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

Best practices for strong password security and management [1]

October 16, 2025 by ES and UIS Communications [2]

Phishing scams and data breaches grow more sophisticated every year. Your password is the first defense against unauthorized access to personal and institutional data. Whether signing in to your University of Colorado account or personal apps, following strong password practices is one of the easiest ways to protect yourself.

1. Use passphrases – not just passwords

Longer is stronger. Instead of short, complex strings that are hard to remember, it's better to create passphrases — random words strung together.

Example: Buffal0-Galaxy-Watermelon-Sunris5

Avoid using personal information, predictable patterns or phrases you’ve used elsewhere. The key is length and randomness, not special characters alone.

NOTE: Remember the minimal requirements for your CU System account password:

- At least one capital letter.
- At least one numeral.
- At least one special character.
- At least 12 characters in length.
- Cannot be one of your previous passwords.

2. Use passkeys where available

Many major platforms, including Google, Apple and Microsoft, now support passkeys, a new login method that replaces traditional passwords with encrypted, device-based authentication.

Passkeys are:

- Easier to use (no remembering long passwords).
- Resistant to phishing.
- Protected by your device's biometrics (facial recognition, fingerprint or PIN).

3. Use a trusted password manager

A password manager securely stores and generates complex passwords for every site. You only need to remember one primary password or use biometric access.

Read our Consider using a password manager [3] tip for more information.

4. Enable multifactor authentication (MFA)

All passwords benefit from a second layer of security. Whenever possible, enable MFA — especially for CU accounts, banking and social media.

MFA adds a quick verification step (like a code from an app or push notification) that keeps your account protected even if your password is compromised.

Review Using multifactor authentication (MFA) to stay safe online [4] for full guidelines and instructions.

5. Avoid reuse and rotation pitfalls

- Use unique passwords for each account. Reusing a password allows one breach to expose them all.
- Focus on using strong, unique passwords, rather than relying on frequent password changes.
- Use your password manager to audit reused or weak passwords and update them.

Check out how this tip plays out in a real-life scenario in When Password Reuse Opens the Door [5] from the Office of Information Security.

6. Stay alert for scams

Even the strongest passwords can’t protect you if you share them. Be cautious of:

- Unexpected password reset emails.
- Login pages that don’t end in .edu or an official domain.
- Messages asking for your CU or personal credentials via email or text.

If you’re unsure, contact the UIS Service Desk [6] before clicking any links. Read our Spot and stop phishing scams [7] tip for up-to-date guidance on staying vigilant against phishing.

Strong passwords and safe habits protect not only your own personal data but the entire CU community. Use long, unique passphrases, consider passkeys and password managers, and enable MFA to stay secure.

Learn more

- Visit the Office of Information Security [8] for CU’s official security standards and resources.
- Reset your CU account password anytime through the self-service password reset portal [9].

cybersecurity [10], password [11]
Display Title:
Best practices for strong password security and management

Send email when Published:
No

Source URL:https://www.cu.edu/blog/tech-tips/best-practices-strong-password-security-and-management-0

Links
[1] https://www.cu.edu/blog/tech-tips/best-practices-strong-password-security-and-management-0
[2] https://www.cu.edu/blog/tech-tips/author/166688 [3] https://www.cu.edu/blog/tech-tips/consider-using-password-manager-1 [4] https://www.cu.edu/blog/tech-tips/using-multifactor-authentication-mfa-stay-safe-online [5] https://www.cu.edu/security/administrative-assistant-when-password-reuse-opens-door
[6] https://www.cu.edu/service-desk/about#contact [7] https://www.cu.edu/blog/tech-tips/spot-and-stop-phishing-scams [8] https://www.cu.edu/security [9] https://www.cu.edu/blog/uis-news/locked-out-your-account-password-expired-reset-your-password-without-uis-service-desk [10] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [11] https://www.cu.edu/blog/tech-tips/tag/password