Anatomy of an iPhone

Apple iOS 8 has a lot of new features, including default data encryption, Apple Pay, and remote desktop to sync your iPhone and Mac. Here are some of the security concerns you need to watch out for.

Data Encryption

When you set a passcode on your iPhone, **all your data is protected by encryption**:

- Photos and videos
- Messages and attachments
- Email
- Contacts
- Call history
- iTunes content
- Notes and reminders

iCloud

If you sync your iPhone or iPad to your iCloud account, all your data is backed up to the cloud. That means it's safe if you lose your device and use remote lock and wipe. Make sure to set up **two-step verification (2SV)** on your iCloud account to keep it secure.

Touch ID

Instead of a passcode, you can use your fingerprint to unlock the device. Watch out though. The **fingerprint reader on the iPhone 5s** proved hackable with a stolen fingerprint.

Apple Pay

Apple Pay on the iPhone 6, iPhone 6 Plus and the Apple Watch allows you to pay with a credit card instantly with your device while holding the TouchID pad. **Can it be trusted**?

Trusted Pairing

If you plug your iPhone into the USB on a computer you can link your Mac and your iPhone and set up **trusted pairing**. Once trusted pairing is activated, your computer can be used to track your iPhone, share calls, and sync files.

MAC Addresses

MAC addresses are randomized in iOS 8 when your device scans for nearby Wi-Fi networks. This security improvement means location marketers can't read your Wi-Fi location history. But it only works if you set your device to not connect to Wi-Fi hotspots automatically.

SOPHOS

Sophos Secures iOS 8

Learn how to keep all your organization's mobile devices secure at **sophos.com/mobile**.