

Multifactor/2FA Authentication

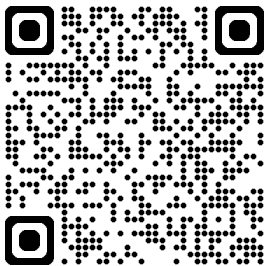
- [2FA - Options and Enrollment Instructions for Google](#)

2FA - Options and Enrollment Instructions for Google

To start, please make sure you have your Yubikey with you, and your device on and logged into your Google Account.

Visit <https://myaccount.google.com/signinoptions/twosv> or follow the QR code below.

(You may have to log in a second time, so be sure that you are on your RESD provided account while doing so.)



Here, you are presented with a list of options.

Please make sure to click on "use hardware key" or "use other device" if prompted.

← 2-Step Verification

2-Step Verification is required for this account

- 2-Step Verification is required for your account and can't be turned off, but you can add or change your second steps






Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

 Passkeys and security keys	✓ 1 security key	>
 Google prompt	✓ 1 device	>
 Authenticator	✓ Added 1 minute ago	>
 Phone number	✓	>
 Backup codes	✓ 10 codes available	>

If you want to use a Yubikey (District Provided) or other hardware security device, you would select Passkeys and security keys.

If you want to use the Gmail or Google app on your personal phone, you would select Google prompt.

If you want to use an authentication program, you would select Authenticator.

If you want to use SMS text messaging, you would select phone number.

Finally, backup codes are provided once 2FA is set up. Your I.T. Technician can also provide those if necessary.