Passwords and Security

macOS Security

For macOS computers (MacBooks, MacBook Airs, MacBook Pros, and iMacs), we'll go over the following kinds of security in detail: access management, device security, and data security

macOS Device Security

Find My Mac

If your Mac is lost or stolen, Find My Mac pretty much the only way to get it back. Find My Mac allows you to locate your lost or stolen Mac on a map, as well as lock your Mac remotely or erase your data from your device remotely. If your Mac has been lost or stolen and is not currently online, you can send it the lock or erase commands, and the next time your Mac connects to the internet it will perform the commands you've sent it.

To Enable Find My Mac...

1. Navigate to **Apple** menu > **System Preferences...**
2. Click on **iCloud** (3rd row, 1st column)
    - If you're not already signed in with your Apple ID, do so.
3. Scroll down to the bottom of the list of iCloud items on the right, and check the box next to **Find My Mac**. It will inform you that Find My Mac will use location services.
4. You're done.

Physical Security: Kensington Locks

In the past, Apple laptops used to have Kensington lock slots on them to add a layer of physical security to your device. With the introduction of the MacBook Air, they began phasing out Kensington locks on their products; currently the only macOS devices they sell with a Kensington lock slot are the iMacs.

While it is possible to get Kensington lock adapters to attach to current generation Mac laptops, LIS does not provide them. It is your responsibility to make sure devices issued to you by the college are not lost or stolen.

macOS Data Security

Data Encryption via FileVault

Every copy of macOS comes with free drive encryption in the form of FileVault. FileVault encrypts your drive quickly and easily. Once it's turned on, you won't know it's there. It's important to keep a copy of your drive's recovery key, in case you need to decrypt the drive in the future for any reason.

If you store PCIs on you Mac, your Mac must be encrypted with FileVault and LIS must have a copy of your recovery key.

Passwords and Security

All new faculty and staff machines will be issued with FileVault encryption enabled by default, and LIS will store a copy of your recovery key, in case of emergency.

To Enable FileVault...

1. Navigate to **Apple** menu > **System Preferences...**
2. Click on **Security & Privacy** (1st row, 6th column)
3. Click the lock icon and enter your computer password.
4. Click the **FileVault** tab.
5. Click the **Turn On FileVault...** button.
    - If you're prompted to restart your Mac, save any work you have open on your Mac, then let it restart, and go through steps 1-4 again.
6. You will be asked how you want to unlock your Mac if you have to reset your computer login password. Select **Create a recovery key and do not use my iCloud account**, the second option. Write down the recovery key and store it in a safe, secure location that will be accessible to you if you can't access your computer's files, then click **Continue**.
7. You will be prompted to enable other users. It's advisable to have the LIS user enabled; contact LIS and setup an appointment. When all users have been enabled, click **Continue**.
8. Click **Restart**.
9. You're done. Your computer will encrypt your drive in the background while you work. You may notice your computer's fans spinning up randomly while you work, but it's nothing to worry about. To check on the progress of the encryption, repeat steps 1-4, and there will be a progress bar with a time estimate.

Encrypted Time Machine Backups

Your data is important. Carthage's data is important. It's important that you have at least one backup of your data, in case something happens to your Mac. Just like it's a good idea for your Mac's internal drive to be encrypted, it's a good idea for your Time Machine backup to be encrypted as well.

If you store PCIs on your Mac, your Time Machine backup must be encrypted as well, and LIS must have a copy of your Time Machine backup's password.

All new faculty and staff machines will be issued with Time Machine backup drives that are encrypted default, and LIS will store a copy of the Time Machine backup drive's password, in case of emergency.

Encrypting an existing Time Machine backup requires a spare drive and monkeying around with permissions settings, so it's best to make an appointment with someone in LIS to have your Time Machine backup encrypted for you. The process only takes a few hours, and if you make the appointment for the morning, your Time Machine backup will be ready for you by that afternoon.

macOS Access Management

Passwords and Security

How to Lock your Mac's Screen

It's best practice to lock your Mac's screen if you're going to leave it unattended for any amount of time. That way, if someone tries to use your computer (or steals it), they can't get access to your personal data, or any of the college's sensitive data that might be stored locally on your computer.

To Enable Screen Lock

1. Navigate to **Apple** menu > **System Preferences...**
2. Click on **Security & Privacy** icon (1st row, 6th column)
3. Click the lock icon and enter your computer password.
4. Under the **General** tab, check the box next to **Require password immediately after sleep or screen saver begins**. If the dropdown menu in the middle of that setting is not set to immediately, click on it and set it to **immediately**.
5. You're done!

Unlike Windows, macOS doesn't have a built-in key combination to lock the screen, but it has something similar. When you've set the screen to lock as soon as sleep begins, you can trigger a screen lock by triggering sleep with the following key combination: **Command** + **Alt/Option** + **Power**.

Personally I find that key combination a little awkward and hard to remember, so I set up a hot corner to lock my Macs.

(Optional) Setup Hot Corner to Lock Screen

1. Navigate to **Apple** menu > **System Preferences...**
2. Click on **Mission Control** (1st row, 4th column)
3. Click on the **Hot Corners...** button in the lower left hand corner.
4. Click on one of the dropdown menus and select **Put Display to Sleep**, then click **OK**. I usually set the lower-left corner of my screen for this, and use the mnemonic "Lower Left = Lock."
5. You're done.

Google Apps, 2-Factor Authentication, and Your Mac

Everyone on campus will be required to enable 2-factor authentication for their Google Apps (i.e., your Carthage email) account. If you've setup your Mac to integrate with your Carthage Google Apps account (e.g., for your Carthage email, calendar, & contacts), you'll have to go through the 2-factor authentication process with your Mac as well.

Logging Into Google on your Mac

1. Navigate to **Apple** menu > **System Preferences...**
2. Click on **Internet Accounts** (2nd row, 2nd column)
3. In the list of services on the right, click **Google**.

4. Enter your full email address (e.g., rlahue@carthage.edu), then click **Next**.
5. Enter your Carthage password, then click **Next**.
6. Enter the code provided by your method of 2-factor authentication, then click **Next**.
7. Select which apps have access to your Carthage Google (email) account, then click **Done**.
    - **Mail.** LIS does not support using your Carthage email with an email client on your computer. LIS only supports using your Carthage email by logging into Gmail in a web browser. LIS will not provide technical support for issues you experience using an email client on your Mac. **Check this box at your own risk.**
    - **Contacts** will let you sync your Carthage Google contacts with your computer. It will not combine your iCloud and Carthage Google contacts together. **You can check this box if you'd like.**
    - **Calendars** will let you use your Mac's built-in Calendars app to view and edit your Carthage Google Calendar. **You can check this box if you'd like.**
    - **Messages** used to let you use Google Chat with the Messages app on your Mac. Google shut down Google Chat and replaced it with Google Hangouts, which uses a different messaging protocol and is not compatible with Messages or any 3rd party chat client (e.g., Adium). **Uncheck this box.**
    - **Notes** used to let you use the information that Google stored in the Notes section of your IMAP Google account. Google's implementation of IMAP is extremely non-standard, and with the rise of Google's products like Google Keep, it's unlikely that you'll get any use out of syncing your Carthage Google "notes" with the Notes app. **Uncheck this box.**

Unique solution ID: #1471
Author: Richard LaHue
Last update: 2017-07-11 21:10