Introduction

Workday is a cloud-based application that is part of the Statewide Personnel System (SPS) used by the State of Maryland and Towson University that enables TU faculty and staff to manage their employee benefits online. Currently, you can view your enrolled benefits and your dependent information in Workday. This self-help document will walk you through how to log into the system and set up 2-factor authentication which is now required.

Obtaining Your Workday ID

After obtaining your Workday ID, please write it down. You will need it to log into Workday SPS system.

1. Open your preferred web browser and navigate to **inside.towson.edu**.
2. Select the **PeopleSoft HCM** tile.

Figure 1

3. Login with your **NetID** and **Password**. You will have to authenticate via Duo to be granted access to the system.
4. Once logged in, click on the **Personal Data Summary** tile.

5. Scroll down to the **Employee Information** section and locate your **Workday Benefits ID**. You will need to remember this for all login attempts to Workday SPS.

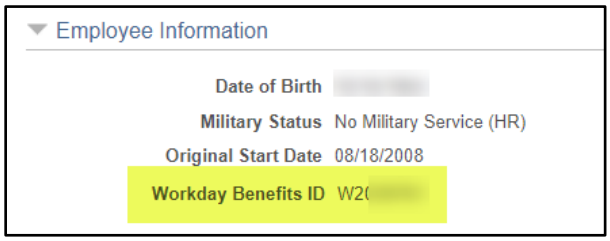

Figure 2

Logging In

1. From your favorite browser, type https://stateofmaryland.onelogin.com.

Note: Please save the above URL in your internet browser to quickly access.

2. The **Workday SPS** login screen will appear.
3. Enter your **Workday ID** under **Workday SPS ID** (as found in the previous section). If you wish, click the **Remember my username** check box.
4. Click **Continue**.

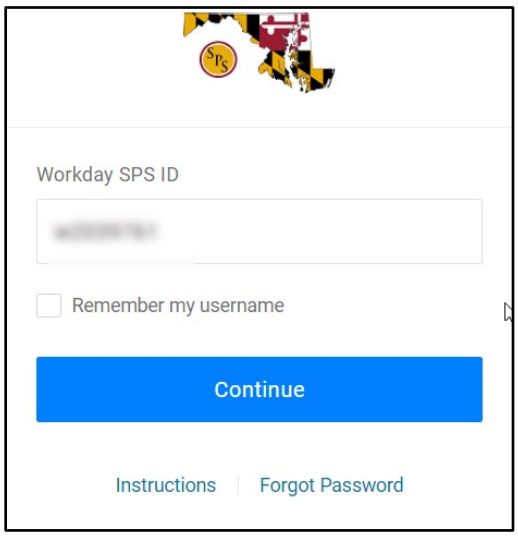

Figure 3

5. Enter the temporary **Password** required for the first login. The naming convention is as follows:
   a. Capital first letter of first name
   b. Lower case first letter of last name (Employees with hyphenated last names should use the first letter of the first last name if they have two last names separated by a hyphen)
   c. 4-digit birth year
   d. Last 4 digits of social security number
   e. **$** [the special character above the 4 on your keyboard]

Example: Js19608567$

Note: New Hires, you will receive an email with your temporary password within three weeks of starting at TU.

6. Click **Continue**.
7. You will be required to set up 2-factor authentication and then to change your temporary password.

Setting up 2-Factor Authentication

You must register at least one authentication method to access Workday. You can select any of the following Authentication Factors. Step by step instructions of each authentication method follows.

Note: It is recommended that you choose at least 2 authentication methods. After choosing an authentication method, instructions follow to set up an additional method or to change your existing method.

1. After entering your temporary password, you will be prompted to set up **2-factor authentication**. This is **required**. Click **Begin Setup**.

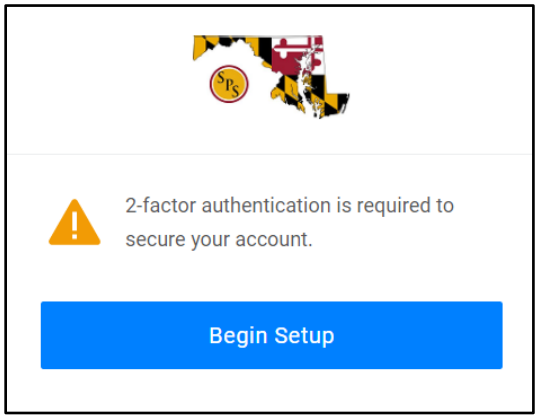

Figure 4

2. The **Select Authentication Factor** dialog box will appear. Choose one authentication factor – they are explained below.

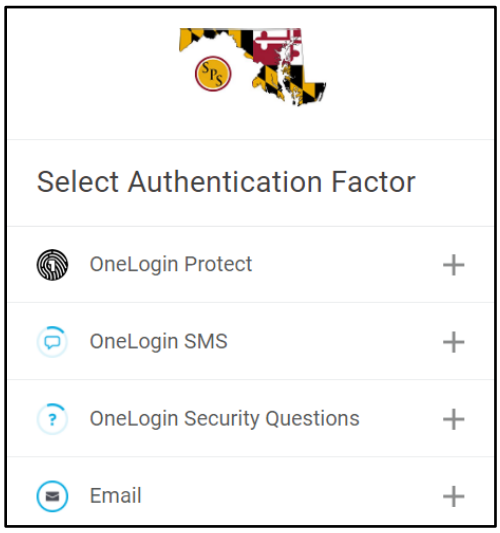

Figure 5

- **OneLogin Protect** – A mobile authenticator app that provides a one-time password.
- **OneLogin SMS** – A security code will be sent to your phone number in the form of a text message. You will be required to register your phone number.
- **OneLogin Security Questions** – You will be prompted to set up 3 security questions and answers.
- **Email** – You will receive an email with a 6-digit authentication code.

OneLogin Protect

OneLogin Protect for Google/iOS is a mobile authenticator app that provides a one-time-password (OTP) as a second authentication factor.

1. From the **Select Authentication Factor** dialog box, select **OneLogin Protect.** From the **OneLogin Protect** dialog box, click **Activate.**

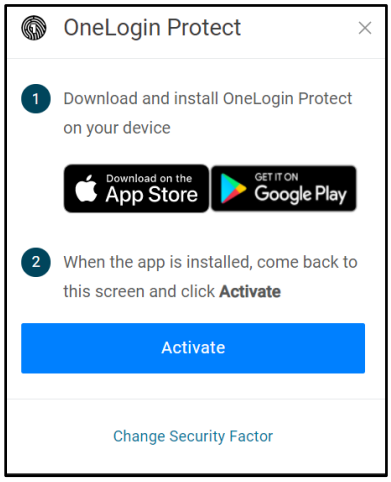

Figure 6

2. Download the app on your mobile device. Do this by launching the App Store or Google Play Store and search for **OneLogin Protect**. Install and launch it.
3. Tap the **+** sign in the upper right and corner of the app. You will be prompted for permission to use your camera.

Figure 7

4. Scan the **QR** code on your computer screen with your mobile device. A green check mark will appear over the code when successfully paired.

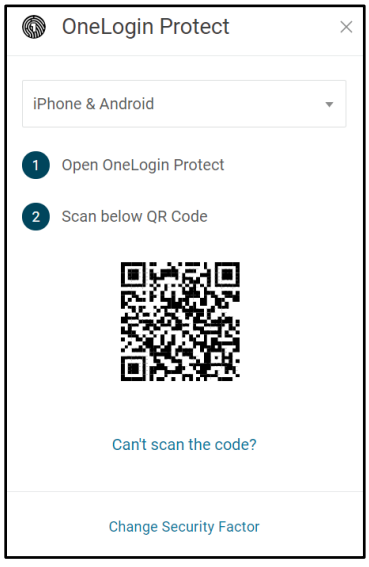

Figure 8

Note: If the code doesn't scan for you, click **Enter the code instead** in the app, and in your browser click on **Can't scan the code?** to receive a registration code.

5. Click **Accept** on the **Terms and Conditions** screen.
6. You will be prompted to change your temporary password. Enter your **Current Password** (temporary) and **New Password** in the **Your password has expired** dialog box and click **Submit**.

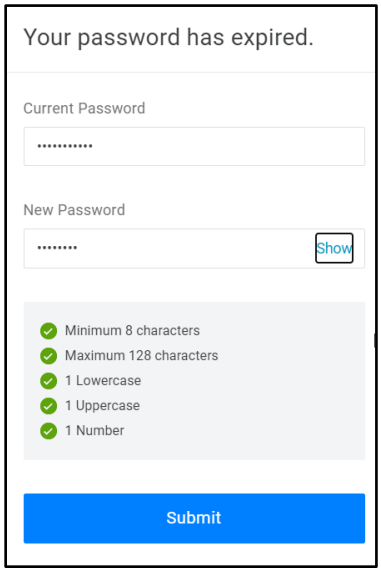

Figure 9

7. Click the **SPS Production** icon.

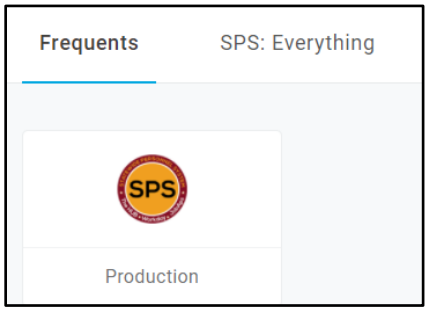

Figure 10

8. You will be asked to **Remember this device**. If you wish to do so, click the check box beside this option or you may click **Skip.**
9. Click **Submit**.

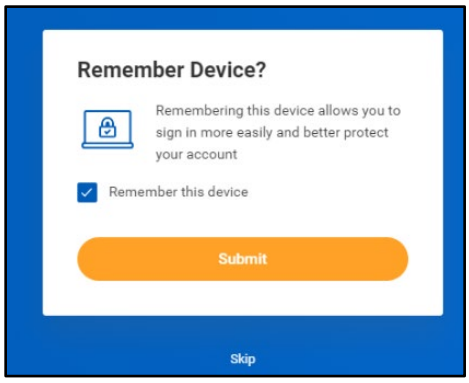

Figure 11

OneLogin SMS

You may set up SMS (text message) security codes as an authentication factor. The user will be prompted upon login to register their phone number to use SMS text messaging as the authentication factor.

1. From the **Select Authentication Factor** dialog box, select **OneLogin SMS**.
2. When the dialog box appears, **Enter your phone number** and click **Continue**.

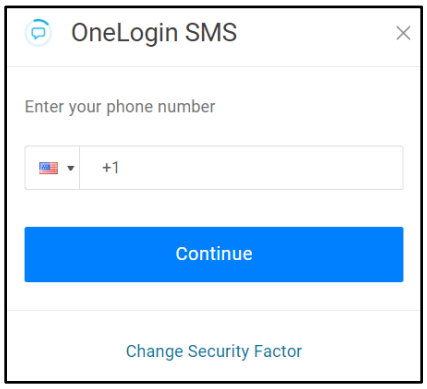

Figure 12

3. You will receive an SMS message from +1(410) 210-4546. Please enter the code from the SMS message in the **Enter your confirmation code** field. If you do not receive the SMS within 2 -3 minutes, or you think that the phone number you entered was entered incorrectly, click the **Try Again** button. That will take you to the previous screen where you can enter your phone number again.

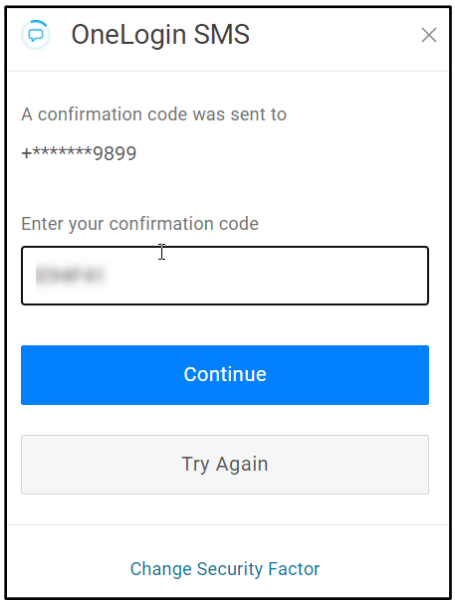

Figure 13

4. Click **Accept** on the Terms and Conditions screen.
5. You will be prompted to change your temporary password. Enter your **Current Password** (temporary) and **New Password** in the **Your password has expired** dialog box and click **Submit**.
6. Click the **SPS Production** icon.
7. You will be asked to **Remember this device**. If you wish to do so, click the check box beside this option or you may click **Skip.**
8. Click **Submit**.

Security Questions

Security questions are a form of authentication that end-users can use to verify their identity when they perform self-service password resets or multi-factor authentication. Security questions are not a very secure factor, since answers to standard security questions are easily found. We encourage you to choose other methods of authentication factors.

1. From the **Select Authentication Factor** dialog box, select **OneLogin Security Questions**. The **OneLogin Security Questions** dialog box will appear.

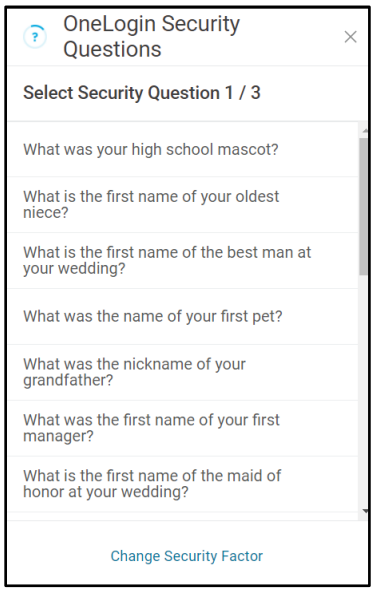

Figure 14

2. You must select 3 security questions and the answers to the security questions must be different. Select a question and fill in the answer in the dialog box that will appear and click **Continue**.

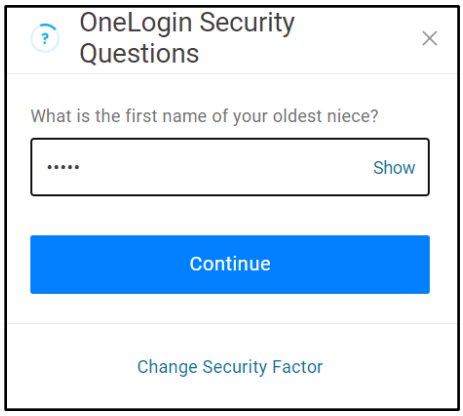

Figure 15

3. You will be prompted to repeat these steps for 2 additional questions. You must have 3 security questions.
4. Click **Accept** on the Terms and Conditions screen.
5. You will be prompted to change your temporary password. Enter your **Current Password** (temporary) and **New Password** in the **Your password has expired** dialog box and click **Submit**.
6. Click the **SPS Production** icon.
7. You will be asked to **Remember this device**. If you wish to do so, click the check box beside this option or you may click **Skip.**
8. Click **Submit**.

Email

OneLogin Email is an authentication factor that sends an email to a user to verify their identity during an authentication request. The user receives an email and is prompted to enter the 6 digit alphanumeric/numeric code they receive in the email.

1. From the **Select Authentication Factor** dialog box, select **Email**.
2. An **Email** dialog box will appear, and you will be prompted to **Enter your confirmation code** and click **Continue**.

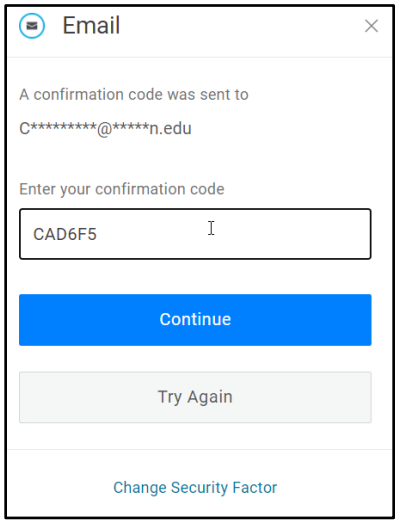

Figure 16

3. You will receive an email from **OneLogin** to your @towson.edu email account, with a unique code that you will need to enter in the confirmation box. Open the email and enter the security code in the **Enter your confirmation code** box.

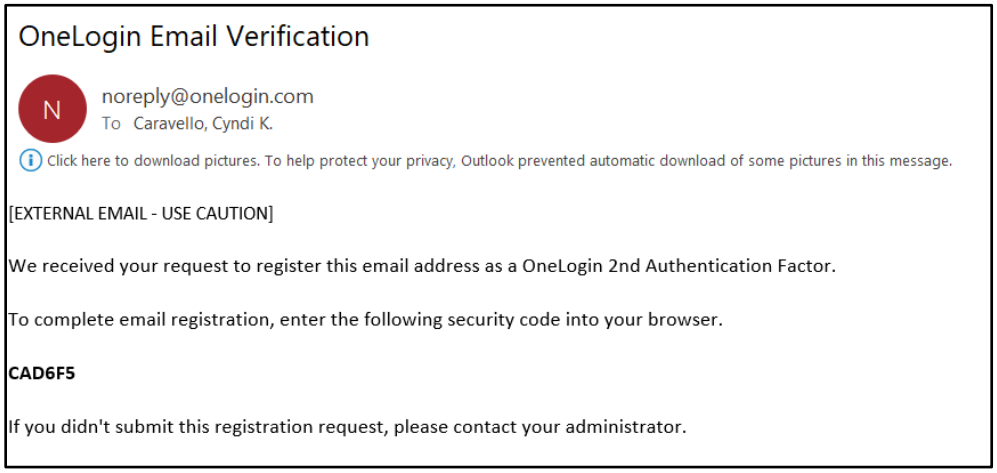

Figure 17

4. You will be prompted to change your temporary password. Enter your **Current Password** (temporary) and **New Password** in the **Your password has expired** dialog box and click **Submit**.
5. Click the **SPS Production** icon.
6. You will be asked to **Remember this device**. If you wish to do so, click the check box beside this option or you may click **Skip.**
7. Click **Submit**.

Changing or Setting Up Additional 2-Factor Authentication Methods

You may add an additional authentication method after making your initial selection. It is recommended that you set up at least 2 authentication methods. You may also change settings of chosen authentication methods.

1. From your favorite browser, type https://stateofmaryland.onelogin.com. The **Workday** login screen will appear.
2. Enter your **Workday SPS ID** and **Password**.
3. Click **Continue**.
4. You will have to authenticate using your chosen method.
5. Click your **user nam**e in the upper right hand corner of the **SPS** screen.

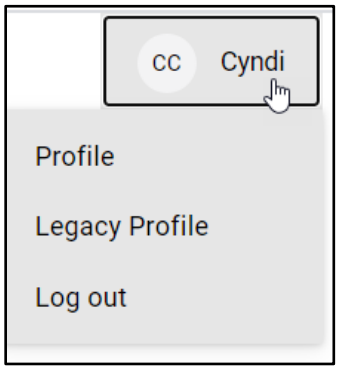

Figure 18

6. Click **Profile**.
7. Click **Security Factors**.

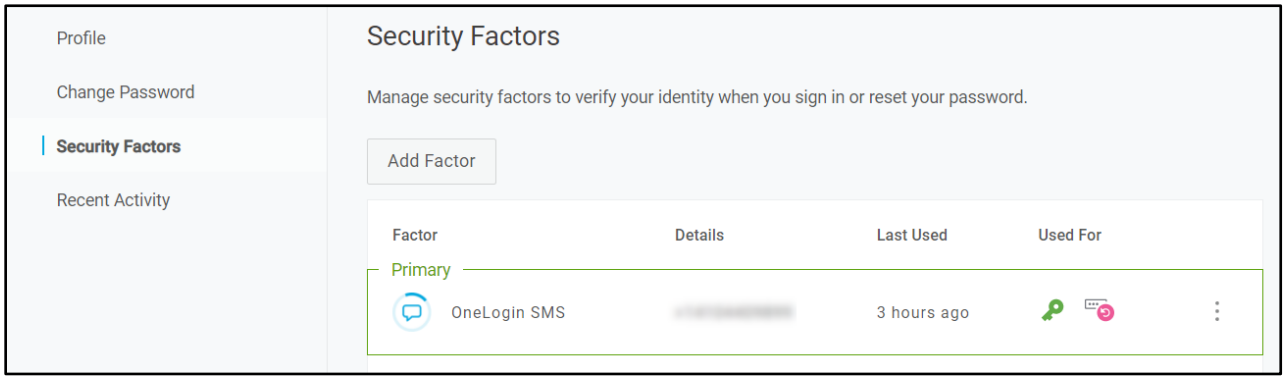

Figure 19

8. You may do the following:
    a. **Add Factor** – Click this button and then choose which security factor you would like to add from the **Select Security Factor** dialog box. Follow the instructions above for detailed instructions on each factor.

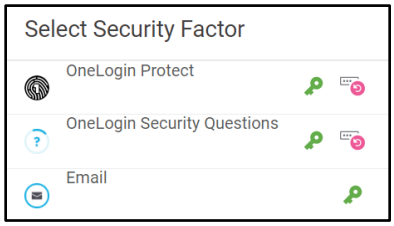

Figure 20

b. Change Options of Primary Factor– Click the vertical lines beside the primary security factor (first factor in list). You have 3 options: **Edit name**, **Remove** or **Show Details**.

c. **Change Primary Security Factor** – The top factor is the primary factor. Click the vertical lines beside a secondary factor. Click **Set as primary**.

Support

For technical assistance with any password or login issues, email TU_HRIS@towson.edu