Smartphones store a lot of personal information, including email or social media accounts, reminders and notes, the number of steps we take each day, and even personal biometric data, such as fingerprint. While all this can make life easier, abusers and stalkers can also misuse this information to monitor, control, and harass victims. In the United States, 71.6% of mobile users have a smartphone, and of those, 94 million devices were iPhones as of 2015.[1] This guide will help users enhance their iPhone's security and privacy by explaining the built-in privacy and security mechanisms on the iPhone and associated accounts.

Apple ID

The first time you purchase an iPhone or iPad, you must create an Apple ID. This ID is used for everything that you do with Apple, including shopping in the iTunes or App Store, accessing iCloud services, using iMessage or FaceTime, or contacting Apple support. Your Apple ID is typically an email address – it can be a personal email address or an email address that ends with @icloud.com (which is also used to access your iCloud Account) or @me.com.

It is possible to add alternative Apple IDs or emails associated with your account. To see which emails are associated with your account, log into your account to manage your Apple ID. From a computer, go here: https://appleid.apple.com/account/home and log in with your Apple ID and password. Once logged in, you can delete old email addresses that you're no longer using and ensure that no other additional emails were added. Here, you can also update passwords, security questions, and other contact information. When updating or creating new passwords, use a strong password, one that others can't guess, and change it if you suspect that someone else may know it. Here is more information and tips on creating passwords: http://techsafety.org/passwordincreasesecurity.

iCloud Services

Most iPhone users also use Apple's iCloud services, which is a cloud-based service that allows users to store their music and other files, such as photos, apps, contacts, emails, and documents. Documents created in apps, such as presentations, spreadsheets, images, PDFs or other types of documents, can also be saved to iCloud Drive.

Access to iCloud can be through all connected Apple devices or by logging into the iCloud account from a computer. If you save your device back up to iCloud, after resetting or updating your phone, you merely have to sign back into your account for all your apps and settings to automatically reset on your device.

There are pros and cons to using iCloud services. On the benefit side, if you purchase a new device or need to reset your device, logging in using your Apple ID will automatically update your device with your

[1] http://www.cnet.com/news/nearly-100m-iphones-in-use-in-the-us-new-study-shows/

apps and settings the way you want it. If you're using iCloud Drive, you can also access the same documents or apps on other devices using the same Apple ID.

On the other hand, using iCloud means that your information is no longer only on one device but accessible from multiple places. Multiple access points can make your information more accessible and therefore, more vulnerable. If someone knew your Apple ID or your iCloud username/password, they might be able to access your data and information.

Some security and privacy measures include determining what of your information you want to be accessible from in the cloud or changing the password to your iCloud account. To select what information on your iPhone or iPad will back up to iCloud, on your device, go to Settings/iCloud, and select what data (Photos, Mail, Contacts, etc.) is backed up to your iCloud. Under that setting, you can also select what you want saved to iCloud Drive.

iPhone Settings

The iPhone itself has many settings that allow you to control access to information on your device. Although time-consuming, one of the ways to ensure that your phone is as private and as secure as possible is to go through each setting. This will help you learn what each setting does, how much control you actually have over your device, and how much information is stored and potentially shareable on your device. It's best to go through each setting; however, the following are some major privacy or section settings to start with.

Find My iPhone

If the "Find My Phone" feature is turned on in the device settings, users can find the location of the device by logging into iCloud. This feature is meant to help you find your device if it is lost or stolen; however, some people could use this feature to locate another person. Users concerned about their location privacy can turn off this feature on their device by going to Settings/iCloud and switch "Find My iPhone" to Off.

Family Sharing

The Family Sharing feature allows up to 6 different accounts to share iTunes, iBooks, and App store purchases; photos and videos; and a Family calendar. Each person needs to be invited and accept the invitation to be part of the Family Sharing group. The Family Organizer is responsible for paying for purchases initiated by other family members and could deny purchases. Purchased content can be shared with anyone in the Family Sharing group.

When joining Family Sharing, you will be asked if you want to share your location information. You can always turn this feature off by going to Settings/iCloud/Share My Location; the setting allows you to determine which family member can or cannot see your location.

Location Settings

Many apps want access to your iPhone/iPad's location. For the most part, you can control which app can access your location information by going to Settings/Privacy/Location Services. There, you can turn off all location services or manually turn off location access for individual apps. Our recommendation is that if you're not using the app, turn off the location. You can always turn the location back on when you need to use the app.

Another location setting to review is System Services, in which the iPhone uses your location information for other features or functionality. To access System Services, go to Settings/Privacy/Location Services and scroll to the bottom of screen and select "System Services." Minimizing location information access here will also help conserve battery life.

Privacy Settings

Some apps want access to contacts, calendar, photos, or the camera. Under Settings/Privacy, you can allow or deny apps' access to other information on your device. Here, every app that's ever requested access to any information on your phone is listed, and you can control what information they access.

Specific App Settings

Toward the end of iPhone's Settings is a list of most of your apps. Under each specific app, you are given additional privacy settings. Also, remember that most apps have privacy, security, or notification settings within the app itself. Review all the apps you've downloaded, and make sure that the settings are set to your preferences.

Touch ID & Passcode

Under the General Setting/Touch ID & Passcode, you can update your Touch ID and passcode. You should always use a passcode on your devices so that if someone were to find your iPhone or iPad, they will need to have your passcode or fingerprint to access your device. iPhone 5s or later, iPad Pro, iPad Air 2, and iPad mini 3 or later all have Touch ID, which uses your fingerprint to access your device. In addition to the Touch ID, you can also set up a custom passcode that is either a 4-digit numeric code, a custom numeric code (that is longer than 4 digits), or a custom alphanumeric code (combination of numbers and letters). The more complex the passcode, the harder it will be for someone to guess.

Jailbreaking iPhones

Some people will "jailbreak" their iPhone, a process in which the hardware restrictions by Apple and wireless carrier are removed so that users can root access the iOS file system and manager, allowing them to download additional software and applications not available in the Apple App Store. This process will make the phone more vulnerable to malware and spyware. In fact, most (if not all) of the commercially available spyware products require a jailbroken iPhone to install.

One way to know if your iPhone is jailbroken is to access the Spotlight Search page (swipe down on your screen) and search for the Cydia app, which is one possible indication that your device might be jailbroken. If your phone is jailbroken or you believe that it is, do a restore of the device and make sure you are running the latest iOS on your device. This will remove software that was downloaded outside of the Apple App Store.

Final Tips

- **Have strong passwords.** Make sure you have a strong password and don't share it. If someone should find out your password, change it as soon as possible.
- **Limit access to your information.** Smartphones make it very easy to access your information from multiple devices. Weigh convenience and privacy and determine what is safest for you.
- **Log out of accounts.** If you're not using a particular app, considering logging off. It might be inconvenient to log back in each time you want to use it, but it will prevent someone from getting into your accounts.
- **Don't share your devices.** The safest option is to not use someone else's device and not share your own device. If you must borrow someone's device, ask to delete your personal information from the device once you're done, such as deleting the phone number you dialed or text message you sent. If you need to use the map app, rather than using the native mapping app (which could store your search), access the map via the web browser and turn on the browser's in-private mode feature. Don't forget to log out of any online accounts you accessed while on someone else's device.