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

Best practices for strong password security and management [1]

September 16, 2024 by ES and UIS Communications [2]

The University of Colorado is proud to be a champion of cybersecurity. This October, during Cybersecurity Awareness Month [3] — the global effort to help everyone stay safe and protected when using technology whenever and however you connect—the Office of Information Security, University Information Services and campus OITs are promoting key behaviors to encourage every employee to stay safe online.

Using long, complex passwords is one of the easiest ways to defend yourself from cybercrime. Combined with the usage of password manager, creating a strong, randomized password is the best choice for minimizing the chances of a security incident.

Follow these best practices to create a strong password:

1. Make your passwords hard to guess.

Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

2. Avoid using common words.

Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L." Get creative. Use phonetic replacements, such as "PH" instead of "F". Or make deliberate, but apparent misspellings, such as "enjin" instead of "engine."

3. Unique account: unique password.

Having different passwords for various accounts helps prevent cybercriminals from gaining access to these accounts and protects you in the event of a breach. It's important to mix things up — find easy-to-remember ways to customize your standard password for different sites.

4. The more random, the better.

As a rule of thumb, the more random and mixed case (i.e. uppercase and lowercase, symbols and numbers) your password is, the harder it will be to guess or crack with cyberattack tools. For example, the password "Ralphie!" would take only two hours to crack using brute force tools, while the randomized password "Km@6Pn!20$Ga" would

take four hundred thousand years, according to the Security.org secure password checker.

For your CU System account password, the minimal requirements are:

- 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.

NOTE: If you've been locked out of your account or have forgotten your password, you can reset your password by following these self-service password instructions [4]. If you experience any issues, contact the UIS Service Desk at 303-860-4357 (HELP).

cybersecurity [5], password [6], new employees [7]
Display Title:
Best practices for strong password security and management
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/best-practices-strong-password-security-and-management
[2] https://www.cu.edu/blog/tech-tips/author/110439 [3] https://www.cu.edu/security/cybersecurity-awareness-month [4] https://www.cu.edu/docs/how-reset-your-cu-system-account-password
[5] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [6] https://www.cu.edu/blog/tech-tips/tag/password
[7] https://www.cu.edu/blog/tech-tips/tag/new-employees