In today's world, a password alone is not enough. That's why we've made Two-Step verification available for Brown students, staff, and faculty. This feature, which uses a product called Duo, will protect your Brown account even if someone is able to access or guess your password. It combines something you know (your password) with something you have (a phone or code).

As of 3/9/2016, most of the Brown community is required to use Two-Step Verification.

Watch the video and read more to learn how it works.

How it Works

You probably recognize the Brown Single Sign On page below from Workday, Canvas, or Banner. After enabling Two-Step, when you log in to a page like this, you'll be prompted to authorize your login in one of several ways, such as tapping a notification on your smartphone, answering a phone call, or entering a pre-generated code. You can authorize your web browser for thirty days to make this process more convenient; you will not be
prompted again in that browser until the thirty day period has passed. In most cases, attackers don't have your computer, so even with this added convenience you remain protected against outside attacks.

Note: The two-step we're discussing above does not apply to your email. If you also want to enable two-step for your email, Google offers a separate but similar feature that you can enable. Again, this is optional and not the two-step described above.