TREND MICRO™

Mobile Security 9.0 for iOS

Product Guide

V1.0

Trend Micro, Incorporated—US Headquarters
224 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 - USA
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763

www.trendmicro.com

Trend Micro™ Mobile Security 9.0 for iOS - Product Guide provides help for analysts, reviewers, potential customers, and users who are evaluating, reviewing, or using Trend Micro Mobile Security for iOS, Version 9.0.

This reviewer's guide can be read in conjunction with the relevant product guides, which can be accessed from the Home Support/Product Support dropdown menu, as well as the individual links below:

- Trend Micro™ Mobile Security for Android Product Guide
- Trend Micro™ Security for Windows Product Guide
- Trend Micro™ Antivirus for Mac® Product Guide
- Trend Micro™ Password Manager for Windows and Android Product Guide
- Trend Micro™ Password Manager for Mac and iOS Product Guide

DOCUMENT PROFILE:

Product Name: Trend Micro™ Mobile Security for iOS

Document Title: Trend Micro™ Mobile Security 9.0 for iOS - Product Guide

Document Filename: PG - TM Mobile Security 9 for iOS - Product Guide v1.0

Document Release Date: November 2, 2020

Team: Consumer Technical Product Marketing

Table of Contents

Trend Micro Mobile Security – Overview

Trend Micro™ Mobile Security (v9.0) 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 recently updated features. 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)

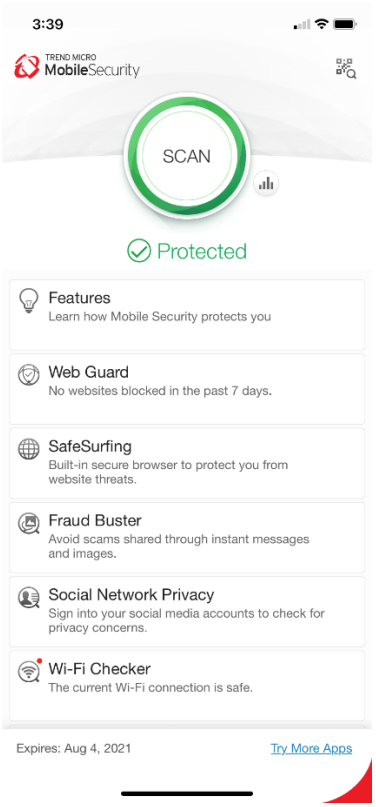

Figure 1. Console (Scrolled Down)

- **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)

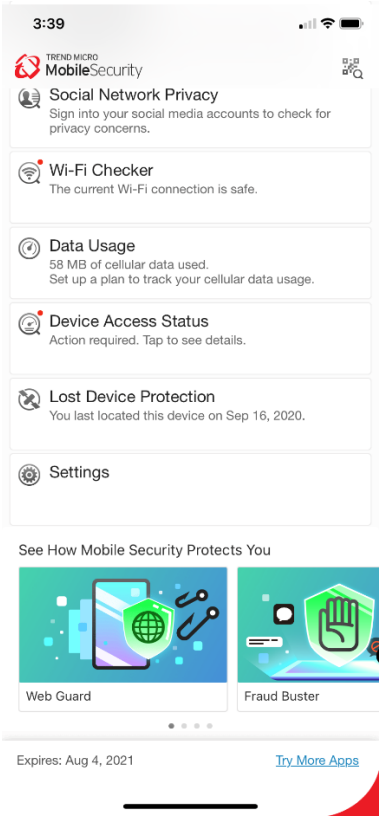

Figure 2. Console (Scrolled Up)

Chapter 1: Introducing Trend Micro™ Mobile Security for iOS

This chapter introduces you to **Trend Micro™ Mobile Security for iOS v9.0.** 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 v9.0 for iOS

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

iOS Security Features	Free	Paid
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 specific features of Mobile Security work. (Note: these demos are subject to change.)	✓	✓

System Requirements

Table 2. Mobile Security v9.0 for iOS - System Requirements

Requirements	Description
Operating System	**iOS 11.0 or later. 64-bit device required for latest versions.**

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:

http://esupport.trendmicro.com/support/consumer/consumerhome.do?locale=en_US

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

v9.0.1127, October 30, 2020 – 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: https://helpcenter.trendmicro.com/en-us/product-support/mobile-security-for-ios/.

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 https://www.trendmicro.com/en_us/forHome/products/premium-services.html#premium-service-bundle-tm-anchor.

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 Mobile Security** 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.

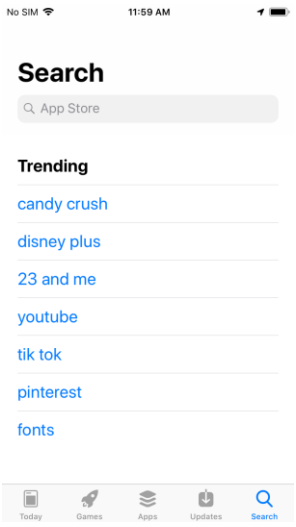

Figure 3. App Store

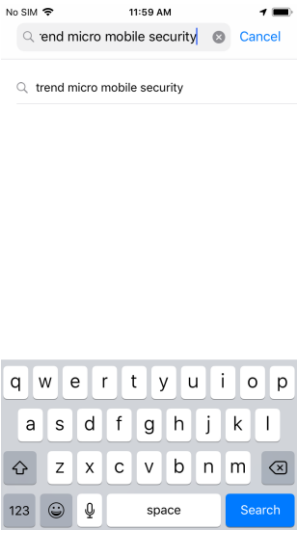

Figure 4. Search App Store

4. Tap the **Download/Install** icon. Trend Micro Mobile Security downloads and installs.
5. When installation is complete, tap **Open**.

Figure 5. Trend Micro Mobile Security

Figure 6. Open

6. A popup appears, saying **"Mobile Security" Would Like to Send You Notifications.**
7. Tap **Allow** 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, check it and click **Accept and Continue.**
9. Click through the demo screens.

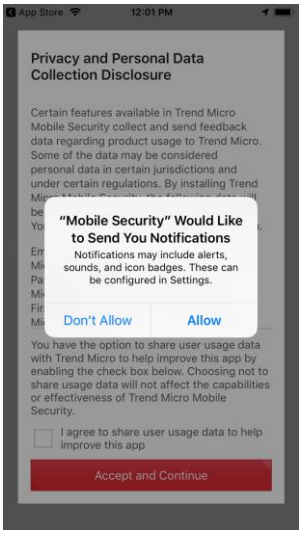

Figure 7. Notifications

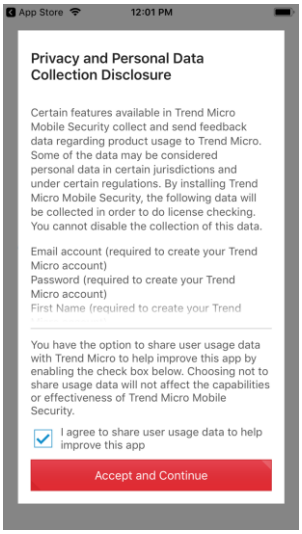

Figure 8. Privacy and Personal Data Collection Disclosure

10. The **Welcome** screen with **License Agreement** appears.
11. Tap the link to the **Trend Micro License Agreement** to read it. If you accept the terms of the agreement, tap **Accept and Continue.** The **Mobile Security Console** appears with a popup.
12. Typically, you're provided with **Buy/Activate** options for **Trend Micro Mobile Security.**
13. You can also **Sign In** to a current **Trend Micro Account**, or **Create an Account.**
14. Proceed with your chosen options and the **Trend Micro Mobile Security Console** displays, with **Demo** screens to help you explore its features.
15. Additional multi-part **Demo** screens at the bottom of the **Console** can be selected to show you more details for using that feature.
16. Tap **Next** to go through the Demo screens; or select a Demo Panel at the bottom to explore a **Selected Feature**; or tap **No Thanks** to finish the additional Demos.
17. One you're done, the T**rend Micro Mobile Security Console** is ready to explore, use, and configure. See **Chapter 3** to explore **Trend Micro Mobile Security Console.**

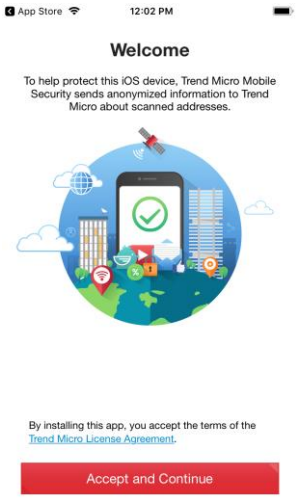

Figure 9. License Agreement

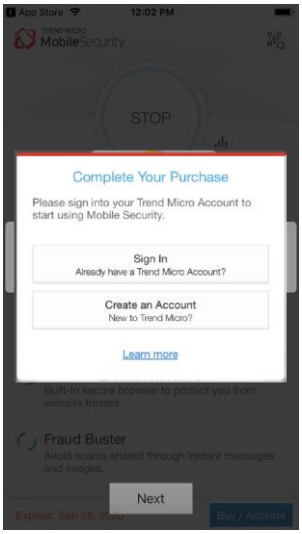

Figure 10. Sign In or Create Account

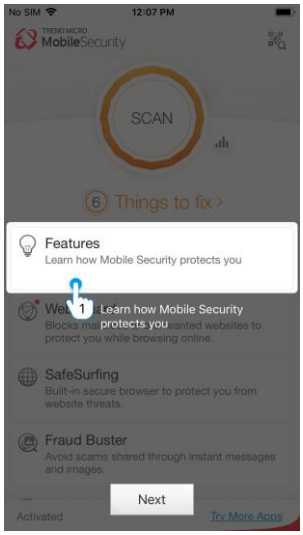

Figure 11. Mobile Security Console

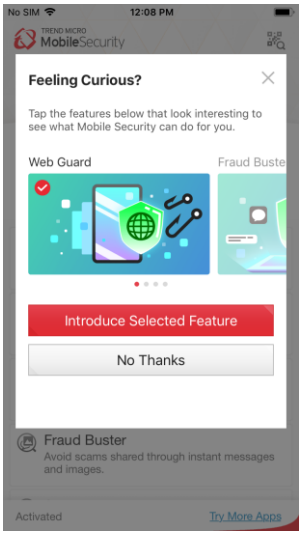

Figure 12. Feeling Curious?

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
- Demos: Web Guard and Wi-Fi Checker
- 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** bar 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 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.
15. Tap the **Demos** to **See How Mobile Security Protects You.**
16. Tap **Renew/Activate** to renew or activate your subscription. Otherwise the indicator shows **Activated**.
17. Tap **Try More Apps** to go to the Apple **App Store** to try more Trend Micro Apps.

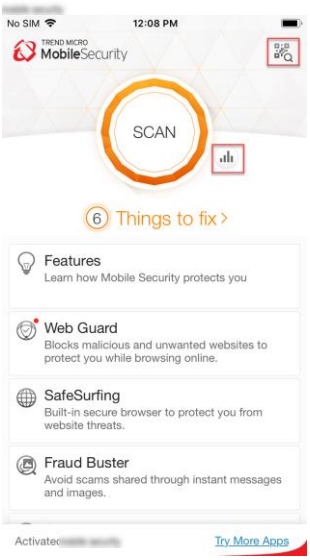

Figure 13. Console – Scrolled Down

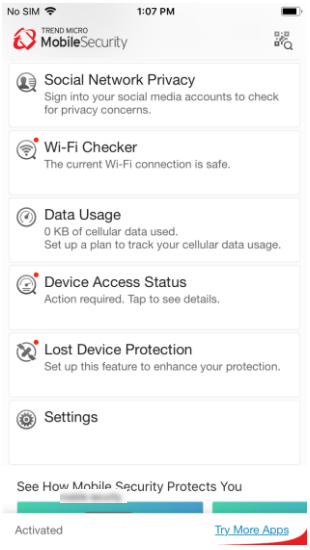

Figure 14. Console – Scrolled Up

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:

1. Tap the **Secure QR Code Scanner** icon in the upper right-hand corner of the Console. A popup appears, asking you to allow Mobile Security to **Access the Camera.**
2. Click **OK.** The **Secure QR Code Scanner** appears.

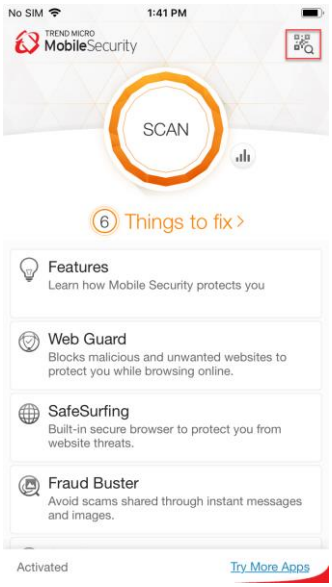

Figure 15. Secure QR Code Scanner Icon

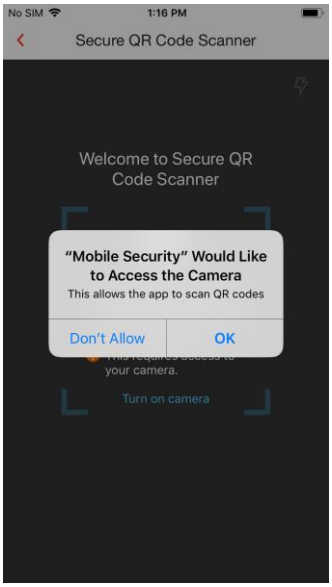

Figure 16. Allow Access to the Camera

3. 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.
4. If the QR Code is dangerous, you'll be blocked from going to the URL or app.

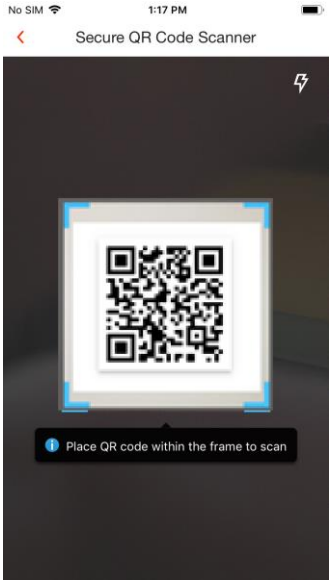

Figure 17. Secure QR Code Scanner

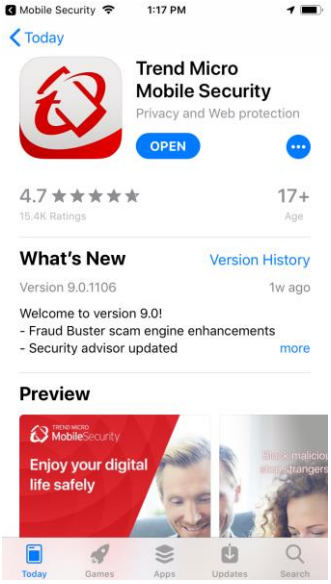

Figure 18. QR Code Resolved

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 viruses, malware, and other threats.

To scan your device:

1. Tap the large **Scan** button to conduct a device scan. The scan begins and Trend Micro Mobile Security checks for things to fix.

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

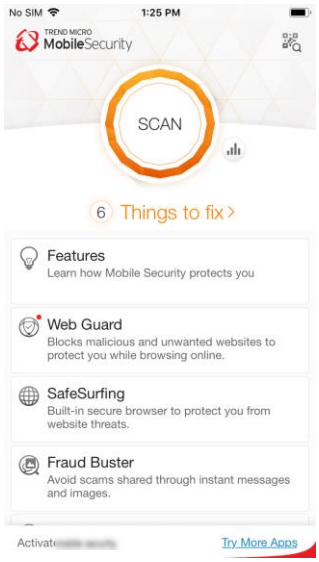

Figure 19. Device Scan Button

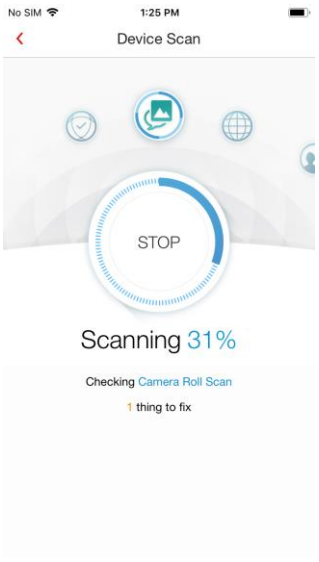

Figure 20. Device Scan in Progress

2. When the scan is complete, it shows **x Things to Fix.**
3. Follow the instructions shown in the **Secure, Privacy,** and **Insight Tabs,** scroll down the pages, and use any buttons shown to address that item, such as **Web Guard, Lost Device Protection, Two-Factor Authentication,** etc.

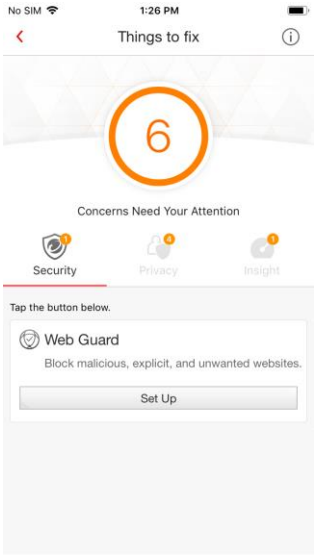

Figure 21. Device Scan Results (1)

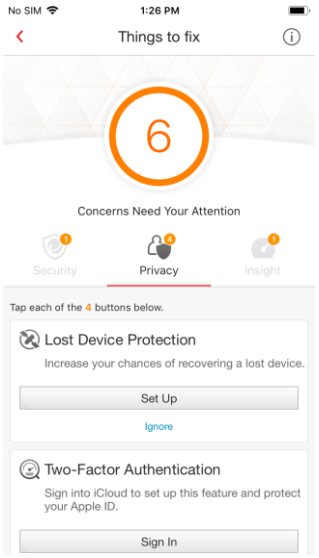

Figure 22. Device Scan Results (2)

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.

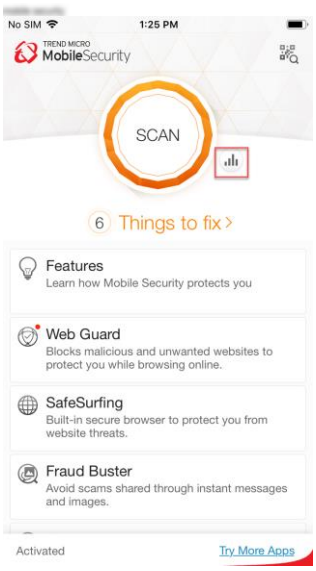

Figure 23. Security Report Icon

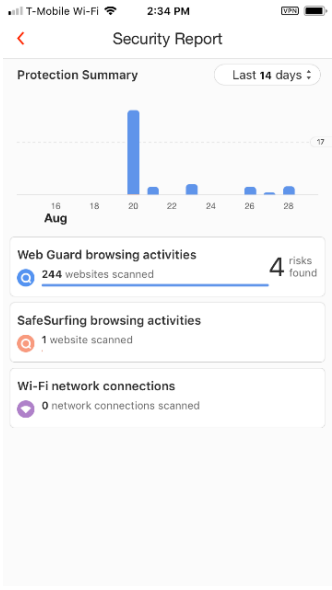

Figure 24. Security Report

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.

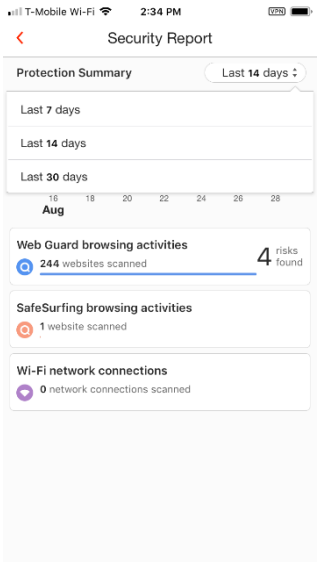

Figure 25. Protection Summary > Last 14 Days

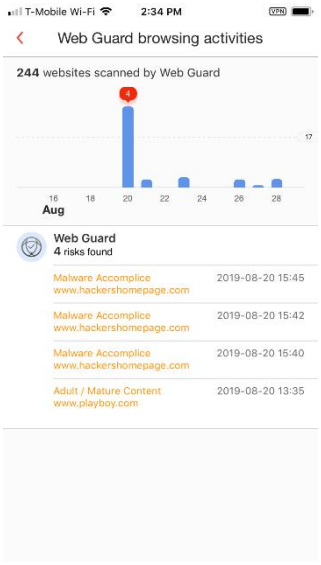

Figure 26. Web Guard Browsing Activities

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.)

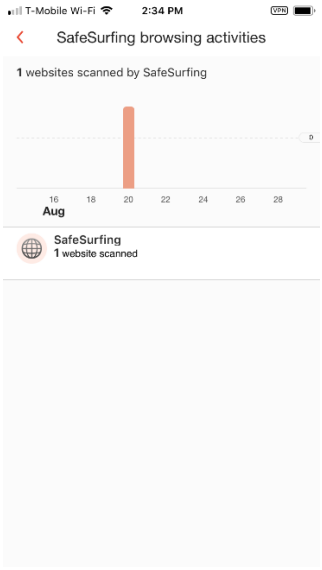

Figure 27. Safe Surfing Browsing Activities

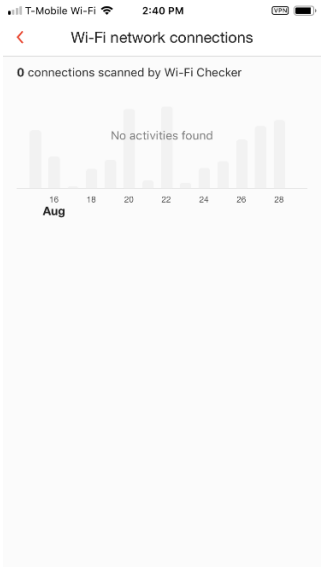

Figure 28. Wi-Fi Network Connections

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.

See the **VPN Settings** section below for setup.

VPN Settings

To turn on the VPN:

1. Tap the **Web Guard** panel in the Console. The **VPN Off** 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.

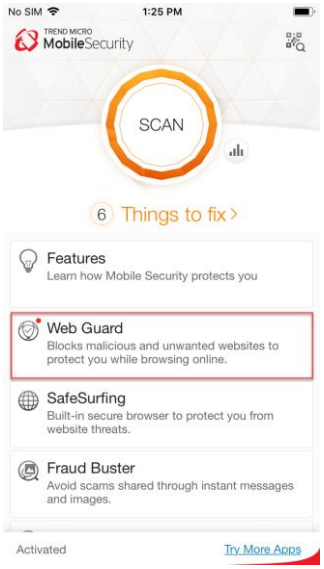

Figure 29. Web Guard

Figure 30. 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**.

Figure 31. Add VPN Configurations

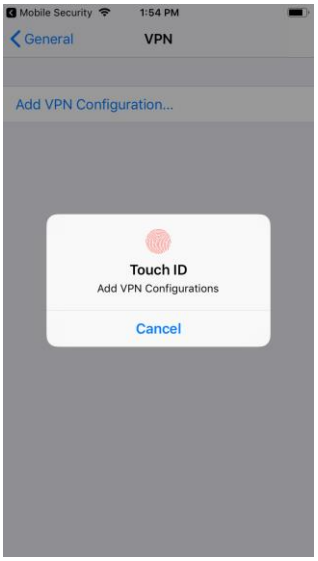

Figure 32. Enter Password or use Touch ID

6. Note the demo popup that remains. We'll show this later, so tap the **X** on the upper right of the popup to close it.
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.)

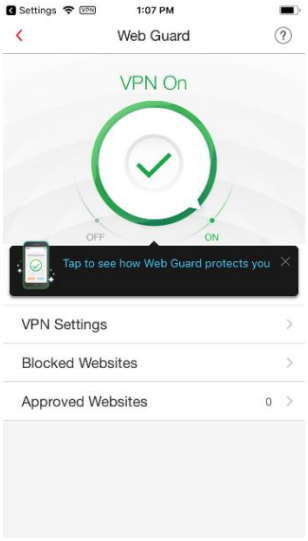

Figure 33. VPN On

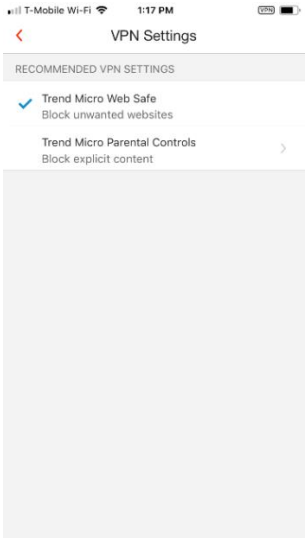

Figure 34. VPN Settings

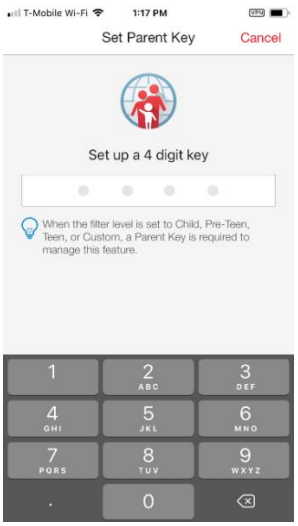

Figure 35. Set up a 4-digit key

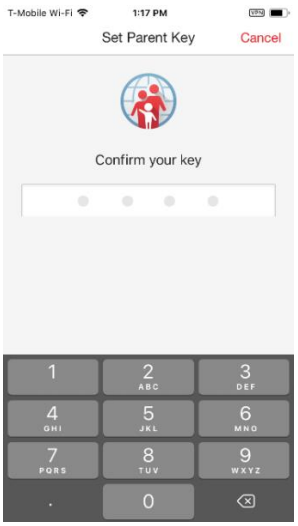

Figure 36. Confirm Your Key

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

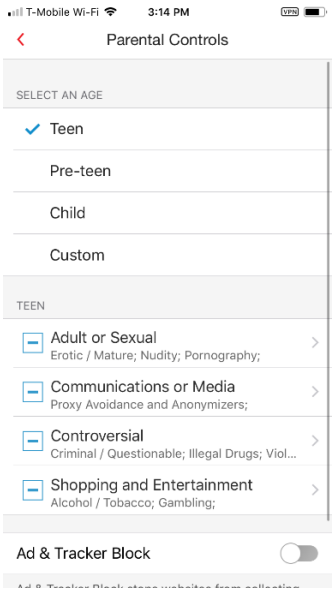

Figure 37. Teen

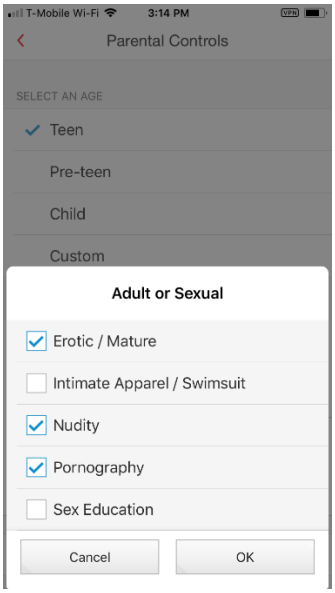

Figure 38. Adult or Sexual

-Communications or Media.

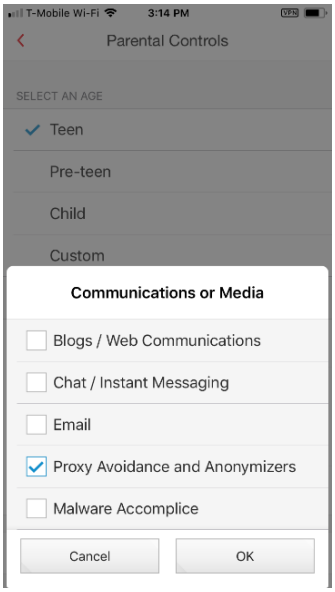

Figure 39. Communications or Media

-Controversial

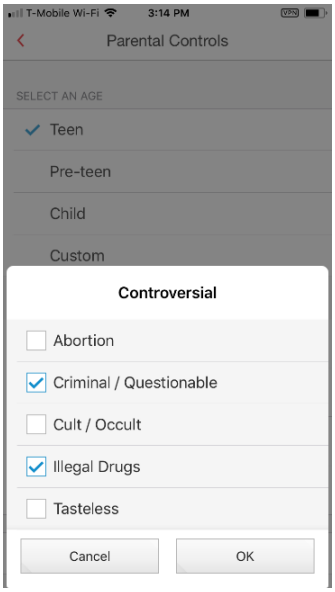

Figure 40. Controversial

-Shopping and Entertainment

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.

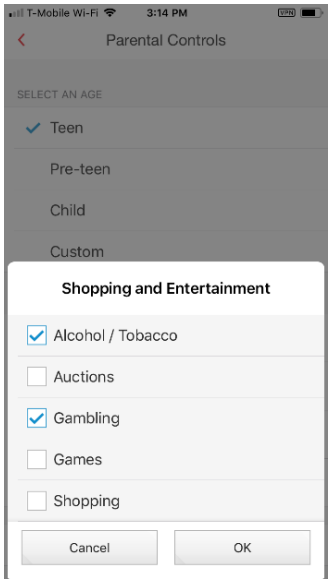

Figure 41. Shopping and Entertainment

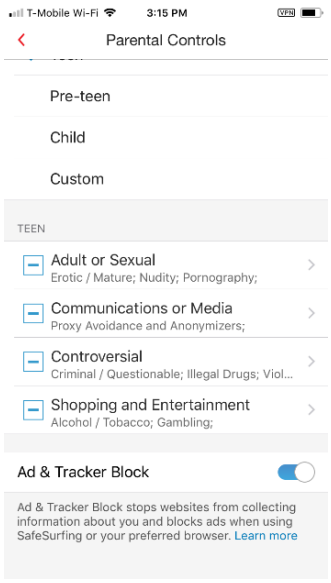

Figure 42. Ad & Tracker Blocker

5. When **Parental Controls** is on, an **Identity** icon appears near the **On** pointer of the VPN dial, indicating **Parental Controls** is active.

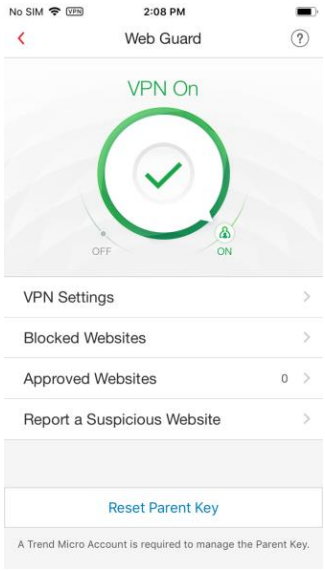

Figure 43. Parental Controls is Active

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.

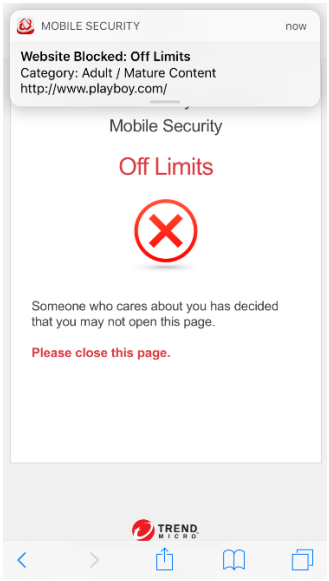

Figure 44. Off Limits

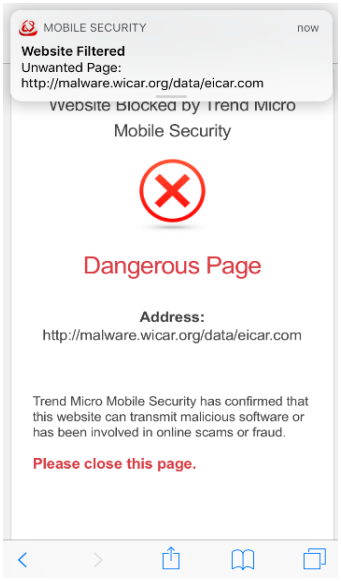

Figure 45. Dangerous Page

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).

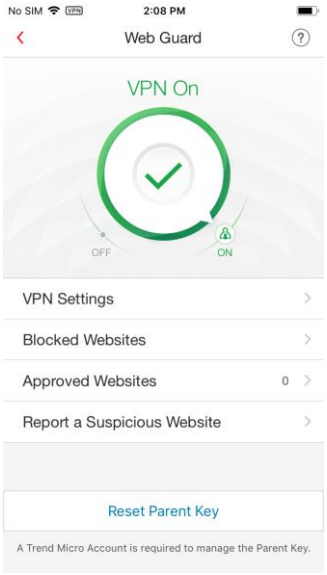

Figure 46. Blocked Websites

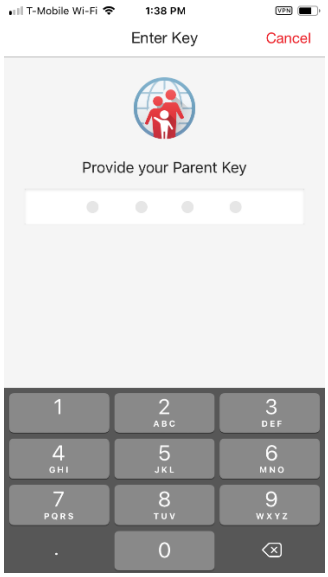

Figure 47. Provide your Parent Key

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.

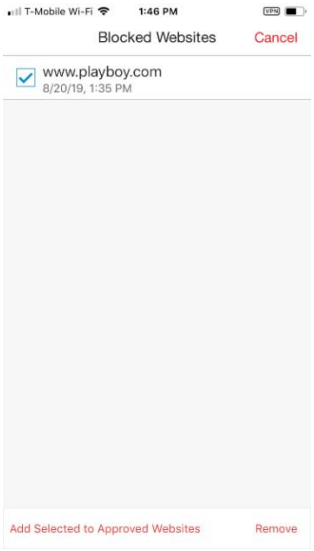

Figure 48. View, Add, or Remove Blocked Websites

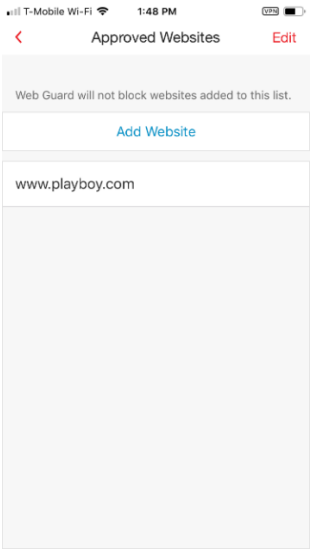

Figure 49. Add Website

Report a Suspicious Website

To report a Suspicious Website:

1. Back in the main **Web Guard** screen, tap **Report a Suspicious Website.**
2. Type the address of the website, e.g., www.example.com, and tap **Send**.
3. To check the rating of this website later, visit the **Site Safety Center.**

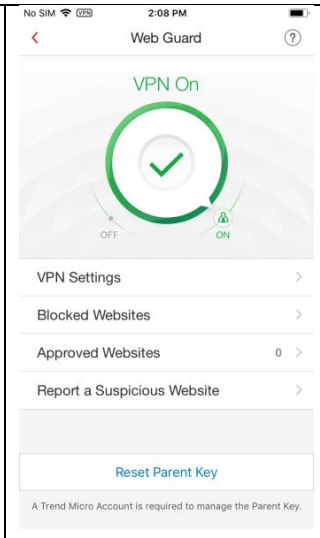

Figure 50. Report a Suspicious Website

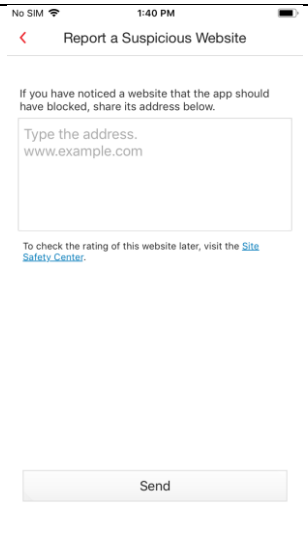

Figure 51. Type the Address of the Website

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**.

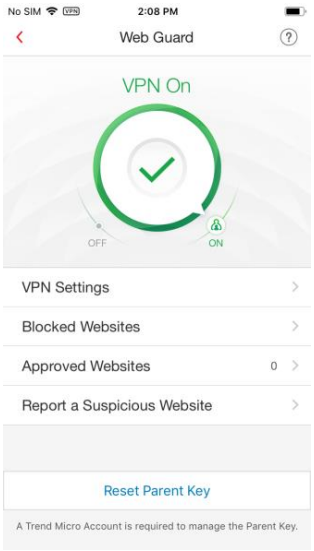

Figure 52. Reset Parent Key

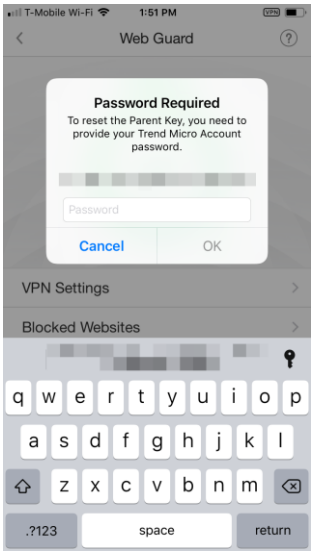

Figure 53. Sign Into Trend Micro Account

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.

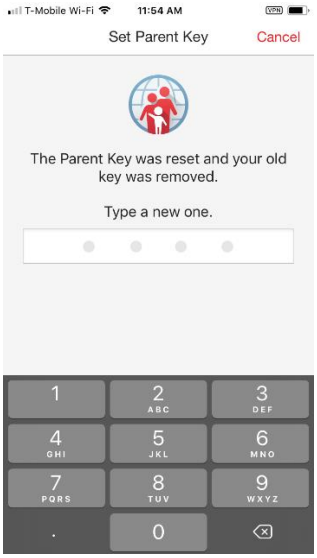

Figure 54. Type New Parent Key

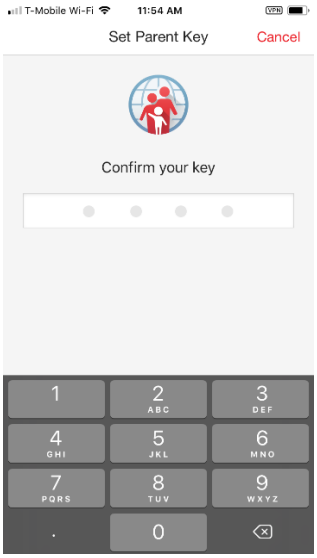

Figure 55. Confirm Your Key

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.

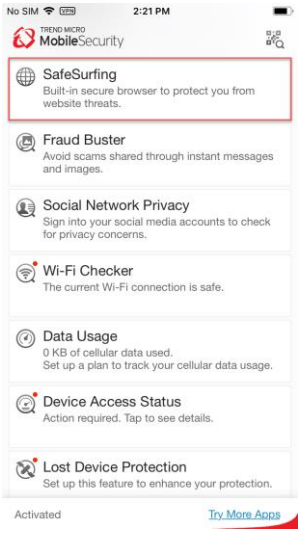

Figure 56. SafeSurfing

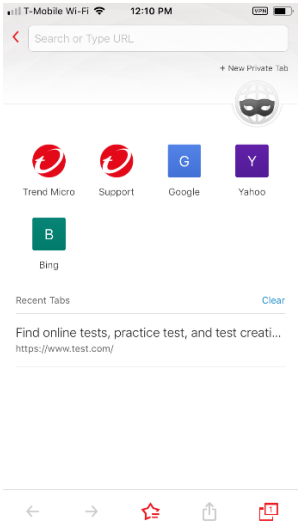

Figure 57. SafeSurfing Browser

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.

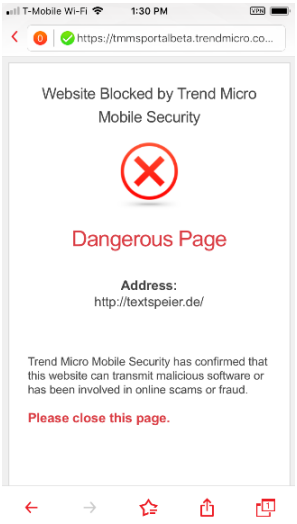

Figure 58. Dangerous Page

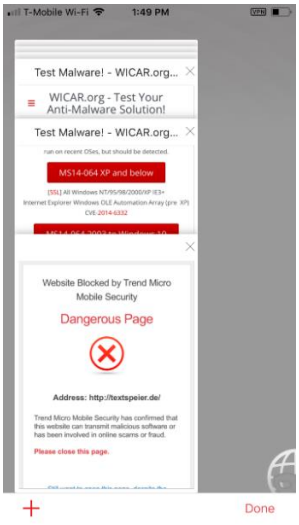

Figure 59. Website History

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.

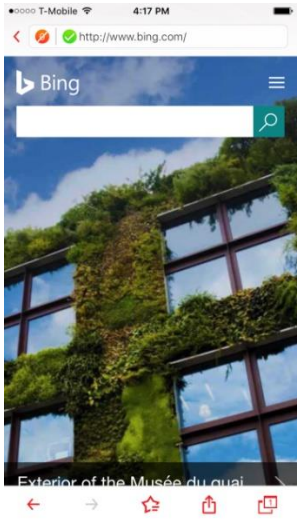

Figure 60. SafeSurfing Browser - Webpage

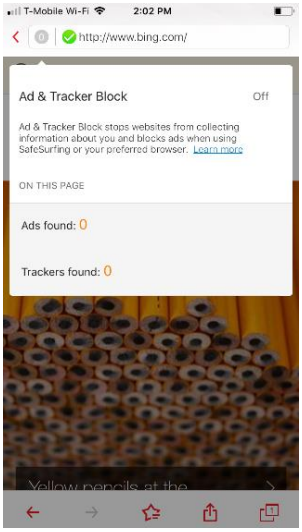

Figure 61. Ad & Tracker Blocker

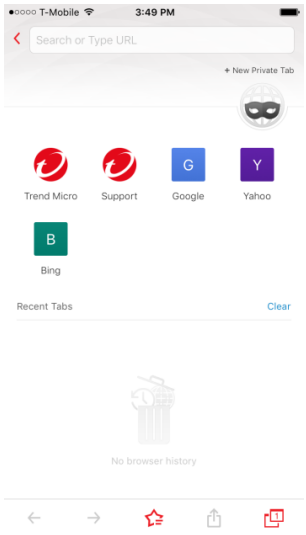

Figure 62. Mask Icon – New Private Tab

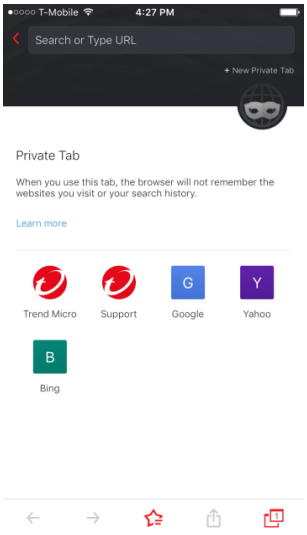

Figure 63. Private Tab

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**.

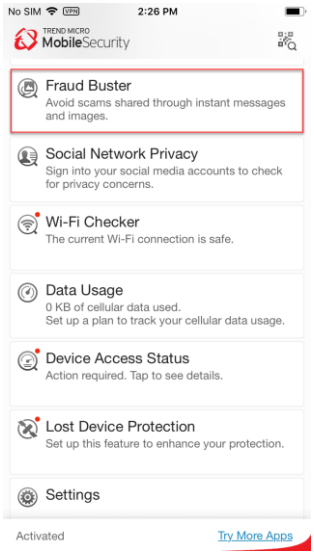

Figure 64. Fraud Buster

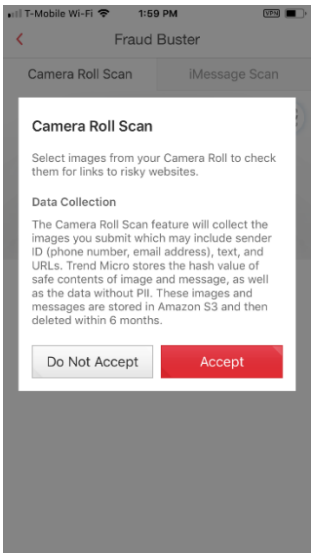

Figure 65. Camera Roll Scan

3. A popup appears, indicating **"Mobile Security" Would Like to Access Your Photos.**
4. If you accept, tap **OK**. Now you'll see a popup instructing you to **Tap to check the safety of a website.**

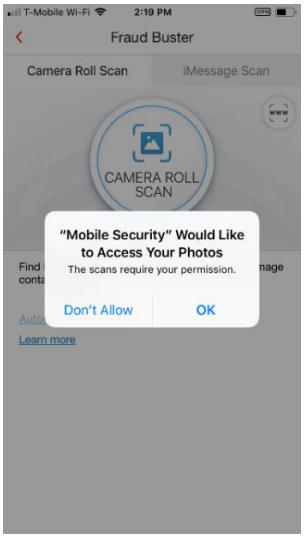

Figure 66. Access Your Photos?

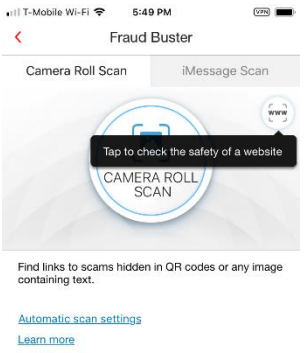

Figure 67. Check Links

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.

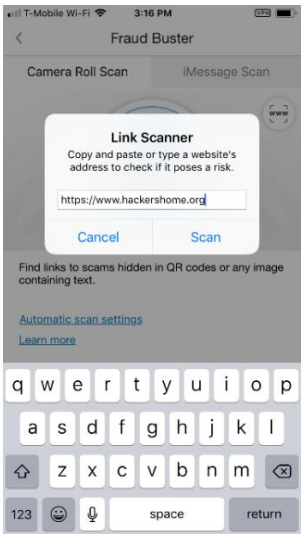

Figure 68. Link Scanner

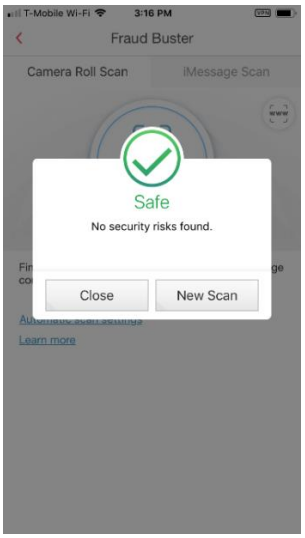

Figure 69. Safe Result

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.

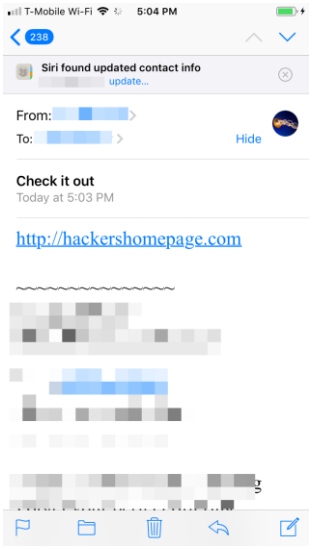

Figure 70. Screenshot the Suspicious Email

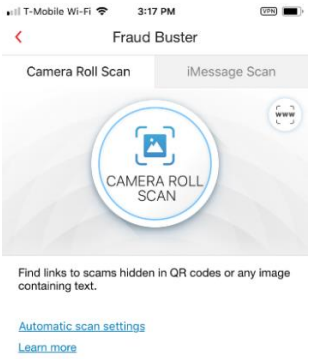

Figure 71. Tap Camera Roll Scan

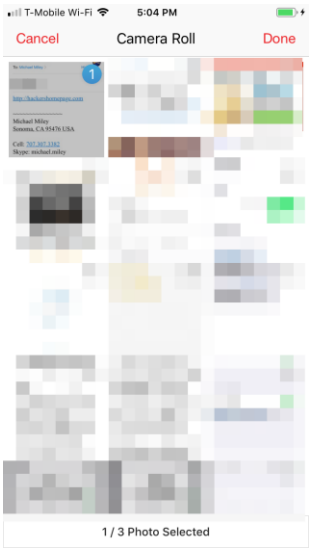

Figure 72. Camera Roll

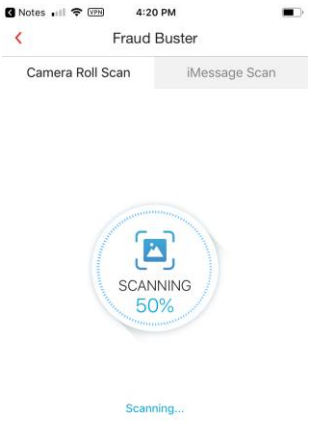

Figure 73. Scanning the Screenshot

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.

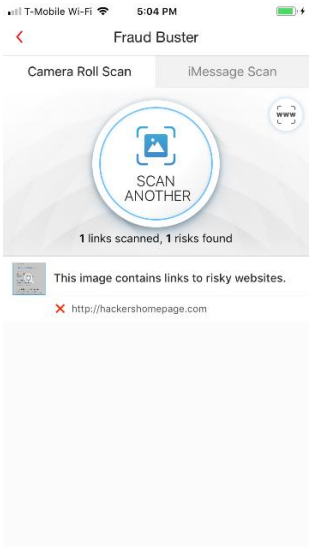

Figure 74. Risky Links in Email

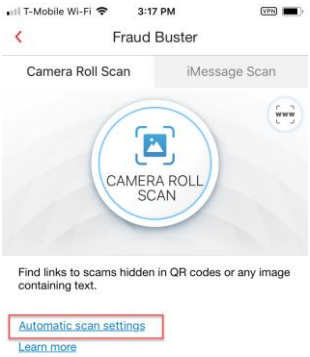

Figure 75. Automatic Scan Settings Link

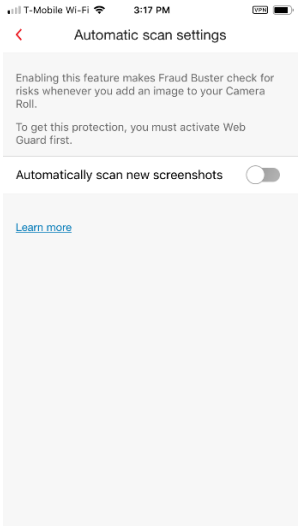

Figure 76. Automatic Scan Settings

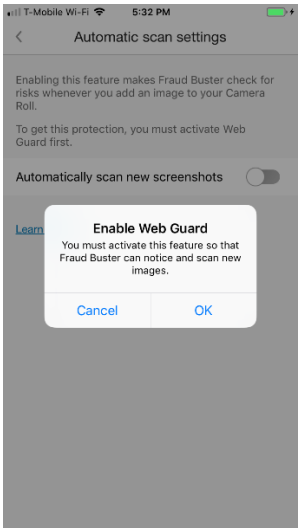

Figure 77. Enable Web Guard Popup

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.

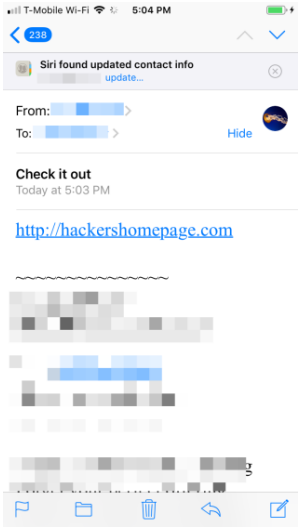

Figure 78. Screenshot the Email

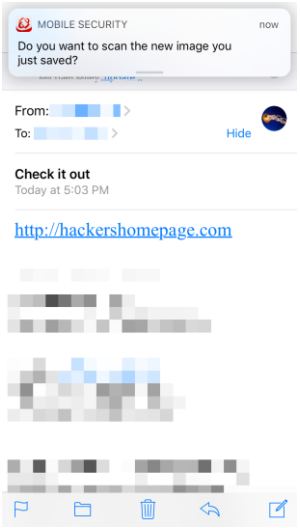

Figure 79. Do you want to scan the new image you just saved?

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.

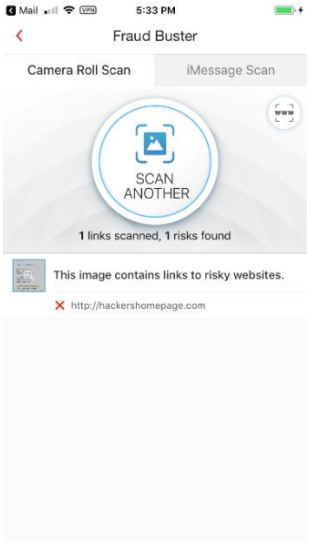

Figure 80. Image Contains Links to Risky Websites

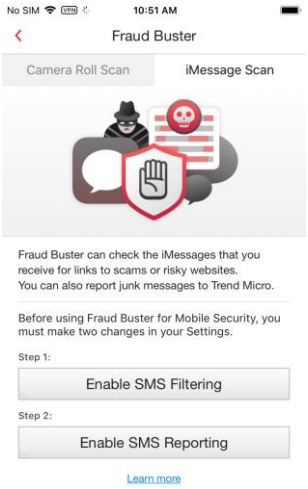

Figure 81. iMessage Scan

To enable iMessage Scan:

1. Tap the **iMessage Scan** tab in the **Fraud Buster** screen. An instruction screen appears, with two steps to enable the protection.

2. Tap **Enable SMS Filtering** and read the instructions shown.
3. When you're done, tap **Open Settings.**

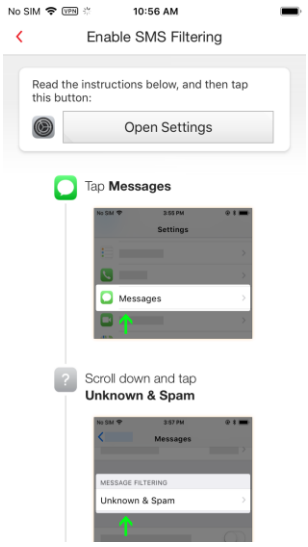

Figure 82. Get Started Demo

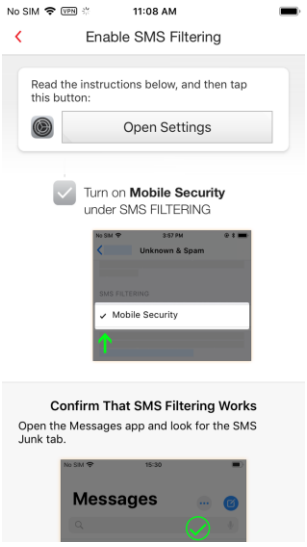

Figure 83. Get Started Demo Scrolled Down

4. Tap **Messages.**
5. Tap **Unknown & Spam.**

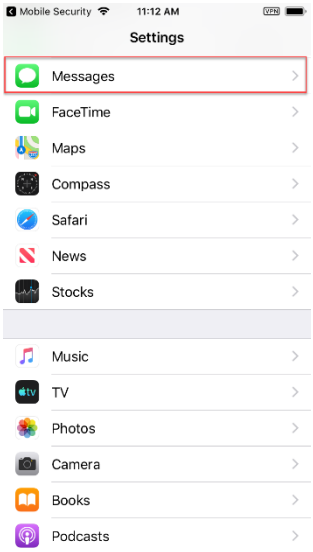

Figure 84. Messages

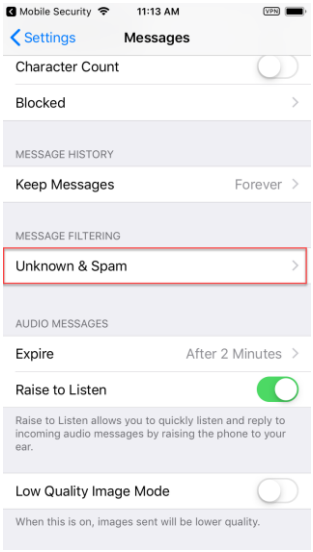

Figure 85. Unknown & Spam

6. Toggle on **Filter Unknown Senders** and **Mobile Security** to enable **Fraud Buster's iMessage Scan.**
7. 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.
8. If you agree to the conditions, tap **Enable**. **SMS Spam Filtering** is enabled.
9. Back in the setup page, tap **Enable SMS Reporting.** The demo screen appears.
10. Read the instructions for enabling **SMS Reporting.**

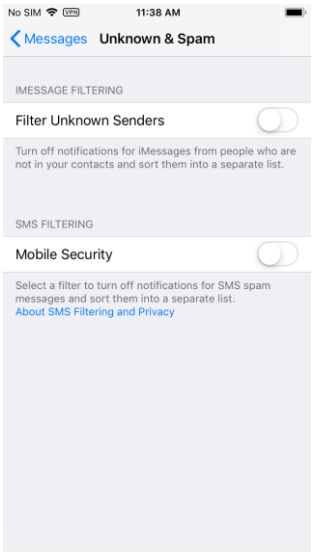

Figure 86. Mobile Security

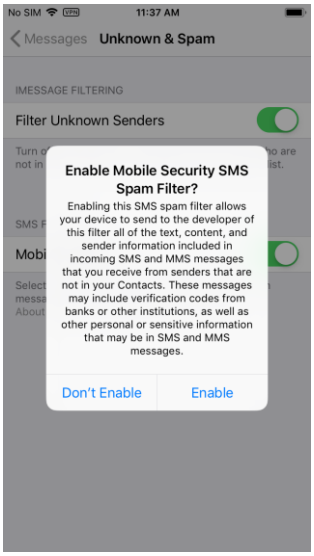

Figure 87. Enable Mobile Security SMS Spam Filter?

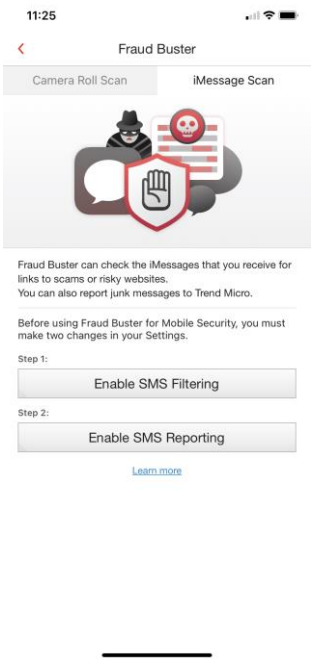

Figure 88. Enable SMS Reporting

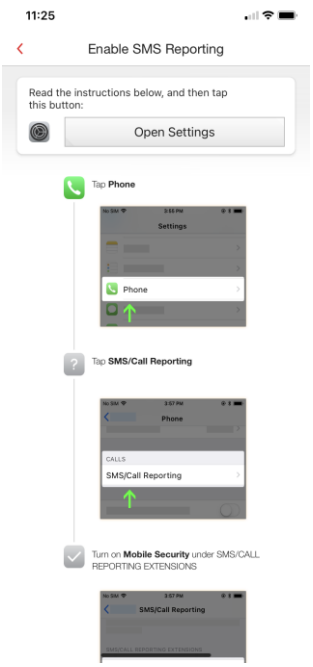

Figure 89. Enable SMS Reporting (Demo 1)

11. When you're finished reading the instructions to Enable **SMS Reporting**, tap **Open Settings.**
12. Back-arrow and locate the **Phone** in **Settings**, then tap it.

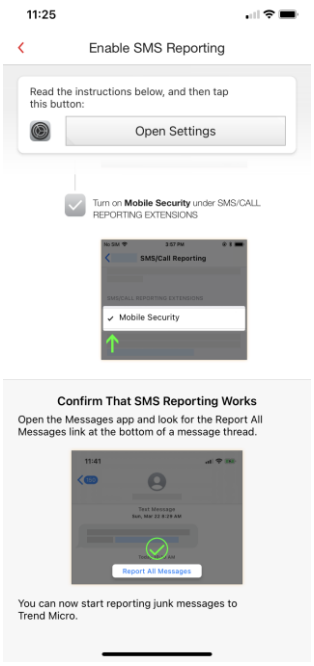

Figure 90. Enable SMS Reporting (Demo 2)

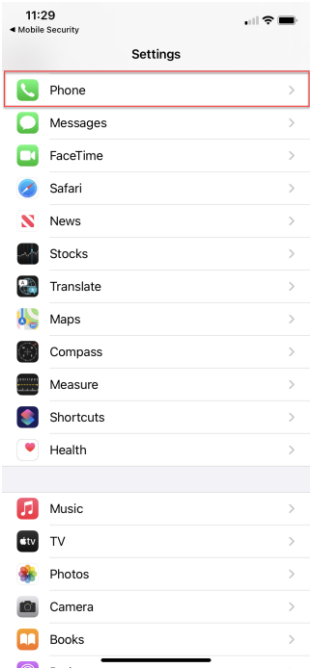

Figure 91. Access Phone Settings

13. Locate **SMS/Call Reporting** and tap it.
14. Tap **Mobile Security** in the **SMS/Call Reporting** screen.

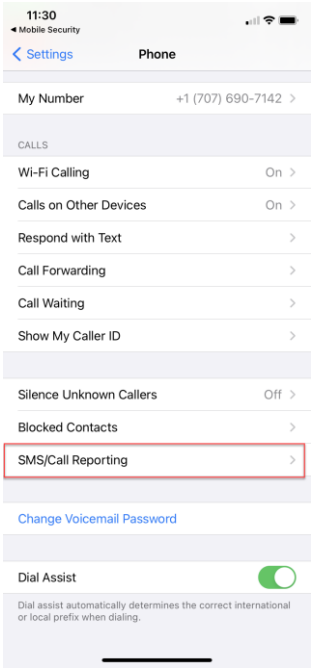

Figure 92. SMS/Call Reporting

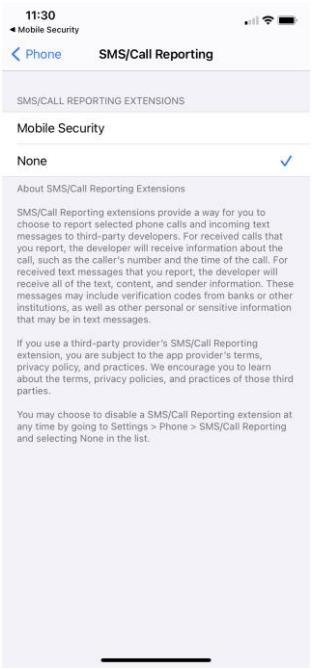

Figure 93. SMS/Call Reporting Settings

15. A popup appears, asking if you want to **Enable SMS/Call Reporting extension Mobile Security?**
16. Tap **Enable** to enable **SMS/Call Reporting** by Mobile Security.
17. **Mobile Security SMS/Call Reporting** is now enabled.
18. Now when you receive an iMessage that contains a suspicious link, **Fraud Buster** will give you a preview.

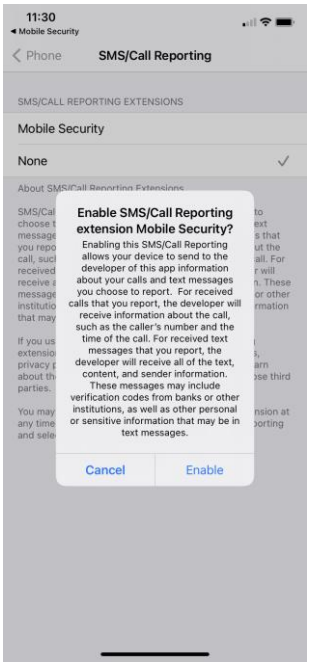

Figure 94. Enable SMS/Call Reporting Extension Mobile Security

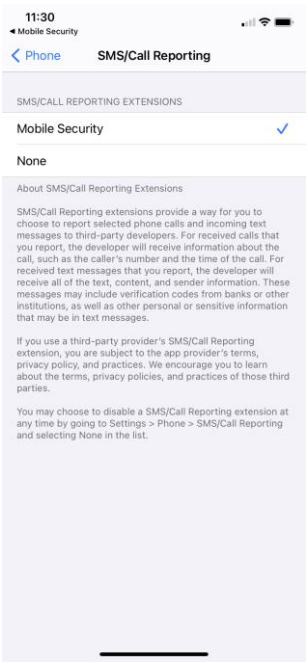

Figure 95. Mobile Security SMS/Call Reporting Enabled

19. When you **Tap to Load Preview**, Mobile Security will scan it and tell you if it's malicious. If it is, a popup will appear saying **Website Blocked.**
20. 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.

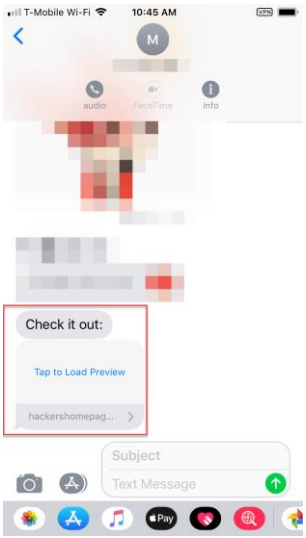

Figure 96. Tap to Load Preview

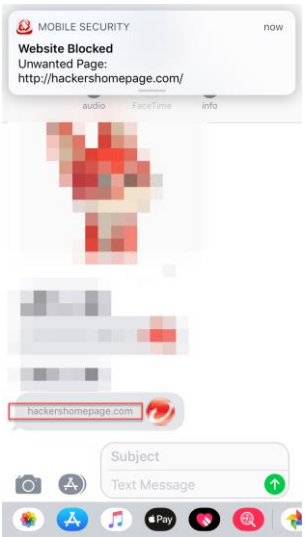

Figure 97. Website Blocked

21. Please close this **Suspicious Page**, then delete the message.
22. Note too that **Security Reports** will now provide running reports on suspicious **iMessages / SMS Spam** received.

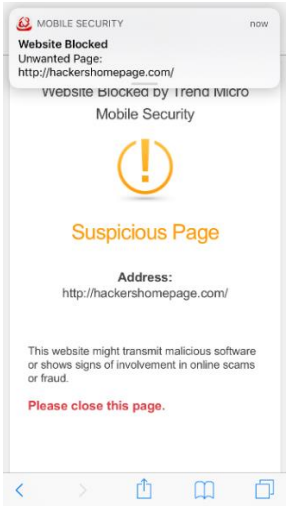

Figure 98. Suspicious Page > Website Blocked

Social Network Privacy

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

Note: **Parental Controls in Web Guard can disable this feature if a child is blocked from using Facebook or Twitter.**

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.

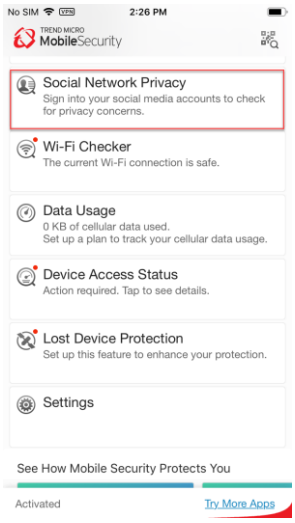

Figure 99. Social Network Privacy

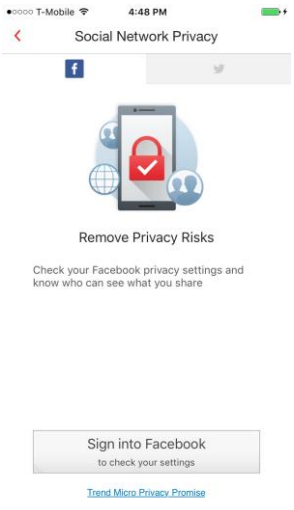

Figure 100. Sign Into Facebook

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.

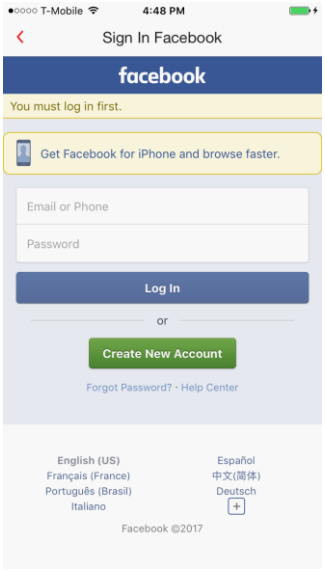

Figure 101. Facebook Login

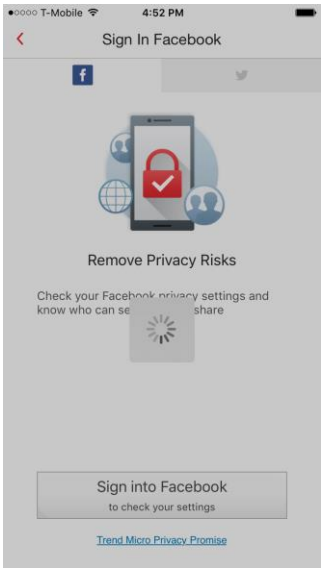

Figure 102. Checking Your Privacy Settings

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.

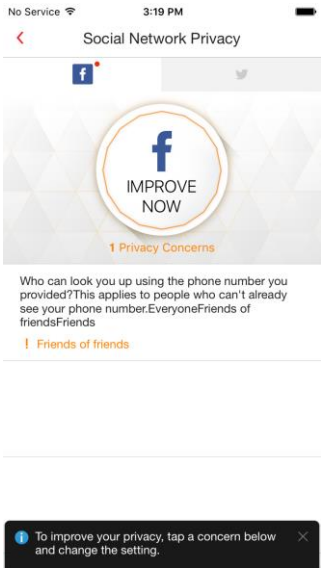

Figure 103. Improve Now

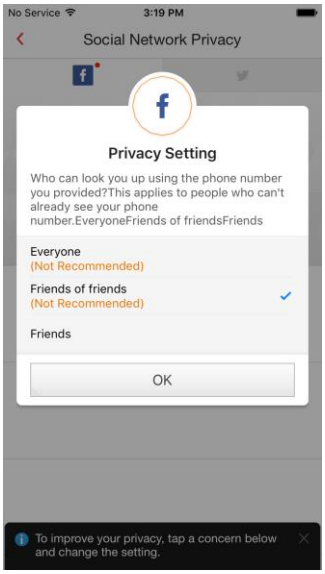

Figure 104. Privacy Setting Editor

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.

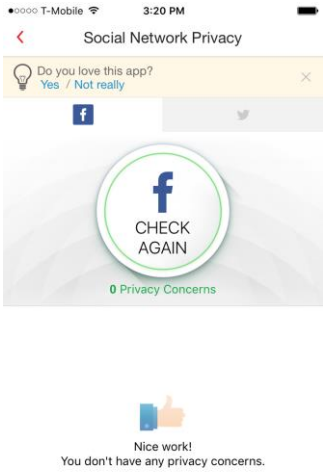

Figure 105. Nice Work!

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.

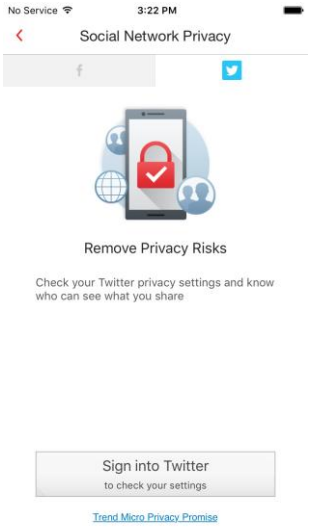

Figure 106. Sign Into Twitter

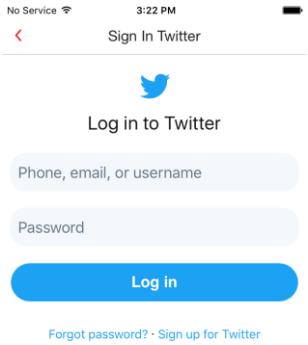

Figure 107. Log In

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.

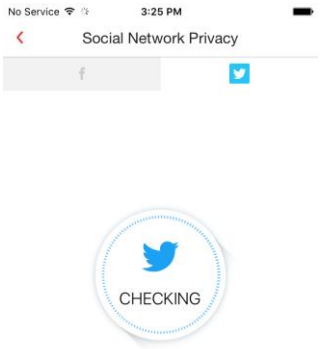

Figure 108. Checking Privacy

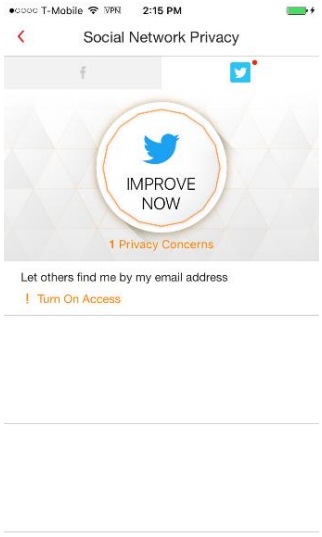

Figure 109. Improve Now

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."

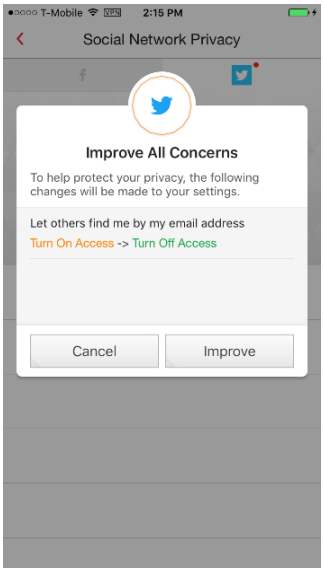

Figure 110. Improve All Concerns

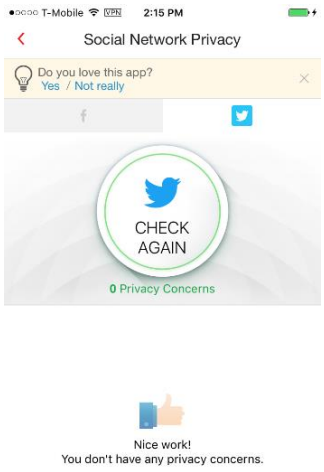

Figure 111. Nice Work!

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.

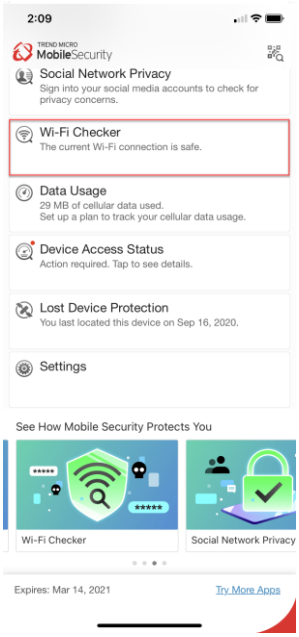

Figure 112. Wi-Fi Checker

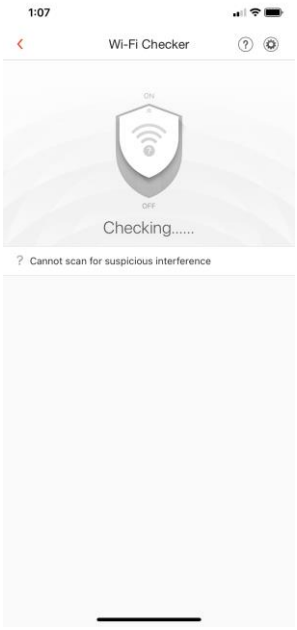

Figure 113. Scanning Wi-Fi

3. If it's safe, it returns the result **No Issue Found.**
4. If it's risky, it returns the result **X Issue Found.**
5. Tap **Trust this Wi-FI Network** despite the risk to add it to the **Approved List.**

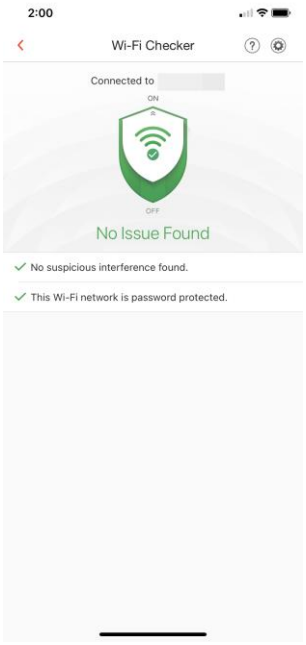

Figure 114. No Issue Found

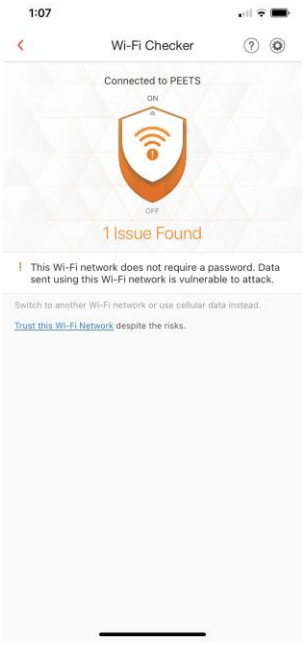

Figure 115. 1 Issue Found

6. A popup appears to add it to the **Approved List,** or you may Cancel.
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.

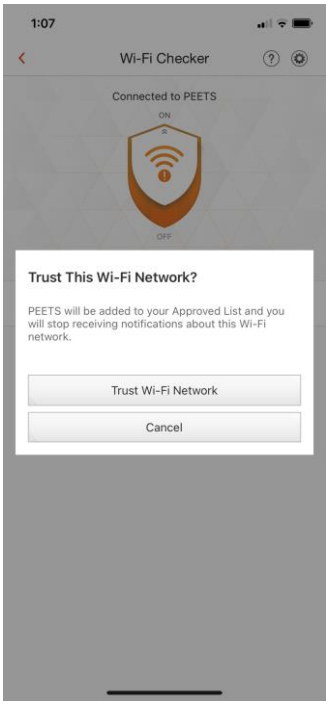

Figure 116. Trust This Wi-Fi Network?

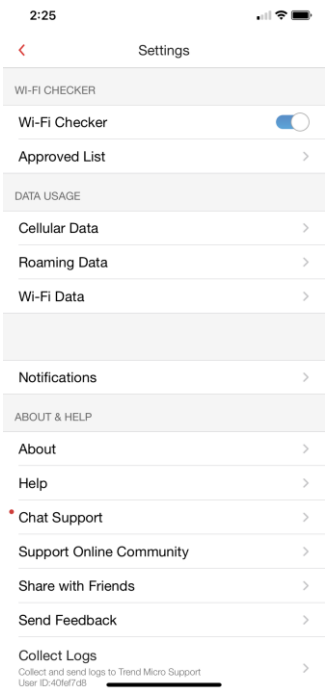

Figure 117. Wi-Fi Checker > Approved List

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

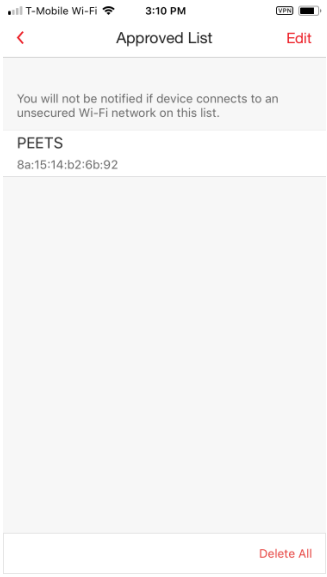

Figure 118. Edit Approved List

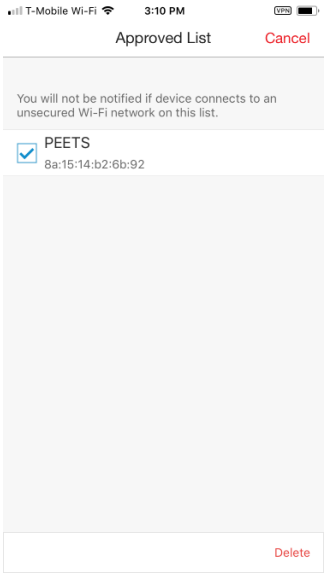

Figure 119. Delete from Approved List

11. A popup appears, asking if you wish to remove the Wi-Fi.
12. Tap **Remove** to remove it from the list.
13. Back in the main screen, tap the **Wi-Fi Checker Shield** to turn it off. The shield indicates **Protection Off.**

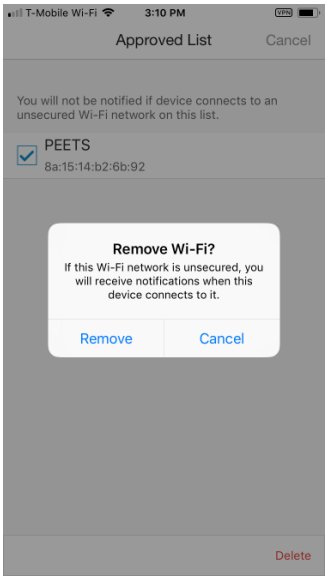

Figure 120. Remove Wi-Fi?

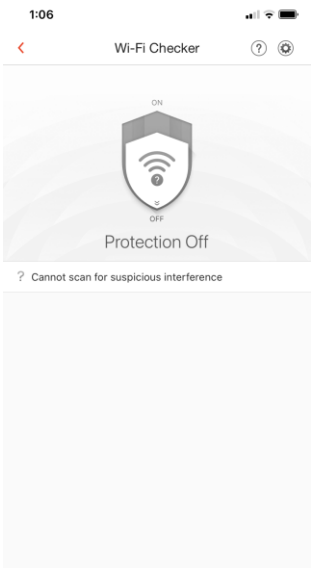

Figure 121. Protection Off

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.

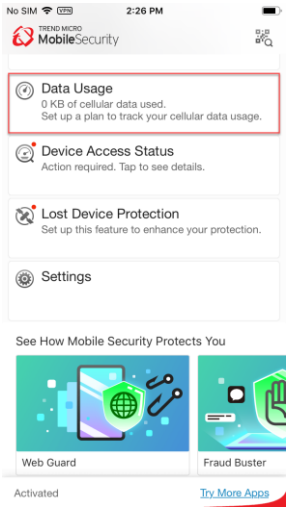

Figure 122. Data Usage

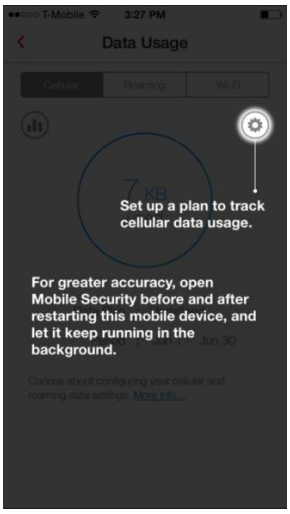

Figure 123. Set Up Cellular Data Usage Plan

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.**

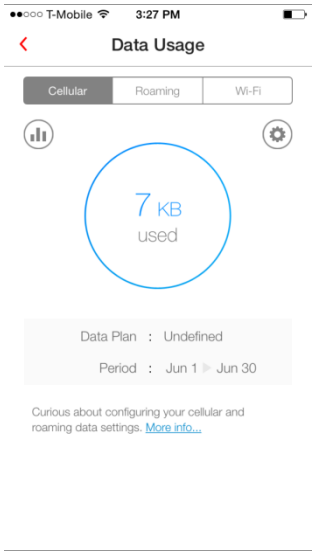

Figure 124. Data usage | Cellular

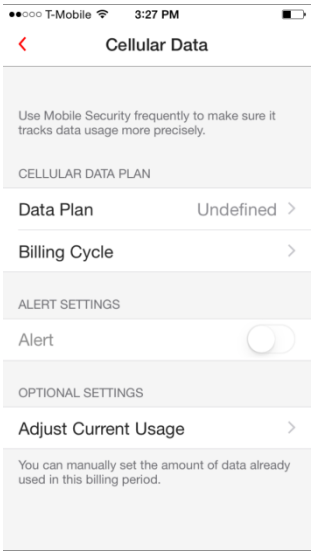

Figure 125. Cellular Data

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

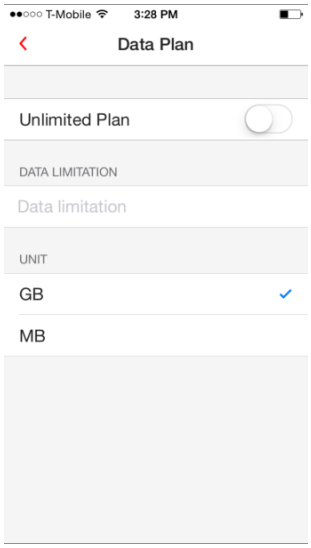

Figure 126. Data Limitation

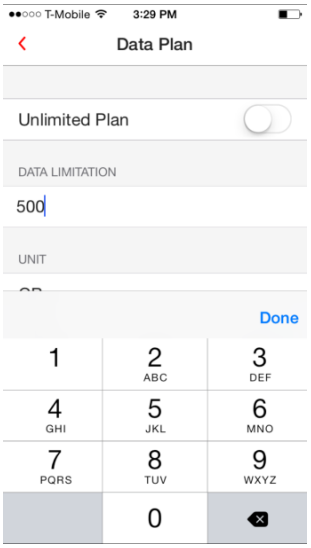

Figure 127. Edit Data Limitation

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.

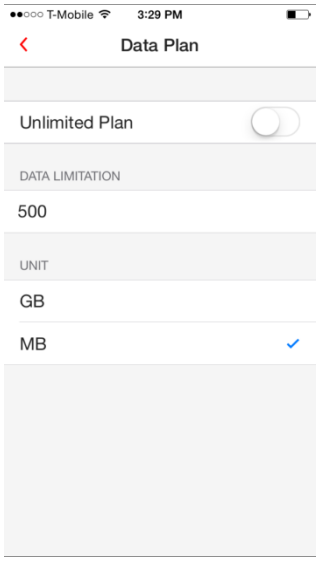

Figure 128. Unit of Measure

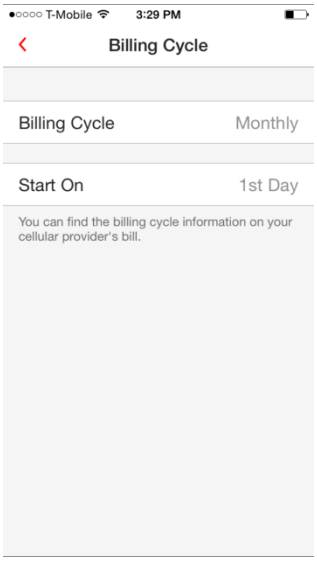

Figure 129. Billing Cycle

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

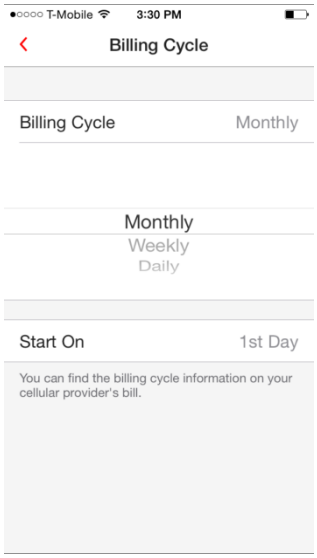

Figure 130. Monthly, etc…

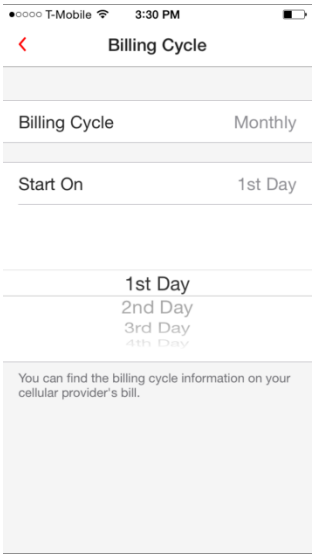

Figure 131. 1st Day

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.

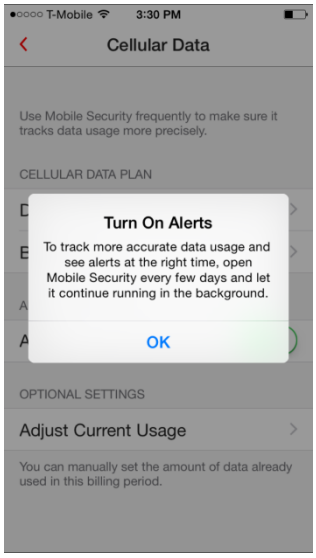

Figure 132. Turn On Alerts

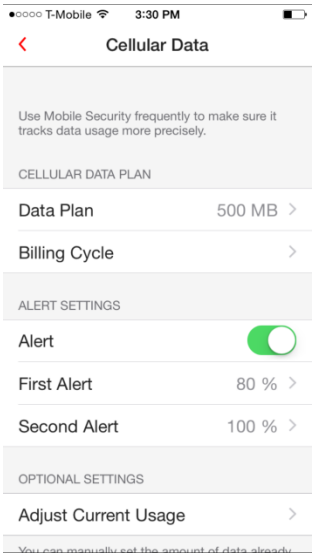

Figure 133. Alert Defaults

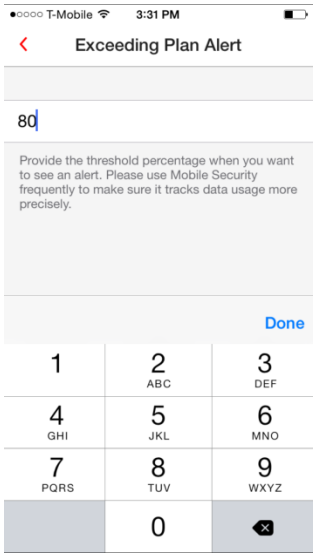

Figure 134. Exceeding Plan Alert

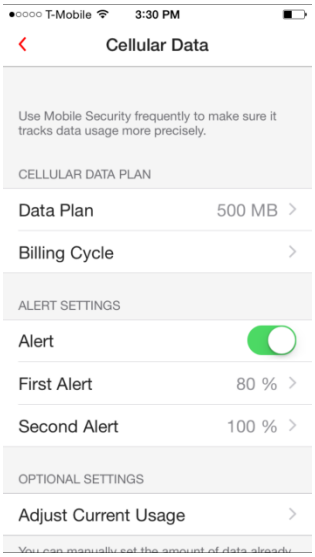

Figure 135. Optional Settings

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.**

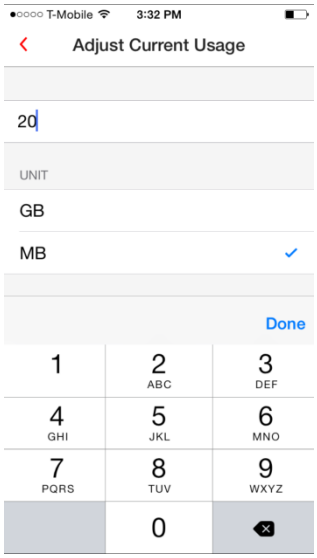

Figure 136. Adjust Current Usage

Figure 137. Cellular Data Usage Console

15. To adjust the **Roaming Data** settings, tap the **Roaming** tab in the main **Data Usage** screen.

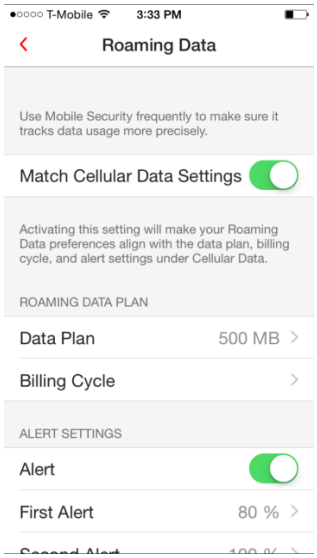

Figure 138. Roaming Data Settings

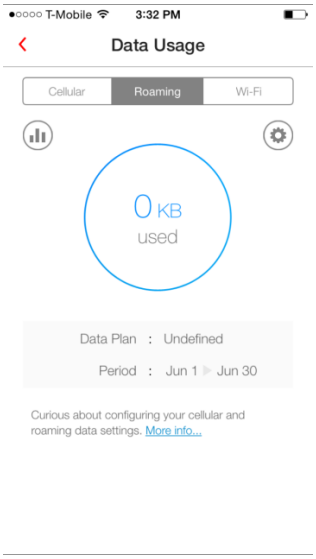

Figure 139. Roaming Data Usage

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.

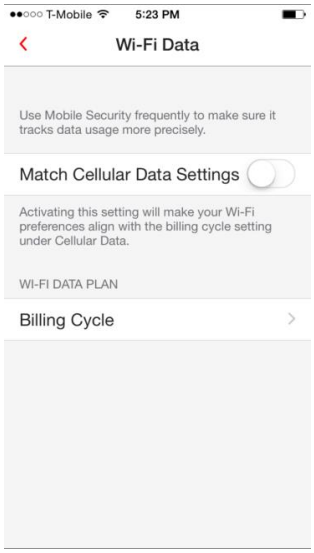

Figure 140. Match Cellular Data Settings

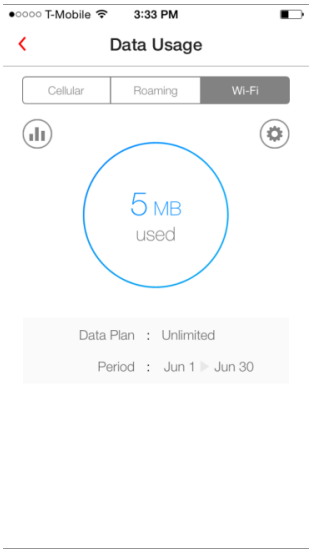

Figure 141. Wi-Fi Data Usage

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**.

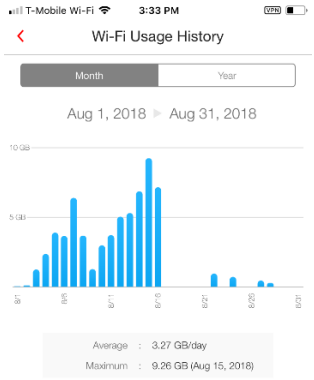

Figure 142. Wi-Fi Usage History | Month

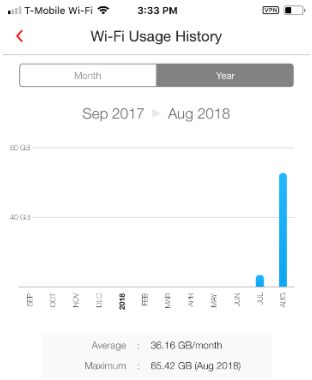

Figure 143. Wi-Fi usage History | Year (to date)

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.

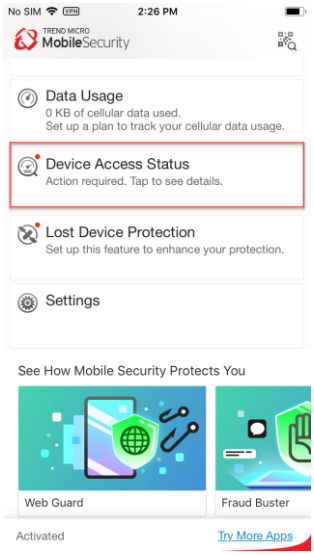

Figure 144. Device Access Status Panel

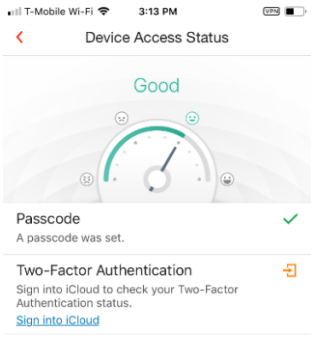

Figure 145. Device Access Status

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.

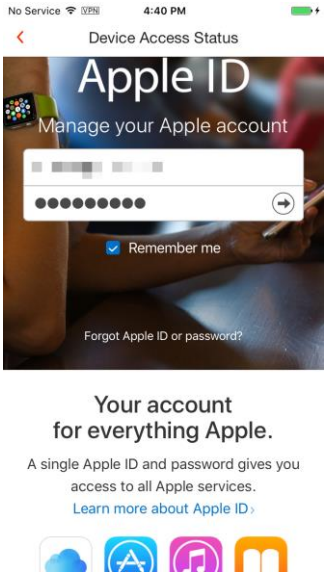

Figure 146. Enter Apple ID and Password

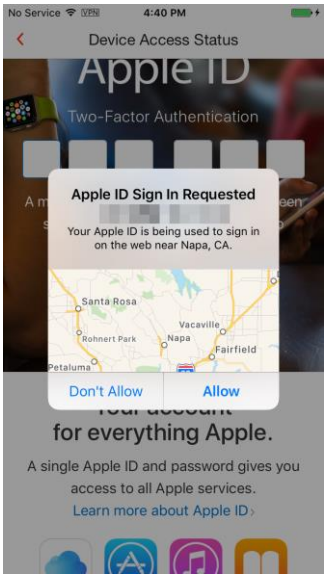

Figure 147. Allow Sign-In

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.

Figure 148. Apple ID Verification Code

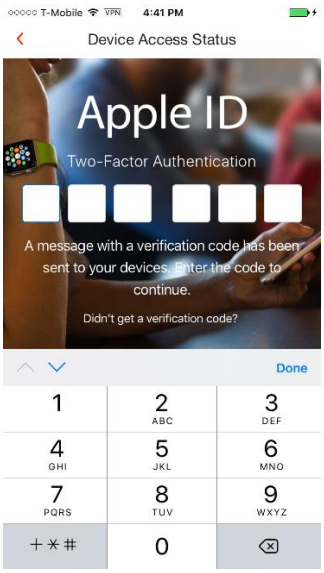

Figure 149. Enter Verification Code

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.

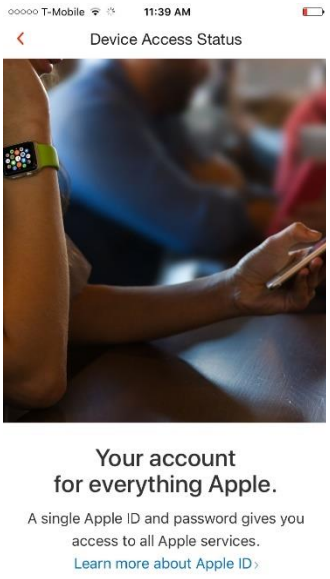

Figure 150. Logged In to Apple Account

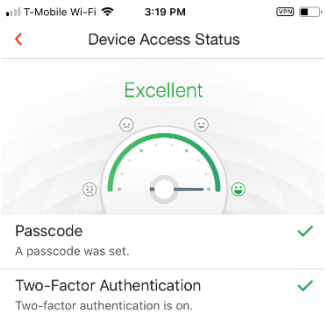

Figure 151. Two-Factor Authentication Verified | Excellent Status

10. The main screen of the **Console** also shows **Excellent, no action required.**

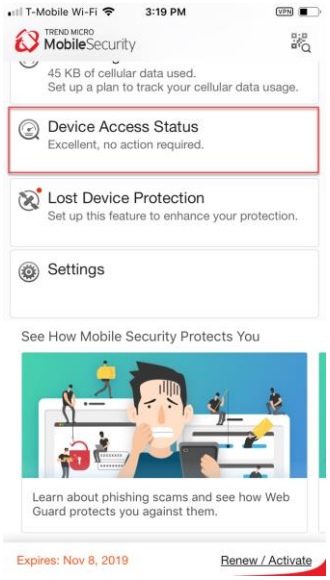

Figure 152. Device Access Status: Excellent

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?**

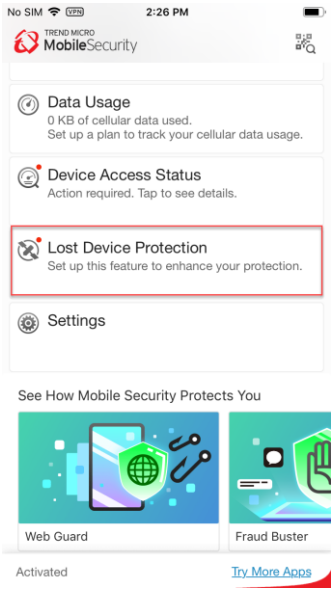

Figure 153. Main Console | Device Protection

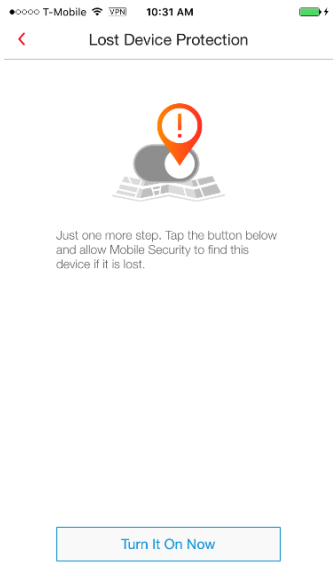

Figure 154. Lost Device Protection

Only While Using the App

Always Allow

Don't Allow

4. If you wish, tap **Always 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.

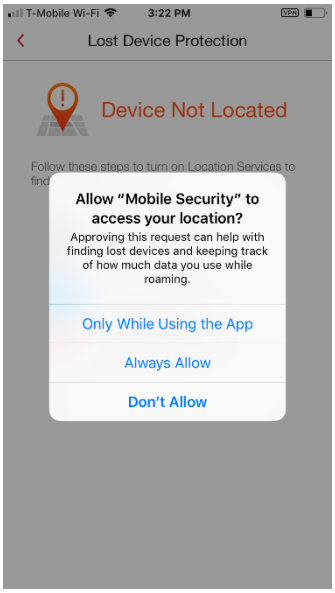

Figure 155. Allow Even When Not Using App

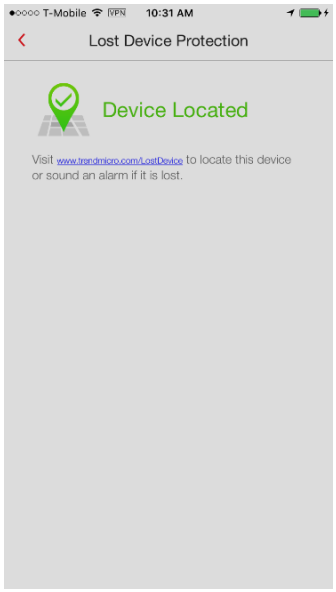

Figure 156. Device Located

Lost Device Protection Portal

To access the Lost Device Protection Portal:

1. Launch your browser on your Mac, PC, smart phone 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.**

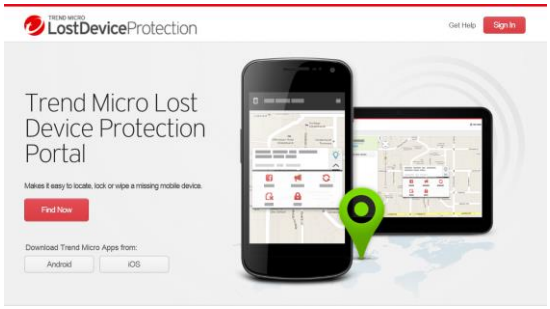

Figure 157. Lost Device Protection Portal Sign In

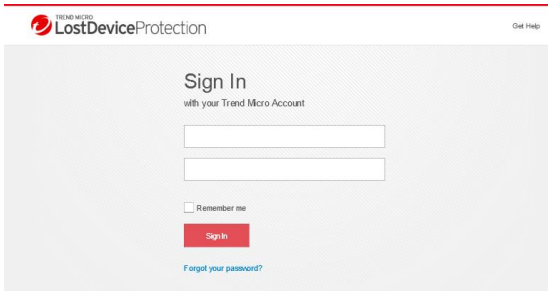

Figure 158. Sign In

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.

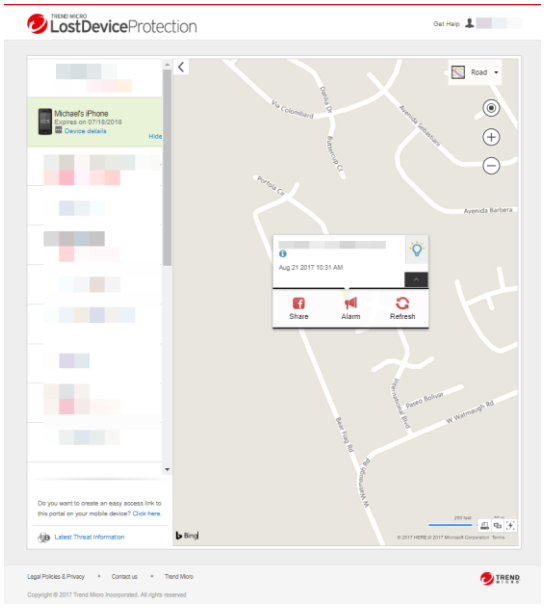

Figure 159. Lost Device Protection Options

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

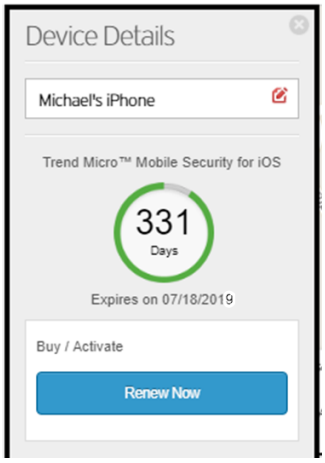

Figure 160. Device Detail

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.

Transfer a subscription to this device. Lets you move an existing sub to this device. It removes it from the other device

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.

Report a Suspicious Website. Provides a form to report a suspicious website.

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.

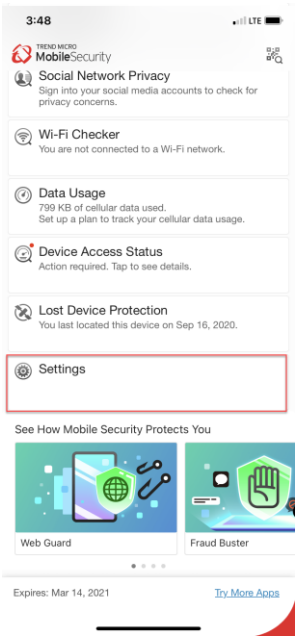

Figure 161. Settings

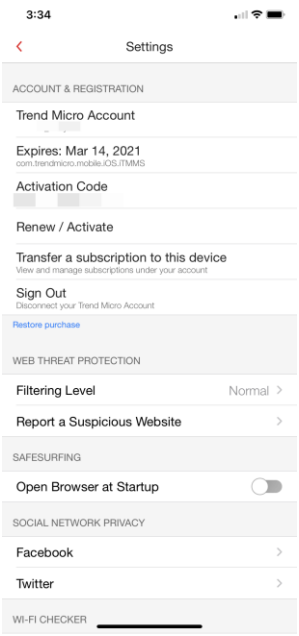

Figure 162. Settings (1)

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.

Help Improve This App. Toggle On/Off to share/not share usage data with Trend Micro.

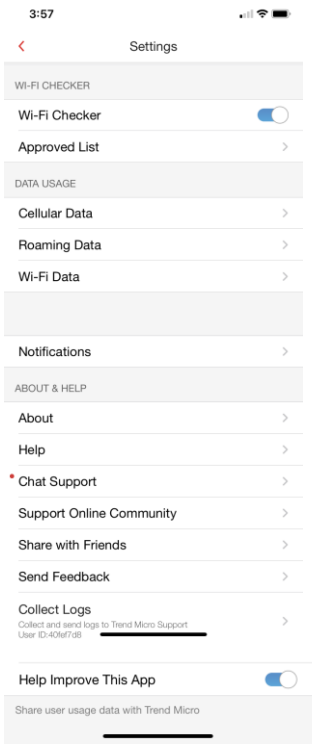

Figure 163. Settings (2)

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 release includes demos for **Web Guard, Fraud Buster, Wi-Fi Checker,** and **Social Network Privacy**. We've selected the **Web Guard** and **Wi-Fi Checker** demos for presentation. You should explore all the demos.

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

Web Guard Demo

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 **Test Web Guard** to see how it protects you.

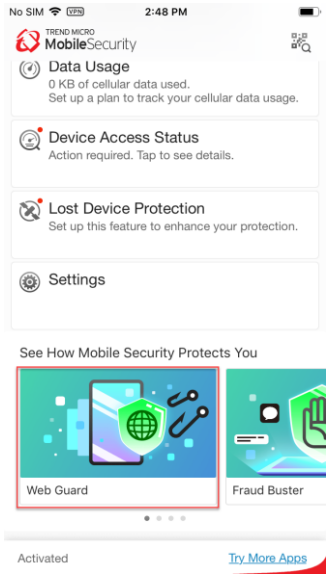

Figure 164. See How Mobile Security Protects You with Web Guard

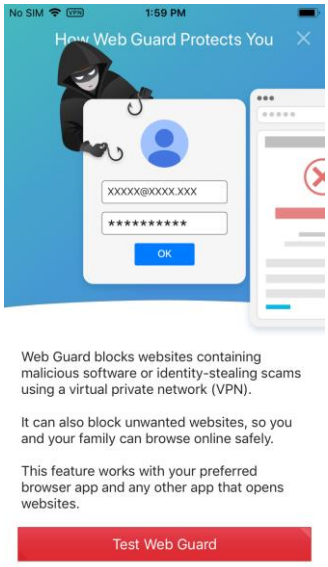

Figure 165. Test Web Guard

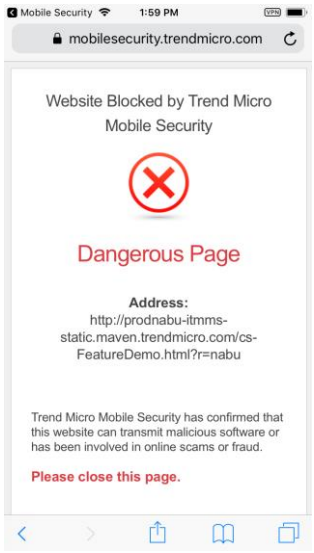

Figure 166. Dangerous Page

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 Wi-Fi Checker.** It describes the dangers of unencrypted Wi-Fi and what **Wi-Fi Checker** provides.
3. Tap **Take a Look** to launch the demo.

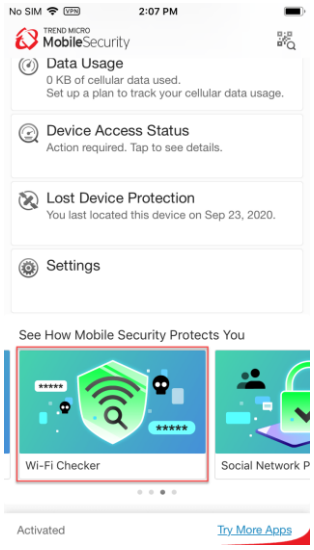

Figure 167. See How Mobile Security Protects You with Wi-Fi Checker

Figure 168. Experience Wi-Fi Checker

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 and a Wi-Fi Checker popup indicating security issues on the network
6. Tap **Next**.

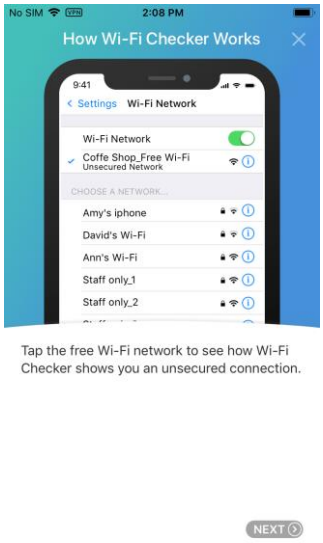

Figure 169. Using Free Wi-FI

Figure 170. Wi-Fi Checker Notification

7. The demo shows **2 Issues Found** and that **Wi-Fi Checker** is on.
8. You're now protected by **Wi-Fi Checker.**

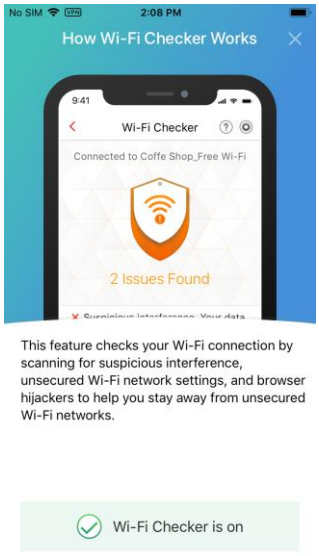

Figure 171. 2 Issues Found

Transferring Licenses Between Devices

Trend Micro Mobile Security allows you to transfer licenses between devices, across your registered subscriptions. 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. The instructions below assume you're already logged into your Trend Micro Account in the app.

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 **Transfer a subscription to this device**.

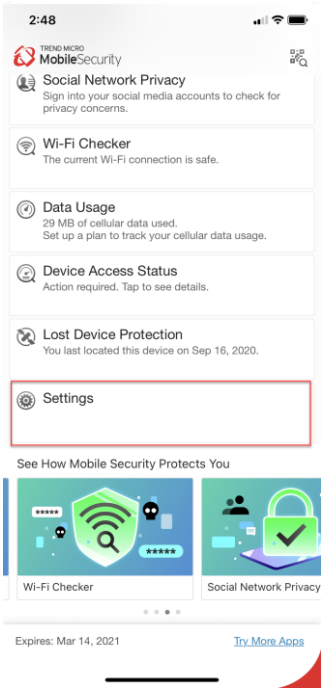

Figure 172. Main Console | Premium Version Expired

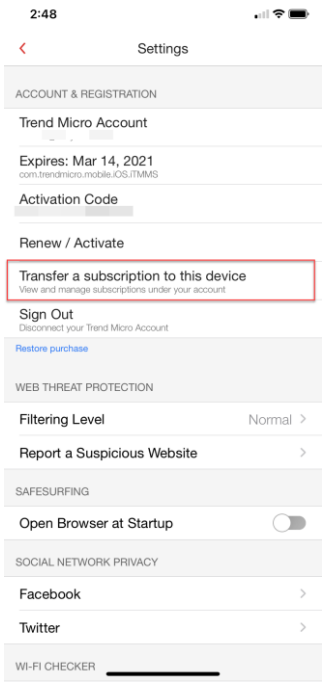

Figure 173. Settings > Set Up Account

3. Use the drop-down arrow to select options in a license. For example, **Titanium Maximum Security** shows four seats by device in use in the subscription that are available for transfer. Upon transfer, that device will lose the protection.
4. Tap a device in the list to begin the transfer. A popup appears, asking if you want to **Transfer Existing License(s).**
5. Tap **OK**. The license is transferred to this device.
6. The **Console** will update and the expiration date for that license will be displayed in the lower left-hand corner.

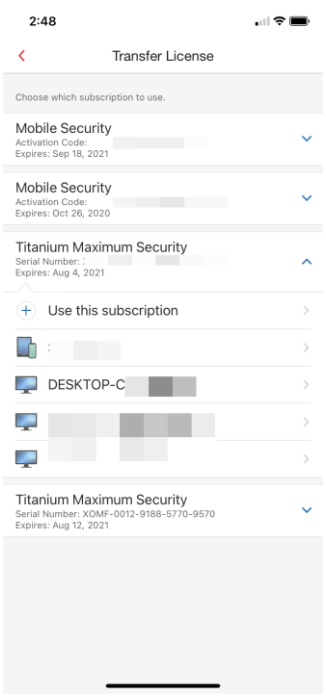

Figure 174. Transfer License

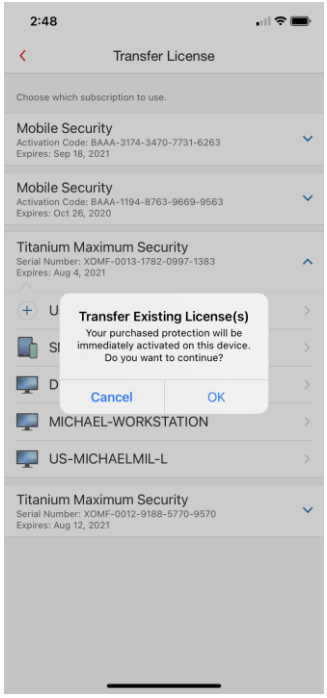

Figure 175. Transfer Existing License(s)

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) on an iPad Pro.

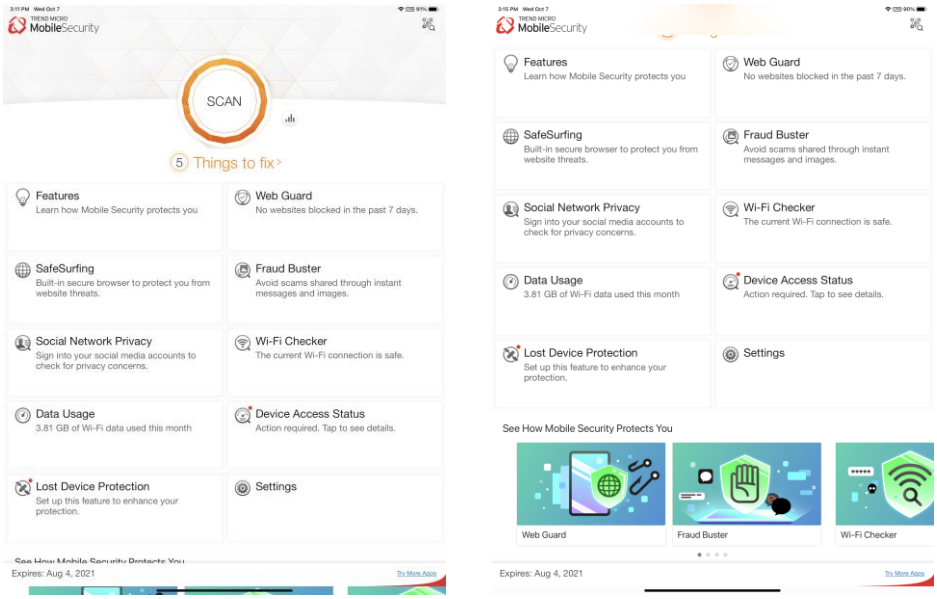

Figure 176. Trend Micro Mobile Security for iOS on the iPad Pro (Scrolling Portrait View)

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

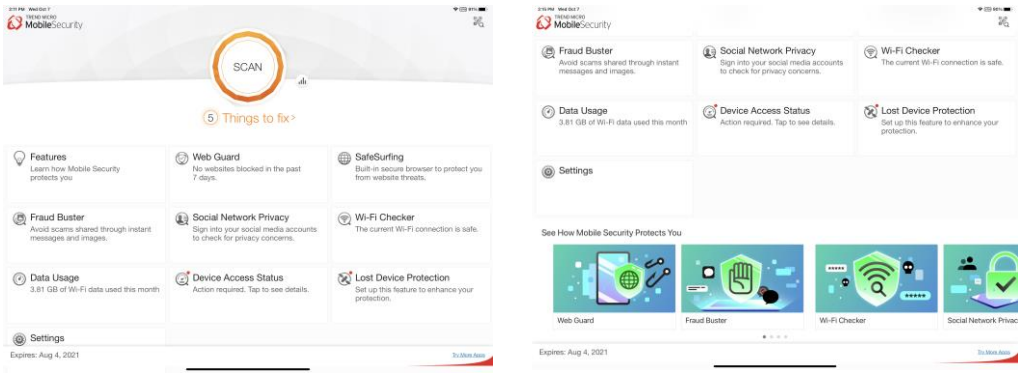

Figure 177. Trend Micro Mobile Security for iOS on the iPad Pro (Scrolling Landscape View)

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.