BlackBerry

Friend or Foe?

(U//FOUO) BlackBerry technology is a complex system of software and hardware that provides its users unparalleled connectivity. Unfortunately, as with any other Personal Information Device (PID), if they are used or handled improperly, they can provide an adversary unparalleled access to a user's data and other sensitive information.

(U//FOUO) This document outlines recommendations for BlackBerry users to assist in securing their data. This document is not intended to replace your organization's policy.

(U//FOUO) Additional information on BlackBerry Enterprise Server configuration can be found in the NSA IA Library on SIPRNet.

www.iad.nsa.smil.mil

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Information Assurance Directorate

NSA/IAD Customer Support

DoD & Military (410) 854-4395
Civilian Agencies (410) 854-4790

System & Network Analysis Center

(410) 854-6632
Fax (410) 854-6604
NSTS 968-7631

9800 Savage Rd
Suite 6704
Ft. Meade MD 20755

National Security Agency
www.nsa.gov

Published March 2011

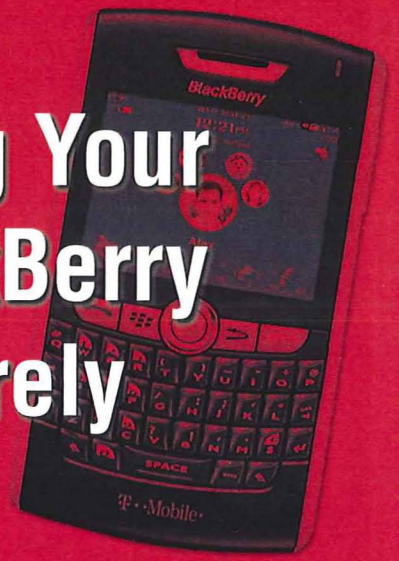
NSA Creative Imaging_33346nl_n51733

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

The Information Assurance Mission at NSA

Using Your BlackBerry Securely



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Information Is A Target. Secure It.

10 Tenets Of Secure BlackBerry Usage

1. (U//FOUO) Never store or process classified information on a BlackBerry device.
2. (U//FOUO) Turn off the radio, power down the device, and remove the battery before entering a classified or sensitive processing area. However, it is recommended that these devices be prohibited from such spaces.
3. (U//FOUO) Maintain a three (3) meter (approx. 10') separation between your BlackBerry and any classified processing equipment.
4. (U//FOUO) Enable an alphanumeric password that is at least eight (8) characters long.
5. (U//FOUO) Maintain physical control over your BlackBerry at all times.
6. (U//FOUO) If you think your device has been tampered with, discontinue its use.
7. (U//FOUO) Lock your device when not in use by using the "Lock Keyboard" icon located on the home screen.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

8. (U//FOUO) Do not download e-mail attachments or files from the Internet unless you are sure of the content.
9. (U//FOUO) Do not solely rely on BlackBerry or any Personal Information Device (PID) for emergency notifications or continuity of operations.
10. (U//FOUO) Never connect or cradle a BlackBerry device to a classified or sensitive computer or system.

Classified Messages

(U//FOUO) In the event that classified messages are stored or transmitted on a BlackBerry device, NSA recommends that the device be destroyed using the proper classified material destruction procedures. Although the BlackBerry "Wipe" command claims to overwrite all memory locations several times, it does not provide the level of assurance required for classified information.

Traveling

(U//FOUO) Often when traveling, a BlackBerry device may leave the possession of its owner during security or customs inspections. It is recommended that before entering such checkpoints, the battery and SIM card (if applicable) be removed from the BlackBerry and placed in a physically different location than the device, such as a bag or coat pocket. As an alternative, the device may be placed in a clear, tamper-evident bag.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Enabling Security Features

(U//FOUO) BlackBerry devices provide several options to help protect the user's information. It is suggested the following options be set:

- (U//FOUO) From the home screen, click on "Options" and then "Security."
- (U//FOUO) The "Password" field should be set to "Enabled."
- (U//FOUO) The "Lock Handheld Upon Holstering" field should be set to "Yes."
- (U//FOUO) From the home screen, click on "Options" and then "Firewall."
- (U//FOUO) The "Status" field should be set to "Enabled."
- (U//FOUO) From the home screen, click on the "Phone" icon, then depress the scroll wheel and click "Options" and then "General Options."
- (U//FOUO) The "Auto Answer Calls" field should be set to "Never."

A Phone Is The Enemy's Cheapest Agent.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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 iOS device 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 iOS device 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 (Settings > General on iPads)
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 iOS device. 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 iOS device 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 iOS device. 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

With the release of iOS 4, some security settings that could only be applied through the iPhone Configuration Utility can now be found in **Settings > General > Restrictions**. This includes disabling the camera and built-in iOS applications like Safari and YouTube.

For other important settings, such as the ability to force encrypted backups, set more complex PINs, and enable remote wipes, the iPhone Configuration Utility is a free tool that Apple provides directly through their website:

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

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 and iPads

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

What This Guide Provides

This pamphlet provides security recommendations for personally managed Apple iPhones and iPads running iOS 4. 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 iOS devices in an enterprise environment. Such issues, including the management of configuration profiles, network infrastructure settings, connecting to VPNs, and Exchange ActiveSync, are covered on Apple's website at http://www.apple.com/support/iphone/enterprise/.

Policy configuration settings for Department of Defense (DoD) and other U.S. Federal Government environments are covered elsewhere. DoD users should consult DISA publications. 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 iOS device. All electronic devices are subject to physical attacks, but the portable nature of cellular phones and iPads puts them at particular risk. Publicly available tools allow an attacker with physical access to your device to bypass some of its security mechanisms.

The best protection against physical attacks is to ensure that your iOS device never falls into the wrong hands. Consider the risks of storing sensitive data on your device. 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 iOS, as these include important security patches. These updates can only be applied through a Internet-connected personal computer running iTunes. It is the responsibility of the individual user to ensure that the device has the latest version of iOS and iTunes software. Regularly check for software updates for iOS and for iTunes. Both updates will occur each time your iOS device is synced with iTunes.

Only sync your iOS device or install iOS updates from a trusted computer.

Do Not Jailbreak Your iPhone or iPad

"Jailbreaking" is the term that refers to the process of modifying the iOS device's operating system in violation of the end-user license agreement. Jailbreaking significantly damages the device's ability to resist attacks because it disables the enforcement of code signatures, which is an important security feature. Jailbreaking an iPhone or iPad makes the attacker's job substantially easier. Most publicly released attacks targeted at iOS devices require that they 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 device by breaking it permanently or corrupting your data.

Enable Auto-Lock and Passcode Lock

The Auto-Lock feature makes the 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 iOS device. With the prompt time set to "Immediately" the device 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: On the same screen, turn off Simple Passcode to enable full alpha-numeric passwords.

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 iOS device 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.

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 iOS device 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"