iPhone Privacy and Security Guide

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

Please note: This handout is up to date as of December 2022. If you have a newer model or operating system, please check Apple's website for the latest capabilities.

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).

It is possible to add alternative Apple IDs or emails to your account. To see which emails are associated with your account, log in to your account using 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. Read more tips about passwords.

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, and PDFs can also be saved to iCloud.

Access to iCloud can be through all connected Apple devices or by logging in to the iCloud account (usually the same as your Apple ID) from a computer. If you save your device backup to iCloud, after resetting or updating your phone, you have to sign back in to 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 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. However, if you are setting up a new device to avoid monitoring from an abusive partner, updating your new device with the same apps and settings can be a risk. See Safely Setting Up and Activating a Phone for more details

On the other hand, using iCloud means that your information is accessible from multiple places rather than only on one device. 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.

Security and privacy measures include changing the password to your iCloud account or limiting which information you want to be accessible from the cloud. To select what information on your iPhone or iPad will back up to iCloud, go to Settings/iCloud on your device and select what data (Photos, Mail, Contacts, etc.) is backed up to your iCloud. Under that setting, you can also select what you want to be 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; the following are some major privacy 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 in to 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 switching 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 to turn off location access when you're not using the app. 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 and select "System Services." Minimizing location information access here will also help conserve battery life.

Privacy Settings

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

Specific App Settings

Scrolling down toward the end of your iPhone's Settings is a list of most of your apps. Under each specific app, you are given additional privacy settings. 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.

FaceID, Touch ID, and Passcode

Depending on the model of your iPhone, there will be options for FaceID, Touch ID, and passcode under General Settings. You can update your FaceID, Touch ID, and passcode there. You should always use a passcode on your devices to prevent anyone from picking up your device and going through it while unattended. 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. iPhone X or higher will have the FaceID option, which uses a mathematical model of your face so that you can scan your face to access your device. In addition to the Face ID and Touch ID features, you can also set up a custom passcode that is either a 4–6-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 the wireless carrier are removed (the equivalent term for Android devices is "rooting"). This allows for downloading additional software and applications that are not available in the Apple App Store. This process will make the phone more vulnerable to malware and spyware. 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.

Additional Tips

Have strong passwords. Make sure you have a strong password and don't share it. If someone learns 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 to determine what is safest for you.

Log out of accounts. If you're not using a particular app, consider logging out. 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 a map app, 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.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource iPhone Safety and Privacy Guide.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada | Femmes et Égalité des genres Canada | Canada