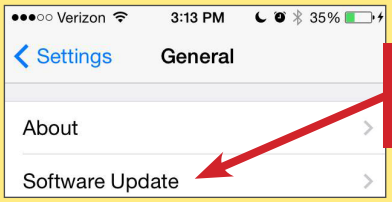
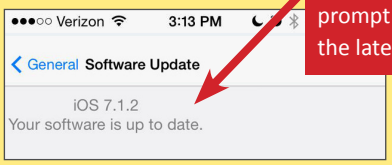
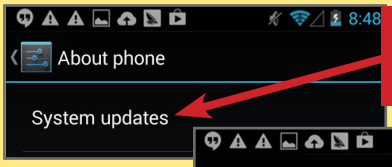
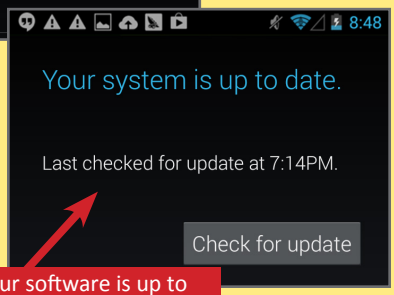
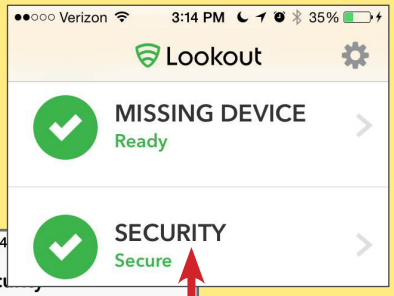
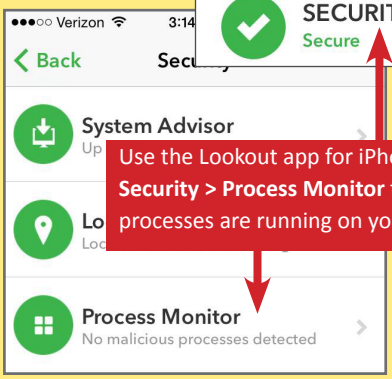
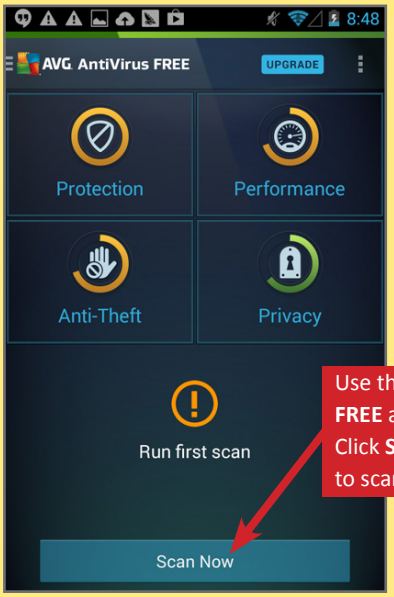
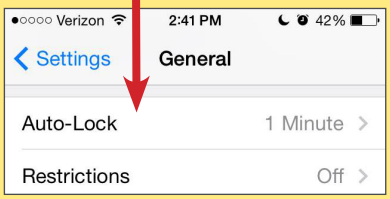
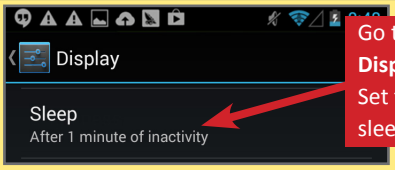
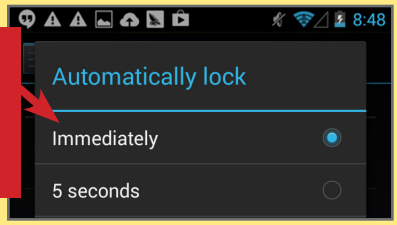
Traveling Safely With Smartphones

Last Updated: 06/16/2014

Traveling with Smartphones - Do's and Don'ts

- Bring a dedicated loaner device; do not bring your personal smartphone.
- Use smartphones with removable batteries when possible.
- Assume that all information on your device could be compromised while traveling in a foreign country.
- Avoid social media, banking, and other sensitive sites while traveling.
- Never store passwords or sensitive information on your smartphone.
- Do not click on links in text messages or emails - especially from people you do not know.
- Do not jailbreak or root your smartphone.
- Examine all mobile devices for evidence of tampering upon your return.

To Do When Traveling	iPhone	Andriod
Ensure that your phone's software is up to date Use apps to ensure that the software on your smartphone is up to date.	 Go to **Settings > General > Software Update**  Check to see if your software is up to date; if not, your iPhone will prompt you to download the latest software	 Go to **Settings > About phone > System updates**  Check to see if your software is up to date; if not, your phone will prompt you to download the latest software
Protect your phone against malware Like a computer, your phone is vulnerable to malware. Use anti-virus apps to ensure that your phone is protected.	  Use the Lookout app for iPhone. Go to **Security > Process Monitor** to see if malicious processes are running on your iPhone	 Use the **AVG Antivirus FREE** app for Android. Click **Scan Now** to scan for viruses
Set your phone to lock automatically In case you lose your device, you want your smartphone to lock automatically to prevent physical access.	Go to **Settings > General > Auto-Lock** Set the Auto-Lock to 1 Minute 	 Go to **Settings > Display > Sleep** Set the phone to sleep **after 1 minute** Go to **Settings > Security > Automatically lock > Immediately** 

Traveling Safely With Smartphones

Last Updated: 06/16/2014

Traveling with Smartphones - Best Practices

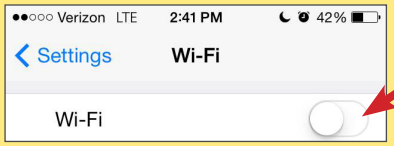
- Assume that your phone may be scanned forensically when you enter a foreign country.
- If possible, encrypt the data on your phone.
- Consider installing a VPN on your device as more secure alternative to saving information locally.

To Do When Traveling

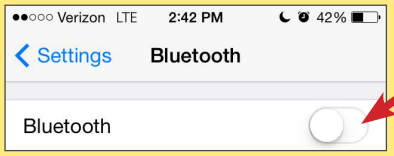
Disable Wi-Fi and Bluetooth

Disable Wi-Fi and Bluetooth on your smartphone; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware and hacking.

iPhone



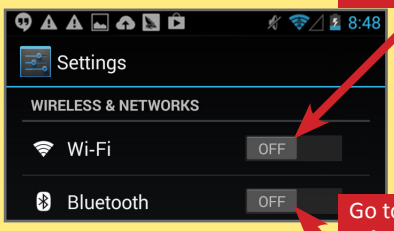
Go to **Settings > Wi-Fi** turn **Wi-Fi** off



Go to **Settings > Bluetooth** turn **Bluetooth** off

Andriod

Go to **Settings > Wireless & Networks > Wi-Fi** turn **Wi-Fi** off

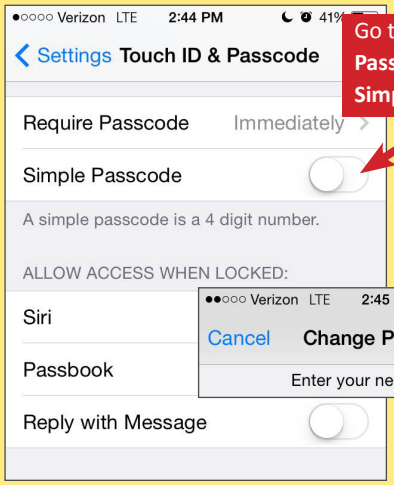


Go to **Settings > Wireless & Networks > Bluetooth** turn **Bluetooth** off

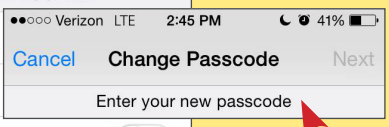
Use a 10+ character password or Screen Lock Pattern

Short passwords are vulnerable to brute force attacks. Choose a password with a combination of letters, numbers, and symbols. If using a Screen Lock Pattern, choose a complicated pattern.

iPhone

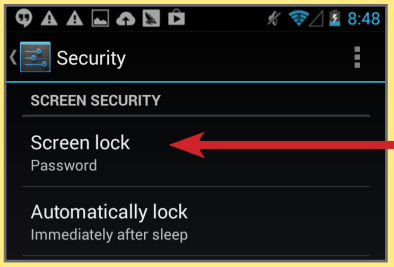


Go to **Settings > Passcode Lock** turn **Simple Passcode** off

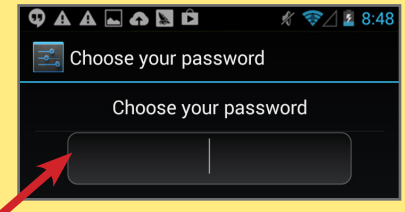


Enter a new passcode with 10+ characters, symbols, and numbers

Andriod

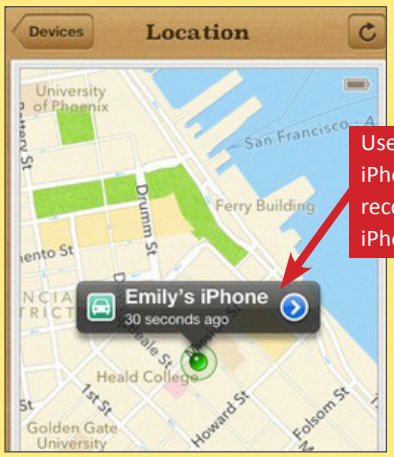


Go to **Settings > Security > Screen lock >** create a screen lock **Password**

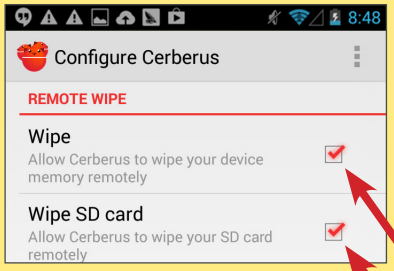


Recover lost or stolen smart-phones and wipe data

Find my iPhone and Cerebus can locate lost devices and wipe data remotely from lost or stolen smartphones.



Use the Find My iPhone app to recover lost or stolen iPhone smartphones



Use the **Cerebus app** to recover lost or stolen Andriod smartphones and wipe data remotely from the device memory and SD card

Useful Links - For more information or questions regarding this card email smartcards@novetta.com

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-network
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx