White Paper

McAfee®

# Top 10 iPhone Security Tips

By Kunjan Shah, Principal Consultant, McAfee® Foundstone® Professional Services

## Table of Contents

With more than 100 million Apple iPhone users, the demand to secure them has never been greater. The latest version of iOS (4.3.4 at the time of this writing) has matured a great deal from its predecessors. This iOS version comes with numerous security features that you can leverage if you're interested in protecting your iPhone and the data it stores and processes.

Take a minute to think about the applications that you have running on your iPhone and the nature of information it processes. You will quickly come to the realization that it stores confidential and private information such as account numbers, passwords to websites, corporate emails, pictures and videos, browser search history, stocks you track, recent places you visited, and much more. It's imperative that this information be protected at all times. Although a lot of stress is placed on protecting personal computers, most people fail to take even the basic security precautions on their iPhones.

This paper offers guidelines on securing your iPhone using features provided by iOS and by following other security best practices. It begins by discussing basic security settings for novice users and then continues to discuss advanced techniques for expert users. This paper is intended for users who want to take proactive measures to secure their iPhones, companies willing to train their employees (before allowing corporate emails on the devices), and administrators working on developing strong policies. It confines its discussion to iPhone security features only and does not discuss similar features that may be available in other mobile device platforms such as Android. However, some of the concepts and standards apply across all these devices.

The model device used for this paper is an iPhone running iOS 4.3.4. Some of these settings and features may not be present in the older or newer versions of iOS.

## Tip 1: Enable Passcode Lock on Your iPhone

The most basic precaution you can take is to enable passcode lock and set it to automatically engage after a brief period of inactivity. By default, a passcode is not required to unlock the iPhone. Most people would put off this security measure for ease of use and convenience. However, the truth is that once you have it enabled, it becomes second nature and you would not notice any difference. It is recommended that you set a strong passcode. In the event of a physical theft, this will increase the effort required to compromise your iPhone. Also, for some other security applications to work such as Find My iPhone, a passcode is mandatory.

### How to setup a passcode lock

1. Navigate to Settings > General > Passcode Lock.
2. Tap Turn Passcode On.
3. You will be prompted to enter a four-digit passcode twice. Choose a passcode that's difficult to guess. See the guidelines on choosing hard passcodes below.

## Choosing a Passcode That's Difficult to Guess

According to research[1] done by Daniel Amitay, the most common passcodes used are: 1234, 0000, 2580, 1111, 5555, 5683, 0852, 2222, 1212, and 1998. While 1234, 0000, and 2580 are easy to remember and thus picked, 5683 is the number representation of "LOVE," once again mimicking a very common Internet password: "iloveyou." Avoid using these commonly used or other easy-to-guess passcodes such as your birthdate.

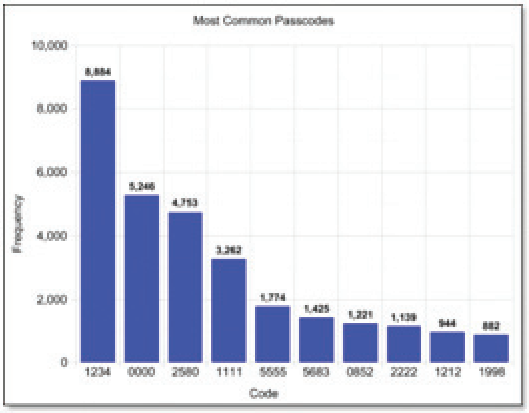
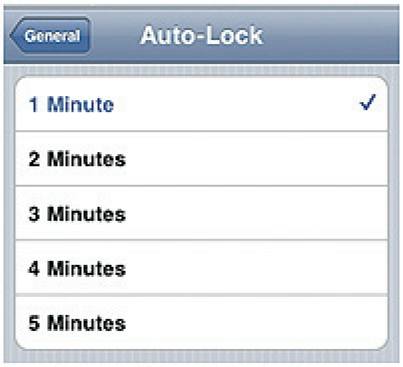


Figure 1. Top 10 frequently used iPhone passcodes.

## Set Auto-Lock Timeout

The iPhone can be configured to auto-lock after a predefined period of inactivity. The most secure setting is one minute. This is also the default setting, unless changed by the user. It is recommended that this setting not be changed from its default value to anything greater and less secure, such as five minutes. Setting it to one minute will reduce the time window that the iPhone is in an unlocked state and ensure that it will be mostly locked in case of a physical security breach.



Auto-Lock

1 Minute ✓
2 Minutes
3 Minutes
4 Minutes
5 Minutes

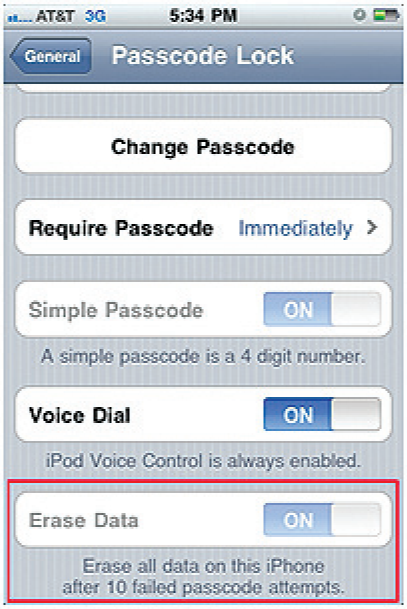
Figure 2. The recommended setting for Auto-Lock.

## Enable Erase Data

It is trivial for a thief to guess the four-digit passcode through brute force attempts. The Erase Data setting could be configured on iPhone to erase all the user's data and settings if 10 failed attempts have been reached. This will thwart all brute force attempts to guess the correct passcode. This setting is disabled by default, but it is recommended that you enable it. If enabled, your iPhone will completely wipe all the data after 10 failed attempts have been recorded. This may sound scary at first, as you don't want your data to be accidentally deleted by a child or prankster. However, after the first few wrong attempts, it stops you from trying for a minute, then on the next failed attempt, it increases the delay to five minutes, and

[1] http://amitay.us/blog/files/most_common_iphone_passcodes.php

keeps on increasing it till 30 minutes for the last few attempts, before wiping the data of the device. It is unlikely that someone would have all this time unless your phone is lost. Also, remember this information can always be restored from Apple iTunes if it is accidently wiped out.



Passcode Lock

Change Passcode

Require Passcode Immediately >

Simple Passcode ON

A simple passcode is a 4 digit number.

Voice Dial ON

iPod Voice Control is always enabled.

Erase Data ON

Erase all data on this iPhone after 10 failed passcode attempts.

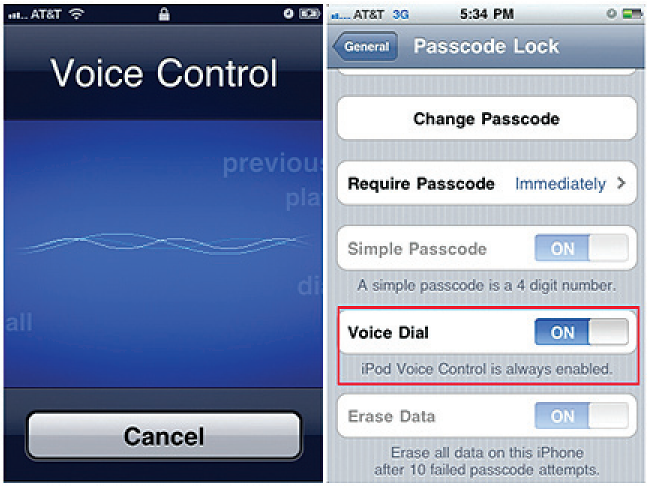
Figure 3. How to enable the Erase Data setting on an iPhone.

## Tip 2: Disable Features That Could Be Accessed Without Entering the Passcode

### Disable the Voice Dial Feature

By default, the Voice Dial feature of an iPhone can be accessed without unlocking it first. To access this feature, press the Home button on a locked iPhone. It will start Voice Dial and prompt you to enter a command. This feature can be used to call anyone from the contact list, play songs, and use other functions. Apple has now provided an option for the users to disable it. To disable it:

1. Navigate to Settings > Passcode Lock > Voice Control.
2. Turn Voice Dial to OFF.



Passcode Lock

Change Passcode

Require Passcode Immediately >

Simple Passcode ON

A simple passcode is a 4 digit number.

Voice Dial ON

iPod Voice Control is always enabled.

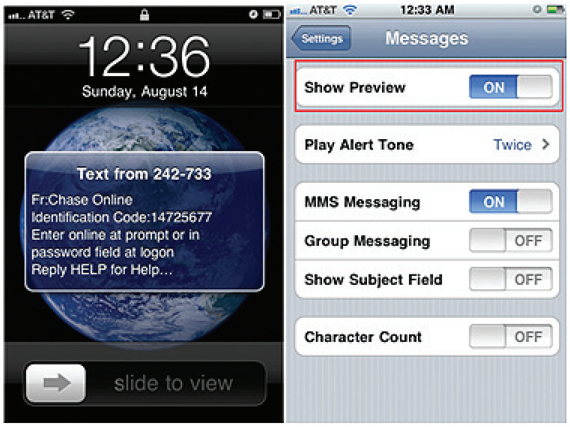
Erase Data ON

Erase all data on this iPhone after 10 failed passcode attempts.

Figure 4. The Voice Dial feature and how to disable it.

### Disable SMS Preview

Messages can be previewed on a locked iPhone by default. Although this is a convenient feature, there are security ramifications when it is used. Many applications send sensitive secondary authentication information such as authentication codes via text message. This information, if compromised, could further compromise your banking and other application credentials through the use of the Reset Password functionality. It is recommended that this feature be disabled at all times. This feature can be disabled by navigating to Settings > Messages > Show Preview and then toggling it to OFF.



12:36
Sunday, August 14

Text from 242-733
Fr:Chase Online
Identification Code:14725677
Enter online at prompt or in
password field at logon
Reply HELP for Help...

Messages

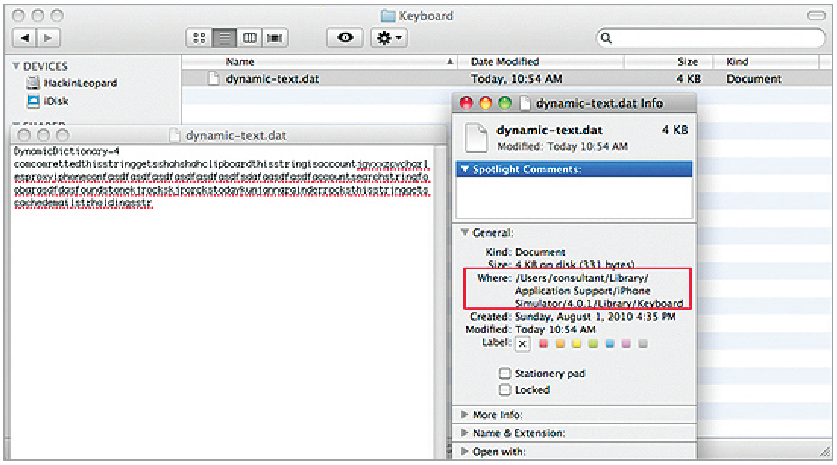
Show Preview ON
Play Alert Tone Twice
MMS Messaging ON
Group Messaging OFF
Show Subject Field OFF
Character Count OFF

Figure 5. The SMS Preview feature and how to disable it.

## Tip 3: Overcoming Privacy Issues Due to the Inherent Design of the iPhone

### Keyboard Cache

All the keystrokes[2] entered on an iPhone could potentially get cached[3] for up to 12 months under the /var/mobile/Library/Keyboard/dynamic-text.dat file for auto-correction, unless appropriate measures are taken. This includes all keystrokes entered by you—such as account numbers—that you may enter on your iPhone to register to banking applications. It should be noted, however, that the iPhone never stores password fields.



| Name | Date Modified | Size | Kind |
|---|---|---|---|
| dynamic-text.dat | Today, 10:54 AM | 4 KB | Document |

dynamic-text.dat

```
DynamicDictionary-4
comcorrettedthisstringgetsshahshahclipboardthisstringisaccount[illegible]
esproxyiphoneconfasdfasdfasdfasdfasdfasdfsdafasdfasdfaccountsearchstringfo
obarasdfdasfoundstonekjrockskjrockstodayfunjonnaraindezrocksthisstringgets
cachedemailstheldingsstr
```

dynamic-text.dat Info

dynamic-text.dat 4 KB
Modified: Today 10:54 AM

Spotlight Comments:

General:
Kind: Document
Size: 4 KB on disk (331 bytes)
Where: /Users/consultant/Library/Application Support/iPhone Simulator/4.0.1/Library/Keyboard
Created: Sunday, August 1, 2010 4:35 PM
Modified: Today 10:54 AM
Label: ☒

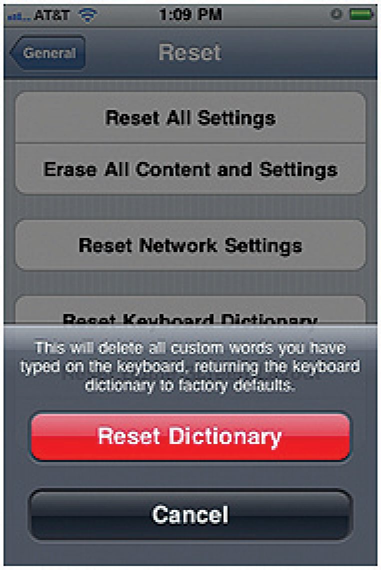
□ Stationery pad
□ Locked

Figure 6. Figure shows keystrokes being cached.

[2] http://www.security-faqs.com/did-you-know-that-the-iphone-retains-cached-keyboard-data-for-up-to-12-months.html
[3] http://stackoverflow.com/questions/1955010/iphone-keyboard-security

### How to delete the keyboard cache

1. Navigate to General > Reset.
2. Tap on Reset Keyboard Dictionary.
3. Confirm on the warning screen



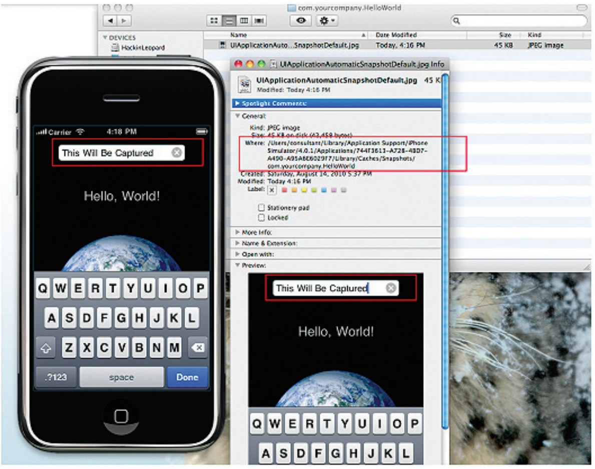
This will delete all custom words you have typed on the keyboard, returning the keyboard dictionary to factory defaults.

Figure 7. How to reset the keyboard cache.

## Automated Screenshots

Every time a user taps the Home button, the window of the open application shrinks and disappears. To create this shrinking effect, iPhone takes an automatic screenshot.[4] These screenshots are stored in the snapshots directory of the application. For example the sample Helloworld application stores them at ~/Library/Application Support/iPhone Simulator/4.0.1/Applications/744F3613-A728-4BD7-A490-A95A6E6029F7/Library/Caches/Snapshots/com.yourcompany.HelloWorld.

The phone presumably deletes the image after you close the application. But anyone who understands this is aware that, in most cases, deletion does not permanently remove files from a storage device. Therefore, forensics experts have used this security flaw to gather evidence against criminals.



UIApplicationAutomaticSnapshotDefault.jpg 45 KB
Modified: Today 4:16 PM

Kind: JPEG image
Size: 45 KB on disk (43,459 bytes)
Where: /Users/consultant/Library/Application Support/iPhone Simulator/4.0.1/Applications/744F3613-A728-4BD7-A490-A95A6E6029F7/Library/Caches/Snapshots/com.yourcompany.HelloWorld
Created: Saturday, August 14, 2010 5:37 PM
Modified: Today 4:16 PM
Label: ☒

□ Stationery pad
□ Locked

Figure 8. Automated screen shots.

[4] http://www.wired.com/gadgetlab/2008/09/hacker-says-sec/
http://www.iphonefootprint.com/2008/09/iphones-privacy-flaw-it-takes-automatic-screenshots-of-all-your-latest-actions/

### How to prevent sensitive information from being captured as screen shots

If an application displays sensitive information such as Social Security numbers, account numbers, and other data in full, then avoid using such an application on the iPhone. However, the risk is still present for built-in applications such as Messaging, Safari, and other common functions. In this case, be mindful of this design flaw and avoid tapping the Home button while viewing sensitive information on the screen. Go to a different page not displaying sensitive information before tapping the Home button.

Advanced users can follow the steps[5] below to disable screen shot writing permanently. Basic users should skip this section as it requires jailbreaking the iPhone. Jailbreaking has its own security issues that are outlined later on. Unless you are familiar with the process and aware of the security issues, you should not try this.

1. Use OpenSSH application to gain root privileges to your jailbroken iPhone.
2. Using the OpenSSH application, enter the following commands in the prompt:

```
# rm -rf /var/mobile/Library/Caches/Snapshots
# ln -s /dev/null /var/mobile/Library/Caches/Snapshots
```

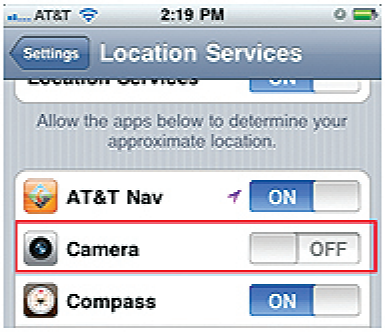
These commands will disable screenshot writing permanently. However, if you wish to undo this action in the future, delete the symlink and the directory will get re-created.

### Geotagging

The storage of location-based data in the form of latitude and longitude inside the images is called geotagging. It is essentially tagging your photograph with the geographic location information. Though most digital cameras do not have GPS hardware built in, smartphones are exceptions. The iPhone has both the camera and GPS locator technology. Thus, the iPhone camera is equipped with automatically adding geolocation information to the pictures it takes. By default, all pictures taken by an iPhone contain this information unless it is manually disabled. Imagine you took some pictures of your house or your car parked in front of it and uploaded this to the social networking sites. Anyone viewing these images could identify the location of your house (if geotagging was not disabled). Now imagine if you were a celebrity hiding from paparazzi and took a photo of your house with your iPhone—you would reveal your whereabouts to them by publishing these pictures. According to the New York Times story,[6] this incident happened to Adam Savage of the popular Mythbusters program.

### How to Disable Geotagging on the iPhone

Apple iOS allows users to turn off location services on a per-application basis.[7] It is recommended that you disable location services for the camera application. This will prevent geotagging. Navigate to Settings > Location Services. Toggle the Camera to OFF as shown below.



Location Services

Allow the apps below to determine your approximate location.

AT&T Nav ON

Camera OFF

Compass ON

Figure 9. How to disable geotagging

[5] http://www.wired.com/gadgetlab/2008/09/hacker-describe/
[6] http://www.fieldtechnologies.com/stop-gps-data-recorded-in-photos-from-revealing-where-you-live/
[7] http://icanstalku.com/how.php

### iPhone's Location Tracking Issue

Earlier this year, it was discovered that the iPhone logs GPS coordinate data for more than a year and saves it in a file named "consolidated.db." This file is also synced over to iTunes upon backup. When this issue was identified, this file was stored unencrypted on the machine during backups.

### How to Disable Location Tracking by iPhone

Apple has now fixed this issue in the iOS version 4.3.3 by reducing the amount of data stored in the file to just the last seven days. It has also provided an option to manually turn off GPS tracking.[8]

Here are some suggestions to remediate this issue:

1. Use the Untrackered[9] application from Cydia on jailbroken devices. This application installs a daemon that runs in the background and cleans the consolidated.db file.

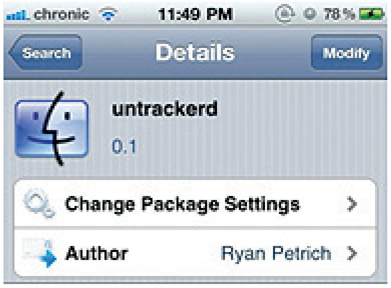
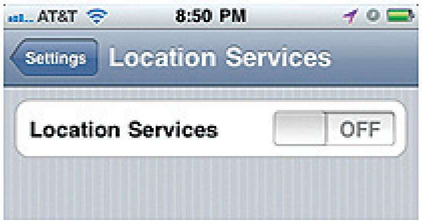


Figure 10. The Untrackered application available on Cydia.

2. Encrypt your iPhone's backup in iTunes.

3. Turn off the iPhone's location services by navigating to Settings > Location Services and toggling it to OFF as shown below.



Location Services OFF

Figure 11. How to disable location services.

4. Migrate to iOS version 4.3.3 or higher.

## Tip 4: Erase All the Data Before Return, Repair, or Resale of Your iPhone

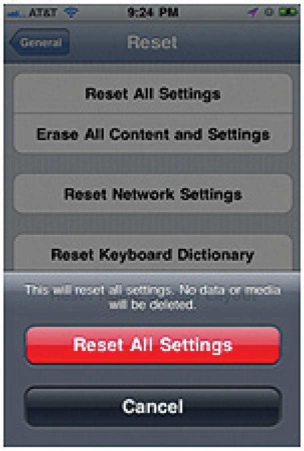
Imagine you bought a new iPhone and want to sell your old one on eBay. You can use the Restore option available in iTunes to reset the iPhone to its factory state. However, that does not use a secure delete function, allowing it to persist data on the device, which could be later recovered with the use of proper forensic tools. A detective from Oregon State Police managed to recover a user's personal data like emails, photos, and more from an out-of-the-box refurbished iPhone that he had bought.[10] All personal data that was available on the phone before being restored was still left in the unallocated blocks of iPhone's NAND memory.

[8] http://www.rmtracking.com/blog/2011/05/17/apple-fixes-gps-glitch/
[9] http://appadvice.com/appnn/2011/04/jailbreak-untrackered-stop-ios-recording-move
[10] http://www.iphonealley.com/news/personal-information-recovered-from-refurbished-iphone

## How to Securely Erase Data from Your iPhone[11]

First method[12]

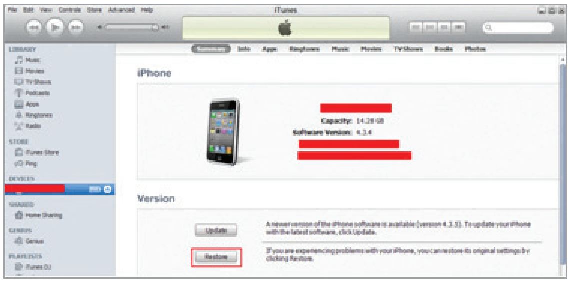
1. Change all your passwords for emails, social networking sites, and banking sites that you have configured on your iPhone.
2. Navigate to Settings > General > Reset.
3. Tap on Reset All Settings as shown below and confirm the warning.
4. Next, navigate to Settings > General > Reset, and tap on Erase All Content and Settings.



This will reset all settings. No data or media will be deleted.

Figure 12. The option to Reset All Settings.

5. Now restore the iPhone using iTunes as shown below.



[redacted]

[redacted]

Capacity: 14.28 GB

Software Version: 4.3.4

[redacted]

A newer version of the iPhone software is available (version 4.3.5). To update your iPhone with the latest software, click Update.

If you are experiencing problems with your iPhone, you can restore its original settings by clicking Restore.

Figure 13. The Restore option in iTunes to reset the phone to its original state.

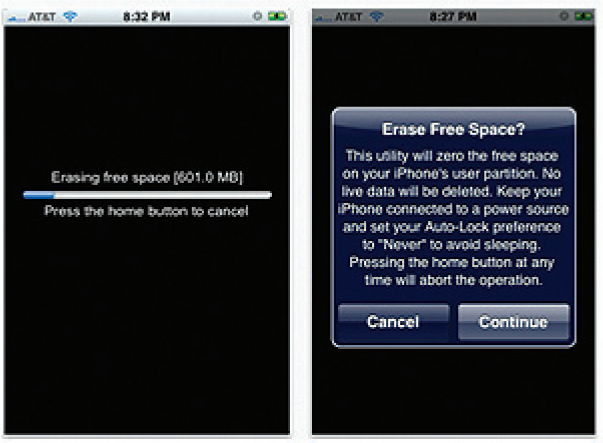
6. Using iTunes, uncheck all Sync options for photos, videos, music, email, and other content.
7. Create three separate playlists as large as the storage capacity of your iPhone.
8. On the Music tab, select the first of your three playlists to sync. Make sure that the storage bar at the bottom looks full after syncing. This will guarantee that the complete memory on the iPhone is overwritten with the contents of your playlist and there are no unallocated blocks left.
9. Repeat this process three times for each of the playlists. This technique is referred to as the unofficial way of three-pass overwrite.
10. Now restore the iPhone again using iTunes.

[11] http://securosis.com/blog/formatting-an-iphone-to-wipe-data

[12] http://www.youtube.com/watch?v=ZlXyFSMrDzM&feature=related

### Alternative Method

1. Reset all the settings. This will delete all the personalized files.
2. Restore iPhone to its factory state using iTunes. This process performs a quick format.
3. Use the iErase application available on the Appstore,[13] developed by Jonathan Zdziarski (iPhone forensics expert).



Erasing free space (601.0 MB)

Press the home button to cancel

**Erase Free Space?**

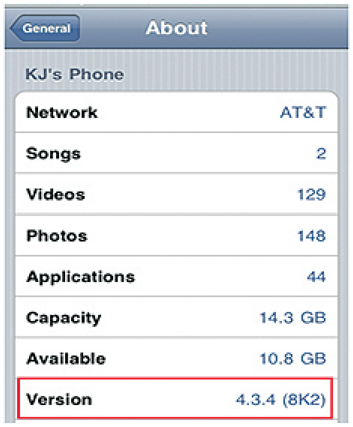
This utility will zero the free space on your iPhone's user partition. No live data will be deleted. Keep your iPhone connected to a power source and set your Auto-Lock preference to "Never" to avoid sleeping. Pressing the home button at any time will abort the operation.

## Tip 5: Regularly Update the iPhone's Firmware

iOS Firmware is the operating system embedded in the iPhone. The iPhone ships with the version of firmware that was current at the time of manufacturing. Apple provides frequent firmware updates that are not limited to bug fixes and security fixes, but also include additional security features. The current firmware version is 4.3.4. It is recommended that you always have the latest version of firmware running on your iPhone. By doing so, you will not be vulnerable to the security issues identified in the previous versions.

### How to Check the Current Firmware Version on Your iPhone

To check the current firmware version, navigate to Settings > General > About. Check the version information available on this screen. As show in the figure below, the current version running on the test phone is 4.3.4.



KJ's Phone

| | |
|---|---|
| Network | AT&T |
| Songs | 2 |
| Videos | 129 |
| Photos | 148 |
| Applications | 44 |
| Capacity | 14.3 GB |
| Available | 10.8 GB |
| Version | 4.3.4 (8K2) |

Figure 14. The current version of the model iPhone.

[13] http://itunes.apple.com/app/ierase-zero-free-space/id300428114?mt=8

### How to Track the Latest Firmware Updates Released by Apple

1. Follow the updates on Twitter http://twitter.com/#!/appleios.
2. If you are a registered Apple developer, you will receive this information in email.
3. Every time you connect your iPhone to iTunes, it prompts you for firmware updates, if they are available.
4. This is a good site for identifying the latest iOS firmware updates: http://ios.e-lite.org/.

### How to Upgrade to the Latest Version of iOS Firmware

1. Connect the iPhone to your computer running iTunes.
2. Launch iTunes.
3. It will prompt you if the latest version of firmware update is available.
4. Accept and follow the steps to update the firmware on your iPhone.

## Tip 6: To Jailbreak or Not to Jailbreak?

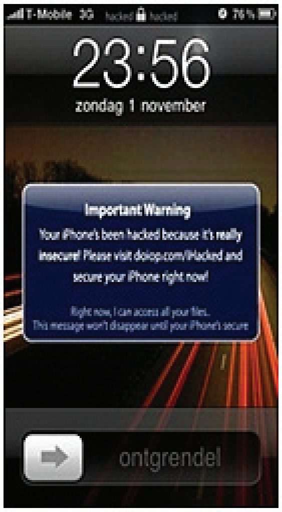
### What Is Jailbreaking?

Jailbreaking is hacking of iOS through the use of custom kernels to bypass limitations imposed by Apple.[14] It allows users to run any application not authorized by Apple, via installers such as Cydia. Jailbreaking was made legal[15] in the US under DMCA of 2010. Thus, there are no legal restrictions preventing users from jailbreaking their iPhones. However, there are some serious security ramifications.

### Cons

1. Jailbreaking makes you more susceptible to worms and other malicious applications.

   Although identified vulnerabilities for iOS put users equally at risk, there are certain vulnerabilities that only target jailbroken iPhones. For example, the Dutch Ransom[16] worm targeted users with the default SSH password on jailbroken iPhones. Thus, using a jailbroken device may increase your risk.



Important Warning

Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your iPhone right now!

Right now, I can access all your files.
This message won't disappear until your iPhone's secure

Figure 15. A message displayed by the Dutch Ransom worm.

2. Applications on a jailbroken device run as root outside of the iOS sandbox.

   By default, all the applications on a non-jailbroken iPhone run as a least-privileged mobile user, jailed in the sandbox architecture of iOS. However, applications on jailbroken iPhones can run as root

[14] http://en.wikipedia.org/wiki/IOS_jailbreaking
[15] http://www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/
[16] http://www.wired.com/gadgetlab/2009/11/iphone-hacker/

and do whatever they please. Also, any self-signed applications can run on the device without being validated by Apple first. Although the primary goal of code signing introduced by Apple was not security per se, it does provide some level of security by limiting the number of malicious applications that are available on the AppStore.

3. It de-motivates you from regularly updating your iOS firmware.

   When you update your iOS, you lose the jailbreaking advantage and need to re-jailbreak it. You also need to re-install all jailbroken applications and extensions. There are tools like PkgBackup that could be used to restore all the applications and hacks, but it is still cumbersome and may prevent you from frequently updating your iOS firmware. As discussed earlier, not running the latest version of iOS may make your iPhone vulnerable to defects and bugs identified in the older versions.

### Pros

Although there are definite usability advantages to jailbreaking an iPhone, we are only discussing security benefits. The jailbreaking community has provided faster fixes than the iPhone development team in several instances. For example, when the zero-day vulnerability in the mobile Safari browser (related to the way it handles PDF documents) was identified, the jailbreaking community quickly released PDF Patcher 2 to remediate it. This protected the users who had jailbroken their iPhones (about 10 percent of the total iPhone user population), while others who didn't were left waiting for Apple to release a fix. Thus, having a jailbroken iPhone may, in fact, work to your advantage by reducing the window of exposure to zero-day vulnerabilities.

### Conclusion

To jailbreak your iPhone or not is a very controversial topic. You will find supporters from both sides. Jailbreaking is definitely not for everyone. If you are a novice user with limited knowledge of security, then you should try to avoid jailbreaking.

## Tip 7: Enable Safari's Privacy and Security Settings on the iPhone

The iPhone Safari browser provides some basic security settings. You can access these settings by navigating to Settings > Safari.

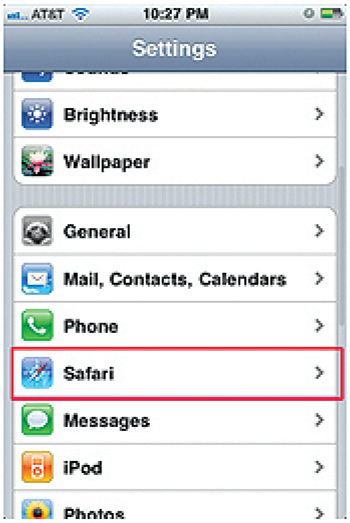
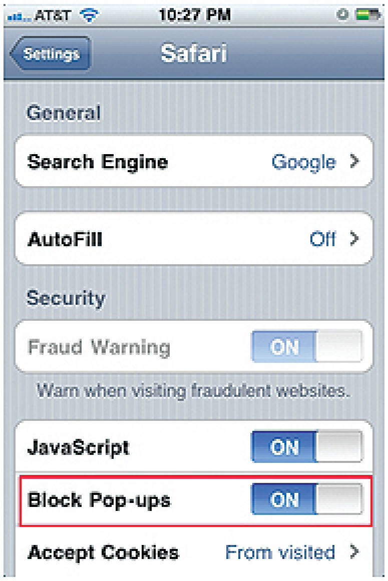


Figure 16. How to access security settings for the Safari browser.

### 1. Enable Block Pop-ups

Clicking on a malicious pop-up could expose your iPhone to malware. Although pop-ups are blocked by default, you can verify this by going to Settings > Safari > Block Pop-ups and making sure it is set to ON.



AT&T 10:27 PM

Settings Safari

General

Search Engine Google

AutoFill Off

Security

Fraud Warning ON

Warn when visiting fraudulent websites.

JavaScript ON

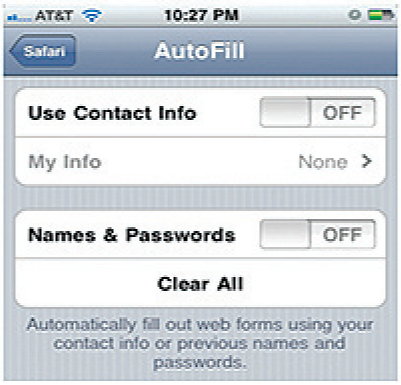
Block Pop-ups ON

Accept Cookies From visited

Figure 17. How to enable Block Pop-ups.

### 2. Disable AutoFill

The iPhone has a feature to remember and then automate completion of forms in the Safari browser. Disable AutoFill to avoid caching of sensitive information such as names, passwords, and other sensitive data that you fill out in the web forms. This is similar to the AutoComplete feature found in the regular non-mobile web browsers. To disable AutoFill, go to Settings > Safari > AutoFill and toggle it to OFF as shown below.



AT&T 10:27 PM

Safari AutoFill

Use Contact Info OFF

My Info None

Names & Passwords OFF

Clear All

Automatically fill out web forms using your contact info or previous names and passwords.

Figure 18. How to disable AutoFill.

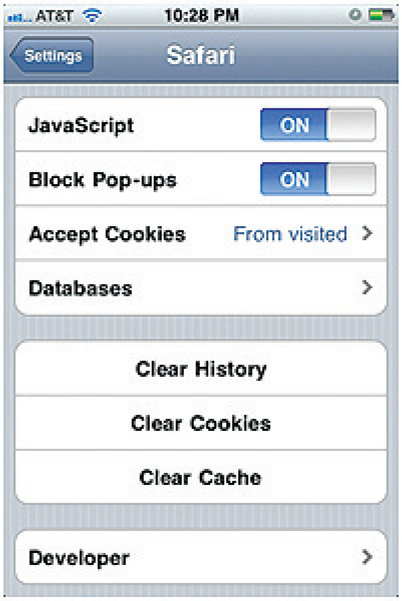
### 3. Enable Fraud Warning

Fraud Warning protects you from unknowingly visiting phishing or other fraudulent sites. When you try to access such a site, Safari warns you and doesn't load the page. To enable this feature:

1. Go to Settings > Safari > Fraud Warning.
2. Toggle this to ON.

### 4. Clear cookies, history, and cache

Delete your browsing history, cookies, and caches using these settings after visiting any sensitive websites such as banking sites. You'll need to tap each option individually. For additional privacy, clear all three.



AT&T 10:28 PM

Settings Safari

JavaScript ON

Block Pop-ups ON

Accept Cookies From visited

Databases

Clear History

Clear Cookies

Clear Cache

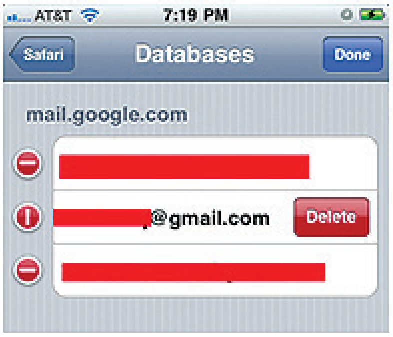
Developer

Figure 19. How to access Clear History, Clear Cache, and Clear Cookies settings.

### 5. Delete Databases

Just a few years ago, deleting your browsing history may have been enough to protect your privacy on the iPhone. However, with HTML 5, there are further steps required to protect your privacy. Some websites may create databases on your iPhone that could disclose sites that you have visited, even after clearing your browsing history. You can delete unnecessary databases that you don't want to have disclosed as shown below.

1. Go to Settings > Safari > Databases.
2. Delete unnecessary databases created without your knowledge.



mail.google.com

[redacted]

[redacted]@gmail.com

[redacted]

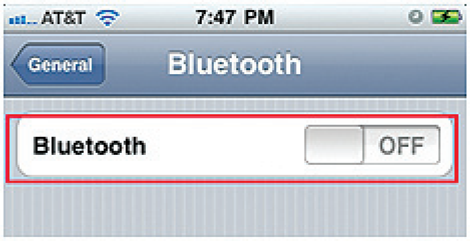
Figure 20. How to delete databases created by sites.

## Tip 8: Using Bluetooth, Wi-Fi, and Email Securely

### Disable Bluetooth When Not in Use

Several applications use iPhone's Bluetooth capabilities to share files and information and for gaming. Attackers could send unsolicited messages or steal sensitive information from Bluetooth-enabled iPhones, using attacks such as BlueJacking[17] and BlueSnarfing.[18] The iPhone does not provide the capability to turn off discovery, so the only preventative measure you can take to disable Bluetooth when it is not being used.

To disable Bluetooth go to Settings > General > Bluetooth, and toggle it to OFF, as shown below,



Bluetooth OFF

Figure 21. How to disable Bluetooth.

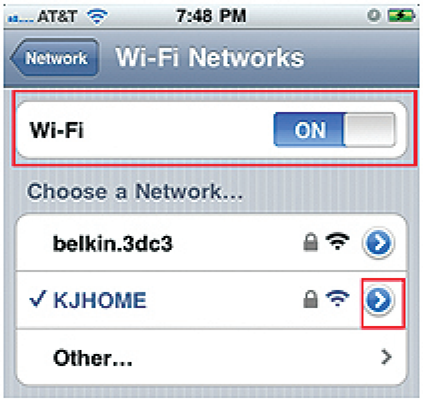
### Disable Wi-Fi When Not in Use

Just as with Bluetooth, it is recommended that you disable Wi-Fi when it is not being used. If Wi-Fi is turned off, then the iPhone connects to the Internet via the cellular data network (if available). In addition to conserving battery, it also eliminates Wi-Fi-related attack vectors. Currently, the cellular data network is more difficult to sniff compared to a Wi-Fi network.

By default, the iPhone also retains settings of the associated networks that it connects to. This allows it to automatically reconnect when in the range next time. Automatic association isn't recommended, as it is easy to spoof networks. Also, for Wi-Fi networks that require HTTP(s) forms authentication, this feature will cause the iPhone to persist credentials on disk. If the iPhone is lost, the confidentiality of these persisted credentials and the resources protected by them may be at risk. You can prevent automatic association by following these steps:

1. Navigate to Settings > General > Wi-Fi.

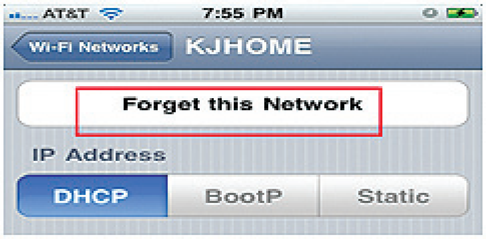
[17] http://en.wikipedia.org/wiki/Bluejacking
[18] http://en.wikipedia.org/wiki/Bluesnarfing



Wi-Fi ON

Figure 22. How to access previously associated network settings.

2. Tap the blue arrow next to the previously associated network SSID.
3. Tap Forget this Network.



IP Address DHCP

Figure 23. How to delete network association.

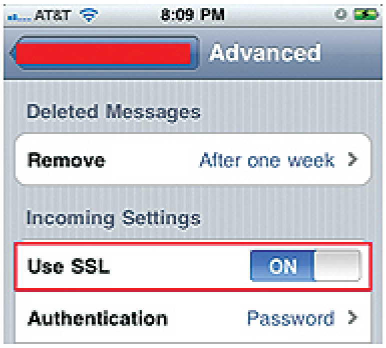
4. Repeat this process for each of the previously associated network SSID.

## Email Security

Make sure that secure sockets layer (SSL) is enabled when accessing emails such as Hotmail or Gmail with the iPhone.

1. Go to Settings > Mail, Contacts, Calendars.
2. Select one of the active mail accounts.
3. Tap on Advanced.
4. Toggle Use SSL option to ON.

If this setting is not used, then messages are not transmitted securely and could be compromised. If you’re unable to connect to your web mail using the iPhone and SSL, consider using an alternative mail account. Hotmail, Gmail, and other popular email services work over SSL.



AT&T 8:09 PM

[redacted] Advanced

Deleted Messages

Remove After one week

Incoming Settings

Use SSL ON

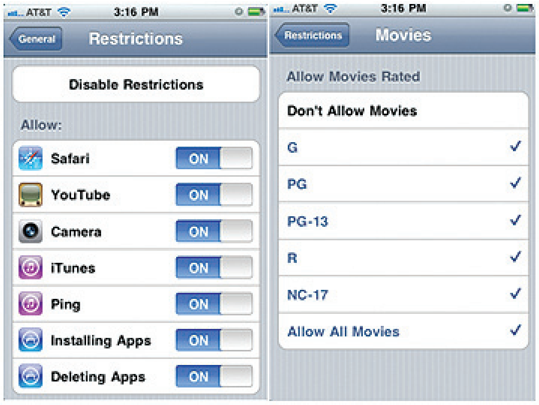
Authentication Password

Figure 24. How to enable SSL for viewing emails securely.

## Tip 9: Enable Restrictions

iPhone users come in all shapes, sizes, and ages. Concerned parents can use the Restrictions option to lock down some of the iPhone's capabilities. This feature can be accessed by navigating to Settings > General > Restrictions. It provides several lock-down capabilities such as:

1. Preventing users from launching and using Safari, YouTube, Camera, or other inbuilt applications.
2. Preventing users from installing or deleting any applications.
3. Preventing changes to any accounts.
4. Restricting explicit content based on ratings, such as PG-13.



AT&T 3:16 PM

General Restrictions

Disable Restrictions

Allow:

| | |
|---|---|
| Safari | ON |
| YouTube | ON |
| Camera | ON |
| iTunes | ON |
| Ping | ON |
| Installing Apps | ON |
| Deleting Apps | ON |

AT&T 3:16 PM

Restrictions Movies

Allow Movies Rated

| | |
|---|---|
| Don't Allow Movies | |
| G | ✓ |
| PG | ✓ |
| PG-13 | ✓ |
| R | ✓ |
| NC-17 | ✓ |
| Allow All Movies | ✓ |

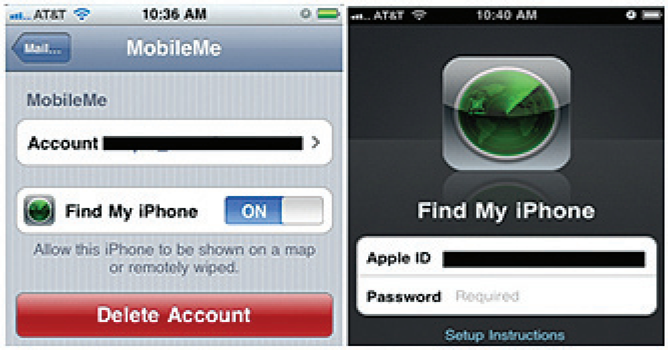
Figure 25. Options available under Restrictions.

## Tip 10: Enable Find My iPhone

Apple has now made the Find My iPhone application/service free with iOS 4.2. It only works on iPhone 4 by default. However, there are workarounds to get it working on the pre-2010 devices.[19] This application uses iPhone's GPS and helps track lost or stolen iPhones. In order for this to work, the application has to be installed and set up before the device is lost or stolen. Follow the steps below to get it installed:

1. Launch AppStore, and download the free Find My iPhone application.
2. Next, go to Settings > Mail, Contacts, Calendar > Accounts, and add a MobileMe account.
3. Log in to the MobileMe account using your Apple ID and password.
4. Once connected, set Find My iPhone setting to ON as shown in the figure below.
5. Now, go to the installed application and log in with your Apple ID and password.

[19] http://lifehacker.com/5696311/how-to-enable-and-use-find-my-iphone-for-free-on-iphone-3gs-and-other-pre+2010-devices



Account [redacted]

Find My iPhone ON

Allow this iPhone to be shown on a map or remotely wiped.

Apple ID [redacted]

Password Required

Figure 26. How to enable Find My iPhone application.

Once the setup is complete, you can use the MobileMe[20] website to track your iPhone if it gets lost.

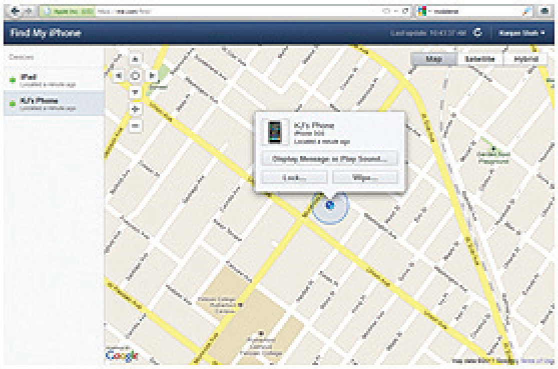
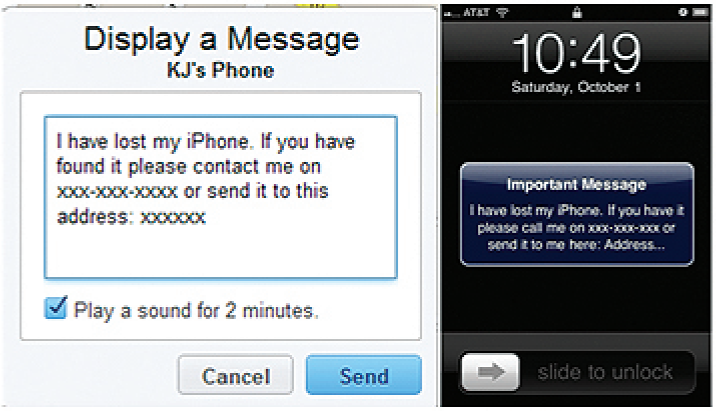


Figure 27. MobileMe application tracks the registered device and shows its location.

In addition to tracking the phone's location, you can also display a message, play a sound, and enable remote wipe on it. This service only works if the device is passcode protected (see Tip 1). If the device is not protected, the thief can easily disable this service by deleting the MobileMe account. However, if the device is password protected, then this service is really useful.



I have lost my iPhone. If you have found it please contact me on xxx-xxx-xxxx or send it to this address: xxxxxx

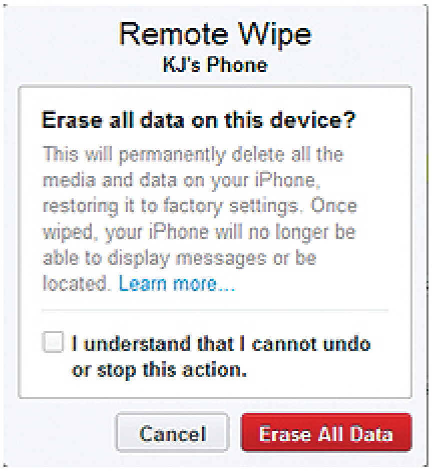
☑ Play a sound for 2 minutes.

Important Message

I have lost my iPhone. If you have it please call me on xxx-xxx-xxx or send it to me here: Address...

Figure 28. How a message could be sent to the lost iPhone and how it is displayed.

[20] https://me.com/find/



Remote Wipe
KJ's Phone

Erase all data on this device?

This will permanently delete all the media and data on your iPhone, restoring it to factory settings. Once wiped, your iPhone will no longer be able to display messages or be located. Learn more...

□ I understand that I cannot undo or stop this action.

Figure 29. How Remote Wipe could be triggered on a lost phone from the MobileMe site.

## Conclusion

The latest version of iOS is very mature and provides several security features. Some of these settings are also enabled by default. It is up to you now to understand and leverage these features to secure your iPhone and the data on it. Regardless of what you do, you will never be completely secure, as there will always be new zero-day vulnerabilities that may put you at risk. However, the goal is to follow these guidelines and best practices and send the attackers off to easier targets.

## About the Author

Kunjan Shah is a principal consultant at McAfee Foundstone Professional Services. Kunjan has more than six years of experience in information security. He has a dual Master's degree in Information Technology and Information Security. Kunjan has also completed his CISSP, CEH, and CCNA certificates. Before joining McAfee Foundstone, Kunjan worked for Cigital. At McAfee Foundstone, Kunjan focuses on web application penetration testing, thick client testing, mobile application testing, web services testing, code review, threat modeling, risk assessment, physical security assessment, policy development, external network penetration testing, and other service lines.

## Acknowledgements

I would like to thank Brad Antoniewicz and the entire McAfee Foundstone research team for reviewing this paper and providing useful feedback.

## About McAfee Foundstone Professional Services

McAfee Foundstone Professional Services offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com