



University Information Technology Services

Two-Step Login Update

Jacob Farmer
jpfarmer@iu.edu

**Let's get something out
of the way...**

This is the most impactful cybersecurity change at IU in recent memory.

“We are working hard to re-balance convenience with essential controls as our community does the work of IU, and we have taken the deliberate decision that the situation compels that we trade off some long-enjoyed convenience for greater security.”

– Vice President Wheeler



**So why are we doing
this *now*?**

Phishing has reached a critical threshold...

In one large attack, phished credentials were used to access the users' tax information and, in some cases, redirect their direct deposits to other bank accounts.

This is new.



What is coming?

And when?

After February 2nd, two-step login will be required at every CAS authentication for all employees and affiliates, including retirees, non-paid faculty, and student employees.



What about employees without a smartphone?

- Almost any phone can be use to authenticate with Duo, including basic mobile devices and landline phones
- U2F authenticators can be used in many circumstances, as long as users understand their capabilities and limitations
- For users who are not able to authenticate via other means, UITS will centrally fund single-button hardware tokens for a limited time. These are available at tabling events and at the Support Center



**For this to be
successful, we need
your help**

1) Please help us spread the word about what is coming, when it is coming, and what it will mean on a day-to-day basis.



2) Help users in your area get set up with two-step login (Duo) as soon as possible.

Feedback from our peer institutions suggest that this personal setup interaction is the single most important part of a successful rollout.



3) For teaching faculty, help them understand that this means they may need to perform two-step login when they come into a classroom to teach.

It also means they may have student employees who will need to use their mobile phones to authenticate while in class.



4) Transition users to mobile device-based authentication wherever possible.

The single-button hardware tokens are becoming far less prominent in the marketplace and are on a slow, but steady, decline.



Questions?

Jacob Farmer

jpfarmer@iu.edu



INDIANA UNIVERSITY
FULFILLING *the* PROMISE