For Flash Drive encryption, we are going to recommend Windows BitLocker which is built into Windows. The important thing to note is that a flash drive can only be encrypted on a non-home version of Windows, which means that, depending on the version of Windows that students have on their computers, they most likely will not be able to set up the encryption on their own computers. But, once the encryption has been set up, it works on any version of Windows 7, 8 and 10. Here are the steps to Encrypt; it will be best to have students do this on one of our lab/classroom computers:

- Plug their USB drive into the computer
- Go to Start (Windows icon) > Computer
- Right-click on their flash drive and select Turn on BitLocker
- Select the option to “Use a password to unlock the drive.” Enter the password that you want to use. Please note that the encryption is only as strong as the password, so we recommend selecting a password with a mix of capital/lower case letters and numbers. If the password is lost or forgotten, it is not possible to retrieve the password or restore the contents of the drive.
- Select Next. Please note that depending on the size of the flash drive, it may take a while to encrypt. While testing this here, it took about 5 minutes to encrypt a small 2GB drive.

After setting this up, you will be prompted to enter the password before opening the drive on any computer. Please note that this will not work on Mac computers.