


Tips To Keep Your Rider Gmail Account Safe

Secure your password

Passwords are the first line of defense against account hijackers. Think of a strong password. Here are some tips:

- Use unique passwords for your accounts. The longer your password is, the harder it is to guess.
- Use a password with a mix of letters, numbers, and symbols.
- Try using a phrase that only you know. For example, for your email you could start with “My friends Tom and Jasmine send me a funny email once a day” and then use numbers and letters to recreate it. “MfT&Jsmafelad” is a password with lots of variations.

To Change your password while signed in to Gmail:

Click on the gear icon  in the upper right corner of the Gmail window and choose **Settings**. Click on **Accounts**. Click on **Google Account settings**. Click on **Sign in and Security**. Under **Password & Sign in Method**, click the arrow next to **Password**. Type in your current password. Type a new password twice and click **Change password**.

Turn on 2-Step Verification for tighter account security

Most people only protect their accounts with their password. However, with 2-Step Verification, you'll protect your account with your password *and* your phone. If someone manages to steal or guess your password, he'll also need to have your phone to get into your account. To set up 2-Step Verification, click on **Settings, Accounts, Google Account settings, Sign in & Security**. Scroll down to **2-Step Verification** and click on the arrow. Click on **Start setup**.

Signing in with 2-Step Verification works a little differently. You'll enter your password as usual, then you'll provide a verification code that you'll get from your phone. You can make this process simpler for the computers or devices that you use often.

Check your account for unusual activity

Regularly review your account for unfamiliar or suspicious activity by reviewing [Recently Used Devices](#)

On your [recent activity](#) page, you can see security-related actions you've taken, like signing in to your Google Account, changing your password, or adding a recovery email address or phone number. It's good practice to review these actions and take note of the time and location where they took place. If you notice anything suspicious -- for example, a sign-in from a browser you've never used, or a location you've never been to -- you should change your password to secure your account. Find out more about [suspicious account activity](#).

For more information on your Rider Gmail account visit us at: www.rider.edu/helpdesk