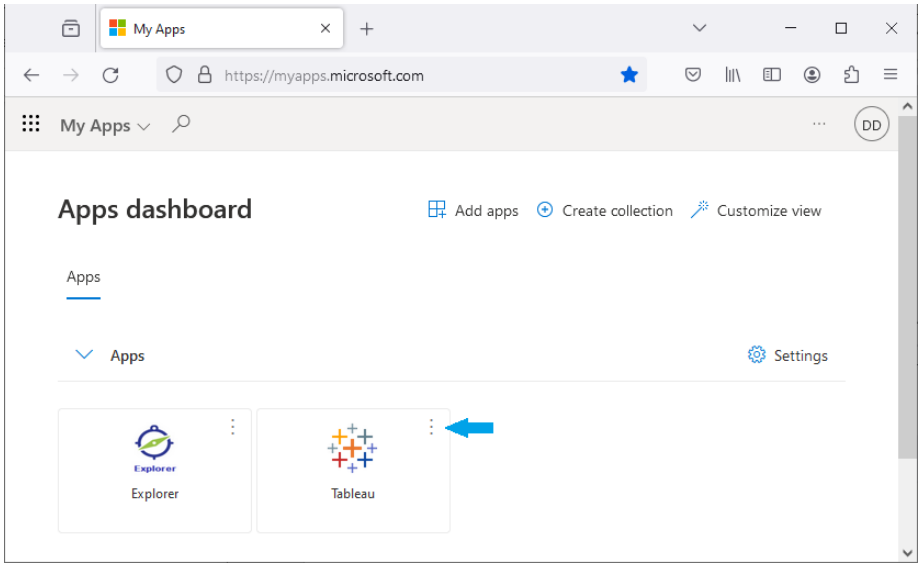


16. **Once you've setup your security using Microsoft Authenticator or another method**, you will be prompted ***on your computer*** to specify a permanent password for your account (see image below). The requirements for a permanent password are:

    - At least 8 characters
    - Must contain 3 of the following: uppercase character, lowercase character, number, special character (*#@$%^&!)
    - Permanent passwords are valid for 60 days, after which you'll be prompted to create a new password.

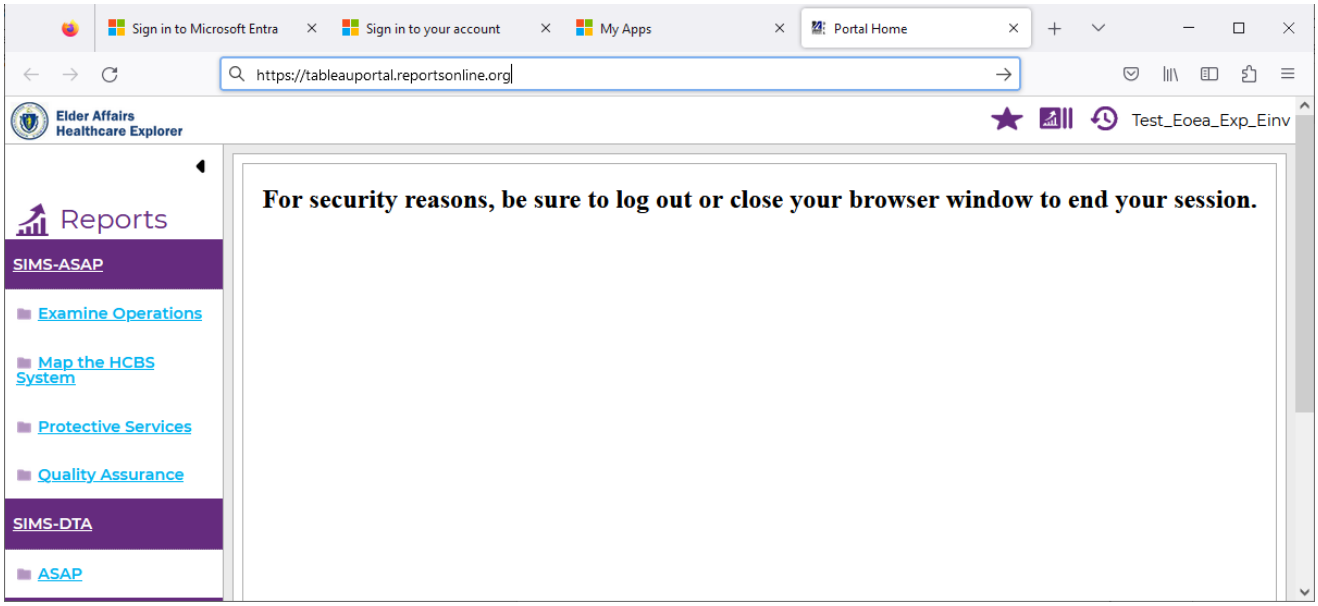


Next, your Myapps landing page (image below) displays an icon for each application to which you have access. You have access to **HCBSExplorer** and possibly other UMass-hosted applications such as E-Invoicing. The image below reflects a user with access to HCBS Explorer. NOTE: an additional "Tableau" icon also appears – please note that if you click on this icon, the reports are not laid out in the manner users are accustomed to. To remove the icon from your Apps dashboard, click on the dots in the upper-right of the Tableau icon (see blue arrow in image below).



17. Click the **Explorer** icon**.** The HCBSExplorer landing page will display in another browser tab, as depicted below. You can access your full set of provisioned Explorer reports as in the previous HCBS Explorer environment.

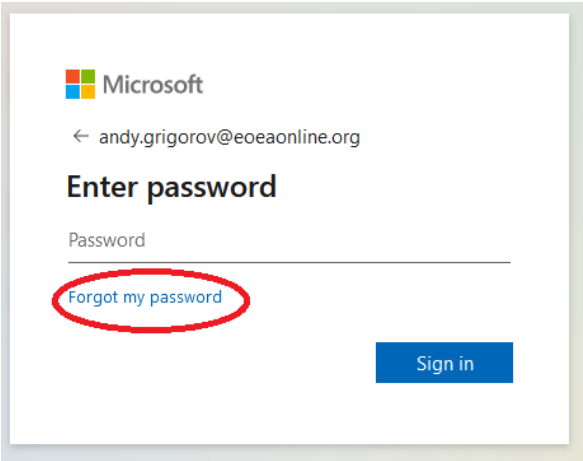
NOTE: If you use the Firefox browser, you may receive a prompt to click on a blue button, "Open Site in New Window" on the first report you attempt to view. This first report only will display in a separate browser tab. **Please be sure to close this separate tab after viewing the first report.**



APPENDIX A – How to Reset Your Password (Self-service)

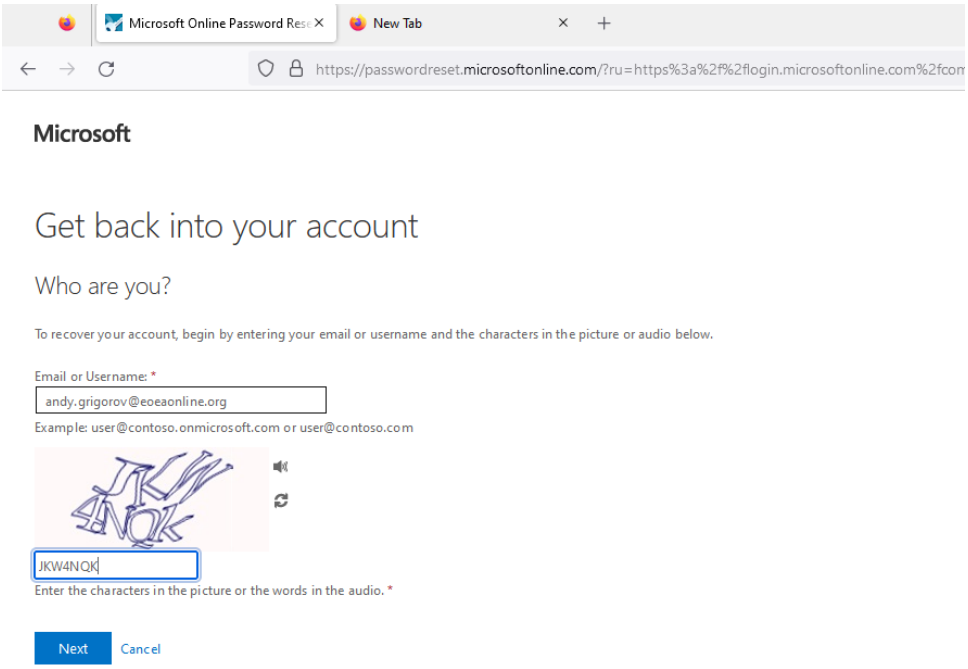
The new environment includes a convenient self-service password reset function. There are two ways to access this function:

- Click “Forgot my password” on the login page (https://myapps.microsoft.com), as shown below:

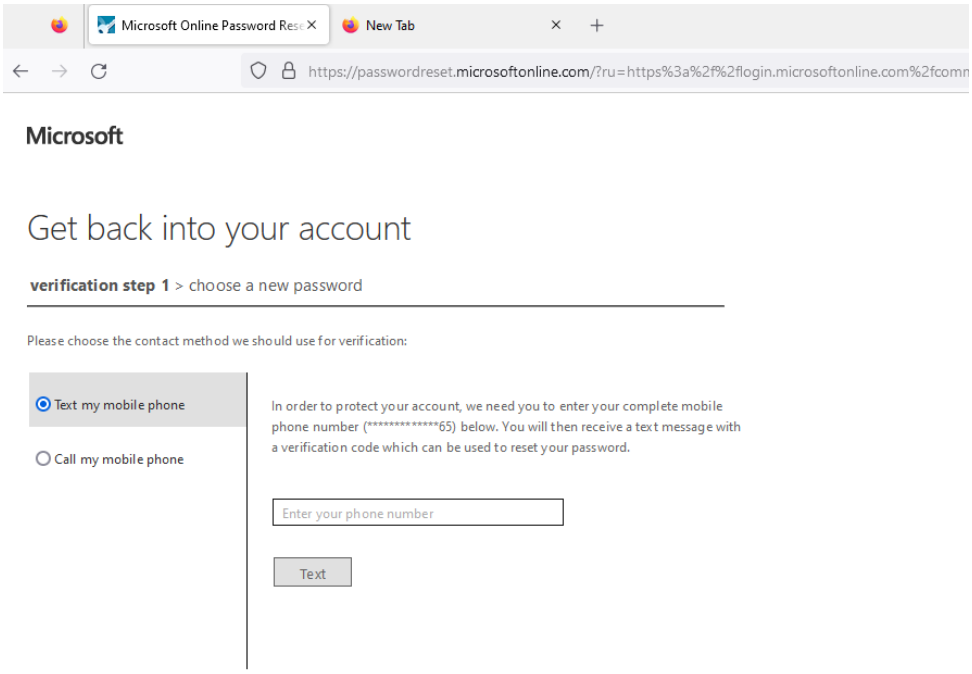


- Go directly to https://passwordreset.microsoftonline.com

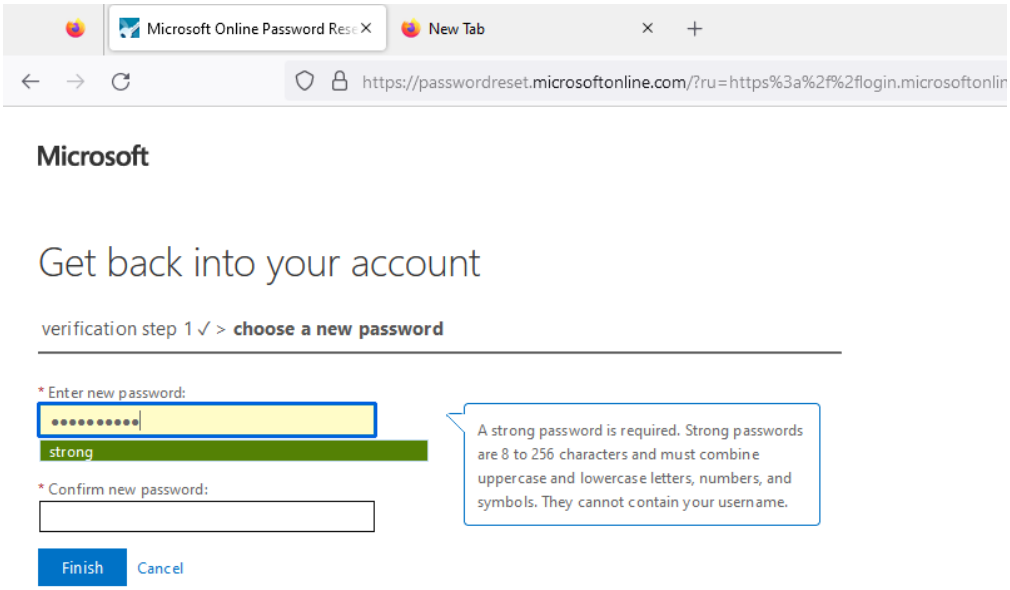
Next, the “Get back into your account” prompt is displayed, as shown below. Provide responses to the prompts, and click Next.



Next, you'll be prompted to use one of the security access methods you specified during account setup, to verify your identify and reset your password (see image below).



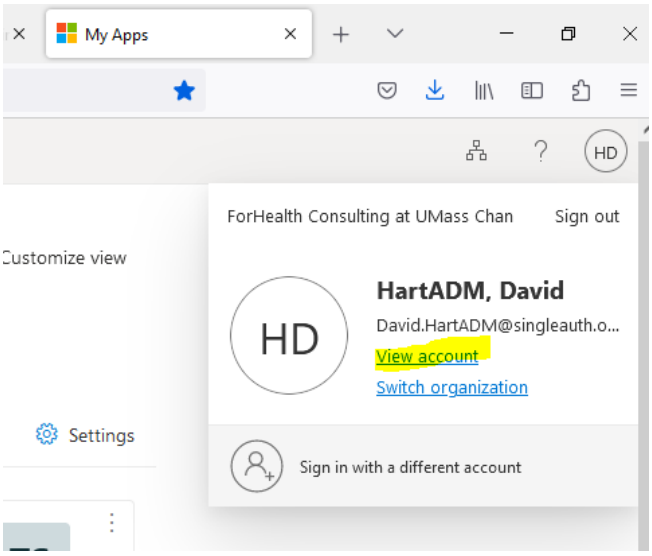
After you've verified your identity, you'll be prompted specify your new password, as shown below:



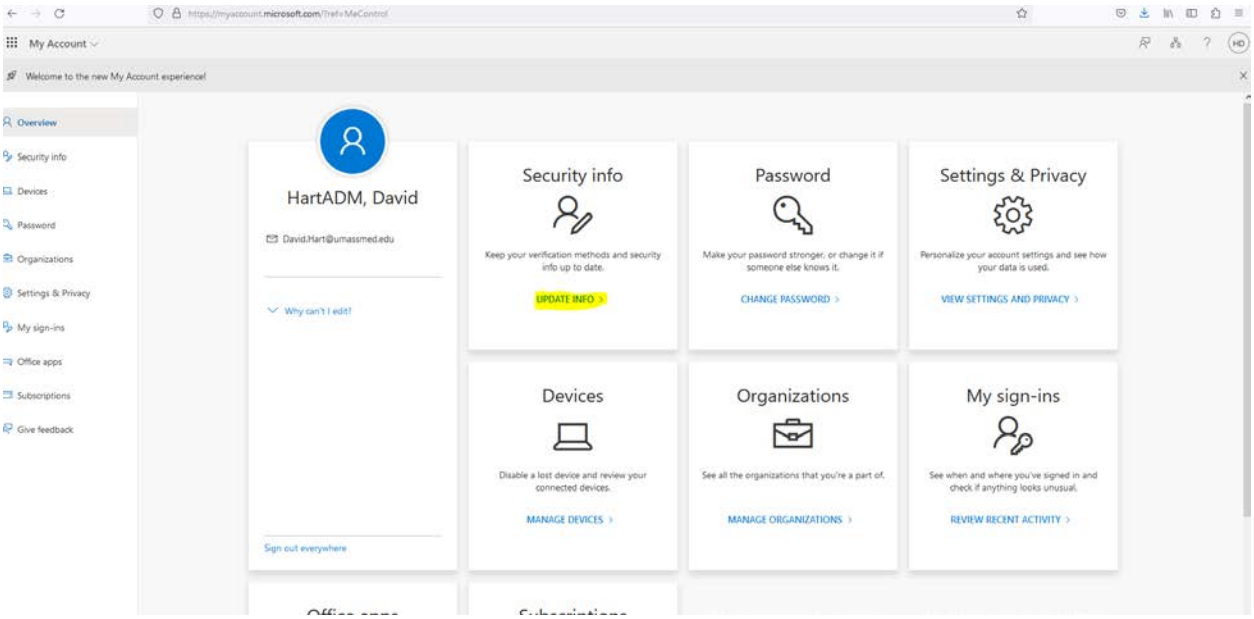
APPENDIX B – How to Make Changes to Your MFA/Security Setup

At some point after configuring your account, you may have a need to specify another phone number or additional authentication method to be used to verify your identify. You can make these changes using the View Account function accessible from the MyApps landing page.

1. In the top-right of your MyApps landing page, click on the circle which contains your last-name/first-name initials ("HD" in the image below). Then, click "View account".



2. In View Account, select Security info as highlighted below:



3. In the Security Info interface (see image below) you can add or change phone and device settings. The selections highlighted below are for functions to add a sign on method, or to change an existing Phone method (e.g., specify a different phone number).