**Account Setup and Configuration**

**For NCSU GitHub account:**

If you are a student or faculty member, you already have access to GitHub Enterprise. Simply login at [https://github.ncsu.edu](https://github.ncsu.edu/)/ with your Unity username and password. Your GitHub Enterprise Account will be created instantly after login.

**For Public GitHub.com account:**

The first thing you need to do is set up a free user account. Simply visit [https://github.com](https://github.com/), choose a user name that isn’t already taken, provide an email address and a password, and click the big green “Sign up for GitHub” button.



The next thing you’ll see is the pricing page for upgraded plans, but it’s safe to ignore this for now. GitHub will send you an email to verify the address you provided.

Clicking the Octocat logo at the top-left of the screen will take you to your dashboard page. You’re now ready to use GitHub.

**Your Avatar**

Next, if you wish, you can replace the avatar that is generated for you with an image of your choosing. First go to the “Profile” tab (above the SSH Keys tab) and click “Upload new picture”.



Now anywhere you interact on the site, people will see your avatar next to your username.

**Your Email Addresses**

The way that GitHub maps your Git commits to your user is by email address. If you use multiple email addresses in your commits and you want GitHub to link them up properly, you need to add all the email addresses you have used to the Emails section of the admin section.



There are different states that are possible for the e-mail addresses. In the above example, the top address is verified and set as the primary address, meaning that is where you’ll get any notifications and receipts. The second address is verified and so can be set as the primary if you wish to switch them. The final address is unverified, meaning that you can’t make it your primary address. If GitHub sees any of these in commit messages in any repository on the site, it will be linked to your user now.

**Two Factor Authentication**

Finally, for extra security, you should set up Two-factor Authentication or “2FA”. Two-factor Authentication is an authentication mechanism that is becoming more and more popular recently to mitigate the risk of your account being compromised if your password is stolen. Turning it on will make GitHub ask you for two different methods of authentication, so that if one of them is compromised, an attacker will not be able to access your account.

You can find the Two-factor Authentication setup under the Security tab of your Account settings.

If you click on the “Set up two-factor authentication” button, it will take you to a configuration page where you can choose to use a phone app to generate your secondary code (a “time based one-time password”), or you can have GitHub send you a code via SMS each time you need to log in.

After you choose which method you prefer and follow the instructions for setting up 2FA, your account will then be a little more secure and you will have to provide a code in addition to your password whenever you log into GitHub.