



# Smartphone Smart Card

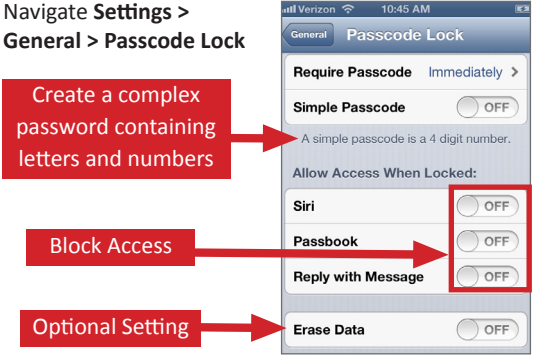
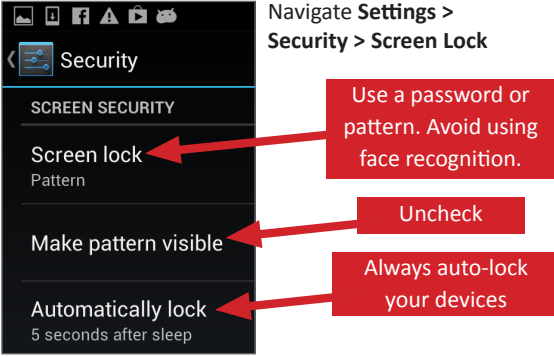



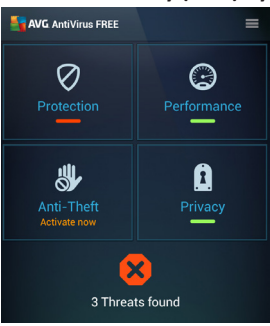


## Smartphones Do's and Don'ts

- Malicious individuals may gain physical access to your smartphone. Protect your device with a password and run apps such as Android Lost and Find My iPhone to help you recover lost or stolen smartphones.
- Malicious emails and text messages can infect your smartphone with malware. Run anti-virus software periodically on your device.
- The camera and microphone can be remotely activated. Do not take a smartphone near classified information, and remove the battery before discussing any sensitive information.
- Wireless networks may be insecure and subject to monitoring. Use VPN when accessing wireless networks, and do not access sensitive information over wireless networks. Turn off Bluetooth when you are not using it to prevent hackers from exploiting your device.
- Apps that you download may gain access to the data stored on your smartphone. Check to see if the app will access your personal data and read user reviews of the app to see if other users experienced trouble after downloading.
- Apps can track your location. Turn off location services to avoid unwanted location tracking.

## Physical Access and Malware Threats

Use the following settings and recommendations to minimize security risks posed by your smartphone and protect your personal data.

Threat	iPhone	Android
<b>Physical Access Threats</b> To prevent others from accessing data on your smartphone, set up a passcode to protect your information. Android has multiple passcode styles including pattern, PIN, password, and fingerprints while the iPhone uses alpha-numerical codes and PINs.	Navigate <b>Settings &gt; General &gt; Passcode Lock</b> 	Navigate <b>Settings &gt; Security &gt; Screen Lock</b> 
<b>Lost or Stolen Phones</b> It is reported that on average 113 cell phones will be stolen every minute in the United States. Download apps such as Find My iPhone or Android Lost to locate, lock, or control your data remotely. These apps allow users to manage data on their smartphones from internet webpages accessed via desktop or portable device.	<b>Find My Phone (Free)</b>  Capabilities: <ul style="list-style-type: none"> <li>• Remote Lock</li> <li>• Erase Data</li> <li>• GPS Locator</li> <li>• Sound Alarm</li> <li>• Send Text Message to Phone</li> <li>• Backup Data Through iCloud Storage</li> </ul>	<b>Cerberus Anti Theft (Free)</b>  Capabilities: <ul style="list-style-type: none"> <li>• Remote Lock</li> <li>• Erase Data</li> <li>• GPS Locator</li> <li>• Sound Alarm</li> <li>• Send Text Message to Phone</li> <li>• Activate Camera</li> <li>• Read Texts Sent</li> <li>• View Call List</li> </ul>
<b>Malware</b> Your smartphone is vulnerable to malware from emails, websites, and downloaded apps. Between 2011 and 2012 alone, smartphones had an increase in malware attacks by over 1,200% with Android being the most susceptible. Download third-party security apps such as Virusbarrier and AVG's Antivirus Security to prevent malware from stealing your information.	<b>Lookout Mobile Security (Free)</b>  Phones are not readily susceptible to viruses. Use this app to prevent passing malware to contacts.  Capabilities: <ul style="list-style-type: none"> <li>• Scan for spyware, adware, and trojans</li> <li>• Scan emails and PDF files before sending</li> </ul>	<b>Antivirus Security (Free) by AVG</b>  Capabilities: <ul style="list-style-type: none"> <li>• App Scanner</li> <li>• File Scanner</li> <li>• Website Scanner</li> <li>• Text and Call Blocker</li> <li>• Remote Lock</li> <li>• Erase Data Remotely</li> <li>• GPS Locator</li> <li>• Kill Slow Tasks</li> </ul>

## Physical Access and Malware Threats


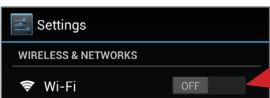
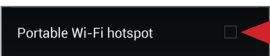
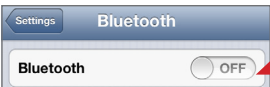

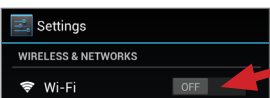
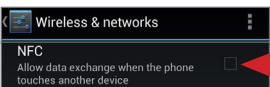
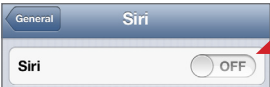
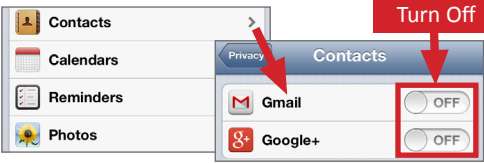
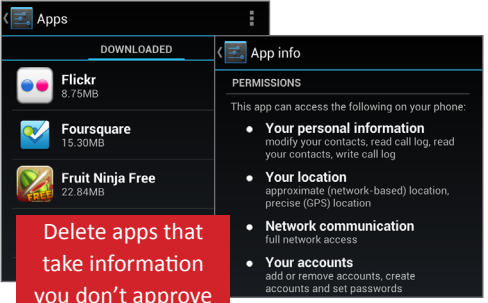

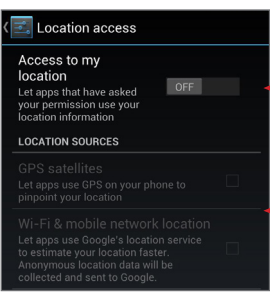
- Updates for smartphones' operating systems are sent out frequently. Install the updates immediately to maximize your protection.
- Jailbroken phones allow malicious apps to bypass vetting processes taken by the app stores. Never jailbreak your smartphones.
- Write down the manufacturer and the serial number of your phone when it is purchased to help identify devices if lost or stolen.
- Avoid linking social networking services like Facebook and Twitter to your smartphones to prevent personal information aggregation.
- Change passwords on your phone frequently (approximately every 6 months) to maximize security.



# Smartphone Smart Card



## Wireless Connections and App Security Settings

Threat	iPhone	Android
<p><b>Wireless Networks</b> Information transmitted via public Wi-Fi networks can be intercepted by third parties. Avoid using public wireless networks when possible and always use a VPN client, such as Shrew Soft VPN (<a href="https://www.shrew.net">https://www.shrew.net</a>) to encrypt your online transactions.</p>	<p>Navigate <b>Settings &gt; Wi-Fi</b></p>  <p>Disable Wi-Fi when not in use</p> <p>Enable Network Permissions</p> <p>Navigate <b>Settings &gt; General &gt; VPN</b> to enable and establish a VPN connection</p>	<p>Navigate <b>Settings &gt; Wi-Fi</b> to manage connections</p>  <p>Disable Wi-Fi when not in use</p> <p>Navigate <b>Settings &gt; More &gt; Tethering &amp; Portable Hotspot</b> and disable <b>Portable Wi-Fi Hotspot</b></p>  <p>Uncheck</p> <p>Navigate <b>Settings &gt; More &gt; VPN</b> to enable and establish a VPN connection</p>
<p><b>Bluetooth</b> Bluetooth involves the wireless communication of two devices within a close proximity. When Bluetooth is enabled, hackers may be able to access the connection to your device and retrieve your contacts, calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and disable it when it is not being used.</p>	<p>Navigate <b>Settings &gt; Bluetooth</b> to disable services</p>  <p>Disable Bluetooth when not in use</p> <p>Navigate <b>Settings &gt; Personal Hotspot</b> to disable broadcasting a personal internet connection.</p>  <p>Never share your Internet connection</p>	<p>Navigate <b>Settings &gt; Bluetooth</b> to manage connections</p>  <p>Disable Bluetooth when not in use</p> <p>Navigate <b>Settings &gt; More &gt; NFC</b> to manage Near Field Communications settings which can be used to transfer data via touching devices together.</p>  <p>Uncheck</p>
<p><b>Data Retaining Apps</b> Downloaded applications frequently collect users' personal information to sell to third party data aggregators. Native applications such as Siri and Google Now will also collect data from users which may include name, email address, credit card numbers, contacts, and device information. These services also record and catalogue the audio during sessions. Avoid using these voice recording services.</p>	<p>Navigate <b>Settings &gt; General &gt; Siri</b></p>  <p>Disable Siri</p> <p>Navigate <b>Settings &gt; Privacy</b> to view and manage which apps are using specific information.</p>  <p>Turn Off</p>	<p>Navigate <b>Settings &gt; Bluetooth</b> to manage connections</p>  <p>Delete apps that take information you don't approve</p>
<p><b>Location Threats</b> The majority of apps will ask permission to track your current location. Users should avoid granting permission to these apps when possible and turn off all location tools when they are not in use. It is also important to note that pictures taken with smartphones retain location information within EXIF data. Never upload pictures taken from your smartphone to social networking sites.</p>	<p>Navigate <b>Settings &gt; Privacy &gt; Location Services</b></p>  <p>Only grant access to apps that require a location function</p> <p>Disable location services when not in use</p>	<p>Navigate <b>Settings &gt; Location Access</b></p>  <p>Disable location services when not in use</p> <p>Uncheck when location services are not in use</p>

### Useful Links

A Parent's Guide to Internet Safety  
Privacy Rights Clearinghouse  
Microsoft Safety and Security  
Online Guardian

[www.fbi.gov/stats-services/publications/parent-guide](http://www.fbi.gov/stats-services/publications/parent-guide)  
[www.privacyrights.org/fs/fs18-cyb.htm](http://www.privacyrights.org/fs/fs18-cyb.htm)  
[www.microsoft.com/security/online-privacy/social-network](http://www.microsoft.com/security/online-privacy/social-network)  
[www.onguardonline.gov/topics/social-networking-sites.aspx](http://www.onguardonline.gov/topics/social-networking-sites.aspx)

NOVETTA   
[www.novetta.com](http://www.novetta.com)