Cybersecurity Matters:
The role of computers and networks in our everyday lives has made protecting data and adding security an important issue. Most data transmitted over a network is sent in clear text making it easy for unwanted persons to capture and read sensitive information.

Additionally, there are legal and ethical restrictions that impact districts, county offices of education, schools and teachers alike. Traditionally, student data consisted of attendance, grades, discipline records, and health records. This information was restricted to a select group of individuals.

Presently, data is now shared through Student Information Systems (SIS) and many other forms of technology.

Cybersecurity Tips:

What to Do to Prevent Data Breaches

- Use unique and strong passwords.
- Safeguard your usernames and passwords.
- Don't treat public computers like personal computers.
- If it isn't your computer don't allow a web browser to save your password and completely log out every time.
- Don't click on links or open attachments in emails unless you know who sent them and what they are.
- Treat your mobile devices like you would cash and do not leave them in vehicles or in the open "for just a sec."
- Invest in flash drives with security features like encryption &/or locking devices.

Ways to Help Determine If You've Been Hacked

- Colleagues are receiving emails or messages you didn't send.
- Your sent messages folder has messages you didn't send, or it has been emptied.
- You cannot log into your email.

Encryption is a "Key" Factor

Encryption is a formula used to turn data into a secret code. Each algorithm uses a string of bits known as a "key" to perform calculations. The larger a key is (the more bits in the key), the greater the number of potential combinations that can be created, thereby making it more difficult to break the code and unscramble the contents.

Image courtesy of Dell.com

Those in need of an encrypted USB drive should contact the LACOE Helpdesk to request Technology equipment.