Gmail and Google Workspace

- Secure your Google account with 2-Step Verification

Secure your Google account with 2-Step Verification

2-Step Verification (also known as two-factor authentication) is an extra security feature in Google Workspace, which is mandated by the MDYHS IT Department. Enabling 2-Step Verification nearly eliminates the risk of unwanted individuals gaining access to your email or documents stored in Google Drive.

How it works

- Extra protection is offered by requiring you to both have something (your phone) and know something (your password) before being allowed into your account.
- You'll keep others out of your account since Google will ask for a verification code anytime access to your account is requested from another device that you have not "trusted."

Set up 2-Step verification

You will need your mobile phone to complete the process.

Follow Google's instructions for setting up 2-Step Verification.

If you use third-party applications (like Thunderbird or Outlook) to access Google mail, you will need to authorize the application or device the first time you use it after setting up 2-step verification. Follow Google's instructions for signing in using App Passwords.Useful tips

- To use the Google Authenticator App on your iPhone, iPod Touch, or iPad, you must have iOS 5.0 or later.
- Be sure to include a backup phone number (or two) during the setup process in case your primary phone is lost or stolen or you replace your phone.
- Print off backup codes during the setup process and store them in a secure place in case your phone is lost or stolen or you replace your phone.

See Google's Account Help for more information about 2-Step Verification.