2022 Cybersecurity Awareness Month [1]

It’s Easy to Stay Safe Online

October is Cybersecurity Awareness Month, a global effort to help everyone stay safe and protected when using technology whenever and however you connect. The theme for the month is "It’s easy to stay safe online" and the University of Colorado is proud to be a Champion and support this online safety and education initiative again this year. Throughout the month, CU will raise awareness of key best practices that we can implement today to enhance cybersecurity and create a more secure world for everyone.

Cybersecurity Threat Prevention and Awareness Round Table

Experts from across CU review top cyber threats, the current cybersecurity climate of the university, and answer attendees’ questions. View the Oct 6 recording [2].

Week 1: Recognize phishing, which is still among the primary threats from cybercriminals.

Phishing – when a cybercriminal poses as a legitimate party in hopes of getting individuals to engage with malicious content or links – 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 and other suspicious characteristics can be a telltale sign that the content is potentially coming from a phishing scam.

- Cybercriminals Like to Phish - Don't Take the Bait [3]
- Phishing Scams FAQs [4]
- Video: Email and Phishing [5]
- Video: Phishing Emails in Real Life [6]

Week 2: Know the classification and sensitivity of the CU data you manage and how to keep it safe.

Classifying or labeling CU data helps determine the security requirements necessary to keep it safe. Data 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 data do you manage?

- Classify and Comply: Understanding your data is the first step to protecting it [7]
Week 3: Create strong, unique passwords and change them regularly.

Having unique, strong, and complex passwords is one of the best ways to immediately boost your cybersecurity. Cracking passwords is one of the go-to tactics that cybercriminals use to access value information. And, if you use the same password on multiple accounts, once a cybercriminal has compromised one of your accounts, they can easily do the same on other accounts.

- Do You Use Any of These Passwords? [8]
- Take the Password Test [9]
- Video: Top 10 Most Entertaining Passwords [10]
- Five Reasons to Avoid Password Reuse [11]

Week 4: Enable multi-factor authentication and learn why it’s important.

Enabling multi-factor authentication (MFA) – which prompts you to input a second set of verifying information, such as a secure code sent to a mobile device – is a hugely effective measure that anyone can use to drastically reduce the chances of a cybersecurity incident.

- Multi-Factor Authentication: Added Protection from Cybercrime [12]