

From: dopmannouncement <dopmannouncement@uabmc.edu>
Sent: Thursday, February 28, 2019 11:35 AM
To: DOPM All Users <DOPMAllUsers@uabmc.edu>
Subject: Computer Tip of the Week -- Required Duo Two-Factor Rollout

Complying with UAB Policy for Duo Authentication of BlazerID

Brought to you by
David Clabough
System Admin in MT-403



SITUATION:

I received the below email stating that soon, UAB Information Security will mandate the use of Dual Authentication for all UAB websites requiring BLAZERID credentials.
What does that mean to me?

SOLUTION:

To increase security all UAB personnel (Staff and students) will be required to sign up for DUO Authentication. Technically this is called "2 Factor Authentication".

This service enhances security of campus web services (anything that requires a BLAZERID sign-in) and it will also eliminate the need to periodically change your BLAZERID password (unless it becomes compromised).

You will need one of the following types of devices:

- a smart phone (iOS or Android),
- a tablet (iOS or Android),
- a non-smart phone that can receive SMS text messages, or
- your office telephone.

Here is the website with all of the information: <https://www.uab.edu/it/home/2-factor>.

You are welcome to go to the website above and set up DUO on your own, however, we, DOPMHelp, will be holding a couple of classes in MT-634 to help get you set up for DUO Authentication. We will send out a DOPM wide email to announce the dates and times.

This is that email from UAB Information Security -- with all the details -- if you're interested

From: UAB IT <vpit-uab@mail.ad.uab.edu>

Sent: Wednesday, February 27, 2019 6:20 AM

<<snip>>

Subject: Duo two-factor authentication requirement for UAB faculty and staff

Beginning in March, UAB will roll out a plan to require faculty, staff and students to use [Duo two-factor authentication](#) to protect their BlazerID credentials.

Passwords alone no longer provide adequate protection against cyberattacks. Duo two-factor authentication adds a second layer of security to your BlazerID account. Attempts have been made by cyber criminals to change direct deposit information in order to steal student refunds and UAB employee paychecks. Duo was implemented to protect UAB students, faculty and staff against such attacks, and its required use has been approved by UAB leadership.

Once you sign up for Duo, you will use a smart phone, analog phone or UAB-provided token to finish logging in to UAB systems. You'll use that credential to approve or deny login attempts on new devices or browsers — so you have control if someone else tries to log in with your BlazerID. Kronos and Canvas do not require Duo two-factor authentication to log in, but email, Oracle and many other systems do.

And the best part? When you enroll in Duo, you never have to change your BlazerID password again, unless your password is compromised.

UAB is a complex organization with diverse employee responsibilities, so it is necessary that some policies, processes and programs apply differently to various entities and academic/administrative and clinical business lines. Based on their area of work, UAB has assigned every employee to either the A (academic/administrative), C (clinical) or Faculty workgroup. Employees in the A and Faculty workgroups will be required to use Duo two-factor authentication. Employees in the C workgroup may opt in but will not be required to use Duo. Additional information on Employee Workforce Groups and access to the UAB Workforce App is available on the [UAB Human Resources web site](#).

UAB IT will roll out two-factor authentication to employees in the A and Faculty workgroups in two-week waves beginning March 18.

- You will receive an email notifying you when your department's wave has begun and alerting you that you have two weeks to sign up for Duo before you are automatically enrolled.
- Once you are enrolled, you need to complete the sign-up process and enroll a Duo two-factor capable device before you can log into UAB systems.
- If you anticipate being on vacation or out of the office without access to your devices or computer, we encourage you to sign up now to avoid any issues once you return.

There are several methods for authenticating using Duo:

- Our recommended method is using the Duo app installed on a smart phone or tablet — using either the push notification or entering a code.
- A new “call me” feature, which will work with any phone and does not require the app, has been rolled out this month.
- Employees who are unable to use the Duo app or the call me feature can request a hard token.

When you log into Duo, you have the option to check a “remember me for 30 days” option, which makes logging in using Duo more convenient.

Sign up for Duo two-factor authentication now at uab.edu/2factor, where you can also learn more about the initiative and the various methods for using Duo two-factor.

Rob Ferrill | Chief Information Security Officer
UAB | The University of Alabama at Birmingham

Was this helpful? Do you have suggestions for a future Tip of the Week? Do you have any other comments?

Let us know at dopmHelp@uabmc.edu

To see an archive of past Tips of the Week: <http://www.uab.edu/medicine/dopm/help/totw>