Face ID Security

November 2017

Face ID Security Overview

With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data.

Face ID and passcodes

To use Face ID, you must set up iPhone X so that a passcode is required to unlock it. When Face ID detects and matches your face, iPhone X unlocks without asking for the device passcode. Face ID makes using a longer, more complex passcode far more practical because you don't need to enter it as frequently. Face ID doesn't replace your passcode, but provides easy access to iPhone X within thoughtful boundaries and time constraints. This is important because a strong passcode forms the foundation of your iOS device's cryptographic protection.

You can always use your passcode instead of Face ID, and it's still required under the following circumstances:

- The device has just been turned on or restarted.
- The device hasn't been unlocked for more than 48 hours.
- The passcode hasn't been used to unlock the device in the last 156 hours (six and a half days) and Face ID has not unlocked the device in the last 4 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a face.
- After initiating power off/Emergency SOS by pressing and holding either volume button and the side button simultaneously for 2 seconds.

When Face ID is enabled, the device immediately locks when the Sleep/Wake button is pressed, and the device locks every time it goes to sleep. Face ID requires a facial match—or optionally the passcode—at every wake.

The probability that a random person the population could look at your iPhone X and unlock it using Face ID is approximately 1 in 1,000,000 (versus 1 in 50,000 for Touch ID). For additional protection, Face ID allows only five unsuccessful match attempts before a passcode is required to obtain access to your iPhone. The probability of a false match is different for twins and siblings that look like you as well as among children under the age of 13, because their distinct facial

features may not have fully developed. If you're concerned about this, we recommend using a passcode to authenticate.

Face ID security

Face ID is designed to confirm user attention, provide robust authentication with a low false match rate, and mitigate both digital and physical spoofing.

The TrueDepth camera automatically looks for your face when you wake iPhone X by raising it or tapping the screen, as well as when iPhone X attempts to authenticate you to display an incoming notification or when a supported app requests Face ID authentication. When a face is detected, Face ID confirms attention and intent to unlock by detecting that your eyes are open and directed at your device; for accessibility, this is disabled when VoiceOver is activated or can be disabled separately, if required.

Once it confirms the presence of an attentive face, the TrueDepth camera projects and reads over 30,000 infrared dots to form a depth map of the face, along with a 2D infrared image. This data is used to create a sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the A11 Bionic processor's neural engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of your face captured across a variety of poses.

Facial matching is performed within the secure enclave using neural networks trained specifically for that purpose. We developed the facial matching neural networks using over a billion images, including IR and depth images collected in studies conducted with the participants' informed consent. We worked with participants from around the world to include a representative group of people accounting for gender, age, ethnicity, and other factors. We augmented the studies as needed to provide a high degree of accuracy for a diverse range of users. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. An additional neural network that's trained to spot and resist spoofing defends against attempts to unlock your phone with photos or masks.

Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:

- The mathematical representations of your face calculated during enrollment.

- The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching.

Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data.

How Face ID unlocks an iOS device

With Face ID disabled, when a device locks, the keys for the highest class of Data Protection—which are held in the Secure Enclave—are discarded. The files and keychain items in that class are inaccessible until you unlock the device by entering your passcode.

With Face ID enabled, the keys aren't discarded when the device locks; instead, they're wrapped with a key that's given to the Face ID subsystem inside the Secure Enclave. When you attempt to unlock the device, if Face ID recognizes your face, it provides the key for unwrapping the Data Protection keys, and the device is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Face ID subsystems to unlock the device.

When the device restarts, the keys required for Face ID to unlock the device are lost; they're discarded by the Secure Enclave after any conditions are met that require passcode entry (for example, after not being unlocked for 48 hours or after five failed Face ID match attempts).

To improve unlock performance and keep pace with the natural changes of your face and look, Face ID augments its stored mathematical representation over time. Upon successful unlock, Face ID may use the newly calculated mathematical representation—if its quality is sufficient—for a finite number of additional unlocks before that data is discarded. Conversely, if Face ID fails to recognize you, but the match quality is higher than a certain threshold and you immediately follow the failure by entering your passcode, Face ID takes another capture and augments its enrolled Face ID data with the newly calculated mathematical representation. This new Face ID data is discarded after a finite number of unlocks and if you stop matching against it. These augmentation processes allow Face ID to keep up with dramatic changes in your facial hair or makeup use, while minimizing false acceptance.

Face ID and Apple Pay

You can also use Face ID with Apple Pay to make easy and secure purchases in stores, apps, and on the web.

To authorize an in-store payment with Face ID, you must first confirm intent to pay by double-clicking the Sleep/Wake button. You then authenticate using Face ID before placing your iPhone X near the contactless payment reader. If you'd like to select a different Apple Pay payment method after Face ID authentication, you'll need to reauthenticate, but you won't have to double-click the Sleep/Wake button again.

To make a payment within apps and on the web, you confirm intent to pay by double-clicking the Sleep/Wake button, then authenticate using Face ID to authorize the payment. If your Apple Pay transaction is not completed within 30 seconds of double-clicking the Sleep/Wake button, you'll have to reconfirm intent to pay by double-clicking again.

Face ID Diagnostics

Face ID data doesn’t leave your device, and is never backed up to iCloud or anywhere else. However, if you contact AppleCare for support with Face ID, you may be asked if you want to provide Apple diagnostic information, including Face ID Diagnostics data. Enabling Face ID Diagnostics requires a digitally signed authorization from Apple that’s similar to the one used in the software update personalization process. After authorization, you'll be able to activate Face ID Diagnostics and begin the setup process from within the Settings app of your iPhone X.

As part of setting up Face ID Diagnostics, your existing Face ID enrollment will be deleted and you'll be asked to re-enroll in Face ID. Your iPhone X will begin recording Face ID images captured during authentication attempts for the next 7 days; iPhone X will automatically stop saving images thereafter. Face ID Diagnostics doesn't automatically send data to Apple. You can review and approve Face ID Diagnostics data—including enrollment and unlock images (both failed and successful) that are gathered while in diagnostics mode—before it’s sent to Apple. Face ID Diagnostics will upload only the Face ID Diagnostics images you have approved; the data is encrypted before it’s uploaded, and is immediately deleted from your iPhone X after the upload completes. Images you reject are immediately deleted.

If you don’t conclude the Face ID Diagnostics session by reviewing images and uploading any approved images, Face ID Diagnostics will automatically end after 90 days, and all diagnostic images will be deleted from your iPhone X. You can also disable Face ID Diagnostics at any time. All local images are immediately deleted if you do so, and no Face ID data is shared with Apple in these cases.

Other uses for Face ID

Third-party apps can use system-provided APIs to ask the user to authenticate using Face ID or a passcode, and apps that support Touch ID automatically support Face ID without any changes. When using Face ID, the app is notified only as to whether the authentication was successful; it can’t access Face ID or the data associated with the enrolled face. Keychain items can also be protected with Face ID, to be released by the Secure Enclave only by a facial match or the device passcode. App developers also have APIs to verify that a passcode has been set by the user before requiring Face ID or a passcode to unlock keychain items. App developers can:

- Require that authentication API operations don't fall back to an app password or the device passcode. They can query whether a face is enrolled, allowing Face ID to be used as a second factor in security-sensitive apps.
- Generate and use ECC keys inside Secure Enclave that can be protected by Face ID. Operations with these keys are always performed inside the Secure Enclave after the Secure Enclave authorizes their use.

You can also configure Face ID to approve purchases from the iTunes Store, the App Store, and the iBooks Store so you don't have to enter an Apple ID password. With iOS 11 and later, Face ID-protected Secure Enclave ECC keys are used to authorize a purchase by signing the store request.

November 2017