How does two step login work?

IT Public - KB0013049

☆☆☆☆☆ 48 views

Question: How does two step login work?

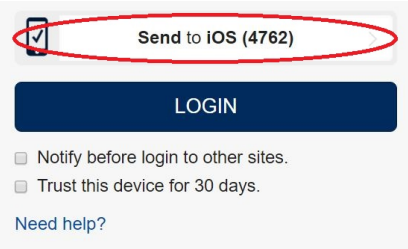
Answer: Two step authentication reduces the ability of a hacker to access your account and data, by requiring two methods to verify you:

1. The NetID and password that you know
2. A phone, tablet device or key fob that you have possession of

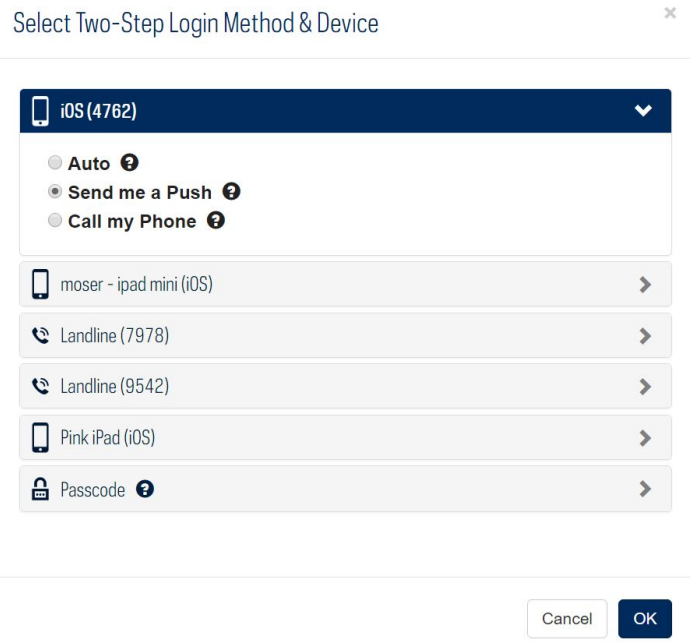
A hacker may gain access to your NetID and password, but it will be more difficult for them to access that device as well.

So how will I login?

1. When you login to an ND service protected by two step (e.g. Gmail, Sakai, Box, and many others), you will enter your NetID and password.
2. If the system needs to verify your login, you will then be presented with a second screen allowing you to select which device and method you wish to use as your "second factor". That screen will look something like:



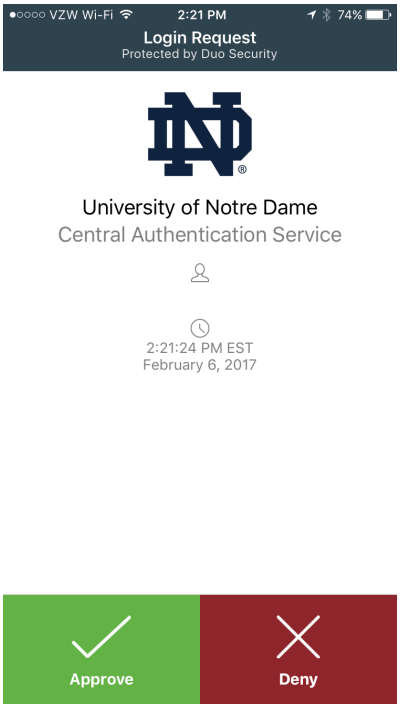
3. If you've enrolled multiple devices, and wish to use a different one for this particular login, click on the top button (circled in red in the image above) and a list of your enrolled devices will appear similar to:



4. Click on the device you wish to use this time.

5. Click **OK**.
6. You'll be returned to the login screen and the new device will now be reflected in the top button.
7. If you are using a computer or device that is NOT shared with others, we recommend you check the box, **Trust this device for 30 days** as shown below.
   a. This will store information on that device or browser so that you won't be prompted for Two Step again until 30 days have elapsed.
   b. Note: Do NOT check this box on a shared computer such as a classroom or lab, as it may allow others using that computer to access your account.

8. Click **Login**.
9. Depending which device you selected, you will receive a notification on that device that you need to respond to.
   a. If you selected a phone to call, that phone will ring and you will need to answer the call and follow the verbal instructions you hear.
   b. If you selected a "push", the Duo mobile app on that device will receive an alert that you will need to respond to. In the example below, you would tap the green **Approve** button.



   c. Note: You must respond to the notification within a short period of time (approx. 60 seconds), or it will timeout and you will need to repeat the process.
10. Once the second factor approval has been received, you will be logged in to the desired service.

Authored by Denise Moser
Last modified 2 months ago