INFORMATION TECHNOLOGY
COLORADO STATE UNIVERSITY

CSU PUEBLO

Hello CSU Community!

During week three, we're focusing on passwords and understanding password managers. Passwords are the keys to your digital castle. Creating, storing, and remembering passwords can be a pain, but the truth is that passwords are your first line of defense against cybercriminals and data breaches. Just like with your house keys, you want to do everything you can to keep your passwords safe.

The key is complexity. According to the World Economic Forum, a 12-character password with only numbers takes 25 seconds to crack. While a 12-character password containing at least one upper case letter, one symbol, and one number would take 34,000 years for a computer to crack.

Watch - The Password Stats:

PASSWORD MANAGERS

As we do more online, we've gone from having just a couple of passwords to now dealing with with hundreds. While people may use the same password for most accounts— that's ***NOT*** safe. If your one password gets stolen because of a breach, it can be used to gain access to all your accounts and sensitive information. However, using a password manager can enable you to be more secure online.

A password manager is software created to manage all your online credentials like usernames and passwords. It stores them in a safe, encrypted database. It also generates new passwords when needed. Most password managers will automatically identify weak and duplicate passwords and reconfigure them into stronger, more well-designed ones. Because the password manager stores all your passwords, you don't need to memorize hundreds of passwords. You only need to remember one super strong password to unlock your password manager app. It couldn't be easier.

Password managers also automatically update the password changing process. Meaning that you won't have to manually update passwords yourself, saving you time.

Password Manager Types:

There are two types of password managers for individuals; **Freestanding**, these managers are managed from one device and do not communicate with other devices. **Cloud-Based**, these managers have a master password to access your vault and can sync with your other devices. Both have pros and cons depending on your needs but there are standard best practices to use password managers:

If you use a password manager be sure to:

1. Always enable Multi-Factor Authentication. MFA adds another layer of security to your password manager.
2. DO NOT enable "Remember My Password." Most browsers offer this option which can compromise your accounts if your device is hacked.
3. DO NOT put all of your passwords in one password manager. A common tip is to separate your most important accounts from each other. So if the password manager is ever hacked, you won't have all of your accounts compromised.

Week Three Event Calendar:

October 17	October 19	October 20 FTC campus	October 21 - FTC Campus	October 21-23
Learn about the CSU Cybersecurity Internship	Advanced Security Practices for Researchers	Hashdump Security Club: Understanding Passwords and How to use Password Managers	Cybersecurity Games and Fun on the LSC Plaza	National Cyber League Individual Game

Hashdump Highlight:

Hashdump is a student information security club on the Fort Collins campus. Their goal is to increase awareness of physical, social, and electronic security. The club participates in various security competitions, hosts demos and workshops, and invites speakers to come and share real world experiences. For more information or to join, visit the Hashdump website.

Learn more about cybersecurity at each campus.

Fort Collins: it.colostate.edu/cybersecurity
Pueblo: https://www.csupueblo.edu/information-technology/security/index.html

CSU SYSTEM
COLORADO STATE UNIVERSITY