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

Reporting a cybersecurity incident [1]

October 28, 2024 by ES and UIS Communications [2]

The University of Colorado is a proud champion of Cybersecurity Awareness Month, and we appreciate everyone's participation in this month's activities.

Remember, you can still complete the Information Security Awareness Skillsoft Percipio course by Oct. 31 for a chance to win $100. Ten winners will be chosen at random and notified in early November.

Cybersecurity awareness is a daily task. Even though Cybersecurity Awareness Month is ending, you can still get involved by visiting CU's Cybersecurity Awareness Month web page [3] .

Cybersecurity incidents happen, but every CU employee has to stay informed and vigilant against security threats, from phishing to data compromises.

Potential cybersecurity threats are constantly evolving in sophistication and complexity. Examples of potential security incidents may include:

- Loss or theft of university-issued or personally owned devices or physical media (e.g. data storage peripherals, hard drives, paper files) storing CU sensitive information.
- Suspected virus or malware.
- Unauthorized access or changes to systems, software or sensitive information.
- Compromised user account.
- Accidental exposure of sensitive information (e.g. misdirected email, paper left on a printer, device left open and unlocked).

I think I may have encountered a cybersecurity incident. What do I do now?

Immediately report the potential incident, even if you are not sure. Immediately reporting potential incidents allows the proper information security teams to act quickly, determine the level of impact and contain the incident – saving valuable time and limiting negative impacts to CU. Visit the Report an Incident [4] web page.

If a security incident happens, no retaliation will be taken against anyone who reports a potential incident in good faith. This is why you should report any incident you believe may be a security threat. There is no harm in being extra vigilant.

Be sure to include the following information in your security report:

1. Contact information

2. College or department involved
3. Brief description of what happened
4. General description of the type of information involved
    1. Was it sensitive, confidential or highly confidential university information?
    2. Was it shared with or accessed by unauthorized people?
5. General description of the impact of the incident, if known
6. Any other known resources affected or other information about the incident

Visit the Reporting an Incident web page [4] for more information.

cybersecurity [5]
Display Title:
Reporting a cybersecurity incident
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/reporting-cybersecurity-incident [2] https://www.cu.edu/blog/tech-tips/author/110439 [3] https://www.cu.edu/www.cu.edu/security/cybersecurity-awareness-month [4] https://www.cu.edu/www.cu.edu/security/reporting-incident [5] https://www.cu.edu/blog/tech-tips/tag/cybersecurity