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

Multi-Factor Authentication: Added Protection from Cybercrime [1]

Multi-factor authentication (MFA), also referred to as two-factor authentication or two-step verification, is a crucial security feature designed to verify your identity before granting access to your accounts.

How MFA works

When you log into an online account, you usually provide a username and password. With

MFA enabled, you'll need to complete an additional verification step. Typically, this involves entering a one-time code sent to your email or texted to your device, which must be used within a limited timeframe.

Other MFA methods can include:

- Extra PIN (personal identification number)
- Answer to a security question such as your place of birth
- Biometric data like facial recognition or fingerprints
- Unique code generated by an authenticator app
- Secure token that confirms your identity through a database or system

Activate MFA when available

It's wise to enable MFA on every account or app that offers it. As MFA becomes increasingly common, it's important to use it for personal accounts such as banking, email, social media, and online shopping. Many workplaces, including CU, also provide MFA options.

Is it worth the extra step of MFA?

Absolutely! It only takes a moment but greatly enhances your security against cybercriminals, even if they have your password.

Learn more about MFA

Visit your campus website for specific guidance.

- CU Anschutz [2]
- CU Boulder [3]
- CU Denver [2]
- UCCS [4]
- System Administration [5]

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime
[2] https://www.cuanschutz.edu/offices/information-security-and-it-compliance
[3] https://oit.colorado.edu/services/it-security [4] https://oit.uccs.edu/security [5] https://www.cu.edu/uis