# Table of Contents

Trend Micro Mobile Security – Overview .................................................................................. 4
Chapter 1: Introducing Trend Micro™ Mobile Security for iOS ......................................................... 6
  Key Features ................................................................................................................. 6
  System Requirements ............................................................................................... 8
  Incompatible Software ............................................................................................. 8
  Internet | 3G-4G Connection ..................................................................................... 8
  Recommended Environment ...................................................................................... 8
  Target Market ............................................................................................................ 8
  Availability ............................................................................................................... 8
  Contacting Trend Micro ......................................................................................... 9
  Consumer Support Line ........................................................................................ 9
  Email and Chat Support ......................................................................................... 9
  Premium Services ..................................................................................................... 9
Chapter 2: Getting Started with Trend Micro™ Mobile Security for iOS .............................................. 10
  Download and Install Trend Micro™ Mobile Security ...................................................... 10
Chapter 3: Exploring Trend Micro™ Mobile Security for iOS .......................................................... 13
  Overview of the Mobile Security Console .................................................................... 14
  Secure QR Code Scanner .......................................................................................... 15
  Device Scan .............................................................................................................. 16
  Security Report .......................................................................................................... 17
  Web Guard ................................................................................................................ 19
  Safe Surfing .............................................................................................................. 26
  Fraud Buster ............................................................................................................. 28
  Social Network Privacy ........................................................................................... 36
  Wi-Fi Checker ........................................................................................................... 40
  Data Usage .............................................................................................................. 43
  Device Access Status .............................................................................................. 49
  Lost Device Protection ............................................................................................. 52
  Settings ...................................................................................................................... 55
  Demos: See How Mobile Security Protects You ............................................................. 57
  Today View for Data Usage and SafeSurfing ............................................................... 63
  Transferring Licenses Between Devices ..................................................................... 65
  Mobile Security on Your iPod or iPad ....................................................................... 67

About Trend Micro ............................................................................................................. 68
Trend Micro Mobile Security – Overview

Trend Micro™ Mobile Security (8.0) for iOS provides comprehensive protection for Apple® iPhone®, iPod Touch®, and iPad® devices. Installing easily from the App Store onto your iPhone, iPod, or iPad, Trend Micro Mobile Security for iOS provides the following essential features. Red indicates new or updated feature. F = Free, P = Premium (Paid).

- **Refreshed User Interface** in the Mobile Security Console provides easier access to all functions (F, P)
- **Secure QR Code Scanner.** Provides threat protection against bad URLs and apps when scanning QR Codes. (F, P)
- **Device Scan.** Scans your device for security issues and provides Things to Fix Scan Results. (F, P)
- **Security Report.** Provides comprehensive security report for configurable span of 7, 14, or 30 days. (F, P)
- **Features.** Comprehensive Features panel provides details on all the functions in Mobile Security (F, P)
- **Web Guard.** Protect yourself or your children by filtering out inappropriate or dangerous websites in favorite browsers; e.g., Safari or Chrome, with a high-performance VPN. (P)
- **SafeSurfing.** The SafeSurfing browser uses the Trend Micro™ Smart Protection Network™ to block malicious websites. (P)
  - **Private Tab in SafeSurfing** does not remember websites or track history.
  - **SafeSurfing** engine boosts performance and provides HTML 5 support for an advanced browsing experience.
  - The URL Scan widget in **Today View** scans URLs to check if they’re safe.
- **Fraud Buster.** Avoid scams through emails, instant messages, and images. (P)
• **Social Network Privacy.** Scan and fix your Facebook™ and Twitter™ privacy settings, to increase your privacy and to protect from data theft. (P)

• **Wi-Fi Checker.** Check Wi-Fi hotspots for security issues. Warns you when a Wi-Fi hotspot is unsecured by a certificate or password, which can open the connection to suspicious interference. (F, P)

• **Data Usage.** Helps users manage monthly data plan usage with Cellular, Roaming, and Wi-Fi monitors. (P)

  The Data Usage widget in Today View reports how much data has been used or is left against your monthly cellular data limit.

• **Device Access Status.** Set a passcode to protect your Mobile Security settings. Sign into iCloud to check your two-factor authentication status. Check if your iOS System has been modified by unauthorized changes. (F, P)

• **Lost Device Protection.** Remotely locate a lost or stolen device on a Google map using GPS, Cell Towers, or Wi-Fi. Trigger an alarm on your device, even if it is in silent mode. (P)

• **Settings.** Configure Mobile Security to your preferred usage settings. (F, P)

• **In-app Demos.** Provides easy-to-understand in-app demos, to teach you about Web Guard and Wi-Fi Checker. (F, P)
Chapter 1: Introducing Trend Micro™ Mobile Security for iOS

This chapter introduces you to Trend Micro™ Mobile Security for iOS v8.0. The topics discussed in this chapter include:

- Key Features
- System Requirements
- Incompatible Software
- Internet | 3-G-4G Connection
- Recommended Environment
- Target Market
- Availability
- Contacting Trend Micro

Key Features

All features of Trend Micro Mobile Security for iOS are available during the Trial. When the Trial has expired, you can use it for Free, but you must buy a subscription (Paid) to enable the full feature set. (Red = updated or new)

Table 1. Trend Micro Mobile Security for iOS 8.0

<table>
<thead>
<tr>
<th>iOS Security Features</th>
<th>Free</th>
<th>Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Console – Refreshed UI provides easier access to key functions.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Secure QR Code Scanner – Scan QR Codes safely; blocks malicious apps and URLs.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Device Scan – Scans devices for all potential security issues that need fixing.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Security Report – Provides comprehensive security report over the span of 7, 14, or 30 days, to show how Mobile Security protects you.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Features – Comprehensive Features panel provides details on all the functions in Mobile Security.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web Guard – Provides Firewall (DNS Settings) and smart VPN to filter unwanted websites, ads, and trackers. Provides Parental Controls with predefined and custom settings.</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
**iOS Security Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Free</th>
<th>Paid</th>
</tr>
</thead>
</table>
| **SafeSurfing** – Built-in secure browser uses the Trend Micro™ Smart Protection Network™ to block malicious websites.  
  - Open Browser at Startup displays SafeSurfing browser when you open Mobile Security.  
  - Do Not Track helps prevent websites from collecting information about you.  
  - Privacy Tab ensures the SafeSurfing browser will not remember the websites you visit or your search history.  
  - Reading Mode removes all distractions except the text, for distraction-free article reading.  
  - Bookmark Folders let you organize your bookmarks by folders.  
  - Customize Launch Page so you can determine which bookmarks display in the Launch page.  
  - Copy / Paste iOS Widget in Today View lets you check suspicious URLs. | | ✓ |
| **Fraud Buster** – Protects you against phishing scams through email, instant messages, and images. | | ✓ |
| **Social Network Privacy** - Scan your Facebook and Twitter privacy settings easily; recommends enhancements and help you make the changes. | | ✓ |
| **Wi-Fi Checker** – Blocks unsecured or dangerous mobile Wi-Fi hotspots. Enables hybrid VPN for protection. | ✓ | ✓ |
| **Data Usage** - Data Usage monitor helps you manage data plan usage and costs for Cellular, Roaming, and Wi-Fi. iOS Widget lets you see your Data Usage in the Today View. | | ✓ |
| **Device Access Status** – Set a passcode to protect your Mobile Security settings. Sign into iCloud to check your two-factor authentication status. Check if your iOS System has been modified by unauthorized changes. | ✓ | ✓ |
| **Lost Device Protection: Remote Locate / Alarm** - Helps you find your devices on a Google map using GPS, cell towers, or Wi-Fi. Enables you to trigger an alarm on your device – even if it is in silent mode. | | ✓ |
| **Settings** – Configure Mobile Security to your preferred usage settings. | ✓ | ✓ |
| **Online Technical Support** - Support provided via online forums, knowledgebase, and email. | | ✓ |
| **In-App Demos** - Provides in-app demos showing you how Web Guard and Wi-Fi Checker works. (Note: these demos are subject to change.) | ✓ | ✓ |
System Requirements

Table 2. Mobile Security 8.0 for iOS - System Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>iOS 9.0 or later. 64-bit device required for latest versions.</td>
</tr>
<tr>
<td>Device Space</td>
<td>Global / EMEA / APAC: 50 MB minimum</td>
</tr>
<tr>
<td>Supported iOS Devices</td>
<td>iPad® Air 1, Air 2, Mini 2, Mini 3, Mini 4, iPad® Pro, iPod® Touch 6</td>
</tr>
<tr>
<td>Other</td>
<td>3G/4G (LTE)</td>
</tr>
</tbody>
</table>

Incompatible Software

To identify software that you should remove from the device before installing Trend Micro Mobile Security, please refer to the following Web site:


Internet | 3G-4G Connection

Trend Micro Mobile Security for iOS uses a Wi-Fi Internet or 3G-4G connection for activating the program online, checking the expiration date, downloading updates, sending Trend Micro URL/web queries and logs to the portal, logging into the management portal, and browsing knowledge-based pages on the Trend Micro Web site.

3G-4G data connections fees are usually charged on a monthly basis, using a fixed allocation with an upper limit. If you exceed this limit, you will be charged additional fees for the amount of time connected or for the amount of data downloaded. Testers are therefore encouraged to use a Wi-Fi router-based connection to the Internet whenever possible.

Recommended Environment

This Product Guide assumes that you are using Trend Micro Mobile Security in conjunction with a PC, Mac, or tablet, so you can log in to the Trend Micro Mobile Security Portal easily at http://www.trendmicro.com/LostDevice and review your Lost Device Protection settings and execute certain actions.

Target Market

Trend Micro Mobile Security is targeted to mobile users who wish to secure their iPhones and iPads from malicious applications, web threats to them and their family, unwanted calls and messages, and device loss. (Also available for Android.)

Availability

September 10, 2019 – App Store, iTunes
Contacting Trend Micro

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Consumer Support Line
(800) 864-6027 – Monday - Friday, 5:00AM - 8:00PM Pacific

Email and Chat Support
Paid users of Mobile Security may obtain free email, chat, and community forum support.
For more information, contact eSupport at: www.trendmicro.com/support/home.

Premium Services
Trend Micro offers Premium Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, and more. For more information, visit www.trendmicro.com/support/home.
Chapter 2: Getting Started with Trend Micro™ Mobile Security for iOS

This chapter gets you started with Trend Micro™ Mobile Security for iOS. Topics discussed in this chapter include:

- Downloading and Installing Trend Micro Mobile Security

Note: Trend Micro Mobile Security is also included with Trend Micro Maximum Security. To download the software, users can simply launch the Trend Micro Security Console. A “Protect Another Device” link to the Mobile Security installer is available in the Console.

Download and Install Trend Micro™ Mobile Security

To download and install Trend Micro Mobile Security:

1. Tap the App Store icon on your iOS device to load it. The App Store screen appears.

2. Tap the Search icon at the bottom to load the search field. The Search field appears and your iOS keyboard pops up.

3. Type Trend Micro in the search field and when the Trend Micro page appears, scroll down to Trend Micro Mobile Security in the list and tap the listing. The Trend Micro install page appears, with Trend Micro Mobile Security at the top.

5. When installation is complete, tap Open.

6. A popup appears, saying “Mobile Security” Would Like to Send You Notifications.

7. Tap OK if you want to allow them. The Privacy and Personal Data Collection Disclosure appears.

8. Read the Privacy and Personal Data Collection Disclosure. If you agree with it, click Continue.
9. The License Agreement appears.

10. Tap the Trend Micro License Agreement link to read it. If you accept the terms of the agreement, tap Accept. The Mobile Security Console appears.

11. You’re now provided with trial and purchase options for Trend Micro Mobile Security.

12. If you already have a Premium account, you can sign in to activate the product. Just follow the instructions in the app.
Chapter 3: Exploring Trend Micro™ Mobile Security for iOS

This chapter provides an overview of Trend Micro Mobile Security for iOS. Topics discussed in this chapter include:

- Overview of the Mobile Security Console
- Secure QR Code Scanner
- Device Scanner
- Security Report
- Web Guard
- Safe Surfing
- Fraud Buster
- Social Network Privacy
- Wi-Fi Checker
- Data Usage
- Device Access Status
- Lost Device Protection
- Settings
- Demo: How Trend Micro Mobile Security Protects You
- Today View for Data Usage and SafeSurfing
- Transferring Licenses Between Devices
- Mobile Security on your iPod or iPad
Overview of the Mobile Security Console

To launch the Mobile Security Console:

1. Tap the Trend Micro Mobile Security icon on your device to load the Console.

2. Tap the Secure QR Code Scanner icon in the upper right-hand corner to scan a QR Code.

3. Tap the Scan button to scan your device for security issues; or Things to fix for the scan results.

4. Tap the Security Report icon to get a security report for 7, 14, or 30 days.

5. Tap Features to get a list of helpful tips on using the features.

6. Tap Web Guard to activate the smart VPN, Filter Websites and set Parental Controls.

7. Tap SafeSurfing to launch the SafeSurfing browser to safely surf the Web.

8. Tap Fraud Buster to avoid scams shared through instant messages and images.

9. Tap Social Network Privacy to check your privacy settings on Facebook™ and Twitter™.

10. Tap Wi-Fi Checker to check Wi-Fi hotspots for no password protection or signs of interference.

11. Tap Data Usage to set up and track your data usage per billing cycle.

12. Tap Device Access Status to review your if a Passcode is set, Two-Factor Authentication, and iOS system modifications.

13. Tap Lost Device Protection to turn on the ability to locate your lost device or trigger an alarm.

14. Tap Settings to configure core settings.


16. Tap Renew/Activate to renew or activate your subscription.
Secure QR Code Scanner

Trend Micro Mobile Security provides a Secure QR Code Scanner that protects you from malicious URLs and apps when scanning QR Codes.

To use Secure QR Code Scanner:


2. Place the QR Code within the frame to scan. The code is scanned securely and the URL/app appears; e.g., Trend Micro Mobile Security on the App Store.

3. If the QR Code is dangerous, you’ll be blocked from going to the URL or app.
Device Scan

The Device Scan scans your device for security issues and vulnerabilities—things you need to fix to ensure your device is fully protected from viruses, malware, and other threats.

To scan your device:

1. Tap the large Scan button to conduct a device scan. The scan begins. Each function of Trend Micro Mobile Security is checked for things to fix.

   As it goes through each function in turn, (i.e., Content Shield, SafeSurfing, Social Network Privacy, etc., the wheel above the scan shows the progress of the scan as it checks each function.)

2. When the scan is complete, it shows x Things to Fix.

3. Follow the instructions shown in the list and use any buttons or links shown to fix that item; e.g., Web Guard, Wi-Fi Checker, Lost Device Protection.

4. Scroll down the page to view other security items; e.g., Data Usage.
Security Report

Trend Micro Mobile Security provides a Security Report, giving you a Protection Summary for the various kinds of protections used during the last 7, 14, or 30 days.

To view the Security Report:

1. Tap the Security Report icon to the right of the Scan wheel. The Security Report appears, with the Protection Summary at the top, showing activity bars over a given timespan.

2. Tap the Timespan drop-down menu, to set the Protection Summary for the Last 7, 14, or 30 days.

3. In this example, tap Web Guard browsing activities, to display the number of websites scanned by Web Guard, along with the number of malicious websites blocked.
4. In this example, tap **Safe Surfing** browsing activities, to display the number of websites scanned by **SafeSurfing**, along with the number of malicious websites blocked.

5. Tap **Wi-Fi network connections**, to view the number of connections scanned by **Wi-Fi Checker**. (In this example, none are shown.)

![Figure 24. Safe Surfing Browsing Activities](image1)

![Figure 25. Wi-Fi Network Connections](image2)
Web Guard

Web Guard uses a hybrid (client-cloud) VPN to protect users from malicious websites, ad trackers, and inappropriate content when using SafeSurfing, Mobile Security’s own browser; another preferred browser, such as Safari or Chrome; or an app that uses its own internal browser. When protecting kids from inappropriate or unwanted content, parents have complete control over what data their kids can see.

VPN Settings

To turn on the VPN:

1. Tap the Web Guard panel in the Console. The Web Guard VPN dial appears.
2. A popup indicates Web Guard needs permissions before you can use this feature. Tap the popup at the top to start the approval for permissions.

Figure 26. Web Guard

Figure 27. VPN Off
3. A popup dialog appears, indicating “Mobile Security” Would Like to Add VPN Configurations.

4. Tap Allow. Enter your device’s password or use Touch ID to Add VPN Configurations.

5. The VPN turns On.

6. Note the demo popup that remains. We’ll show the demo later, so close it for now using the X on the upper right.

7. Tap VPN Settings to configure the settings. The VPN Settings screen appears, with two options.

   **RECOMMENDED VPN SETTINGS**

8. Trend Micro Web Safe is pre-selected to allow ads and tracking, while blocking unwanted websites.

9. Trend Micro Parental Controls can be selected to protection your children.
10. Tap the Trend Micro Parental Controls panel to set the Parental Controls settings. The Set Parent Key screen appears.

11. Type a 4-digit key to secure Parental Controls, then confirm it.

12. The Parental Controls Settings screen appears for you to configure it. (See below.)

**Trend Micro Parental Controls**

To use Parental Controls:

1. Select a pre-defined age group, Teen, Pre-teen, or Child; or select Custom to pick the settings you prefer.

2. Tap each category you wish to modify, select the subcategories you wish to add, then tap OK to save your changes:
   - Adult or Sexual

![Figure 32. Set up a 4-digit key](image1)

![Figure 33. Confirm Your Key](image2)

![Figure 34. Teen](image3)

![Figure 35. Adult or Sexual](image4)
- Communications or Media.
- Controversial

3. Toggle the **Ad & Tracker Block** to **On** to protect you from ad or to stop websites from collecting information about you.

4. Tap the back-arrow in the top menu to return to the **Web Guard** screen.
5. When Parental Controls is on, an Identity icon appears near the On pointer of the VPN dial, indicating that Parental Controls is active.

6. Note that at any time, you can Reset the Parent Key. To do so, you’ll need your current key. See the second section following for details.

Test the filters:

1. To test the filters, go to your chosen browser; e.g., Safari, and type a website prohibited by the filter.

2. The Parental Controls filter will block the website, providing a Website Blocked: Off Limits notification, as well as an Off Limits webpage.

3. Dangerous websites will also be blocked.
Blocked Websites | Approved Websites

To edit Blocked | Approved Websites:

1. Back in the main screen, tap the Blocked Websites panel to get a list of all websites the user has attempted to access.

2. Provide your Parent Key.

3. View the Blocked Websites, or tap Edit, the Checkbox, then Remove to remove the website(s).

4. Alternately, tap Add Selected to Approved Websites to add it to the Approved Websites list.

5. Note that you can manually add a website to the Approved Websites list by tapping Add Website.

6. As before, to delete a website, tap Edit, select the Approved Website(s), then tap Delete and the Remove popup to delete the website(s) from the Approved Websites list.
**Reset Parent Key**

To reset the Parent Key:

1. Back in the main Web Guard screen, tap Reset Parent Key. A popup appears, to sign into your Trend Micro Account, so you can reset the Parent Key.

2. Enter your ID and Password and tap OK.

3. Another screen appears, indicating the Parent Key was reset and your old key was removed.

4. Type a new one, then confirm it. Your new Parent Key is now active.
Safe Surfing

To ensure Safe Surfing:

1. Tap the SafeSurfing panel to open the SafeSurfing browser. The browser appears.

2. In the location field, enter the URL of a website you wish to browse and tap Go.

   In this example, we use a dangerous page from the Malware Domain List.

3. Because this site is malicious, SafeSurfing blocks it to protect you.

4. If you still want to visit this website despite the risk, tap Still want to open this page, despite the risk? (This is not recommended.)

5. Close the dangerous page by tapping the Website History icon in the lower right-hand corner of the SafeSurfing browser. Websites recently searched or visited display on the page.

6. Tap the close X in the upper right-hand corner of the webpage(s) displayed, then tap Done. This returns you to the main SafeSurfing browsing page.
7. Browse again to any website; e.g., www.bing.com. The website opens.

8. If you wish to protect yourself from websites collecting information about you, tap the Block icon to the left of the location field. The Ad & Tracker Block screen appears, with the toggle turned off by default.

9. Enable Ad & Tracker Block by enabling the Content Shield VPN Settings for Trend Micro Total Safe or Parental Controls.

10. To browse websites without leaving a search or visit history, back in the main SafeSurfing browser window tap the Mask icon to open a New Private Tab.

11. Using the Private Tab, browse to any website. The SafeSurfing browser will not remember the websites you visit or your search history.

12. Use the Back and Forward Arrows to move between websites still open in memory.

13. Tap the Star to add websites to Favorites.

14. Tap the Up-Arrow/Share tool to share websites with your friends, using any of the options provided.
Fraud Buster

Use Fraud Buster to avoid scams shared through emails, instant messages and images. Using the Camera Roll Scan, you can analyze an image, typically a screenshot of an email or text you’ve received, by scanning it for URLs and if any are found, it runs a Web Threat Protection (WTP) check on it, to check if the website is malicious. It can also scan QR Codes for the same and the scan can be automated. You can also scan iMessages for scams and bad URLs, to simplify the checking process for messages.

To use the Fraud Buster Camera Roll Scan:

1. Tap the Fraud Buster panel. A popup appears, informing you of Fraud Buster’s data collection scope, which may include sender ID, text, and URLs, saved as hash values and deleted within 6 months.

2. If you accept, tap Accept.

4. If you accept, tap OK. Now you’ll see a popup instructing you to Tap to check the safety of a website.

5. Tap the WWW Link Scanner icon and popup appears for you to copy and paste or type a website’s address to check if it poses a risk.

6. Tap Scan once you’ve entered the URL. Fraud Buster scans the URL and returns the result. In this case, the URL is Safe from security risks.
7. Now, say that you’ve received an email or message containing a link that you think is suspicious. You want to test it out before tapping it by using Fraud Buster.

8. Take a screenshot of the email or message with the link showing by holding the Top Side button, clicking the Home button, and then releasing both on your iOS device. A screenshot will be taken and stored in your Camera Roll.

9. Now tap the Camera Roll Scan button.

10. The Camera Roll screen appears, with a list of your images and screenshots.

11. Tap the selection button for the most recent screenshot in the upper left-hand corner of the image. The image will show that it has been selected (1), then tap Done.

12. Fraud Buster’s Camera Roll Scan scans the image for the URL and returns the result.
13. If the link in the email is malicious, Fraud Buster indicates it; e.g., *This image contains links to risky websites.* You should delete the email or message.

14. You can automate this process if you wish. Refresh the screen by tapping the back-arrow, then in the main screen of the Console, tap the Fraud Buster panel again.

15. Note the **Automatic Scan settings** link. Tap it to open the settings.

16. The **Automatic Scan Settings** screen appears.

17. Tap **Automatically scan new screenshots** to toggle the feature on.

18. If **Web Guard** is not already enabled, a popup appears for you to enable it.

19. Tap **OK** and Web Guard is enabled.
20. Now take a screenshot of the suspicious email, with the link showing as before. A notice automatically appears at the top of your phone, asking Do you want to scan the new image you just saved?

21. Tap the popup to scan the image. The image is scanned as before and returns the result.

22. If the image contains links to risky websites, Fraud Buster’s Camera Roll Scan will let you know.

23. If the image contains links to risky websites, you should delete the email or message.

To enable iMessage Scan:

1. Tap the iMessage Scan tab in the Fraud Buster screen. An instruction screen appears.
2. Tap **Get Started** to learn about how to enable the **iMessage Scan**.

3. Follow the four steps shown to get protection.

4. Tap **Settings**.

5. Tap **Messages**.

7. Toggle on Mobile Security to enable Fraud Buster’s iMessage Scan.

8. A popup appears, asking if you wish to **Enable Mobile Security SMS Spam Filter?**
   Read the popup carefully. Enabling the feature allows your device to send various content to Trend Micro.

9. If you agree to the conditions, tap **Enable**.

10. Now when you receive an iMessage that contains a suspicious link, Fraud Buster will give you a preview.
11. When you Tap to Load Preview, Mobile Security will scan it and tell you if it’s malicious. If it is, popup will appear saying Website Blocked.

12. If you tap the link, your browser will load, Mobile Security will repeat the warning, and the browser page will indicate that the website has been blocked—in this case providing a message Suspicious Page.

13. Please close this page, then delete the message.
Social Network Privacy

Trend Micro Mobile Security also provides **Social Network Privacy**, to scan and edit your Facebook™ and Twitter™ privacy settings.

**To Scan Facebook:**

1. Tap the **Social Network Privacy** panel in the main **Console**. The **Social Network Privacy > Remove Privacy Risks** screen appears for you to sign into your Facebook account to check your privacy settings.

2. Tap **Sign into Facebook**. A screen appears for you to sign in.

3. Enter the email address and password for your Facebook account and tap **Log In**.

4. Mobile Security scans Facebook for privacy concerns. When it’s done checking, it presents you with the analysis.
5. Tap **Improve Now**, to fix all the privacy concerns at once; or tap the particular item panel. A window appears, showing the items that should be changed.

6. In this example, select **Friends**, then tap **OK** to make the change.

7. Mobile Security makes the change, telling you “Nice work! You don’t have any privacy concerns.”

8. Tap **Check Again** if you want to double-check your privacy settings, to make sure the changes have been made.
To Scan Twitter:

1. Back in the main Console, tap the Social Network Privacy Shield to the left, then tap then the Twitter icon in the menu to open the window to Sign into Twitter.

2. Tap Sign into Twitter and a window appears for you to enter your phone, email, or username and password.

3. Tap Log in to begin scanning your Twitter privacy settings.

4. Mobile Security checks the settings and returns the result.

5. As with Facebook, tap Improve Now, or tap the individual settings panel(s) to change the setting.
6. A popup appears to show you the privacy settings that will be change. Tap **Improve** to change the settings.

7. Mobile Security improves the privacy settings and tells you “Nice Work! You don’t have any privacy concerns.”
Wi-Fi Checker

To use Wi-Fi Checker:

1. Tap Wi-Fi Checker to check if the Wi-Fi network you’re connected to is safe.

2. Wi-Fi Checker scans the network to check for any signs of interference and if the Wi-Fi network is password-protected.

3. If it’s safe, it returns the result No Risks Found.

4. If it’s risky, it returns the result Risks Found.

5. Tap Switch to another Wi-Fi or Use 3G/4G instead to use another network.
6. Tap Trust this Wi-Fi despite the risk to add it to the Approved List.

7. Wi-Fi Checker adds it to the list, but notifies you of security risks. Tap the X to close the notification.

8. Tap to Settings > Wi-Fi Checker > Approved List to edit it.

9. Tap Edit to begin the edit.
10. Select the Wi-Fi in the Approved List you wish to remove, then tap Delete.

11. A popup appears, asking if you wish to remove the Wi-Fi.

12. Tap Remove to remove it from the list.

Figure 108. Delete from Approved List

Figure 109. Remove Wi-Fi?
Data Usage

Trend Micro Mobile Security provides a Data Usage monitor to help you track your data usage against the Cellular and Roaming data plans you’ve chosen with your provider, as well as your Wi-Fi data usage. For greater accuracy, open Mobile Security before and after restarting your mobile device and keep it running in the background.

To use Data Usage:

1. In the main screen of the Console, tap Data Usage below the Features panel. The Data Usage instruction screen appears, advising you to set up a plan to track your cellular data usage.

   **Note:** A similar instruction screen also appears for Roaming and Wi-Fi data usages.

2. Tap the instruction screen to display the Data Usage > Cellular screen, then the circular Settings icon on the right to open Cellular Data Settings.

3. The Data Plan defaults to Undefined. Tap Data Plan to change this setting by first toggling the Unlimited toggle off. You’re provided with a field to enter a Data Limitation.

---

**Figure 110. Data Usage**

**Figure 111. Set Up Cellular Data Usage Plan**

**Figure 112. Data usage | Cellular**

**Figure 113. Cellular Data**
4. Tap the **Data Limitation** field, then enter the data amount, and tap **Done**.

5. Choose the Unit of measure (GB or MB).

6. Return to the main **Cellular Data** settings screen and tap **Billing Cycle** to set the cycle. The **Billing Cycle** screen appears.
7. Tap Billing Cycle to enter the billing cycle pick list, then scroll to the proper cycle. When done, tap Billing Cycle again to close the pick list.

8. Tap Start On to set the start date of the billing cycle; when the pick list appears, scroll to the day the billing cycle begins; then tap Start On again to close the setting.

9. Back in the main Cellular Data settings screen, toggle Alert on. A popup appears for you to Turn On Alerts, saying “To track more accurate data usage and see alerts at the right time, open Mobile Security every few days and let it continue running in the background.”

10. Tap OK to close the dialog. The Alert toggle is turned on, and the First and Second Alerts appear, set by default to 80% and 100% of your data plan.
11. To adjust the Exceeding Plan Alerts, tap each respectively to change the percentage at which the alert will activate, then tap Done.

12. If necessary, scroll down to Optional Settings to manually set the amount of data already used in this billing period by tapping Adjust Current Usage. An edit screen appears.

13. Enter the amount you’ve already used in this billing period and tap Done; then adjust the Unit if needed.

14. Return to the main Data Usage screen. The Data Usage for Cellular data displays a graph of your settings, providing Predicted Data Usage and Days Left in Billing Cycle.
15. To adjust the Roaming Data settings, tap the Roaming tab in the main Data Usage screen.

16. Either manually adjust each setting to fit a separate Roaming data plan (e.g., 650 MBs), or toggle Match Cellular Data Settings on to match that group of settings.

17. Finally, adjust the Wi-Fi Data settings in the same way as the previous two, either manually or by matching the cellular data settings and billing cycle.
18. View a graphical report of usage for the Month and Year for Cellular Data, Roaming Data, or Wi-Fi Data, by tapping the respective tab.

19. Then tap the Graph icon in the upper left of the Data Usage screen. A graph of Usage History appears. For example, the Wi-Fi Usage History for the current Month or Year.

Figure 130. Wi-Fi Usage History | Month

Figure 131. Wi-Fi usage History | Year (to date)
Device Access Status

Trend Micro Mobile Security automatically checks the access status of your device. **Device Access Status** monitors whether you have a **Passcode** on your device, the status of your **Apple Two-Factor Authentication**, and if your **iOS System** has been compromised by unauthorized modifications.

To check your Device Access Status:

1. In the main **Console** window, tap **Device Access Status**. The **Device Access Status** screen appears, with a rating on the two items of your device status.

2. In this example, a **Passcode** for the device has already been set and your **Two-Factor Authentication** status needs to be checked in iCloud.

![Figure 132. Device Access Status Panel](image1)

![Figure 133. Device Access Status](image2)
3. Tap **Two-Factor Authentication** to sign into iCloud to check your **Two-Factor Authentication** status. A screen appears to log into your Apple account.

4. Enter your **Apple ID** and **Password** and tap the right-hand arrow to log in. A popup appears, asking for you to allow the sign-in. 

5. Go to one of your other Apple devices, where the same screen will appear.

6. On that second device, tap **Allow** to allow the login. Apple presents you with a six-digit **Apple ID Verification Code** on the second device.

7. Back on the first device, enter the **Verification Code** into the **Two-Factor Authentication** screen.
8. You’re automatically logged into your Apple Account and the Two-Factor Authentication verification is complete.

9. The Device Access Status gauge shows Excellent and your Two-Factor Authentication has been verified.

10. The main screen of the Console also shows Excellent, no action required.
Lost Device Protection

To enable Lost Device Protection:

1. Back in the main Console, tap Lost Device Protection. The Lost Device Protection screen appears, with instructions to turn on Location Services.

2. Tap Turn It On Now to turn on the services.

3. A popup appears, asking if you wish to Allow “Mobile Security” to access your location?
   - Only While Using the App
   - Always Allow
   - Don’t Allow

4. If you wish, tap Allow to allow this function. A Device Located screen displays, with a link to the Lost Device Protection Portal.

5. Copy and email this link to your PC or Mac, so you can access the portal later if your device is lost or stolen.
Lost Device Protection Portal

To access the Lost Device Protection Portal:

1. Launch your browser on your Mac, PC, smartphone or tablet and type http://www.trendmicro.com/LostDevice into the search field, and hit Enter. The Lost Device Protection Portal webpage appears.

2. Tap Find Now or Sign in to sign into your Trend Micro account. The Sign In page appears.

3. Enter the email address and password you used to create your Trend Micro Account and click Sign in.

4. The Lost Device Protection Portal appears, with the location of your device shown on the Google map. Zoom the map for a closer view.

5. Click Share to share the device’s location with a trusted nearby friend.

6. Click Alarm to sound a one-minute alarm on your misplaced device, even if it has been set to silent mode.

7. Click Refresh to refresh the Google map.
8. Click **Device Details** (below the device icon on the upper left of the portal) to view device details about your subscription.

![Image of Device Details](image_url)

**Figure 148. Device Detail**
Settings
To Access System Settings:

1. Tap Settings at the bottom of the main Console to open Settings.

2. Scroll down to review the options in the Settings screen.

ACCOUNT & REGISTRATION
Trend Micro Account. Shows the account to which you’re registered.
Expiration Date. Expiration date for your subscription
Activation Code. Shows the 20-digit activation code in use.
Renew / Activate. Renew now or use an Activation Code.
Sign Out. Disconnect your Trend Micro account (needs password).
Restore Purchase. Manage your account and subscriptions.

WEB THREAT PROTECTION
Filtering Level. Set filtering level.
High. Blocks websites showing any signs of transmitting malicious software, including suspicious websites that may not actually cause problems.
Normal. Protects against malicious software, online fraud, and other threats, without aggressively blocking minor security risks.
Low. Only blocks sites confirmed as fraudulent or malicious.

SAFESURFING
Open Browser at Startup. Toggle to On and the SafeSurfing Browser will automatically open when you launch Mobile Security.
SOCIAL NETWORK PRIVACY

Facebook. Sign in or out of your Facebook Account.

Twitter. Sign in or out of your Twitter Account.

Wi-Fi CHECKER

Wi-Fi Checker. Toggle on to check Wi-Fi security.

Approved List. Tap to edit Wi-Fi Approved List.

DATA USAGE

Cellular Data. Set settings for cellular data monitoring.

Roaming Data. Set settings for roaming data monitoring.

Wi-Fi Data. Set settings for Wi-Fi data monitoring.

Notifications. Tap to set notifications:

> Notify me before my protection expires.
> Notify me about new surveys.
> Notify me about the security report every two weeks.

ABOUT & HELP

About. Provides version number.

Help. Takes you to Mobile Security for iOS Support

Chat Support. Takes you to the chat line.

Support Online Community. Start or join a conversation about Mobile Security for iOS.

Share with Friends. Share with friends on social media.

Send Feedback. Rate and review this app on App Store. Send feedback to the Trend Micro Community.

Collect Logs. Collect a log to assist with troubleshooting.

Remote Config Debug. Lets you enabling debugging for troubleshooting.

Help Improve This App. Toggle On/Off to share/not share usage data with Trend Micro.
Demos: See How Mobile Security Protects You

At the bottom of the Mobile Security Console, you’ll find demos that help you to understand how Trend Micro Mobile Security protects you. Simply tap the leading image to see a multi-stage demo on the security feature. The current TMMS release includes demos for Web Guard and Wi-Fi Checker.

**Note:** In-app demos are subject to change or additions.

To view the Web Guard demo:

1. Tap the **Web Guard** demo image at the bottom of your **Console**. The first page of the demo appears.
2. Tap **Experience Phishing Scams** to see how a phishing scam works.

![Figure 152. See How Mobile Security Protects You with Web Guard](image1)

![Figure 153. Experience Phishing Scams](image2)
3. The demo loads a virtual inbox, showing an Online Docs email that appears to be from a trustworthy sender, but isn’t.

4. The demo shows how you’d open the email. Tap Next to view the resulting email.

5. The demo shows how you’d tap the doc to open it. Tap Next to view the result.

6. The shows how you’d normally be taken to a fake website, where you’d enter your ID and Password and the hacker would steal it.

7. With Web Guard, however, tapping the doc in the email wouldn’t take you to the fake website because Web Guard would block it.

8. Tap Test Web Guard to view the result.

10. To exit the demo, tap Mobile Security in the upper left of the screen, then tap the X box in the upper right to close the demo.

Figure 158. Suspicious Page Blocked

Figure 159. Exit Demo (X)
Wi-Fi Checker Demo

To view the Wi-Fi Checker demo:

1. At the bottom of the Mobile Security Console, swipe the demo image to the left. The Wi-Fi Checker demo appears.

2. Tap the demo image. A screen appears, to Experience Unsecured Wi-Fi.

3. Tap the Experience Unsecured Wi-Fi button to launch the demo.

4. The demo begins, showing how you want to use the free Wi-Fi at a coffee shop.

5. Tap Next. The demo shows you connecting to the Free Wi-Fi at the coffee shop.

6. Tap Next.
7. The demo shows you using your social media app as you normally would.

8. Tap Next. A few days later...

9. Someone has hacked your social media account and used it to scam your friends.

10. Tap Experience Wi-Fi Checker, then in the following screen, See How Wi-Fi Checker Works.

---

**Figure 164. Connecting to Social Media**

**Figure 165. A Few Days Later...**

**Figure 166. Social Media Hacked**

**Figure 167. See How Wi-Fi Checker Works**
11. Tap the free Wi-Fi connection, then **Next**.

12. A notification displays when **Wi-Fi Checker** detects security risks in the connection.

13. Tap **Next**.

14. Wi-Fi Checker indicates **Risks Found**, scanning for suspicious interference, unsecured Wi-Fi settings, and browser hijackers, to help you stay away from unsecured Wi-Fi.

15. Tap the **X** in the upper right to close the demo.

**Figure 168. Tap Free Wi-Fi Simulation**

**Figure 169. Wi-Fi Checker Security Issues Found**

**Figure 170. Wi-Fi Checker is On**
Today View for Data Usage and SafeSurfing

To Access the Today View for Data Usage and Safe Surfing:

1. The Today View in iOS provides reminders and notification widgets at-a-glance on your device.

2. To access the Today View, swipe down from the upper border of your iOS device, then to the right. The Today View scrolls into view.

3. At the bottom, tap Edit to edit what’s displayed in Today View. Apps that can display a widget in Today View are displayed.

4. In More Widgets, find and tap the Data Usage and SafeSurfing plus signs to enable them in Today View. The widgets move to the active widgets list.

5. Use the position bars to move the widgets up or down, then tap Done.

6. The Data Usage widget shows your data usage to date for this month.

7. The SafeSurfing widget pastes and scans the URL from the clipboard and warns you if it’s dangerous.
8. Using the Apple Notes app, type and copy a potentially dangerous URL into the clipboard, then swipe down Today View to test it.

9. If the page is dangerous or suspicious, Trend Micro Mobile Security will block it.

Figure 175. Browsing a URL

Figure 176. Suspicious Page
Transferring Licenses Between Devices

Trend Micro Mobile Security allows you to transfer licenses between devices, whether they’re iOS or Android. You may do this when the license on your device has expired or when you wish to activate Trend Micro Mobile Security using an existing license.

To Transfer a License Between Devices:

1. At the bottom of the main screen in the Console, tap Settings. The Settings screen appears.
2. Tap Set Up Account. A screen appears for you to sign in.
3. You have two options at this juncture:
   - Select an account to sign in.
   - Sign in with different account
   - Create an account. (Not used.)
4. In this example, we choose the first option. A popup appears for you to Use Available Subscription.
5. Tap Next.
6. The **Transfer License** screen appears

7. Tap the panel for the license you wish to use. A popup appears letting you **Transfer Existing License(s)**.

8. Tap **OK**. The license is transferred.

9. The **Console** will update and the expiration date for that license will be displayed in the lower left-hand corner.

10. The second transfer option, to **Sign in with a different account**, will provide the same transfer process as the first if a license is available in that account.
Mobile Security on Your iPod or iPad

Trend Micro Mobile Security for iOS is the same program on your iPod Touch or iPad as your iPhone, with the same key functionality. Below shows the vertical scrolling screen (Portrait View).

**Note:** The screens below show the expiry notices below the functions that are disabled when your Trial or Subscription expires.

---

**Figure 184. Trend Micro Mobile Security for iOS on the iPad (Scrolling Portrait View)**

When you hold your iPad horizontally (Landscape View), Trend Micro Mobile Security automatically reconfigures the panels.

---

**Figure 185. Trend Micro Mobile Security for iOS on the iPad (Scrolling Landscape View)**
About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely. For more information, visit www.trendmicro.com.