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

Are You Taking These 10 Steps to Keep Data Safe? [1]

As the risk of cyberattacks grows, we all play a crucial role in keeping CU's data secure, whether working from the office or remotely. By adopting these simple yet crucial steps, we can significantly reduce the risk of cyber threats and ensure the security of our confidential data.

1. Use strong, unique passwords

Weak passwords make it easy for cybercriminals to gain access to your accounts. Create strong passwords by using passphrases, combining random numbers, letters, and symbols. Avoid reusing passwords across multiple sites, as a single compromised password can put all your accounts at risk. Password managers can help you manage complex passwords safely. Never share your password, write it down, or allow your browser to save it automatically.

Visit Can Your Passwords Withstand Cybercrime [2] for more information.

2. Enable multi-factor authentication (MFA) and use a VPN

Multi-factor authentication (MFA) adds an extra layer of protection by requiring an additional verification step, like a one-time code or biometric data. Enable MFA wherever possible, especially for sensitive accounts like email and banking. Additionally, use a Virtual Private Network (VPN) for added security. It encrypts your connection, which is crucial when accessing the internet on public Wi-Fi.

Visit Multi-Factor Authentication: Added Protection from Cybercrime [3] for more information.

3. Be cautious with email attachments and links

Cybercriminals often use emails with malicious links or attachments to trick you into giving away valuable information. Never share your username, password, or confidential details in response to unsolicited emails or phone calls. Verify the legitimacy of any email requests before clicking links or opening attachments and be wary of urgent threats or offers that seem too good to be true.

Visit Avoid Being a Phishing Scam Victim [4] for more information.

4. Keep software and apps updated

Software updates often include security patches that protect against new vulnerabilities. Always install the latest updates for your operating systems and apps to ensure your devices are secure. Stick to university-approved applications to reduce the risk of malicious software and consult your campus IT team before installing new software.

5. Use university-provided computers

When accessing or handling confidential university data, only use university-provided computers and devices. If you must use a personal computer, it’s safer to use remote desktop services to connect to your university computer. This reduces the risk of exposing sensitive data on unprotected devices.

6. Understand and protect university data

If you handle confidential university data, such as health information, student records, or financial details, you are responsible for protecting it. Share this data only with those who have a legitimate need to know and ensure you’re encrypting it when transmitting or storing it. Always be mindful of data security when sending emails, checking recipients carefully before hitting "send." Consult your supervisor if you are uncertain about the data you are working with.

Visit Data Classification [5] for examples of public, confidential and highly-confidential data.

7. Follow university guidelines on artificial intelligence (AI)

AI tools can provide valuable support, but they come with risks. Be sure to follow the university’s guidelines and policies when using AI to avoid compromising data or systems. Stay informed about potential security risks and ensure you're using AI tools in a responsible and secure manner.

Visit Explore Resources on Using Artificial Intelligence at CU [6] for more information.

8. Complete required security training

CU provides online courses to help you understand best practices for keeping our systems and data secure. Completing these courses helps you stay up to date with the latest security protocols and your role in keeping a safe digital environment.

Visit Available Training [7] for a list of required and recommended courses.

9. Report potential incidents immediately

If you suspect a security incident, report it promptly to your campus IT or information security team. Early detection is key to containing any potential damage. Be proactive—delaying a report can make an incident harder to resolve.

Visit Reporting an Incident [8] for more information and your campus contact information.

10. Trust your instinct

If something feels off, trust your instincts. Whether it's an unexpected email, a suspicious link, or unusual behavior on your devices, report it to your campus IT or information security team and they will investigate it.

Learn about information security on your campus

Each campus employs an information security officer along with other security staff to safeguard data. They evaluate risks, implement security protocols, and address security incidents. It is advised that you bookmark this webpage should you need to contact them later.

Updated 3/7/2025

Groups audience:
Office of Information Security
Right Sidebar:
Information Security Campus Contact
IT Departments Campus Contact

Links
[1] https://www.cu.edu/security/are-you-taking-these-10-steps-keep-data-safe
[2] https://www.cu.edu/security/can-your-passwords-withstand-cybercrime
[3] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime
[4] https://www.cu.edu/security/avoid-being-phishing-scam-victim [5] https://www.cu.edu/data-governance/resources-support/data-classification [6] https://www.cu.edu/security/explore-resources-using-artificial-intelligence-cu [7] https://www.cu.edu/security/awareness/available-training
[8] https://www.cu.edu/security/reporting-incident