Enable 2-Step Verification

2-Step Verification must be enabled on your account before setting up an application specific password. An application-specific password is required to sync your Google account with certain devices, such as Mac OS X or iOS devices. Please follow the steps below to enable 2-Step Verification.

**Note:** After enabling 2-Step verification you will need to re-authenticate any desktop or mobile applications.

1. Log in to your Google account. Click the profile button in the top-right corner and click **Account**.

2. Click the **Security** tab. Click **Setup** 2-Step Verification.
3. Enter a phone number to receive your verification code. You may choose to receive the code via text message or voice call. Click **Send code**.

4. Once you receive your code, enter it on the following screen and click **Verify**.
5. Click **Next**.

---

**Trust this computer?**

Trusted computers only ask for verification codes once every 30 days.

If you lose your phone, you might be able to access your account from a trusted computer without needing a code. We recommend that you make this a trusted computer only if you trust the people who have access to it.

- **Trust this computer**
  - You can always change which computers you trust in your Google Account settings.

[Back]  [Next]

---

6. Click **Confirm**. 2-Step Verification is now enabled on your account.

---

**Turn on 2-step verification**

You’ll only be asked for a code whenever you sign in using your helpdesk@wmich.edu account every 30 days, on each trusted computer or device.

If you lose your phone, you can always change it in account settings.

The Google Apps SLA (Service Level Agreement) does not apply to any services that are used in connection with 2-step verification, if the verification process relies on third-party voice or data providers to deliver the verification code. Details of the agreement are available here.

[Back]  [Confirm]