Published on *University of Colorado* (https://www.cu.edu)

Be Aware — Smart MFA begins in October [1]

September 27, 2022 by Employee and Information Services [2]

October is Cybersecurity Awareness Month, a global effort to help everyone stay safe and protected when using technology whenever and however you connect. The University of Colorado is proud to be a champion of Cybersecurity Awareness Month [3] and this year's theme: "It's easy to stay safe online."

Throughout the month of October, the Office of Information Security and campus OITs are promoting key behaviors to encourage every employee to take control of their online lives. There are all kinds of ways to stay safe and secure online but even just practicing these two cybersecurity basics, strong passwords and multi-factor authentication, can make a huge difference:

Multi-Factor authentication, or MFA, is a security measure that requires anyone logging into an account to use a two-step process to verify their identity. This ensures that it is twice as hard for someone to access your online account without authorization. When it is available, always turn it on because it is not only easy to use but incredibly effective. Data shows us that over 99% of account hacks could have been prevented by use of MFA.

Some examples of MFA can include an extra Personal Identification Number, answering security questions, a code emailed or texted to you, facial or fingerprint recognition, and more. CU System uses Duo [4] for multifactor authentication.

As more applications require Duo verification for access, UIS is exploring secure options to reduce the number of times users receive an MFA challenge. Smart MFA will roll out to all CU System authentications in October.

What is Smart MFA?

Adaptive multi-factor authentication, also known as Smart MFA, analyzes additional factors when a user attempts to log in and assigns a level of risk associated with that login attempt. For example:

- Where is the user who is trying to access information? Is the location different than normal?
- When are they attempting to access information? Is it during regular hours?
- What kind of device are they using? Is it different than the one they normally use?
- Are they on a private network or a public network?

Depending on the risk level calculated, the user may be prompted for an additional authentication factor, such as using Duo.

How does Smart MFA work?

For Smart MFA to assess the level of risk associated with a specific login attempt, it first needs to collect data and identify what is “normal” for the four questions outlined above.

How will CU System staff be impacted by Smart MFA?

After enough data is collected, ideally by Oct. 25, you may notice a request to authenticate using Duo when accessing an application that previously only required a password.

Over time, as your device, location and timing are determined to be low risk, you may find some applications require you to use MFA less often.

To learn more about multi-factor authentication in general and Smart MFA, visit the previous Smart MFA Tech Tip [5].

multi-factor authentication [6], cybersecurity [7]
Display Title:
Be Aware — Smart MFA begins in October
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/be-aware-%E2%80%94-smart-mfa-begins-october
[2] https://www.cu.edu/blog/tech-tips/author/76185
[3]
https://click.communications.cu.edu/?qs=774e500784cf9c3007cf2abe4fb0f1cb67ddc1e5407196cfc3eb6d970f3a7c96
[4]
https://click.communications.cu.edu/?qs=774e500784cf9c3045d01e539726ed12d35da6d4b8ae5d09cb73d1210ac15
[5]
https://click.communications.cu.edu/?qs=774e500784cf9c309a10299ab4ac28a146a3148c1e0155a3e3b2ed154956
[6] https://www.cu.edu/blog/tech-tips/tag/multi-factor-authentication [7] https://www.cu.edu/blog/tech-tips/tag/cybersecurity