FAQ: Two-Step Verification for Brown Accounts
Stephanie Obodda - 2017-11-14 - 0 Comments - in Two Step Verification

- **Who can use Two-Step at Brown?**
  All students, staff, and Brown-paid faculty can currently use Two-Step. It will be available for unpaid (medical) faculty in early 2016.

- **Will this be required?**
  Yes, all staff, graduate students, and undergraduate students have already set it up. Faculty should set it up by 3/9/16.

- **How do I set this up? How do I use it?**
  See brown.edu/go/twostephelp for all instructions.

- **What happens if I don't do this before my deadline?**
  Your account will be auto-enrolled, and the first time you log into a service like Banner, Canvas, Workday, or VPN after the deadline, you will be prompted to complete the setup before you can continue to the service. What you will see is described on this page. We recommend setting it up beforehand because it is easier and more convenient.

- **When will I be prompted to verify?**
  When logging into the Brown single sign on screen (seen below) with your Brown account.

- **Does this apply to my email account, too?**
  No. Google has a similar feature but it works a little differently. You can enable it separately, but it is not required. For more information, visit https://accounts.google.com/SmsAuthConfig

- **Can I use this if I don't have a smartphone?**
  Yes, you can use it on "non-smart" cell phones and even landlines. You can also use the bypass codes instead of a phone. Also, the IT Service center has tokens for anyone who needs them.
- **What if I get a new phone with the same number?**
  If you get a new smartphone with the same number, you can use the Reactivate link in MyAccount's Two-Step Verification to load your account. (Not a smartphone? You don't need to do anything). We have more detailed instructions in our article [Set up a Replacement Smartphone (same phone number) for Two-Step Verification](#).

- **What if I share a phone with someone else?**
  If you add a phone number that is already in use, you will be asked to verify that you have access to the phone by receiving a text message or phone call with a verification code.

- **Can I add an international number?**
  Yes, just add a + in front of the country code (for example, a German number would start +49).

- **What should I do if I will be traveling? Does this work outside of the US?**
  Please see our article [Use Two-Step Verification When Traveling](#).

- **If I request a new set of codes, does the first set continue to work?**
  No, only your latest set of codes works.

- **What should I do if I am locked out of my account?**
  Contact the IT Service Center at (401) 863-4357. They will verify your identity and can disable it temporarily.

- **How can I add additional devices or phone numbers after setting up Two-Step?**
  The process is the same as when you originally added your current device: just click the "Add Devices" button in the two-step verification section of MyAccount. See this article for more: [Add Phones and Devices for Two-Step Verification](#).

- **When do my bypass codes expire?**
  See this article for details: [Use Bypass Codes with Two-Step Verification](#).

- **What if I get an unexpected Duo notification on my phone when I am not logging in myself?**
  Yikes! This means that your account's password must have been compromised and Duo is keeping someone from maliciously accessing your account. You should:
    1. First, deny the fraudulent login attempt from Duo.
    2. Second, log into [myaccount.brown.edu](http://myaccount.brown.edu) and change your Brown password.
    3. If you used the same password for other accounts, change those as well.
I received a message about being locked out of my account. What should I do?
This means that there were 10 invalid authorization attempts (these might have been malicious or might have been a mistake - for example, if you accidentally typed in 10 incorrect codes, or let 10 requests time out without approving). You will need to contact the IT Service Center to unlock your account.

What else should I be aware of?
If after logging in with two-step, you are directed to an unexpected location, this could mean that your account might have been compromised. You should change your password and contact the IT Service Center to report this.