What This Guide Provides

This pamphlet provides security recommendations for personally managed Apple iPhones running iPhone OS 3. In this situation, the user exercises administrative control over the device, whether the device was purchased by that user or by the enterprise.

This pamphlet does **not** address the substantial security and configuration issues involved with deploying or using iPhones in an enterprise environment. Such issues, including the management of configuration profiles, network infrastructure settings, connecting to VPNs, and Exchange ActiveSync, are covered in Apple's *iPhone OS Enterprise Deployment Guide*.

Policy configuration settings for Department of Defense (DoD) and other U.S. Federal Government environments are covered elsewhere. DoD users should consult DISA publications such as *Wireless STIG V5R2* (http://iase.disa.mil/stigs/stig/index.html). Other U.S. Federal Government users should consult NIST publications such as SP 800-124 *Guidelines on Cell Phone and PDA Security* and SP 800-53 *Recommended Security Controls for Federal Information Systems* (http://csrc.nist.gov/publications/PubsSPs.html).

Maintain Physical Security

Always maintain physical control of your iPhone. All electronic devices are subject to physical attacks, but the portable nature of cellular phones puts them at particular risk. Publicly available tools allow an attacker with physical access to your iPhone to bypass some of its security mechanisms.

The best protection against physical attacks is to ensure that your iPhone never falls into the wrong hands. Consider the risks of storing sensitive data on your iPhone. This includes corporate information, credit card numbers, saved passwords, and personal data. If a mobile device falls out of your control, consider all the data contained on it compromised.

Apply the Latest Software Updates

Always apply the latest software updates for the iPhone, as these include important security patches. It is the responsibility of the individual user to ensure that the device has the latest version of the iPhone OS and iTunes software. Regularly check for software updates for iPhone OS and for iTunes. Both updates will occur each time your iPhone is synced with iTunes.

Only sync your iPhone or install iPhone OS updates from a trusted computer.

Do Not Jailbreak Your iPhone

"Jailbreaking" is the term that refers to the process of modifying the iPhone's operating system in violation of the end-user license agreement. Jailbreaking significantly damages the iPhone's ability to resist attacks because it disables the enforcement of code signatures, which is an important security feature. Jailbreaking an iPhone makes the attacker's job substantially easier. Most publicly released attacks targeted at the iPhone require that it first be jailbroken.

Another concern related to jailbreaking is the quality of the tools and applications provided by the jailbreaking community. These free applications are developed with little oversight and limited testing. They may include viruses or other malware, and they may inflict lasting harm on your iPhone by breaking it permanently or corrupting your data.

Enable Auto-Lock and Passcode Lock

The Auto-Lock feature makes the iPhone screen lock automatically after a specified inactivity period. Ensure that Auto-Lock is activated. A value of 3 minutes or less is recommended.

Go to Settings > General > Auto-Lock
Set "Auto-Lock" to 3 Minutes

By itself, Auto-Lock does not constitute a security feature, but when combined with Passcode Lock, it will deter a casual attempt to access your data. Use the Passcode Lock feature to assign a four-digit PIN to your iPhone. With the prompt time set to "Immediately" the iPhone will always require entry of the correct PIN in order to unlock the screen.

Go to Settings > General > Passcode Lock
Set "Passcode Lock" to ON
Set "Require Passcode" to Immediately

Note: More sophisticated Passcode Lock policies are possible by using the enterprise management tools.

For additional security, use the Erase Data feature to erase all user-created data after ten failed passcode attempts. This feature also greatly increases the time between failed access attempts to slow down more persistent attackers.

Go to Settings > General > Passcode Lock
Set "Erase Data" to ON

Do Not Join Untrusted Wireless Networks

When possible, avoid or limit the use of wireless networks. When not actively using wireless, turn it off to prevent any accidental exposure.

Go to Settings > Wi-Fi
Set "Wi-Fi" to OFF

Resist the temptation to use free Wi-Fi access points. These typically offer no protection for wirelessly transmitted data, meaning that anyone in the vicinity could intercept all traffic, transmitted or received. Instead, if it is absolutely necessary to use a wireless network, choose a known one and ensure that its traffic is encrypted, preferably with WPA. Protected networks are designated in the list of available networks by a picture of a lock next to their names.

To avoid accidentally joining an untrusted network, turn off "Ask to Join Networks." This will not prevent your iPhone from reconnecting to networks it has joined in the past, but it will require future wireless connections to be made manually by selecting a network from a list of available networks.

Go to Settings > Wi-Fi
Set "Ask to Join Networks" to OFF

Note: Even if this setting is disabled, your phone will still automatically rejoin previously visited networks that have not been explicitly forgotten.

Another precaution is to choose "Forget this network" at the end of every wireless session. This will reduce the chance that your iPhone may accidentally join another wireless network with the same name. It is important to select this option before leaving the physical range of the network in question. Otherwise, the network will no longer appear in the list of available networks, and it will not be possible to remove it.

Go to Settings > Wi-Fi
Select a network from the list
Set "Forget this network"

Disable Bluetooth Unless Needed

Bluetooth should only be turned on when absolutely necessary. When not in use, it should be disabled to prevent other devices from discovering your iPhone and attempting to connect to it.

Go to Settings > General > Bluetooth
Set "Bluetooth" to OFF

Disable Location Services Unless Needed

Location Services can be used by Applications on your iPhone to track your location. Unless there is some critical need for Applications to know your location at all times, Location Services should be turned off, or toggled on and off only as needed.

Go to Settings > General
Set "Location Services" to OFF

Applications that use Location Services will ask to use Location Services the first time they are launched. Consider these requests carefully and only enable Location Services when absolutely necessary.

Secure Safari Settings

AutoFill should be disabled in Safari. This will prevent Safari from storing potentially sensitive contact information on your device, such as usernames and passwords.

Go to Settings > Safari
Set "AutoFill" to OFF

JavaScript support can be disabled to prevent maliciously crafted JavaScripts from harming your iPhone. However, disabling JavaScript can make many websites unusable, so it may be necessary to leave it on. If it is practical:

Go to Settings > Safari
Set "JavaScript" to OFF

Cookies can compromise personal information and browsing habits. To prevent this from happening, disable them when possible or set your iPhone to only accept cookies from visited sites. The following setting is unlikely to break the functionality of most websites:

Go to Settings > Safari > Accept Cookies
Set "Accept Cookies" to From visited

Secure Mail Settings

Ensure that all Mail connections are encrypted. This requires that your email server support encryption, which most do. Without encryption support, your messages will be sent in the clear, which could make it possible for someone to intercept and read them.

Go to Settings > Mail, Contacts, Calendars

For each account in the list:
Go to SMTP, select a server name from the list
Set "Use SSL" to ON

For each account in the list:
Go to Advanced
Set "Use SSL" to ON

When accessing web mail through Safari, make sure the login page is encrypted before entering your data. If it is encrypted, the URL will start with "https" instead of "http," and a lock icon will appear to the right of the URL.

Remote image loading should be disabled in Mail. This can prevent maliciously crafted images from harming your iPhone. It will also prevent attackers from linking your network address information to your email account.

Go to Settings > Mail, Contacts, Calendars
Set "Load Remote Images" to OFF

Consider the iPhone Configuration Utility

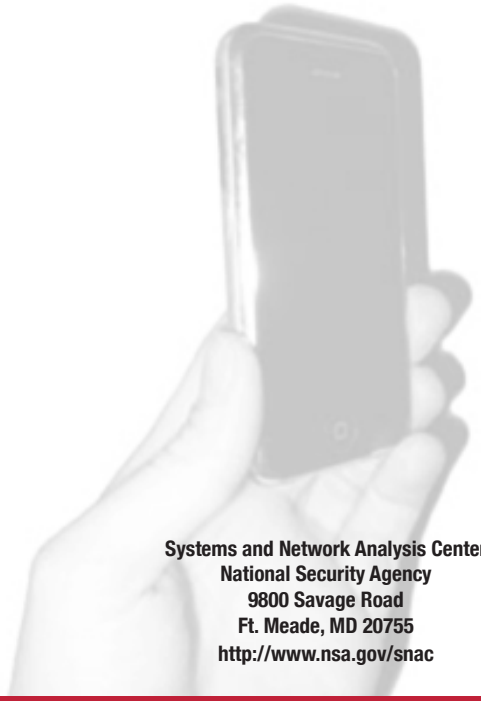
Some security settings can only be applied through the iPhone Configuration Utility, a free tool that Apple provides directly through their website:

http://www.apple.com/support/iphone/enterprise/

This tool provides the ability to set longer and more complex PINs than four numbers, the ability to disable the camera, the ability to remotely wipe the device, and many other options. Full instructions on how to use this tool are provided at the same location.

The Information Assurance Mission at NSA

Security Tips for Personally Managed Apple iPhones



Systems and Network Analysis Center
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755
http://www.nsa.gov/snac