

Enabling Verified Duo Push for all OSU students and employees

Dear OSU Community,


As we continue to see round after round of increasingly sophisticated and malicious phishing attacks targeting the OSU community, we are working to improve our security posture and increase our resiliency by adopting new security measures. Beginning Monday, November 6, we will be activating Verified Duo Push for all OSU students and employees.

What is Verified Duo Push? Check out this brief video of one of our Service Desk student employees talking about this change: <https://beav.es/qqb>.

How will this impact me?

Verified Duo Push will impact the way users engage with Duo to approve a login request. Instead of sending you a push notification asking you to approve the request, Duo will show you a one-time, unique verification code that you will need to enter in the Duo Mobile app.

What you will see on your browser:




Enter code in Duo Mobile

Verify it's you by entering this verification code in the Duo Mobile app...

866

Sent to "iOS" (***-***-****)

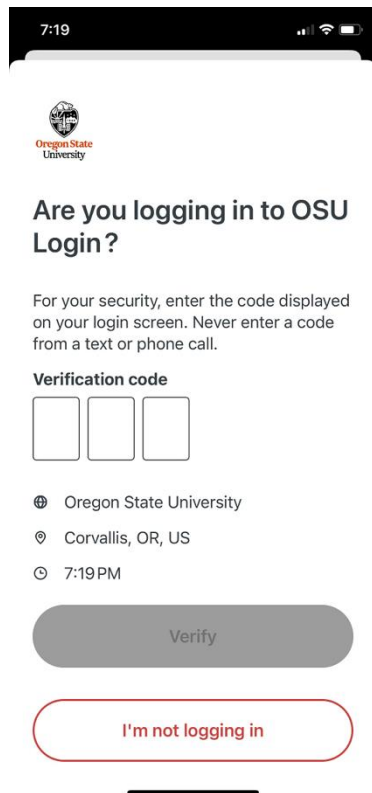


[Other options](#)

☒ Remember me

[Need help?](#) Secured by Duo

What you will see in Duo Mobile (on your phone):



Why is this happening?

Across the board, higher education continues to be a preferred target for cyber attackers. Phishing attacks continue to evolve and are increasingly sophisticated and convincing, making them much harder to spot at first glance and much easier to fall for. Cyber attackers also rely on tactics such as push harassment and push fatigue, sending a user multiple push notifications to get the user to approve a malicious access request and give the attacker access to login credentials.

The verification code option for Duo Push provides additional security against push harassment and fatigue attacks by asking the user to enter a verification code, making it difficult for attackers to log in as you and access your information without that verification code. It also provides improved fraud reporting, directing users to the fraud report option in Duo Mobile when they receive unexpected Duo Push login requests.

Gaining access to a single ONID account can have a measurable impact: it can give cyber attackers access to an individual's data, including sensitive personal, financial and health information, and it can create a doorway for access to all of OSU's institutional data. To protect

the community and university, we must stay vigilant and minimize opportunities for attackers to infiltrate OSU's cyber boundary so we can protect ourselves, the community, and the university.

Will there be other changes in Duo security measures coming up?

Yes. One of the next steps in increasing our Duo security measures will be to retire the use of Duo tokens in the near future. When this occurs, token users will need to use Verified Duo Push on the Duo Mobile app or a YubiKey. The Office of Information Security will work with the appropriate campus partners to make YubiKeys available to faculty, staff and students who need them.

For self-service help with setting up a YubiKey or Duo Mobile, visit our Duo knowledge base:

<https://oregonstate.teamdynamix.com/TDClient/1935/Portal/KB/?CategoryID=8235>

Resources and more information

If you have any questions or concerns regarding this change, please contact the Service Desk at beav.es/help or by calling 541-737-8787.