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

Cybersecurity is a year-round priority for everyone at CU



October 21, 2022 by ES & UIS Communications

University Information Services is proud to collaborate with campus OITs and the Office of Information Security on Cybersecurity Awareness Month, a global effort to help every day users learn how to protect sensitive information when using technology whenever and however they connect.

We each have a crucial role to play in cybersecurity. This year's campaign focused on key security topics every CU employee should know about: Passwords, Multi-Factor Authentication, Phishing and Data Classification.

Passwords & Password Manager

Having unique, lengthy and complex passwords is one of the best ways to immediately improve your cybersecurity. Additionally, you can use a password manager to generate and securely store strong passwords so you don't have to remember them all.

Video of Passwords Video Infographic.mp4

Additional Password Resources:

- Do You Use Any of These Passwords? [1]
- Tech Tips on Password Managers [2]
- Five Reasons to Avoid Password Reuse [3]
- Take the Password Test [4]

Multi-Factor Authentication

Multi-factor authentication, or MFA, is a security measure that requires anyone logging into an account to verify their identify by inputting an additional security key, such as a randomized code sent to their phone or generated by an app. This extra step ensures that it is twice as hard for someone to access your online account without authorization. When MFA is available, always turn it on because it is both easy to use and incredibly effective. Data shows us that over 99% of account hacks could have been prevented by use of MFA.

Video of What does MFA mean?

Additional MFA Resources:

- Tech Tip on MFA and Smart MFA [6]
- Six Reasons You Need Multi-Factor Authentication [7]

Phishing

Phishing is a tactic where a cybercriminal poses as a legitimate party in hopes of convincing individuals to engage with malicious content or voluntarily sharing sensitive information. Phishing remains one of the most popular tactics among cybercriminals today.

However, while phishing has gotten more sophisticated, keeping an eye out for typos, poor graphics, convoluted email address and other suspicious characteristics can be a telltale sign that the content is potentially coming from a fraudulent sender.

Video of Phishing

Additional Phishing Awareness Resources:

- Tech Tip: How to report any phishing emails to Microsoft [9]
- Cybercriminals Like to Phish - Don't Take the Bait [10]
- Phishing Scams FAQs [11]

Data Classification

Correctly lassifying or labeling CU information helps determine the security requirements necessary to keep it safe. Information classified as Highly Confidential and Confidential must be protected from compromise, such as unauthorized or accidental access, use, modification, destruction, or disclosure. What type of information do you manage?

Additional Data Classification Resources:

- CU Data Classification [12]
- Classify and Comply: Understanding your data is the first step to protecting it [13]
- Incident Reporting [14]

Looking Ahead

Cybercrimes continue to rise annually. Since our university runs on data, we rely on strong cybersecurity to protect that data. Every employee at CU has a role to play in that security — by employing MFA and signing onto the VPN daily, being vigilant about phishing emails, using strong passwords, and staying knowledgeable about the classification of the data they use.

Behind the scenes, UIS continues to mitigate security risks by installing critical patch updates, upgrading enterprise software and strengthening our network infrastructure. In collaboration with the campuses and the Office of Information Security, UIS is committed to keeping your data protected!

Display Title:

Cybersecurity is a year-round priority for everyone at CU

Send email when Published:

No

Source URL:https://www.cu.edu/blog/uis-news/cybersecurity-year-round-priority-everyone-cu

Links

[1] https://www.cu.edu/security/do-you-use-any-these-passwords [2] https://www.cu.edu/blog/tech-tips/use-strong-passwords-and-password-manager [3] https://expertinsights.com/insights/5-reasons-you-should-never-reuse-passwords/ [4] https://www.cu.edu/security/take-password-test [5] https://www.cu.edu/file/what-does-mfa-mean-what-does-mfa-mean [6] https://www.cu.edu/blog/tech-tips/multi-factor-authentication-and-smart-mfa [7] https://expertinsights.com/insights/6-reasons-you-need-multi-factor-authentication-mfa/ [8] https://www.cu.edu/file/phishing-phishing [9] https://www.cu.edu/blog/tech-tips/report-any-phishing-emails-uis-and-microsoft [10] https://www.cu.edu/security/cybercriminals-phish-dont-take-bait [11] https://www.cu.edu/security/awareness/phishing-scams-faqs [12] https://www.cu.edu/security/data-classification [13] https://www.cu.edu/security/classify-and-comply-understanding-your-data-first-step-protecting-it [14] https://www.cu.edu/security/reporting-incident