Multi-Factor Authentication (MFA) [1]

What is MFA?

In order to provide added protection to university data CU employs 2-factor or "multi-factor" authentication. In addition to using their username and password, under certain circumstances, users must also authenticate using a phone (second factor of authentication) in addition to their username and password (first factor of authentication). The advantage of adding a second factor of authentication is that in the event that a user's credentials (username/password) are compromised, that alone will be insufficient for someone to gain access to sensitive university data. They would also need to gain possession of the user's phone in order to make use of the compromised credentials. CU uses Duo Security [2] to provide this second factor of authentication and increase the protection of university data.

Factors of Authentication

1. Something you know
    1. Username and Password/Passphrase
    2. PIN
    3. Answering Security questions
2. Something you have
    1. Device such as a phone, token, security badge, etc.
3. Something you are
    1. Biometrics such as fingerprint scan, retinal scan, etc.

CU Systems using MFA

- HCM
    - To protect sensitive user data users are required to authenticate using MFA to access certain self-service HCM pages within the university portal CU Resources tab.
    - Highly privileged users, such as certain IT staff and Employee Services staff with elevated access to the HCM system, are required to authenticate using MFA when logging into the HCM system.

Groups audience:
University Information Services

Links
[1] https://www.cu.edu/uis/access-it-security/identity-and-access-management/multi-factor-authentication-

mfa
[2] https://duo.com/