

How to use your secure token

Whenever you log into VPN, MyApps, or Mosaic/HR SuccessFactors with your BCM username and password, you will then be prompted for a verification code. Open your Google Authenticator app to see the latest code, and type that code into the field prompting for the code. *NOTE: A new code is generated by your app every 30 seconds, so be sure to enter your code and click OK/Enter before a new code is generated.*



Video, documentation, and more

If you have colleagues who need to install multi-factor authentication, or if you want to learn more about MFA, visit the IT Service Portal at it.bcm.edu and search for **MFA**. The Multi-factor Authentication page includes more information about MFA, printable documentation, and a step-by-step installation video.

For personal assistance from the Help Desk, send an email to it-support@bcm.edu or call 713-798-8737.

Install Multifactor Authentication in 3 minutes



INFORMATION TECHNOLOGY

Office of Information Technology
Visit the IT Service Portal online at it.bcm.edu
and search for **MFA**.

What is Multi-factor Authentication, and why do I need it?

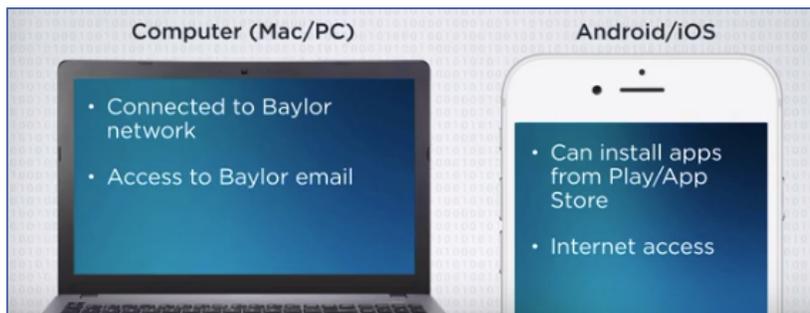
Multi-factor authentication (MFA) confirms your identity when logging into an MFA-enabled system, asking for your username and password (something you know) and an MFA secure token (something you have) generated on your phone.

These two layers of security keep your and Baylor's data safer than with only a username and password. With MFA, even if someone entered your username and password, they would not have the MFA secure token from your phone to successfully log in.

You must have MFA to use VPN, MyApps, and Mosaic HR/SuccessFactors.

What you'll need

You need a **Baylor-connected computer** that can access your Baylor email, and an **iPhone or Android smartphone** with internet access to install an authenticator app.



Step 1: Request your MFA secure token

1. On your Baylor-connected computer, navigate to the Defender website at **mytoken.bcm.edu**, log in with your BCM username and password, then click **Sign in**.
2. Click the **Request a software token** button, then click **Next**.
3. Open the email from **multifactor_authentication@bcm.edu** in your BCM inbox. Click the link in the email to return to the Defender website, or copy the verification code and paste it in the Defender website.
4. A QR (Quick Response) code will appear. Leave it on your computer screen and move to your smartphone.

Step 2: Install your authenticator app

1. On your phone, open the **App Store (iPhone)** or **Play Store (Android)**, then search for and install the **Google Authenticator** app.
2. Open the **Google Authenticator** app, and tap **Begin Setup (iPhone)** or tap **SKIP for the next two screens (Android)**.
3. Tap **Scan barcode**, and tap **Allow** or **OK** to let the app use your camera.
4. Point your camera at your computer screen to scan the QR code. A six-digit code should now appear in your app.
5. In the Defender website on your computer, click the **Finish** button.