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

It takes two: Using multifactor authentication to stay safe online [1]

October 14, 2024 by ES and UIS Communications [2]

The University of Colorado is a proud champion of Cybersecurity Awareness Month, a global effort to promote cybersecurity best practices and increase awareness of security threats among organizations and individuals.

Visit CU's Cybersecurity Awareness Month web page [3] for more information and to learn how to get involved.

Multifactor authentication, or MFA, is one of the strongest defenses against cyberattacks and phishing attempts. When logging into an online account with MFA enabled, you'll be prompted to confirm your identity through an additional security measure.

Additional MFA security measures can consist of:

- Personal Identification Number (PIN)
- Biometric confirmation like a fingerprint or facial recognition
- A unique, changing code from an authenticator app
- Security questions

MFA often requires a second device to confirm your login, like with an authenticator app or Duo Mobile. This feature makes it extremely hard for cybercriminals to access your account, even if they have your login details, as they would need physical access to your second device to confirm their login attempt.

Smart MFA saves you time

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?

Duo Mobile, the MFA application used to verify CU users' identity when accessing CU applications, has Smart MFA enabled. When Smart MFA has collected enough data to identify your "normal" login behaviors based on the questions outlined above, you may no longer have

to authenticate your access with a second device, while still maintaining the high level of security that MFA provides.

Is using MFA worth it?

Without a doubt. Data on cyberattacks, phishing and security breaches show that over 99% of incidents could have been prevented by using MFA. In short, MFA adds an additional layer of security that is unmatched by other methods. By preventing ransomware attacks and data breaches, MFA saves everybody time and gives peace of mind.

MFA is worth enabling on your personal accounts too, whenever available.

For more information on MFA, review the Office of Information Security's MFA web page [4] and watch What does MFA Mean [5].

cybersecurity [6], multi-factor authentication [7]
Display Title:
It takes two: Using multifactor authentication to stay safe online
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/it-takes-two-using-multifactor-authentication-stay-safe-online
[2] https://www.cu.edu/blog/tech-tips/author/110439 [3] https://www.cu.edu/security/cybersecurity-awareness-month [4] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime
[5] https://vimeo.com/751302523 [6] https://www.cu.edu/blog/tech-tips/tag/cybersecurity
[7] https://www.cu.edu/blog/tech-tips/tag/multi-factor-authentication