imits

Information Management / Information Technology Services

One person. One record. Better health.

Mobile Device Security Guide

imits
Information Management / Information Technology Services
One person. One record. Better health.

Contents

1. Preamble

This document describes actions that can be taken to enhance security and privacy of mobile devices.

2. Security Controls

The following measures will reduce likelihood of a breach of confidentially.

Control	
1	Enable auto-screen locking after 15 minutes non-use
2	Use complex passwords (blend of upper and lower case letters with numbers and characters)
3	Enable encryption on the device
4	Install file encryption app to encrypt specific files
5	Encrypt removable storage (example SD and MMC cards)
6	Ensure firmware is current and updates occur in a timely manner
7	Disable simple passcode feature
8	Enable "erase data feature. The device will wipe data after a defined number of failed logon attempts

9	Enable remote erasure feature.
10	Enable auto-screen locking after 15 minutes non-use
11	For sensitive personal information avoid using cloud storage services such as iCloud, Google Drive, OneDrive, DropBox etc.
12	If a cloud service is to be used, consider activating 2 step authentications. Sometimes referred to as multi-factor authentication or two factor authentication.
13	Consider a VPN service for end to end encryption.
14	When connecting to public, open, or untrusted Wi-Fi (e.g. in coffee shops or airports) use WPA2 encryption. Always confirm access point name and access code with an employee of the establishment you are in.
15	The device's memory and storage should be "wiped" prior to disposal or when it leaves the user's control for extended periods (e.g. 3rd party repair, retirement or donation).
16	Sensitive information that may need to be downloaded to the device for reading or printing should be deleted when no longer required.

3. Password guidance

Item	Setting
Minimum password length	Password should be a minimum of 8 characters.
Password complexity	Include lowercase and uppercase alphabetic characters, numbers and symbols. Passwords should contain characters from **three** of the following four categories: 1. Uppercase characters 2. Numeric digits (0 through 9) 3. Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ 4. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.
Password History	A password should not be re-used within 8 change cycles.
Account Lockout Threshold	An account should lock a user out after 10 invalid logon attempts. Note: Where mobile devices are involved, the device should auto-wipe after 10 failed login attempts.

4. Step by Step Guide "How to"

Full encryption for an iPhone or any iOS device is a quick and painless process. From start to finish it will only take about 30 seconds, which is a small price to pay for the peace of mind it offers. The steps below will work for any device running iOS 3 or newer, including iPad and iPod Touch devices.

How to encrypt an iPhone:

1. Open the Settings menu on your iPhone.
2. Go to Touch ID & Passcode (iTouch & Passcode in older versions of iOS)
3. Select "Turn Passcode On" option.
4. Create a strong alphanumeric password that's at least six characters long. If it's too weak, the iPhone will reject it. Optionally, use the following website to generate a strong password for you.
5. Return to the Touch ID & Passcode screen.
6. Scroll to the bottom.
7. You will see "Data protection is enabled" at the bottom, meaning your iPhone is secure.

That's it! With data protection enabled you'll have to enter your passcode every time you reboot or wake the device from sleep. It's an extremely small inconvenience when compared to the privacy you'll gain from full disc encryption.

Enable Erase Data

The Erase Data option sounds scary, but it's an extremely effective way to protect your iPhone from persistent evasive attacks, such as thieves who might steal your phone from a purse, backpack, or pocket. With this feature enabled your phone will wipe all data if someone enters an incorrect passcode ten times. No data means no leaks, so your identity stays safe.

Enable the Erase Data feature:

1. Open the settings menu.
2. Go to Touch ID & Passcode (iTouch & Passcode in older versions of iOS)
3. Scroll down to "Erase Data" and make sure it's switched on.

Set a Short Passcode Delay

Another simple but worthwhile security feature is the passcode delay. The moments between using your phone and when the passcode lock enables are critical, as your data is completely unprotected during that time. Setting the delay to zero instantly locks your device when you aren't using it.

Set the Passcode Delay to Immediate:

1. Open the settings menu.
2. Go to Touch ID & Passcode (iTouch & Passcode in older versions of iOS)
3. Set "Require Passcode" to "Immediately"

Remotely Erase Data

Lost and stolen iPhones are surprisingly common. People know the devices are valuable, as is the information contained within. There are a few features you can enable that help protect your data if you misplace your phone, starting with Apple's own locator service.

First, enable the phone location feature:

1. Go to Settings
2. Click on "iCloud"
3. Scroll to "Find My iPhone" and enable it.

If your iPhone is lost or stolen, you can locate it by visiting iCloud.com or by installing Find My iPhone on another iOS device. Both of these options show you a map with a precise location of your phone. From here you can either track down your device or take more drastic measures when necessary.

To locate a lost phone via the internet:

1. Go to iCloud.com/#find
2. Enter your Apple ID
3. Click "Find My iPhone"

If your device was stolen, follow the steps above to locate the iPhone, then choose the device from the selection menu. From here you can activate the remote wipe feature, which removes all data from the phone immediately.

Encrypting Your Backups with iTunes

The iPhone's passcode locking and encryption feature prevents data from being accessed while it's on the device. When you back up files on your computer through iTunes, however, they are stored in a raw format, making them a potential target for data loss. Fortunately it's easy to configure iTunes to encrypt all backup data stored on your PC.

Encrypt backups with iTunes:

1. With iTunes installed, plug your iPhone into your computer.
2. Click the iPhone's name in the Devices section of iTunes.
3. Click the "Summary" tab.
4. Click the box next to "Encrypt iPhone backups", then apply the changes.

It's worth noting that if you encrypt backups through iTunes, you'll only be able to access that information from the computer that created the encryption. Any other PC, even with iTunes installed and synchronized to your iPhone, won't be able to access the backups.

Does iCloud Encrypt Data?

Local iPhone encryption is separate from data shared with Apple's iCloud service. When you encrypt your device you control the decryption key in the form of your passcode, meaning you're the only person who can ever access that data. It's a slightly different story with iCloud backups, however.

Even with full device encryption enabled, information sent through iCloud must be decrypted first. Then, when the files reach the iCloud service, they're re-encrypted by Apple on Apple's servers. This affords more privacy than raw file storage, but it carries the privacy risk of removing the decryption keys from your control. Basically, Apple has the ability to decrypt your information, not you, not directly.

Apple has a tremendous record for respecting and protecting user data, but third party hacks are always a concern. If Apple's servers are breached your data can be compromised. This has happened in the past and resulted in personal material being released to the public. Although you'll lose the convenience of cloud-backed data restores, the smartest way to protect your private information is to disable iCloud and rely on local encryption you can control.

iPhone Encryption Doesn't Encrypt Internet Traffic – Use a VPN

Encrypting your iPhone protects against local data theft. Files are stored in an encoded format and are nearly impossible to decrypt, even if someone has access to your device. This offers a tremendous amount of data privacy, but one thing it doesn't do is protect information that is sent from your phone wirelessly.

When you're on an encrypted iPhone, files currently in use are decrypted so you can access them. This includes anything you happen to be doing online, such as e-mails or bank transactions. While some apps encrypt their traffic by default, the only way to ensure complete privacy is to use a virtual private network.

VPNs act like a tunnel between your iPhone and the internet. When you go online, raw data is sent to servers around the world along with details about your device and your location. With a VPN active this information is encrypted and unreadable, making your browsing and online activity secure once again.

Data Security when Selling an iPhone

When it's time to upgrade your iPhone, you'll likely sell or give away your old device. Before you do, make sure you remove all personal data from the iPhone, including Apple account information and any stray files stored on the device. The factory reset process only takes a few minutes to complete. Make sure you have backups of all your data before beginning, as the erasure can't be undone.

How to erase data from an iPhone:

1. If you have an Apple Watch paired with your iPhone, unpair it.
2. Back up your device through iTunes.
3. Sign out of iCloud and iTunes.
4. Go to Settings.
5. Navigate to General > Reset > Erase All Content and Settings
6. Enter your passcode and tap "Erase"
7. When the process is complete, your iPhone will no longer contain any personal data.

Encrypt Photos, Files, and Other Information

Encryption doesn't have to be an all or nothing affair. Some apps encrypt the data they send or store by default, providing a little bit of extra security for sensitive information. If you want to encrypt things like photos, notes, or downloaded files, however, you'll need to use a third party app.

Below is a selection of apps that offer a wide range of encryption options. Keep your cloud storage files safe, lock down your photos, and make sure your data stays your own.

Secure Filebox Encrypted File Manager

Secure Filebox was built to store a wide variety of data in a completely safe and 256-bit AES encrypted form. Organize and manage everything from photos to text files, voice recordings, and images, all from a single interface.

SAFE – Secure Email & Encrypted File Storage

SAFE provides native file encryption support for all of your iPhone documents. It also protects data sent across the internet by delivering complete e-mail encryption.

Simplesum Safe

An easy to use file manager that helps you organize and encrypt data with ease. A built-in picture viewer and tagging feature makes it a great one-stop resource for encrypted file and photo browsing.

AESCrypt

Cloud storage services are prime targets for data theft, especially since the most common ones don't offer native encryption. By using AESCrypt and its desktop counterpart, you can encrypt files stored on Dropbox Google Drive, Evernote, etc., and view them on any iOS device.