Two Factor Authentication for Google

Add an extra layer of security to your Jordan District Google account with two-factor authentication, also known as 2-Step Verification. Once enabled, cyber criminals will not be able to access your account with only a stolen password. Your Google account will require a second form of authentication, most often through a push notification on your phone.

How to Enable Two-Factor Authentication:

1. Open your Google Account (myaccount.google.com).
2. In the navigation panel on the left, select ***Security***.
3. Under "**How you sign in to Google**," select the arrow for ***2-Step Verification***.
4. Select ***Get Started*** and follow the on screen steps.

Now for the Verification! After you enable two-factor authentication, you must complete a second step to verify it's you attempting to sign in to your Google account on a new device. There are a few ways to do this, but we recommend you sign in with Google prompts. It's easier to tap a prompt than enter a verification code and prompts are the most secure form of verification.

Google prompts are push notifications you'll receive on either 1) Android phones that are signed in to your Google Account or 2) iPhones with the Gmail app, the YouTube app, or Google app signed in to your Jordan District Google Account.

Based on the device and location info in the notification, you can:

- Allow the sign in if you requested it by tapping **Yes**
- Block the sign-in if you didn't request it by tapping **No**

You can set up other verification methods in case you are unable to get Google prompts or lose your phone. These methods include:

- Use a verification code from a text message or call.
  - ✔ A 6-digit code may be sent to a number you've previously provided. Codes can be sent in a text message (SMS) or through a voice call, depending on the setting you chose. To verify it's you, enter the code on the sign-in screen.
  - ✔ **Tip:** Although any form of 2-Step Verification adds account security, verification codes sent by texts or calls can be vulnerable to phone number-based hacks.
- Call the help desk at extension 88737 (or 801-567-8737) to get a backup code.
  - ✔ **Important: Never give your backup codes to anyone**