

راهنمای سریع استفاده از نسخه
موبایل (اندروید) کوئیک هیل



شرکت فناوری ارتباطات و اطلاعات فانوس
نماینده رسمی محصولات امنیتی کوئیک هیل در ایران
۰۲۱۷۷۱۴۲۵۲۶ www.quickheal.co.ir info@qhi.ir

Quick Heal
Security Simplified



تیم فنی شرکت فناوری ارتباطات و اطلاعات فانوس به عنوان نخستین نماینده رسمی کوئیک هیل در ایران چکیده بیش از ۷ سال تجربه کار با آنتی ویروس کوئیک هیل را به صورت کاربردی و ساده، در این جزوه آموزشی گرد آورده است.

در صورت داشتن هر نوع سوال، پیشنهاد یا انتقادی می توانید با شرکت فناوری ارتباطات و اطلاعات فانوس از طریق ایمیل info@qhi.ir، تلفن ۰۲۱-۷۷۱۴۲۵۲۶، پیامک ۳۰۰۰۴۶۲۵، وبسایت www.quickheal.co.ir و نیز وبلاگ اطلاع رسانی امنیتی این شرکت blogs.quickheal.co.ir ارتباط برقرار فرمایید. سوالات فنی خود را با ایمیل support@quickheal.co.ir مطرح نمایید.

کاربران طرح جزیره امن می توانند برای ارتباط با شماره تلفن ۰۱۱-۴۲۷۲۲، پیامک ۱۰۰۰۴۲۷۲۲، ایمیل support@42722.ir تماس و یا به وبسایت طرح <http://42722.ir> مراجعه فرمایند.

بدیهی است استفاده از این جزوه تنها ویژه شبکه توزیع، مشتریان شرکت فناوری فانوس مجاز می باشد و حق نسخه برداری برای این شرکت محفوظ است.

فهرست مطالب

۴	آنتی ویروس کوپیک هیل توتال سکیوریتی اندروید
۵	نصب کوپیک هیل توتال سکیوریتی اندروید
۶	نیازمندی های سیستمی
۷	نصب کوپیک هیل توتال سکیوریتی
۱۴	پورتال مدیریت ابزار راه دور (RDM)
۲۵	داشبورد
۲۷	ویژگی ها
۸۲	راهنما (Help)
۸۵	خاتمه

آنتی ویروس کوپیک هیل توتال سکیوریتی اندروید

کوپیک هیل توتال سکیوریتی اندروید، ارائه دهنده راهکار جامع حفاظتی برای گوشی‌های اندروید در برابر انواع تهدیدات، بدافزارها و ویروس‌ها طراحی شده است. کار با آن بسیار ساده و کاربرپسند بوده و کاربر می‌تواند از ویژگی‌های مهم امنیتی و جذاب کاربردی مانند اسکن دستگاه، بهینه‌سازی دستگاه، امن‌سازی داده، حفظ حریم خصوصی و تنظیمات پیشرفته استفاده نماید.

نصب کوپیک هیل توتال سکیوریتی اندروید

فرایند نصب و استفاده از کوپیک هیل توتال سکیوریتی اندروید ساده می باشد. در زمان نصب، به دقت به راهنماها و پیغام های نمایش داده شده توجه نموده و دستورالعمل ها را دنبال نمایید. نرم افزار Quick Heal Total Security برای پلتفرم Android طراحی شده است.

پیش از شروع به نصب به موارد زیر توجه نمایید:

- ابتدا مطمئن شوید که آنتی ویروس دیگری بر روی دستگاه شما نصب نباشد. (نصب چند آنتی ویروس بر روی یک دستگاه ممکن است موجب اختلال در عملکرد دستگاه گردد.) اگر آنتی ویروس دیگری بر روی دستگاه شما نصب است، ابتدا آنرا حذف نمایید.
- پیش از نصب Quick Heal Total Security همه برنامه ها را ببندید.

نیازمندی‌های سیستمی

آنتی‌ویروس توتال سکیوریتی کوپیک‌هیل اندروید می‌تواند بر روی همه دستگاه‌هایی که از اندروید (Android) پشتیبانی می‌کنند، نصب شود.

نسخه‌های قابل پشتیبانی سیستم‌عامل اندروید و دقت صفحه نمایش به شرح زیر می‌باشند:

نسخه‌های اندروید: ۲.۳، ۳.۰، ۴.۰ و بالاتر

دقت صفحه نمایش (Resolutions):

صفحات نمایش کوچک - ۲۴۰ در ۳۲۰

صفحات نمایش معمولی - ۳۲۰ در ۴۸۰

صفحات نمایش بزرگ - ۴۸۰ در ۶۰۰

صفحات نمایش خیلی بزرگ - ۶۰۰ در ۱۰۲۴ (اخیراً برای تبلت اضافه شده)

نصب کوپیک هیل توتال سکیوریتی

برای نصب آنتی ویروس توتال سکیوریتی کوپیک هیل اندروید ابتدا برنامه نصب کننده را از سایت های رسمی دانلود کنید:

الف) دانلود نرم افزار

کاربران عادی:

کاربرانی که پکیج کوپیک هیل توتال سکیوریتی را از بازار تهیه کرده اند، وارد سایت زیر شده و کلید محصول (لایسنس) ۲۰ کاراکتری دریافتی را وارد فیلد صفحه کرده و Submit را فشرده تا لینک برنامه نصب (Setup) نمایش داده شود.

<http://quickheal.co.ir/installer>



مشتریان طرح جزیره امن:

کاربران طرح جزیره امن وارد سایت زیر شده و شماره تلفن و کد رهگیری دریافتی (از مراکز مخابراتی / تلفن / آنلاین و سایت اینترنتی / پیامک) را وارد کرده و لینک دانلود نرم افزار، لایسنس محصول و راهنما را دریافت نمایند.

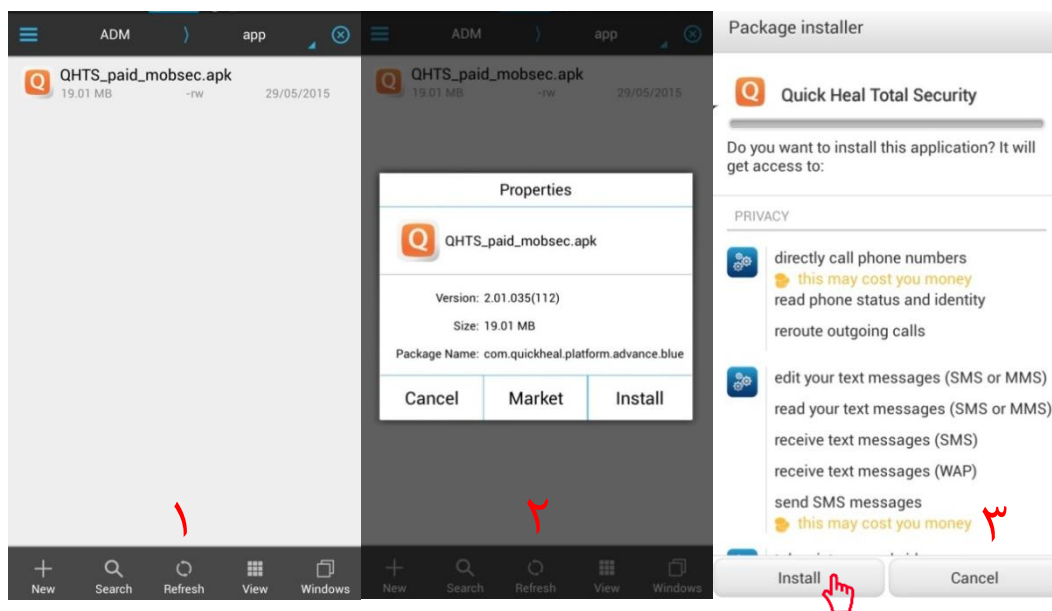
<http://42722.ir/dw>



ب) نصب آنتی ویروس کوپیک هیل توتال سکیوریتی اندروید

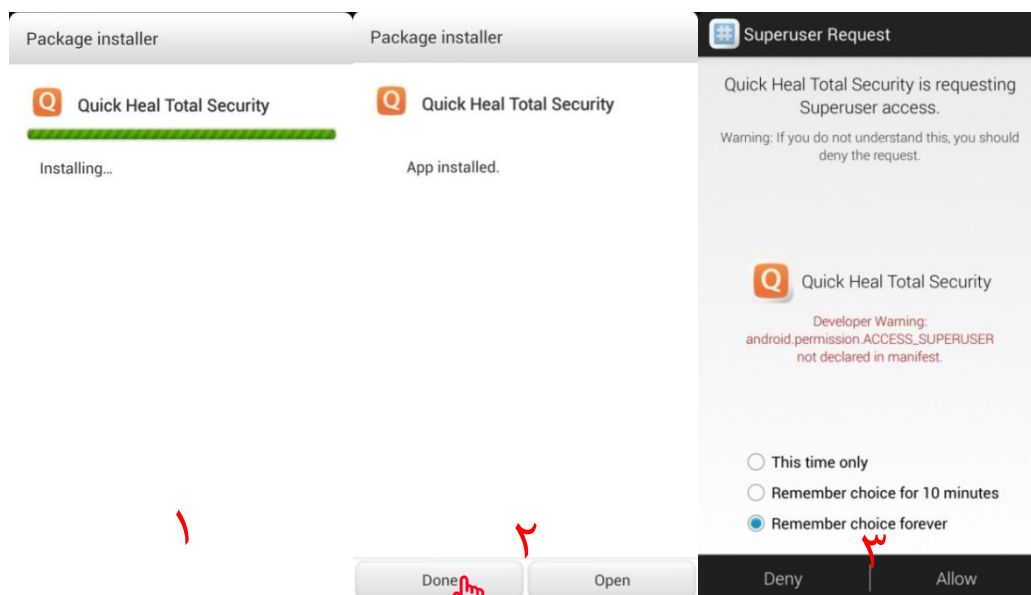
برای نصب آنتی ویروس کوپیک هیل توتال سکیوریتی اندروید، گام های زیر را دنبال نمایید:

۱. اگر فایل نصب برنامه را مستقیماً از روی گوشی موبایل خود از وبسایت دانلود کردید، بر روی فایل نصب (.apk) ضربه بزنید تا نصب شروع شود.
اگر فایل را از روی کامپیوتر خود دانلود کردید، فایل را از روی رایانه، داخل دستگاه کپی کرده و سپس بر روی فایل نصب (.apk) درون دستگاه ضربه بزنید.
یک صفحه نمایش داده می شود و رضایت شما مبنی بر ادامه نصب را می پرسد.



۲. بر روی **Install** کلیک کنید.

پس از تکمیل فرایند نصب کوپیک هیل توتال سکیوریتی اندروید، دو دکمه **Open** و **Done** نمایش داده می شود.

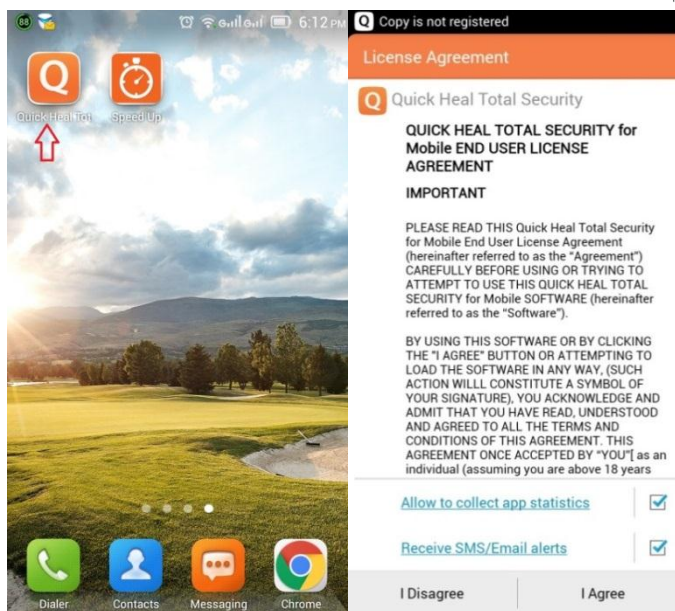


۳. بر روی دکمه **Done** ضربه بزنید.

برنامه Quick Heal به لیست همه برنامه‌های (All apps) دستگاه شما افزوده شد.

۴. آنتی ویروس کوپیک هیل برای اجرا نیاز به سطح دسترسی Superuser دارد. در صورت نیاز به تایید اعطای سطح دسترسی، گزینه Remember choice forever را انتخاب و بر روی Allow ضربه بزنید.

۵. برای اجرای برنامه به لیست برنامه‌ها رفته و بر روی آیکن Quick Heal Total Security کلیک کنید. توافقنامه استفاده از نرم‌افزار را با انتخاب I Agree بپذیرید.



به صورت پیش فرض گزینه *Collect app statistics* تیک شده است. این گزینه کمک می‌کند تا اطلاعات آماری برای مقاصد پژوهشی به Quick Heal Total Security ارسال گردد. اطلاعات ارسال تنها اطلاعات آماری مربوط به ویروس‌ها و بدافزارها بوده و هیچ‌گونه اطلاعات شخصی و خصوصی را شامل نمی‌شود. اگر نمی‌خواهید اطلاعات تجزیه و تحلیل ارسال گردد، تیک این گزینه را بردارید. گزینه Receive SMS/Email alerts به صورت پیش فرض انتخاب شده است. این گزینه باعث می‌شود تا هشدارها و بروزرسانی‌های کوپیک هیل توتال سکیوریتی به شما ارسال شوند. اگر نمی‌خواهید پیام‌های هشدار و امنیتی را دریافت نمایید این گزینه را غیرفعال کنید.

۶. پس از اتمام نصب و قبول توافقنامه، به صفحه فعال‌سازی (Activation) هدایت می‌شوید تا محصول خود را ثبت نمایید.

ج) ثبت نام و فعال سازی

پس از نصب، برای استفاده از همه ویژگی‌های امنیتی، دریافت آپدیت و پشتیبانی فنی باید محصول خود را ثبت و فعال نمایید.

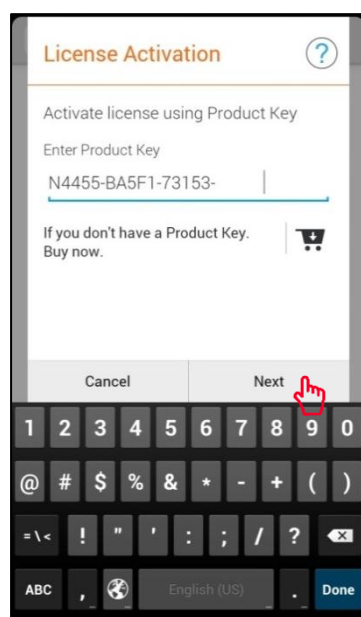
همچنین می‌توانید کوپیک هیل توتال سکیوریتی قبلی خود را پس از حذف از گوشی اول، بر روی موبایل دیگر نصب و فعال سازی مجدد نمایید. البته باید همان شماره موبایل قبلی که در زمان ثبت نام اولیه وارد کردید، مجدداً وارد نمایید.

هنگامی که می‌خواهید دستگاه گوشی خود را عوض کنید، مطمئن شوید که محصول خود را از گوشی قدیمی خود غیرفعال (deactivated) و حذف (uninstall) کرده‌اید.

ثبت لایسنس (کنترل خانواده)

برای ثبت محصول و لایسنس خود مراحل زیر را دنبال نمایید:

۱. پس از اجرای برنامه و قبول توافقتنامه (I Agree) صفحه فعال سازی نمایش داده می‌شود.
۲. کلید محصول (لایسنس) ۲۰ کارکتری را وارد نمایید. بر روی **Next** ضربه بزنید.



توجه: اگر هنوز لایسنس را خریداری نکرده‌اید می‌توانید همین الان به صورت آنلاین از فروشگاه اینترنتی کوپیک هیل به نشانی <http://shop.quickheal.co.ir> خریداری نمایید.

۳. اطلاعات خودتان را وارد نمایید. بر روی **Next** ضربه بزنید.

Name: نام خودتان را وارد نمایید. مثلاً: Reza Taghavi

Mobile Number: شماره موبایل خودتان را وارد کنید. مثلاً 9121111111

Email ID: آدرس ایمیل خودتان را وارد نمایید. مثلاً reza.taghavai20@gmail.com

توجه: اگر حساب کاربری گوگل بر روی گوشی شما فعال باشد، آدرس ایمیل Google شما در فیلد Email ID نشان داده خواهد شد. اگرچه می‌توانید آدرس ایمیل را به دلخواه خودتان عوض کنید.

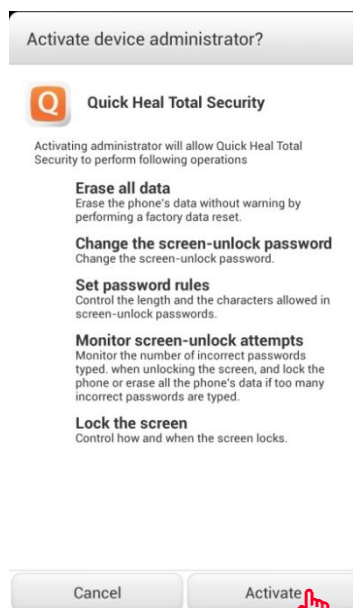
۴. یک رمز عبور برای دسترسی به نرم‌افزار وارد نمایید (حداقل ۶ کاراکتر). مجدداً رمز عبور را در فیلد Confirm Password وارد نمایید. رمز عبور را در جای مطمئن یادداشت کنید.

۵. برای مواقع ضروری شماره تلفن‌های جایگزین (مثلاً شماره یکی از اعضای خانواده یا دوستان) معرفی نمایید. می‌توانید با وارد کردن بخشی از نام تلفن یا شماره موبایل، از منوی بازشونده، مخاطب موردنظر را انتخاب و بر روی آن ضربه بزنید. نام یا شماره تلفن‌های جایگزین باید در لیست مخاطبین (دفترچه تلفن) گوشی شما وجود داشته باشد. (مثلاً Baba یا 0911111111).

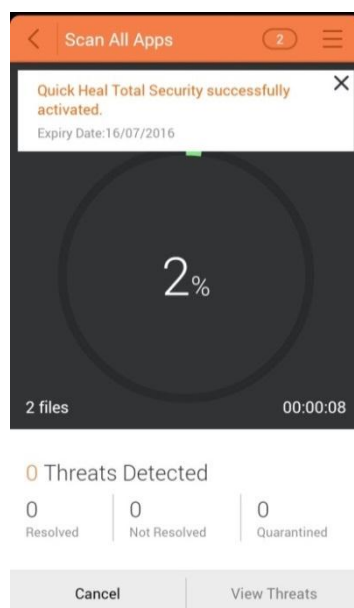
می‌توانید تا ۳ شماره جایگزین معرفی نمایید.

اگر می‌خواهید که آنتی‌ویروس کوپیک‌هیل توسط کاربران غیرمجاز (که رمزعبور کوپیک‌هیل شما را ندارند) حذف نشود، گزینه **Uninstallation Protection** را انتخاب کنید. در این صورت به هنگام حذف آنتی‌ویروس کوپیک‌هیل از روی دستگاه شما، رمز عبور کوپیک‌هیل پرسیده خواهد شد. این گزینه در نسخه‌های دارای لایسنس، به صورت پیش‌فرض فعال است. بر روی **Activate** ضربه بزنید تا فعال‌سازی صورت پذیرد.

توجه: اگر گزینه **Uninstallation Protection** را انتخاب نمایید، شما به صفحه فعال‌سازی مدیریت دستگاه (Activate device administrator) یا ADA هدایت می‌شوید. در صفحه ADA دکمه **Activate** را کلیک کنید تا محافظت در برابر حذف غیرمجاز کوپیک‌هیل صورت پذیرد.



پس از پایان احراز اصالت شماره موبایل شما، یک پیام نصب و فعال‌سازی موفق به همراه تاریخ انقضای لایسنس نمایش داده خواهد شد. به محض تکمیل فرایند فعال‌سازی، توتال سکیوریتی کوپیک‌هیل به صورت خودکار همه برنامه‌های نصب شده بر روی دستگاه را اسکن و ویروسیابی می‌کند.



د) فعال سازی مجدد

اگر می‌خواهید دستگاه خود را فرمت نمایید و یا گوشی خود را عوض کنید، می‌توانید ابتدا آنتی‌ویروس کوپیک‌هیل را از روی دستگاه خود حذف (UnInstall) نمایید.
سپس تا انتهای زمانی لایسنس کوپیک‌هیل، آنرا بر روی دستگاه دیگر نصب و استفاده نمایید.

ه) تمدید محصول

در صورت انقضای لایسنس، برای تمدید با شرکت فناوری ارتباطات و اطلاعات فانوس، نماینده انحصاری شرکت تکنولوژی‌های کوپیک‌هیل در ایران تماس حاصل فرمایید.

کاربران عادی:سایت: <http://quickheal.co.ir>

تلفن: ۰۲۱-۷۷۱۴۲۵۲۶

ایمیل: sales@quickheal.co.ir**کاربران طرح جزیره امن:**سایت: <http://42722.ir>

تلفن: ۰۱۱-۴۲۷۲۲

ایمیل: sales@42722.ir

پورتال مدیریت ابزار راه دور (RDM)

پس از فعال‌سازی می‌توانید به صورت اختیاری از امکانات مدیریت راه دور ابزار کوپیک‌هیل نیز به صورت رایگان استفاده نمایید. پورتال مدیریت راه دور ابزار کوپیک‌هیل (Quick Heal RDM) امکان کنترل و مدیریت از راه دور دستگاه‌های شما را می‌دهد. زمانی که موبایل در دسترس‌تان نیست، یا مفقود شده و یا به سرقت رفته، با استفاده از پورتال RDM کوپیک‌هیل می‌توانید ویژگی‌های مختلف کوپیک‌هیل توتال سکیوریتی را بر روی دستگاه خود اجرا کنید.

همچنین در صورت استفاده از چندین محصول کوپیک‌هیل به صورت همزمان، می‌توانید با ورود به کنترل پنل خود، لایسنس آنها را برای مدیریت متمرکز اضافه نمایید.

از طریق این پورتال ویژگی‌های زیر بر روی دستگاه قابل مدیریت و کنترل می‌باشند:

پشتیبان‌گیری از اطلاعات

شما می‌توانید از اطلاعات شخصی خود بر روی فضای ابری امن کوپیک‌هیل پشتیبان بگیرید تا هر زمان که نیاز به اطلاعات خود داشتید (مثلاً خراب شدن یا تعویض دستگاه) آن‌را از فضای ابری بر روی دستگاه خود برگردانید.

مکان‌یابی

- ردیابی دستگاه - این گزینه به شما کمک می‌کند تا هنگامی که دستگاه (موبایل / تبلت) شما مفقود شده یا به سرقت رفته، مکان آن را رهگیری نمایید. این ویژگی کمک می‌کند که دستگاه مفقود شده یا مسروقه خود را بیابید.
- زنگ زدن دستگاه - اگر دستگاه در نزدیکی شما گم شده، می‌توانید صدای آهنگ ویژه کوپیک‌هیل را به صدا آورده تا بتوانید آن را پیدا کنید.

قفل کردن

زمانی که دستگاه شما مفقود شد و یا به سرقت رفت، برای جلوگیری از سوءاستفاده از اطلاعات شخصی‌تان، می‌توانید آن‌را قفل نمایید. زمانی که دستگاه خود را با استفاده از RDM قفل نمایید، عکس اطراف دستگاه و موقعیت مکانی آن بر روی نقشه در پنل RDM شما نمایش داده خواهد شد.

باز کردن قفل

اگر دستگاه مفقود شده پیدا شد یا دستگاه را به اشتباه قفل کردید، می‌توانید قفل آن‌را از راه دور باز کنید.

حذف اطلاعات

زمانی که دستگاه شما مفقود شد یا به سرقت رفت، اطلاعات شخصی خود را از راه دور حذف نمایید. در این حالت اطلاعات هم از حافظه‌ی داخلی و هم خارجی (SD Card) حذف می‌شود.

شماره گیری / دریافت تماس خودکار

شما می‌توانید به صورت مخفی از گوشی مسروقه یا گم شده با یک شماره موبایل دیگر تماس برقرار نمایید. همچنین می‌توانید یک شماره مطمئن تعریف نمایید، تا به محض تماس آن شماره به موبایل مسروقه، به صورت خودکار و مخفی پاسخ داده شود.

عکس گرفتن خودکار

شما می‌توانید از مناطق اطراف دستگاه گم شده یا مسروقه عکس بگیرید و تصاویر به حساب کاربری ابری‌تان و آدرس ایمیل‌تان ارسال خواهد شد.

ضبط خودکار صدا

شما می‌توانید (هر بار) یک دقیقه صداهای اطراف دستگاه خود را به صورت مخفیانه ضبط نمایید. فایل‌های صدا به صورت خودکار به حساب کاربری ابری‌تان و آدرس ایمیل‌تان ارسال خواهد شد.

ضبط خودکار فیلم

شما می‌توانید (هر بار) یک دقیقه ویدئوی اطراف دستگاه خود را به صورت مخفیانه ضبط نمایید. فایل‌های ویدئو به صورت خودکار به حساب کاربری ابری‌تان و آدرس ایمیل‌تان ارسال خواهد شد.

اسکن ابزار

در صورت نیاز می‌توانید از راه دور دستگاه خودتان را اسکن و ویروسیابی نمایید.

اسکن کامل

می‌توانید از راه دور اسکن کامل را بر روی دستگاه‌تان اجرا نمایید.

اسکن کارت حافظه

می‌توانید از راه دور تنها حافظه جانبی دستگاه خود را اسکن نمایید.

اسکن پس زمینه

می‌توانید از راه دور تنظیمات اسکن پس زمینه دستگاه‌تان را تغییر دهید.

پشتیبان گیری خودکار

می توانید از راه دور تنظیمات پشتیبان گیری خودکار دستگاه خود را تغییر دهید.

کنترل خانواده

می توانید از راه دور تنظیمات کنترل خانواده دستگاه خود را تغییر دهید.

بروزرسانی پایگاه داده ویروس

می توانید از راه دور آنتی ویروس کوپیک هیل توتال سکیوریتی دستگاه خود را بروزرسانی و آپدیت نمایید.

محافظت از حریم خصوصی

می توانید از راه دور یک لیست مخاطبین خصوصی برای خود ایجاد کرده و تاریخچه تماس ها و پیامک های آنها را امن نمایید تا از دسترس دیگران مخفی بماند.

انتقال همه تماس ها

موقعی که دستگاه در دسترس شما نیست (مثلاً فراموش کرده اید گوشی خود را به محل کار خود بیاورید) می توانید یک شماره تعیین نمایید تا همه تماس های ورودی به آن شماره انتقال یابند. همچنین می توانید انتقال تماس را از طریق ارسال یک پیامک فعال یا غیرفعال نمایید.

قالب دستور پیامکی به شرح زیر است:

<شماره ای که می خواهید تماس ها به آن انتقال یابد> <رمز عبور> START_FORWARD

مثال:

START_FORWARD 123456789 09111111111

همچنین می توانید انتقال تماس را با ارسال پیامک با قالب زیر متوقف نمایید:

<شماره ای که می خواهید تماس ها به آن انتقال یابد> <رمز عبور> STOP_FORWARD

تنظیم حفظ حریم خصوصی

می توانید تماس ها و پیامک ها از شماره های ناخواسته را مسدود نمایید. همچنین می توانید پیامک هایی که دارای متن مورد نظر شماست را فیلتر نمایید. غیرفعال کردن این ویژگی، ویژگی «فیلتر پیامک ها و تماس ها» را نیز غیرفعال می کند.

پس از ایجاد حساب کاربری، یک ایمیل فعال سازی به آدرس ایمیل شما ارسال می شود. لطفاً ایمیل خود را باز کرده و طبق راهنما بر روی لینک مربوطه کلیک نمایید.

الف) ایجاد حساب کاربری در RDM

پیش از ایجاد حساب کاربری در RDM، می‌بایست نرم‌افزار کوپیک‌هیل را بر روی دستگاه خود نصب، و با یک لایسنس معتبر ثبت و فعال‌سازی نمایید.

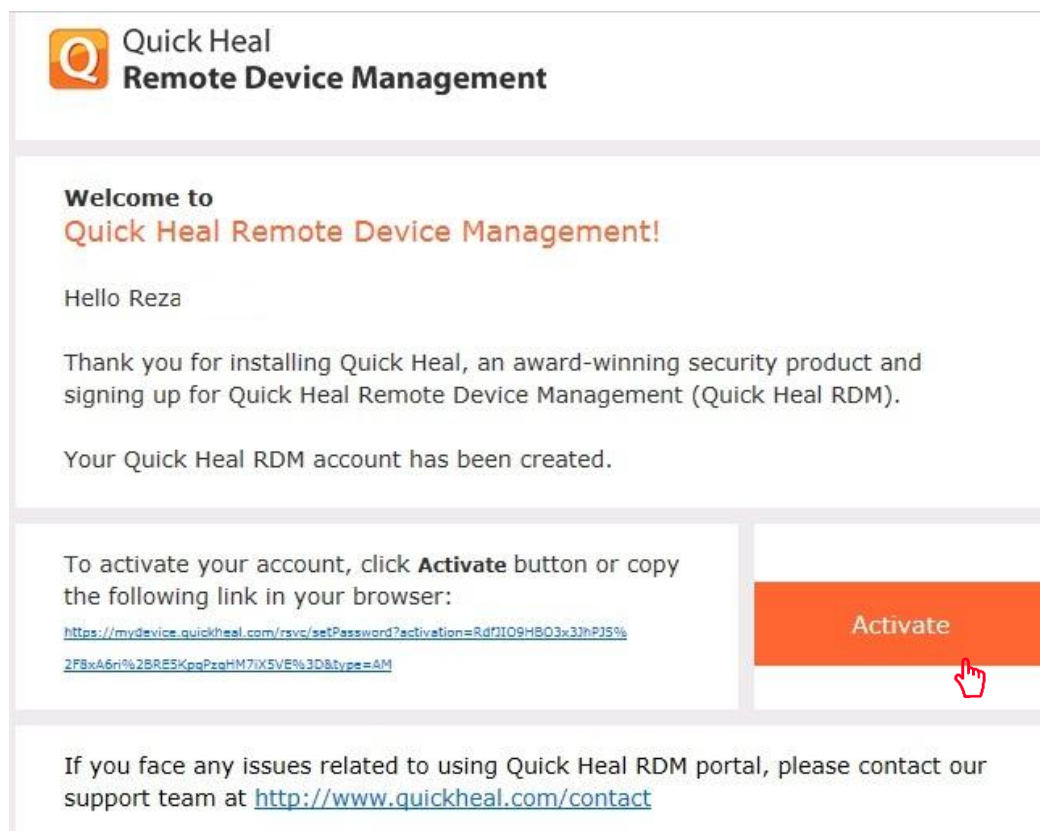
چند روش برای ایجاد حساب کاربری RDM وجود دارد. روش نخست، پس از نصب محصول، ایمیل راهنمای ایجاد حساب کاربری RDM به صورت خودکار برایتان ارسال خواهد شد.

در روش دوم، شما با مراجعه به وب‌سایت پورتال به نشانی <https://mydevice.quickheal.com>، مستقیماً اقدام به ایجاد حساب کاربری RDM می‌نمایید.

در روش سوم، با استفاده از حساب کاربری گوگل (Google account) خود، اقدام به ایجاد حساب کاربری RDM می‌نمایید.

ابتدا روش نخست را شرح می‌دهیم:

۱. پس از ثبت نام کوپیک‌هیل توتال سکیوریتی یک ایمیل برای شما ارسال می‌شود که راهنمایی لازم جهت ایجاد حساب کاربری RDM به شما ارائه می‌گردد.



۲. ایمیل خود را چک کرده و بر روی دکمه **Activate** کلیک و یا لینک داده شده را در نوار آدرس مرورگر کپی و اجرا کنید.

۳. رمز عبور را تعیین و **Save** را کلیک کنید.

اکنون حساب کاربری شما با موفقیت ایجاد شده است. از این پس شما می‌توانید وارد پورتال RDM کوپیک‌هیل شده و دستگاه خود را از راه دور مدیریت نمایید.

ب) ایجاد حساب کاربری در RDM به صورت دستی

همچنین شما می‌توانید با ورود به وبسایت پورتال کوپیک هیل به صورت مستقیم اقدام به ایجاد حساب کاربری RDM نمایید:

۱. وارد سایت پورتال RDM کوپیک هیل به نشانی <https://mydevice.quickheal.com> شوید.
۲. نام کاربری یا آدرس ایمیل، شماره موبایل معتبر، کلید محصول (لایسنس) و عبارت امنیتی خود را وارد نمایید.
۳. پس از مطالعه توافقنامه استفاده از نرم‌افزار گزینه *I agree to the Quick Heal License Agreement and Privacy Policy* را انتخاب کنید.
۴. بر روی دکمه *Sign up* کلیک کنید.
- در این مرحله یک ایمیل حاوی راهنمای چگونگی فعال‌سازی حساب کاربری Quick Heal RDM به آدرس ایمیل‌تان ارسال می‌شود.
۵. ایمیل خود را چک کرده و بر روی دکمه *Activate* کلیک و یا لینک داده شده را در نوار آدرس مرورگر کپی و اجرا کنید.
- سپس شما به صفحه تعیین رمز عبور (set password) هدایت خواهید شد.
۶. رمز عبور را وارد و بر روی دکمه *Save* کلیک کنید.

اکنون حساب کاربری شما با موفقیت ایجاد شده است. از این پس شما می‌توانید وارد پورتال RDM کوپیک هیل شده و دستگاه خود را از راه دور مدیریت نمایید.

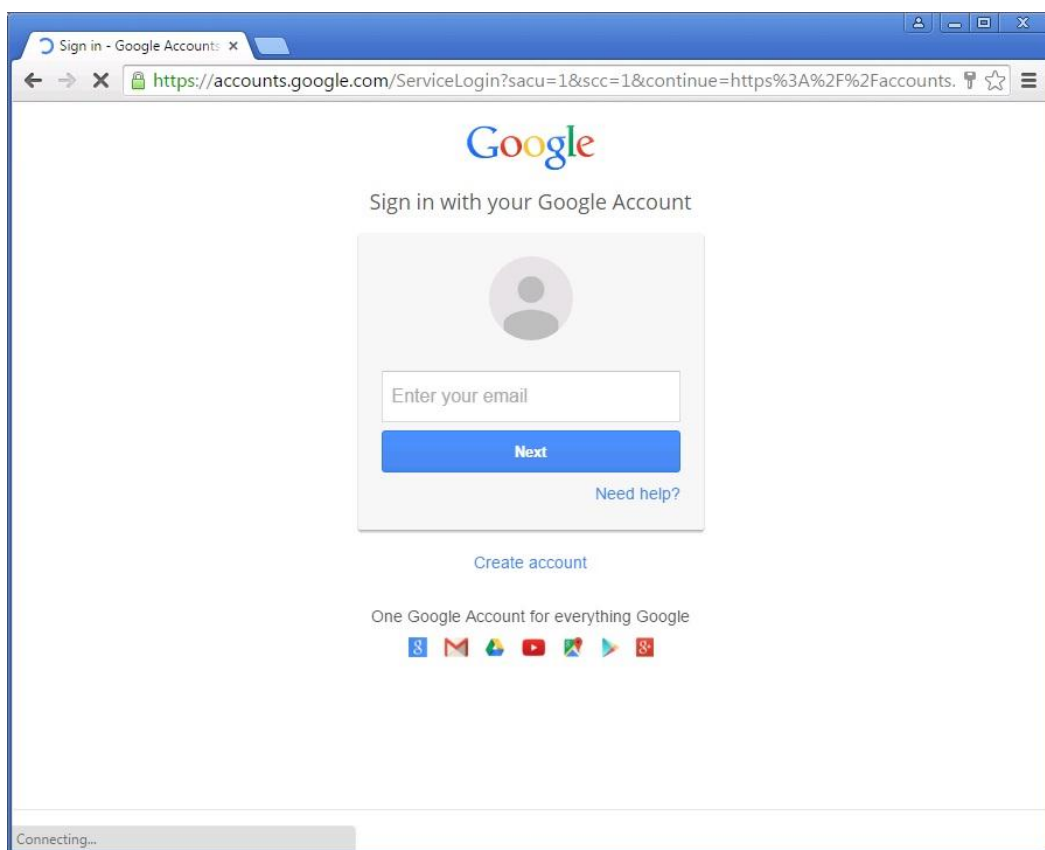
ج) ایجاد حساب کاربری با حساب کاربری گوگل

اگر از قبل حساب کاربری گوگل دارید، می‌توانید با استفاده از آن یک حساب کاربری در پورتال مدیریت راه دور ابزار کوپیک هیل (RDM) بسازید.

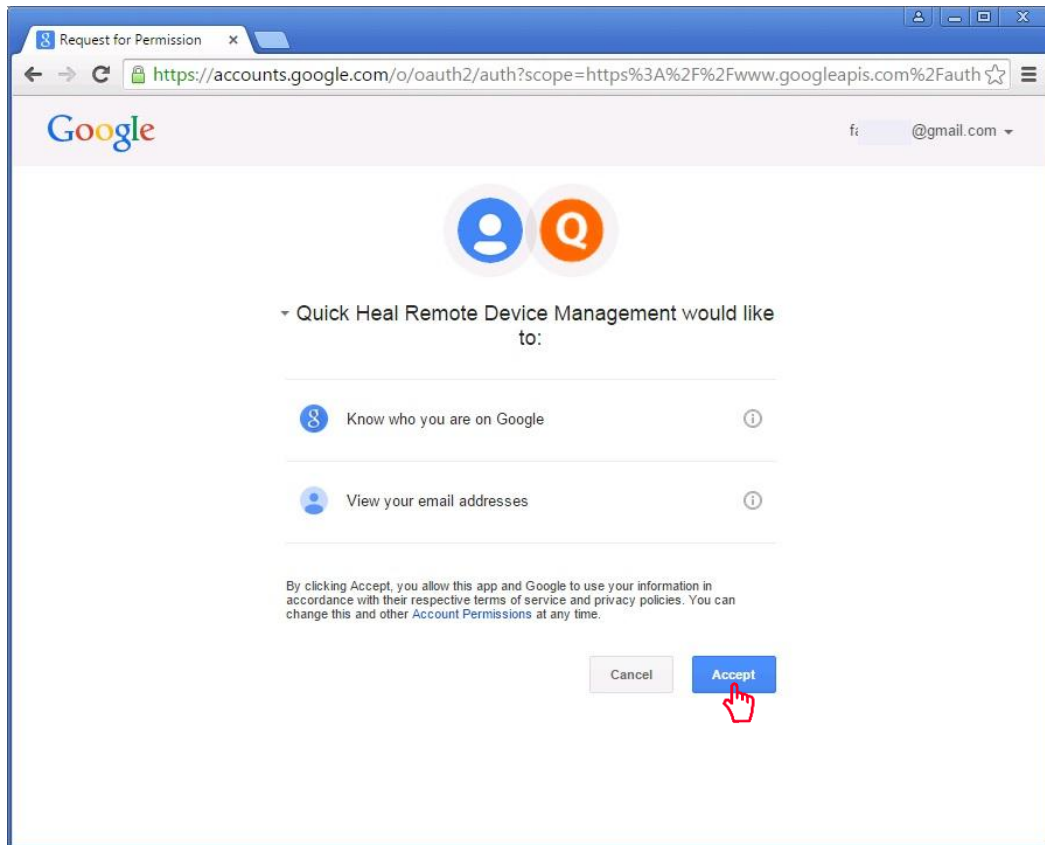
برای ایجاد حساب کاربری RDM با استفاده از حساب کاربری گوگل وارد پورتال RDM کوپیک هیل به نشانی <https://mydevice.quickheal.com> شده و گام‌های زیر را دنبال کنید:

۱. بر روی دکمه **Sign in with Google**  در پایین کادر لاگین کلیک کنید.

۲. نام کاربری (ایمیل) و رمز عبور حساب کاربری گوگل خود را وارد کنید.



۳. توافنامه استفاده از سرویس را خوانده و بر روی دکمه *Accept* کلیک کنید.



۴. نام کاربری یا آدرس ایمیل، شماره موبایل معتبر، کلید محصول (لایسنس) و عبارت امنیتی خود را وارد نمایید.

۵. پس از مطالعه توافقنامه استفاده از نرم افزار گزینه *I agree to the Quick Heal License Agreement and Privacy Policy* را انتخاب کنید.

۶. بر روی دکمه *Sign up* کلیک کنید.

اکنون حساب کاربری شما با موفقیت ایجاد شده است. از این پس شما می توانید وارد پورتال RDM کوپیک هیل شده و دستگاه خود را از راه دور مدیریت نمایید.

توجه: پس از ایجاد حساب کاربری RDM کوپیک هیل، اکنون باید دستگاه خود را با استفاده از منوی *Add Device* پیکر بندی نمایید.

د) افزودن دستگاه جدید به RDM کوپیک هیل

در اولین ورود به پورتال، صفحه ی *Add Device* برای افزودن دستگاه ظاهر می شود. برای مدیریت از راه دور دستگاه، باید دستگاه های (رایانه، لپ تاپ، موبایل، تبلت) خود را به پورتال معرفی نمایید.

برای افزودن دستگاه جدید گام های زیر را دنبال کنید:

۱. وارد پورتال RDM کوپیک هیل شوید: <https://mydevice.quickheal.com>

۲. صفحه *Add Device* به صورت خودکار نمایش داده خواهد شد.

همچنین می توانید با استفاده از آخرین منو (*Add Device*) وارد این صفحه شوید.

۳. در بخش *Name*، یک نام دلخواه برای دستگاه خود وارد کنید.

شما می توانید هر نامی را برای دستگاه خود تعیین نمایید. (مثلاً *MyMobile1*)

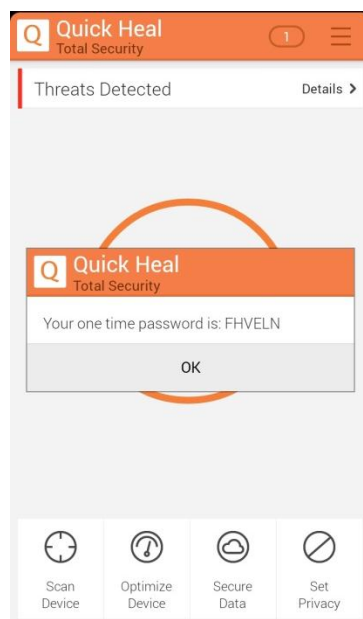
۴. در بخش *Product Key*، کلید محصول (لایسنس) از پیش تکمیل شده است.

در صورتی که این دستگاه، دستگاه چندم برای یک پورتال می باشد، کلید محصول موردنظر خود را وارد نمایید.

۵. بر روی **Add** کلیک کنید.

یک رمز عبور یکبار مصرف (OTP) به دستگاه شما ارسال می‌شود.

توجه: دقت کنید که دستگاه (مثل موبایل یا تبلت) به اینترنت دسترسی داشته باشد تا بتواند رمز عبور یکبارمصرف را دریافت نماید.



۶. آنتی‌ویروس کوپیک هیل بر روی دستگاه خود را اجرا و رمز **OTP** را دریافت کرده، آنرا در بخش **One Time Password** وارد و بر روی دکمه **Submit** کلیک کنید.

اکنون دستگاه شما با موفقیت به پورتال **RDM** کوپیک هیل متصل شده است.

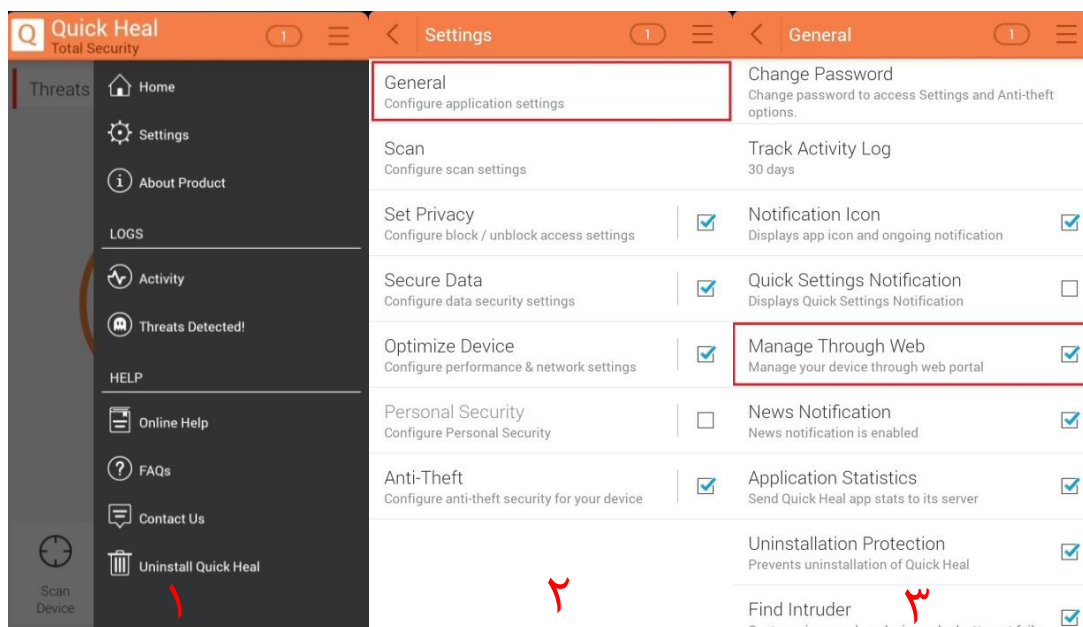
توجه: در صورتی که پس از گذشت چند دقیقه، رمز **OTP** را بر روی دستگاه خود دریافت نکردید، بر روی دکمه **Resend OTP** کلیک کنید تا مجدداً **OTP** جدید برایتان ارسال گردد.

هـ) فعال کردن مدیریت از طریق وب

برای مدیریت توتال سکیوریتی کوپیک هیل دستگاهتان، از طریق پورتال مدیریت از راه دور کوپیک هیل، همواره باید گزینه *Manage Through Web* را فعال بگذارید. همچنین می‌توانید در صورتی که تمایل ندارید دستگاه شما از طریق پورتال وب RDM کوپیک هیل کنترل شود، این گزینه را غیرفعال نمایید.

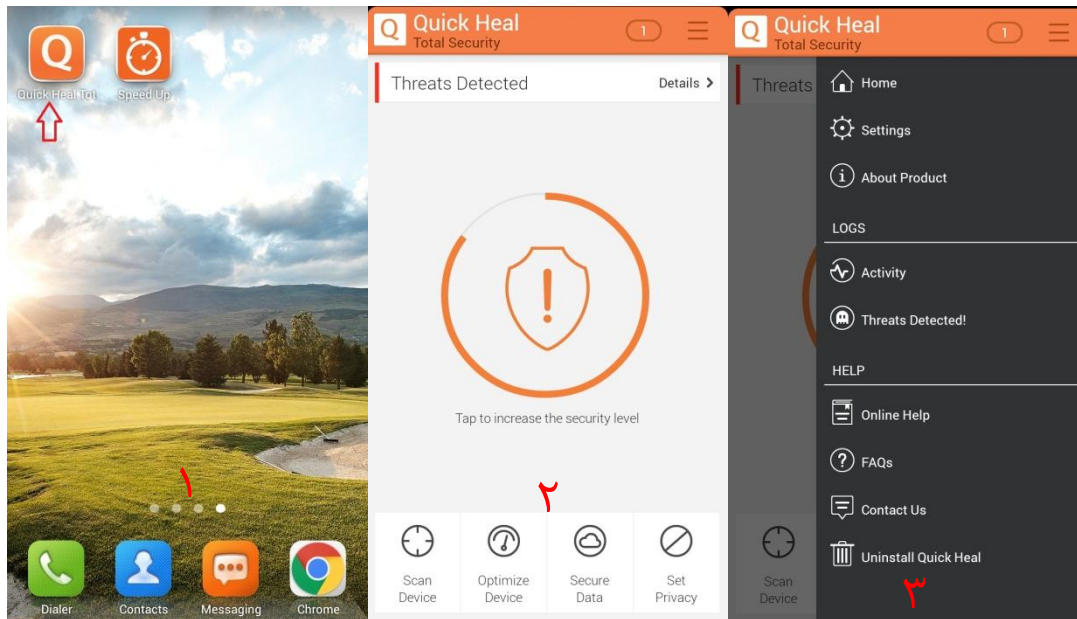
برای فعال کردن گزینه مدیریت از طریق وب (*Manage Through Web*) گام‌های زیر را دنبال نمایید:

۱. برنامه *Quick Heal Total Security* را اجرا کنید.
۲. بر روی آیکن منوی اصلی برنامه (آیکن  در بالا سمت راست) ضربه بزنید تا منوی اصلی باز شود. بر روی گزینه دوم یعنی *Settings* ضربه بزنید.
۳. بر روی *General* ضربه بزنید تا تنظیمات عمومی نمایش داده شود.



۴. گزینه *Manage Through Web* را تیک بزنید تا امکان مدیریت از راه دور دستگاه مهیا گردد.

داشبورد



هنگامی که کوپیک هیل توتال سکیوریتی را اجرا کنید، داشبورد اصلی آن بر روی صفحه نمایش موبایل شما نمایش داده می شود. داشبورد شامل موارد زیر است:

مرکز پیام

مرکز پیام حاوی اعلان ها و اخطارهای ضروری کوپیک هیل می باشد. اگر اخطار (notification) را برای یک ویژگی فعال کرده باشید، پیام ها و اخطارها در این بخش نمایش داده خواهد شد.

منوی اصلی

منوی اصلی یا سراسری در ناحیه اخطارها قرار دارد. با این منو شما می توانید انواع ویژگی ها برای امن سازی دستگاه و اطلاعات خود را تنظیم کنید.

شرایط داشبورد

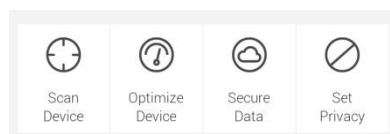
شرایط داشبورد، وضعیت رویدادهای مختلف مثلاً آیا اسکن پس زمینه فعال است یا خیر، لایسنس شما در حال انقضاست یا منقضی شده است و... را نمایش می دهد. پیام های شرایط داشبورد به شما یادآوری می کند که اقدامات لازم را انجام دهید تا از حوادث ناگوار که ناشی از رویدادهای زیر می باشد جلوگیری نمایید.

- هم اکنون ثبت نام کنید (Register Now!)
- لایسنس امروز منقضی می شود (License expires today!)
- دستگاه امن است (Device is secure!)

پوسته امنیتی

پوسته امنیتی بر اساس تدابیر امنیتی که شما بر روی دستگاه و اطلاعات خود تنظیم کرده‌اید، سطح امنیتی را با یک نمودار گرافیکی نمایش می‌دهد. شما می‌توانید در صورت نیاز امنیت دستگاه را افزایش دهید.

منوها



منوهای داشبورد شامل موارد زیر است:

اسکن دستگاه (Scan Device)

می‌توانید با استفاده از این ویژگی حافظه (memory) اصلی، کارت حافظه و برنامه‌های نصب شده را اسکن نمایید.

بهینه‌سازی دستگاه (Optimize Device)

می‌توانید کارایی دستگاه خود را بررسی و سرعت آنرا افزایش داده، و مصرف شبکه را کنترل و مدیریت نمایید.

امن‌سازی اطلاعات (Secure Data)

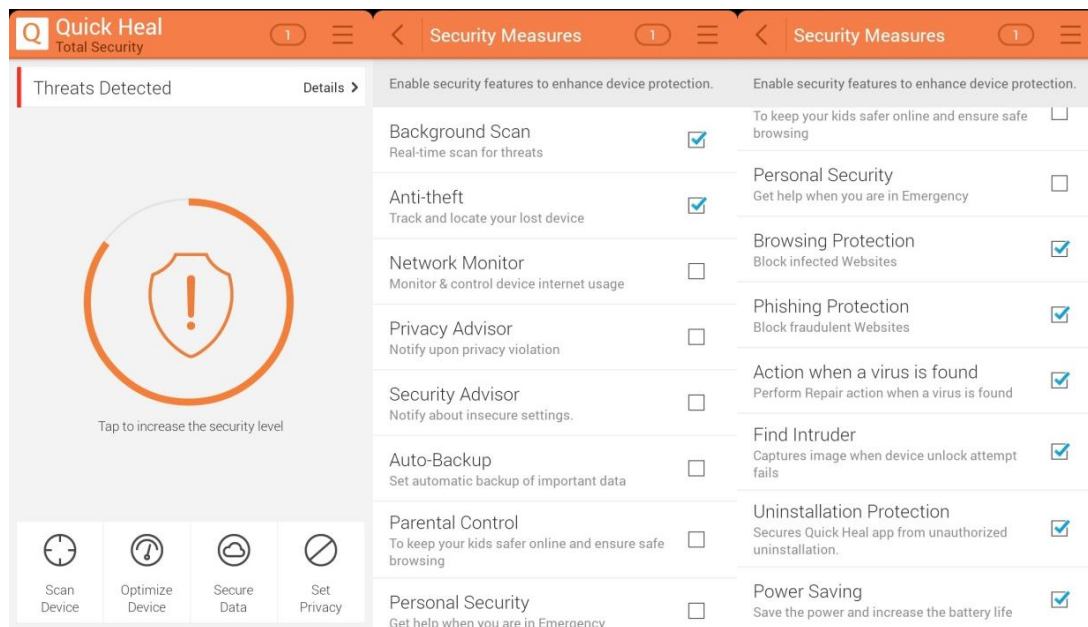
این ویژگی کمک می‌کند تا اطلاعات خود را امن سازید. شما می‌توانید از اطلاعات مهم خود بر روی بستر ابری و امن کوپیک‌هیل (پورتال اینترنتی خود) پشتیبان تهیه و در صورت نیاز آنرا بر روی گوشی بازگردانید.

تنظیم حفظ حریم خصوصی (Set Privacy)

می‌توانید تماس‌ها و پیامک‌ها از شماره‌های ناخواسته را مسدود کرده؛ برخی از مخاطبین خود را خصوصی کرده و تنها شما به تاریخچه تماس‌ها و پیامک‌های آنها دسترسی یافته؛ کنترل خانواده را برای اعمال محدودیت برای کودکان و دیگر کاربران تنظیم نمایید.

ویژگی‌ها

توتال سکیوریتی کوپیک هیل ویژگی‌های مختلف امنیتی ارائه می‌دهد تا دستگاه و اطلاعات شما امن گردند. منوی ویژگی‌ها شامل موارد زیر می‌باشد:



الف) پوسته امنیتی

پوسته امنیتی، سطح امنیتی را با یک نمودار گرافیکی نمایش می‌دهد. این نمودار منطبق بر تدابیر امنیتی است که شما بر روی دستگاه و داده‌های خود تنظیم کرده‌اید. در صورت نیاز می‌توانید سطح امنیتی دستگاه خود را افزایش دهید.

برای افزایش سطح امنیتی گام‌های دیسک را دنبال کنید:

۱. ضربه بر روی گراف دایره‌ای امنیتی داشبورد (صفحه اول) بزنید تا وارد تنظیمات تدابیر امنیتی (Security Measures) شوید.

۲. در صفحه Security Measures می‌توانید هر کدام از ویژگی‌های امنیتی را فعال نمایید تا امنیت دستگاه و اطلاعات شما افزایش یابد.

ویژگی‌های امنیتی شامل موارد زیر می‌باشد:

Background Scan (اسکن پس‌زمینه)

اگر بخواهید دستگاه به صورت مداوم اسکن گردد، این گزینه را فعال کنید. این ویژگی باعث می‌شود تا پیش از نصب هرگونه برنامه یا کپی یا دانلود یا ورود هر نوع فایل به موبایل، اسکن و ویروس‌یابی شوند. در نتیجه هرگونه تهدید پیش از ورود به دستگاه شناسایی و امنیت پیشگیرانه و بلادرنگ ارائه خواهد شد.

Anti-Theft (ضد-سرقت)

اگر می‌خواهید زمانی که دستگاه شما مفقود یا به سرقت رفت، آن را ردیابی و مکان‌یابی کنید، این ویژگی را فعال کنید. اگر این گزینه غیرفعال باشد، در صورت مفقود شدن موبایل، نمی‌توانید دستگاه خود را ردیابی کنید.

Action on Detected Virus (اقدام هنگام یافتن ویروس)

در صورتی که می‌خواهید هنگام شناسایی ویروس در دستگاه، اقدامی بر روی آن انجام شود این گزینه را فعال نمایید. نوع اقدام بر روی ویروس شناسایی شده بر اساس تنظیمی که شما انجام داده‌اید به صورت خودکار انجام می‌گیرد. اقدام‌ها شامل Repair (تعمیر)، Delete (حذف) و Skip (پرش از ویروس) می‌باشد.

Auto-Backup (اسکن پس‌زمینه)

برای پشتیبان‌گیری اطلاعات خود بر روی فضای ابری و امن کوپیک‌هیل این گزینه را فعال کنید. در هر زمان که نیاز شد، می‌توانید اطلاعات خود را بازیابی کنید. این ویژگی کمک می‌کند تا هنگام تعویض موبایل یا گم شدن گوشی قبلی، به اطلاعات خود دسترسی یابید.

Browsing Protection (محافظت مرور)

اگر می‌خواهید هنگامی که از روی دستگاه (موبایل / تبلت) به اینترنت متصل می‌شوید، وب‌سایت‌های آلوده مسدود گردند، این ویژگی را فعال کنید. این ویژگی دستگاه شما را در برابر انواع وب‌سایت‌های آلوده محافظت کرده و امنیت شما را در برابر انواع تهدیدات و بدافزارها تامین می‌کند.

Network Monitor (نظارت بر شبکه)

برای نظارت، مانیتورینگ و کنترل استفاده از اینترنت، این ویژگی را فعال نمایید. این گزینه به شما کمک می‌کند تا میزان مصرف پهنای باند خود را مدیریت نمایید.

Parental Control (کنترل خانواده)

در صورتی که می‌خواهید برخی از وب‌سایت‌ها بر اساس نوع محتویات آنها مسدود گردند، این ویژگی را فعال نمایید. شما می‌توانید بر اساس طبقه‌بندی وب‌سایت‌ها هر نوع از وب‌سایت‌ها مثلاً وب‌سایت‌های خبری، بازی، شبکه‌های اجتماعی یا هر نوع دیگر را مسدود یا مجاز نمایید. با استفاده از این ویژگی مطمئن می‌شوید که فرزندان یا دیگر کاربران دستگاه شما به سایت‌ها با محتویات ناخواسته دسترسی نیابند.

Personal Security (امنیت شخصی)

اگر این ویژگی فعال باشد، شما می‌توانید در زمان‌های اضطراری پیام درخواست کمک به همراه موقعیت مکانی به شماره‌های جایگزین (شماره والدین / دوست / اعضای خانواده که قبلاً معرفی کرده‌اید) ارسال کنید. مثلاً فرزند شما در شرایطی قرار دارد که امکان برقراری تماس تلفنی با شما را ندارد. با ۵ تا ۷ بار فشردن دکمه خاموش / روشن دستگاه، کوپیک هیل به صورت خودکار یک پیام درخواست کمک به همراه آدرس مکان جغرافیایی وی برای شما ارسال می‌کند. پیشنهاد می‌شود این ویژگی را فعال نگه دارید. در صورتی که غیرفعال باشد، شما نمی‌توانید پیام هشدار یا اختار را به شماره‌های جایگزین بفرستید.

Phishing Protection (محافظت فیشینگ)

اگر این ویژگی فعال باشد، وبسایت‌های کلاهبردارانه و جعلی که قصد سرقت اطلاعات ارزشمند مانند اطلاعات بانکی، رمزهای عبور، اطلاعات امنیتی اجتماعی و اطلاعات هویتی کاربران را دارند، مسدود می‌شوند.

Power Saving (صرفه‌جویی در انرژی)

اگر این ویژگی فعال باشد، در مصرف انرژی صرفه‌جویی شده و با اقداماتی که صورت می‌دهد دستگاه شما مدت زمان بیشتری می‌تواند از باتری استفاده نماید. شما می‌توانید همه برنامه‌های در حال اجرا را ببندید، مصرف شبکه را متوقف کنید، و روشنایی صفحه نمایش را کاهش دهید.

Privacy Adviser (مشاور حفظ حریم خصوصی)

اگر این ویژگی فعال باشد، در صورت هرگونه نقض حریم خصوصی، به شما اطلاع‌رسانی خواهد شد. هنگامی که می‌خواهید یک برنامه را بر روی دستگاه خود نصب کنید، ممکن است برخی از آنها از اطلاعات کاربری استفاده کنند که شاید شما تمایل نداشته باشید. پیش از نصب هر برنامه، دسترسی‌های برنامه به بخش‌های مختلف دستگاه نمایش داده خواهد شد.

Security Adviser (مشاور امنیتی)

اگر تنظیمات امنیتی دستگاه شما پایین می‌باشد، این ویژگی را فعال کنید تا اعلان امنیتی دریافت نمایید. این ویژگی امنیت دستگاه شما را ارتقا می‌دهد.

Uninstallation Protection (محافظت در برابر حذف)

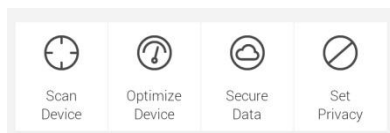
اگر این ویژگی فعال باشد، افراد غیرمجاز نمی‌توانند برنامه کوپیک هیل را از روی دستگاه حذف نمایند. هرگاه دستگاه به سرقت رود یا گم شود، ممکن است بخواهید با آن ارتباط برقرار کنید (از طریق SMS یا پورتال اینترنتی)

تا دستگاه خود را ردیابی کنید یا اقدامات دیگری (مثلاً حذف اطلاعات مهم یا قفل کردن گوشی) انجام دهید. برای ارتباط موفق، مهم است که کوپیک هیل بر روی دستگاه فعال باشد.

Find Intruder (شناسایی نفوذ غیر مجاز)

اگر این ویژگی فعال باشد، در صورتی که فردی دو بار پسورد (الگوی) ورودی گوشی موبایل را اشتباه وارد نماید، از فرد مزاحم (شخص نفوذ کننده) عکس می گیرد و بعداً کاربر می تواند تصویر آن فرد مزاحم را مشاهده نماید.

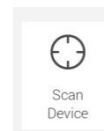
ب) منوهای داشبورد



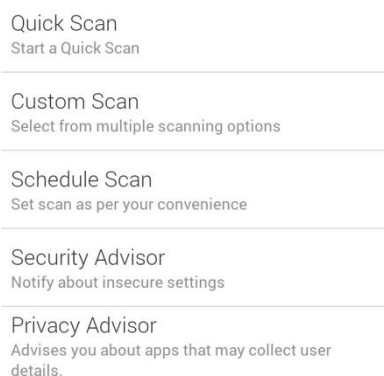
منوهای اصلی داشبورد شامل موارد زیر است:

Scan Device (اسکن دستگاه)

با اسکن دستگاه، می توانید دستگاه خود را اسکن و ویروسیابی کرده و تدابیر امنیتی لازم را در برابر انواع آسیب پذیری ها و حفره ها و نقض حریم خصوصی تنظیم نمایید. با اسکن دستگاه مطمئن می شوید که آیا دستگاه شما امن است یا خیر. همچنین می توانید اقدامات مناسبی برای بهبود امنیت دستگاه خود انجام دهید.

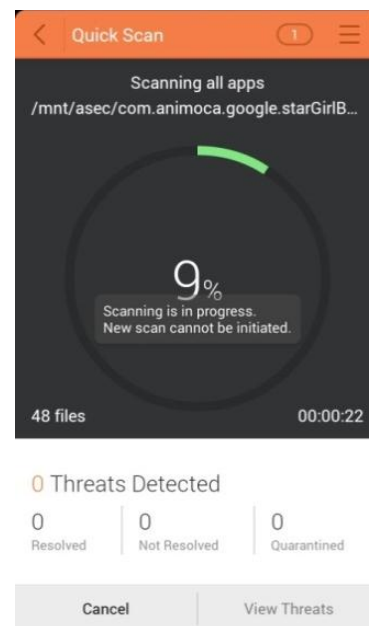


برای اسکن بر روی دکمه **Scan Device** داشبورد کلیک کنید تا منوی زیر ظاهر شود:



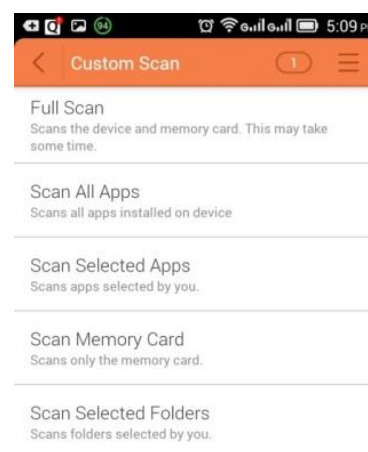
Quick Scan (اسکن سریع)

یک اسکن سریع که همه برنامه‌های نصب شده بر روی دستگاه را اسکن می‌کند.



Custom Scan (اسکن سفارشی)

با انتخاب این گزینه، گزینه‌های مختلف اسکن نمایش داده خواهد شد که می‌توانید یکی از آنها را انتخاب، سفارشی و بر اساس نیاز خود اسکن کنید. این گزینه‌ها شامل:



Full Scan (اسکن کامل)

گزینه Full Scan، یک اسکن کامل می‌باشد که کل دستگاه و کارت حافظه جانبی آن را اسکن می‌کند. هرچند ممکن است این گزینه زمان بیشتری برای اجرا نیاز داشته باشد.

Scan All Apps (اسکن همه برنامه‌ها)

همه‌ی برنامه‌های نصب شده بر روی دستگاه را اسکن می‌کند.

Scan Selected Apps (اسکن برنامه‌های انتخابی)

از میان تمامی برنامه‌های نصب شده بر روی گوشی، تنها برنامه‌های انتخاب شده توسط کاربر را اسکن می‌کند. هنگامی که این گزینه را انتخاب می‌کنید، همه برنامه‌ها در پنجره لیست برنامه‌های انتخابی (Select Apps list) نمایش داده می‌شود. با ضربه بر روی برنامه‌های موردنظر، آنها را تیک کرده سپس بر روی Scan کلیک کنید.

Scan Memory Card (اسکن کارت حافظه)

تنها حافظه جانبی را اسکن می‌کند.

Scan Selected Folders (اسکن پوشه‌های انتخابی)

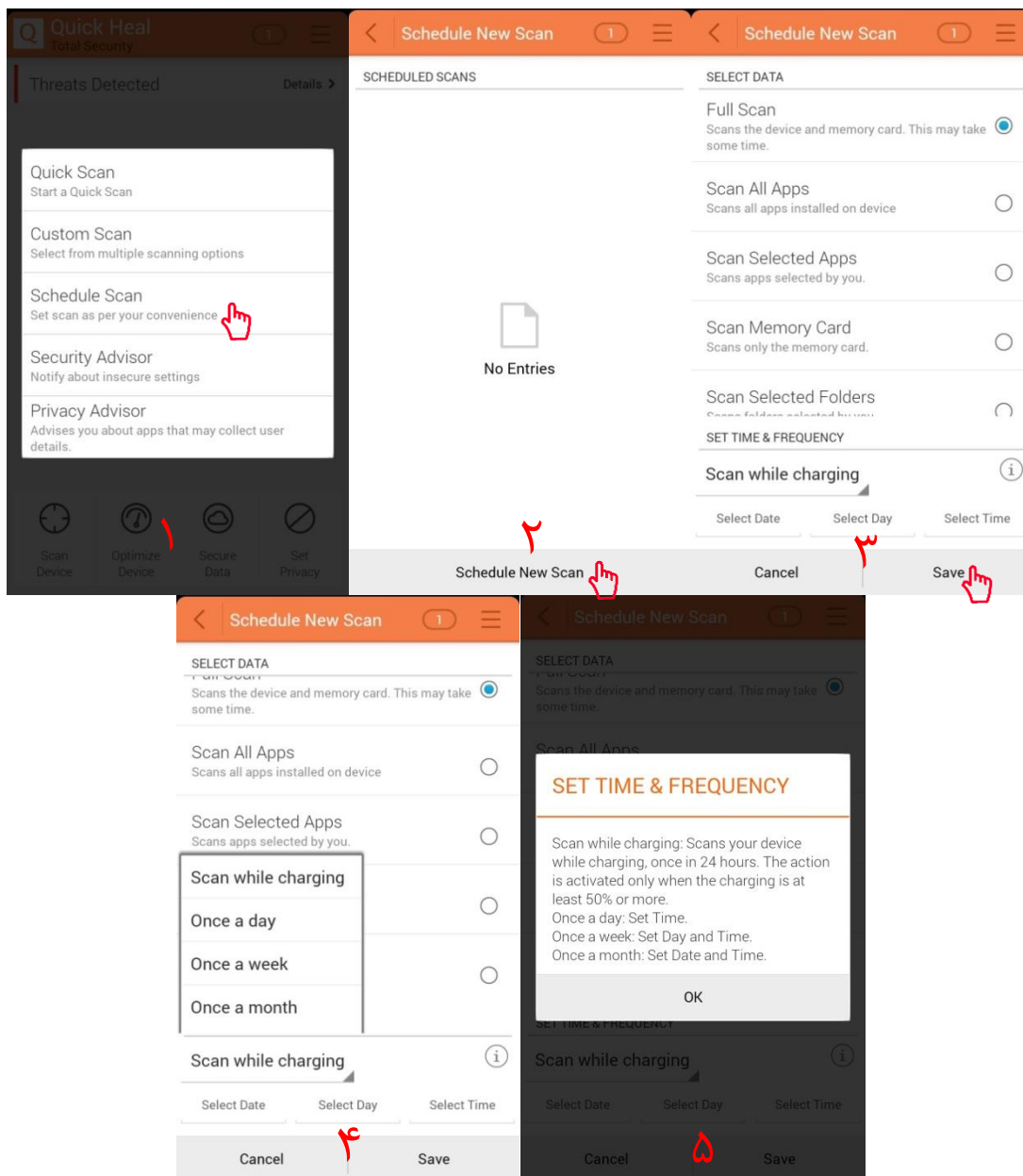
با استفاده از این گزینه می‌توانید تنها پوشه‌های موردنظر را اسکن کنید. پس از انتخاب این گزینه، همه پوشه‌ها در پنجره‌ی لیست پوشه‌های انتخابی (Select Folders list) نمایش داده می‌شوند. پوشه‌های موردنظر خود را با ضربه بر روی نام آنها انتخاب و سپس بر روی **Scan** ضربه بزنید.

Schedule Scan (زمانبندی اسکن)

زمانبندی اسکن به شما کمک می‌کند تا در زمان‌ها و با تکرارهای خاص به صورت خودکار گوشی را اسکن کنید. با استفاده از این ویژگی می‌توانید دستگاه خود را در زمان‌های از پیش تعیین شده به صورت خودکار اسکن کنید.

برای ایجاد یک زمانبندی اسکن گام‌های زیر را دنبال کنید:

۱. گزینه **Scan Device** داشبورد را انتخاب کنید.
۲. گزینه **Schedule Scan** را ضربه بزنید.
- اگر شما از قبل طرح زمانبندی اسکن ایجاد کرده باشید، صفحه برنامه‌ریزی اسکن (Scheduled Scans)، آنها را نمایش می‌دهد.
۳. برای ایجاد یک زمانبندی اسکن بر روی **Schedule New Scan** ضربه بزنید.
۴. در زیر **Select Data**، یکی از گزینه‌های اسکن شامل: **Full Scan** (اسکن کامل)، **Scan All Apps** (اسکن همه برنامه‌ها)، **Scan Selected Apps** (اسکن برنامه‌های انتخابی)، **Scan Memory Card** (اسکن کارت حافظه)، **Scan Selected Folders** (اسکن پوشه‌های انتخابی) را انتخاب کنید.
۵. در زیر بخش **Set Time & Frequency**، زمان و تکرار آغاز اسکن خودکار را تعیین کنید.
- زمان و تکرار شامل موارد مقابل می‌باشد: **Scan while charging** (اسکن در زمان داشتن شارژ)، **Once a day** (یکبار در روز)، **Once a week** (یکبار در هفته)، و **Once a month** (یکبار در ماه).



توجه ۱: اگر گزینه Scan while charging انتخاب شود، دستگاه هر ۲۴ ساعت یکبار، زمانی که باتری حداقل ۵۰٪ یا بیشتر شارژ دارد، انجام می‌گیرد.

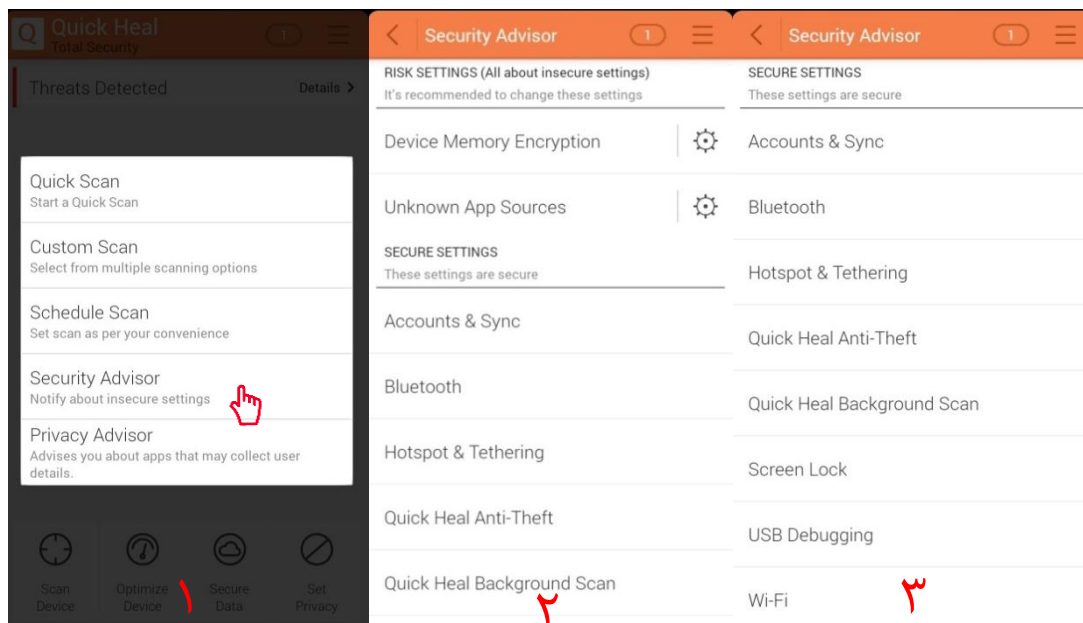
توجه ۲: اگر گزینه Once a day انتخاب شود، زمان (ساعت:دقیقه) باید تعیین گردد.

توجه ۳: اگر گزینه Once a week انتخاب شود، روز هفته و زمان باید تعیین گردد.

توجه ۴: اگر گزینه Once a month انتخاب شود، تاریخ و زمان باید تعیین گردد.

Security Adviser (مشاور امنیتی)

با این ویژگی می‌توانید آسیب‌پذیری‌ها و حفره‌های امنیتی موجود در دستگاه خود را بررسی نمایید. شما می‌توانید تنظیمات امنیتی گوشی خود را ارتقا دهید تا تلاش‌ها برای سوء استفاده از نقاط آسیب‌پذیری گوشی خود را متوقف سازید.



برای پیکربندی مشاور امنیتی (Security Advisor) گام‌های زیر را دنبال کنید:

۱. گزینه Scan Device داشبورد را انتخاب کنید.

۲. گزینه Security Adviser را بزنید.

۳. در صفحه Security Adviser، تنظیمات امنیتی در طبقه‌بندی‌های زیر نمایش داده می‌شوند:

- Risk Settings: تنظیمات امنیتی که ناامن می‌باشند در این بخش لیست می‌شوند.

- Secure Settings: تنظیمات امنیتی که امن و مطمئن هستند، در این بخش لیست می‌شوند.

تنظیمات امنیتی که در زیر Risk Settings لیست شده‌اند، شامل یک آیکن تنظیمات (Setting) می‌باشند که بعد از آنها قرار گرفته‌اند. با کلیک بر روی آیکن تنظیمات، می‌توانید سطح امنیتی آنها را افزایش دهید. پس از ضربه بر روی آیکن تنظیمات، شما به صفحه تنظیمات مربوطه هدایت می‌شوید و می‌توانید آن‌را پیکربندی نمایید.

تنظیمات امنیتی شامل موارد زیر می‌باشد:

Accounts and Sync (حساب‌ها و همگام‌سازی)

دستگاه از حساب‌ها یا سایت‌های همگام‌سازی شده اطلاعات دریافت کرده و در نتیجه خطر هک شدن و سوءاستفاده از حساب‌های کاربری را افزایش می‌دهد. پیشنهاد می‌شود زمانی که به این گزینه اندروید نیاز ندارید، این گزینه خاموش (OFF) باشد.

Bluetooth (بلوتوث)

ممکن است نقل و انتقال داده‌ها از طریق بلوتوث، دستگاه و اطلاعات شما را به خطر بیندازد. پیشنهاد می‌شود زمانی که بلوتوث نیاز ندارید، آن‌را خاموش (OFF) کنید.

Device Memory Encryption (رمزنگاری حافظه دستگاه)

با استفاده از این گزینه می‌توانید اطلاعات موجود در دستگاه خود را رمزنگاری نمایید. این قابلیت امنیتی به شما اطمینان می‌دهد که اطلاعات شما از دسترس افراد غیرمجاز دور می‌ماند.

توجه: گزینه تنظیمات Device Memory Encryption تنها در سیستم‌عامل‌هایی که از این ویژگی پشتیبانی می‌کنند، در دسترس می‌باشد.

Hotspot & Tethering (اشتراک اینترنت از طریق هات‌اسپات و تدرینگ)

اشتراک اینترنت موبایل از طریق هات‌اسپات وای‌فای (Wi-Fi Hotspot)، تدرینگ کابل USB، و بلوتوث به رایانه یا دیگر ابزارهای موبایل، خطر هک شدن را افزایش می‌دهد. برای جلوگیری از هک اطلاعات، زمانی که به اشتراک‌گذاری اینترنت موبایل خود نیاز ندارید، این گزینه را خاموش (OFF) کنید.

توجه: تنظیمات Hotspot و Tethering تنها در سیستم‌عامل‌ها و شرکت‌های تولیدکننده موبایل / تبلت پشتیبانی کننده، در دسترس می‌باشد.

Quick Heal Anti-Theft (ضد-سرقت کوپیک‌هیل)

از دستگاه و اطلاعات شما محافظت می‌کند. با استفاده از این ویژگی شما می‌توانید، زمانی که گوشی‌تان به سرقت رفت، آن را ردیابی و مسدود کنید، اطلاعات شخصی خودتان را از راه دور حذف کنید، از گوشی مسروقه با شماره دلخواه خود تماس برقرار کنید، به صورت مخفیانه بر روی گوشی مسروقه تماس دریافت کنید، از راه دور از اطراف گوشی خود عکس بگیرید، صدا و یا فیلم ضبط کنید.

Quick Heal Background Scan (اسکن پس‌زمینه کوپیک‌هیل)

از دستگاه شما در برابر انواع تهدیدات محافظت پیشگیرانه می‌کند. این ویژگی پیش از نصب هر نوع برنامه یا کپی اطلاعات به داخل دستگاه آنها را اسکن می‌نماید. این گزینه را فعال نگه دارید.

Screen Lock (قفل کردن صفحه نمایش)

اگر این گزینه خاموش باشد، ممکن است اطلاعات شخصی شما مورد سوء استفاده قرار گیرد. مطمئن شوید که یکی از گزینه‌های قفل صفحه نمایش فعال بوده تا از اطلاعات دستگاه شما حراست شود.

Unknown App Source (قفل کردن صفحه نمایش)

اگر برنامه‌ای از طریق هر یک از منابع، به غیر Google Play نصب شود، ممکن است امنیت دستگاه شما مورد تهدید قرار گیرد. بنابراین توصیه می‌شود گزینه امکان نصب از منابع نرم‌افزاری ناشناخته را خاموش (OFF) کنید.

USB Debugging (قفل کردن صفحه نمایش)

اگر این گزینه روشن باشد، دستگاه شما در خطر هک قرار گرفته و اطلاعات شما می‌تواند مورد سوء استفاده قرار گیرد. برای امنیت بیشتر این گزینه را خاموش (OFF) کنید.

Wi-Fi (بی سیم وای فای)

ارتباطات از طریق شبکه‌های باز (Open) یا نا امن Wi-Fi می‌تواند اطلاعات شما را در معرض خطر قرار دهد. توصیه می‌شود تنها به شبکه‌های امن Wi-Fi متصل شوید.

Privacy Adviser (مشاور حفظ حریم خصوصی)

با این گزینه شما می‌توانید برنامه‌هایی که اطلاعات شخصی شما مانند اطلاعات حساب کاربری، لیست مخاطبین، شماره‌های اجتماعی (مثل شماره ملی)، رمز عبور و... را جمع آوری می‌کنند، شناسایی کنید. همچنین اگر برنامه‌هایی بخواهند SMS ارسال کنند، تماس با شماره‌های ویژه بگیرند (تا با تماس مبلغی به آن شماره واریز شود)، یا بدون اطلاع شما به اینترنت دسترسی یابند، مطلع می‌گردید. همچنین می‌توانید برنامه با دسترسی‌های مختلف مانند دسترسی به حساب کاربری، دسترسی به مخاطبین، خواندن اطلاعات هویتی، مکان‌یابی، دسترسی به پیام‌ها، و دسترسی به شبکه را مانیتور و نظارت کنید.

برای تنظیم مشاور حریم خصوصی گام‌های زیر را دنبال کنید:

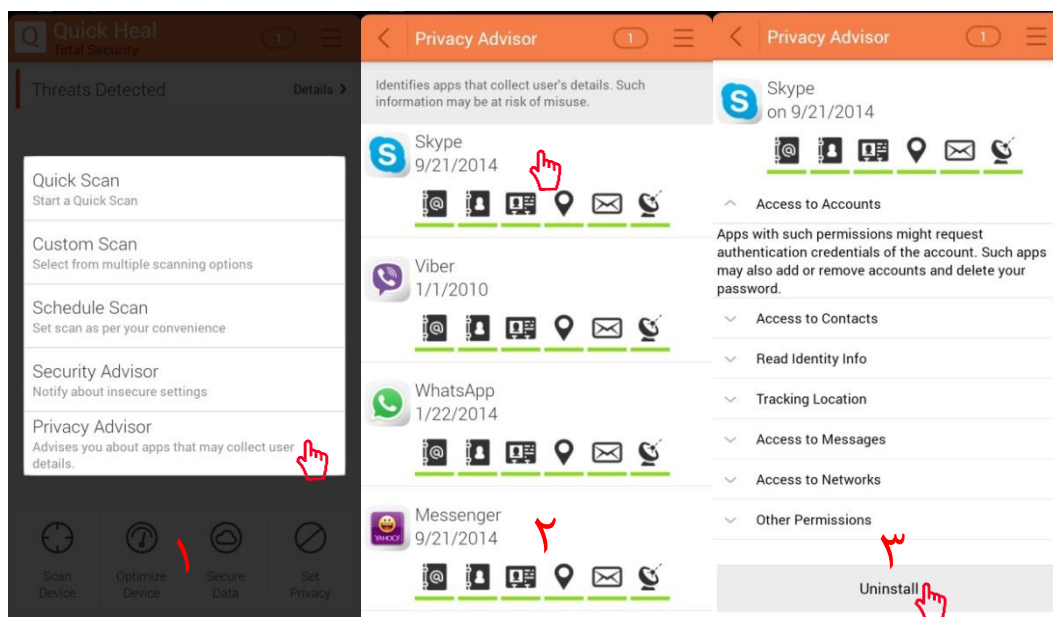
۱. بر روی داشبورد نرم‌افزار بر روی منوی *Scan Device* ضربه بزنید.

۲. بر روی منوی *Privacy Adviser* ضربه بزنید.

برنامه‌ها با اجازه‌های دسترسی که به آنها اختصاص داده شده، نمایش داده می‌شوند.

برای مشاهده اجازه‌های دسترسی اختصاص یافته به یک برنامه، بر روی نام برنامه ضربه بزنید. اگر متوجه شدید

که یک برنامه از اطلاعات مهم و حیاتی شما استفاده می‌کند، می‌توانید با ضربه بر روی دکمه *Uninstall*، آنرا حذف کنید.



انواع اجازه‌های دسترسی که یک برنامه ممکن است استفاده کند شامل موارد زیر است:

Access to Accounts (دسترسی به حساب کاربری)

برنامه‌ها با این اجازه‌ی دسترسی ممکن است با استفاده از حساب کاربری شما درخواست احراز هویت کرده و از آن استفاده کنند. چنین برنامه‌هایی ممکن است حساب‌های کاربری شما را حذف یا یک حساب کاربری به دستگاه شما بیفزایند و یا رمز عبور شما را حذف کنند.

Access to Contacts (دسترسی به مخاطبین)

برنامه‌ها با این اجازه‌ی دسترسی، می‌توانند لیست مخاطبین خصوصی (دفترچه تلفن) شما را بخوانند، مخاطب جدید درج نمایند و یا با ارسال لیست مخاطبین شما به سرورهای خود، آنها را به خطر بیندازند.

Read Identity Info (خواندن اطلاعات هویتی)

برنامه‌ها با این اجازه‌ی دسترسی، می‌توانند وضعیت گوشی شما مانند شماره IMEI گوشی، شماره تلفن و شماره سریال گوشی را بدون رضایت شما به سرورهای خود ارسال نمایند.

Tracking Location (ردیابی مکان)

برنامه‌ها با این اجازه‌ی دسترسی، می‌توانند مکان دستگاه شما را در سرورهای خود همواره به روز کرده و موقعیت جغرافیایی شما را دنبال نمایند که می‌تواند خطرآفرین باشد.

Access to Messages (دسترسی به پیام‌ها)

برنامه‌ها با این اجازه‌ی دسترسی، مجازند تا پیامک‌های گوشی شما را خوانده، یا یک پیامک جدید بنویسند و یا پیامک ارسال نمایند. برنامه‌های مخرب ممکن است پیام‌های محرمانه شما را خوانده یا پیش از آنکه به دست شما برسند، آنها را حذف نمایند.

Access to Network (دسترسی به شبکه)

برنامه‌ها با این اجازه‌ی دسترسی، مجازند تا از شبکه شما در پس‌زمینه استفاده نمایند.

Other Permissions (دسترسی‌های دیگر)

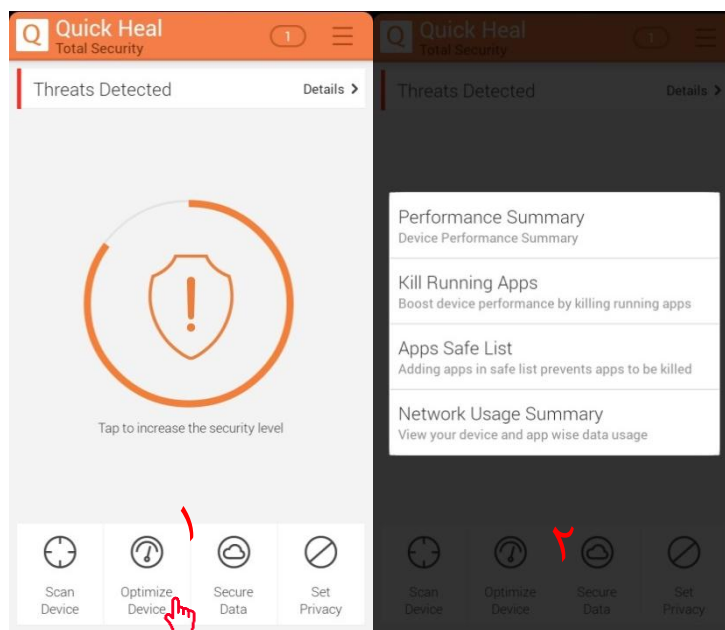
برنامه‌هایی که مجوزهای دسترسی در اختیار دارند که در لیست فوق قرار ندارد، در این بخش ذکر می‌شوند.

Privacy Audit Notification (اعلان ممیزی حفظ حریم خصوصی)

زمانی که شما برنامه جدیدی بر روی دستگاه نصب می‌کنید، یک اعلان ممیزی حفظ حریم خصوصی در بخش هشدارهای (notification) آنتی‌ویروس کوپیک‌هیل توتال سکیوریتی برای مدت ۱۵ روز نمایش داده می‌شود. شما می‌توانید بررسی کنید که برنامه‌ها از چه اجازه‌های دسترسی استفاده می‌کنند. هر زمان که متوجه شدید یک برنامه، حریم خصوصی شما را نقض می‌کند یا اطلاعات شخصی شما در معرض خطر قرار دارند، می‌توانید آن برنامه را فوراً حذف کنید.

Optimize Device (بهبودسازی دستگاه)

گزینه «بهبودسازی دستگاه» کارایی دستگاه شما را بررسی کرده، کارآمدی آن را با انجام تدابیر امنیتی موردنیاز افزایش داده، سرعت دستگاه را با توقف اجرای برنامه‌های زائد افزایش داده و گزارشی از میزان مصرف شبکه را ارائه می‌دهد. Optimize Device شامل گزینه‌های زیر است:



Performance Summary (گزارش عملکرد)

با این گزینه، وضعیت فعلی کارایی دستگاه خود را مشاهده کنید. این گزینه شامل تعداد برنامه‌های درحال اجرا، میزان استفاده پردازنده CPU، سطح باتری و میزان استفاده از حافظه می‌باشد.

براساس کارایی دستگاه، یک نمودار نمایانگر سطح کارایی پایین (Low)، متوسط (Medium)، و بالا (High) نمایش داده می‌شود. اگر سرعت دستگاه شما پایین است، می‌توانید با توقف اجرای برنامه‌ها با استفاده از گزینه‌های زیر، سرعت آن را افزایش دهید:

Speed Up Device (افزایش سرعت دستگاه)

با استفاده از این گزینه می‌توانید همه برنامه‌های در حال اجرا را بسته و کارایی دستگاه را افزایش دهید.

View Running Apps (نمایش برنامه‌های در حال اجرا)

این گزینه به شما کمک می‌کند تا همه برنامه‌های در حال اجرا را مشاهده کرده و با انتخاب هر کدام از آنها، اجرای آنها را متوقف سازید. همچنین می‌توانید جزئیات همه برنامه‌های در حال اجرا را مشاهده، آنها را بر اساس میزان مصرف حافظه، مصرف CPU، و مصرف RAM و یا نام مرتب سازید. همچنین می‌توانید برنامه‌های دلخواه را به لیست برنامه‌های مطمئن (Safe List) بیفزایید.

در صفحه Performance Summary (خلاصه کارایی)، هنگامی که بر روی View Running Apps کلیک کنید، صفحه Running Apps (برنامه‌های در حال اجرا) ظاهر می‌شود. برای بستن یک برنامه، آن برنامه (ها) را انتخاب و بر روی Kill App ضربه بزنید. همچنین می‌توانید بعضی از برنامه‌ها را به Safe List (لیست مطمئن) بیفزایید تا در زمان Speed Up کردن دستگاه (با کلیک بر روی آیکن آن در صفحه اصلی موبایل) آن برنامه‌ها از حالت اجرا خارج نشوند.



Kill Running Apps (بستن برنامه‌های در حال اجرا)

با استفاده از این ویژگی می‌توانید سرعت دستگاه خود را افزایش دهید. ممکن است چندین برنامه بر روی دستگاه خود اجرا کنید، یا گاهی اوقات برخی برنامه‌های متفرقه به صورت خودکار اجرا می‌شوند، این برنامه‌ها حافظه اشغال کرده و سرعت دستگاه را کاهش می‌دهند. شما می‌توانید با از بین بردن آنها، کارایی و سرعت دستگاه خود را بهبود بخشید.

برای توقف اجرای یک برنامه، کافی است از لیست برنامه‌های در حال اجرا با تیک کردن مربع کنار نام برنامه، یک یا چند برنامه را انتخاب و بر روی **Kill App** ضربه بزنید.

برای افزودن یک برنامه به لیست مطمئن (Safe List)، کافی است از لیست برنامه‌های در حال اجرا، با تیک کردن مربع کنار نام برنامه، یک یا چند برنامه را انتخاب و بر روی **Add to Safe List** ضربه بزنید. اگر می‌خواهید یک برنامه را از «لیست برنامه‌های مطمئن» خارج کنید، از مسیر **Apps Safe List < Optimize Device** اقدام کنید.

Apps Safe List (لیست برنامه‌های مطمئن)

با استفاده از **Apps Safe List** می‌توانید برنامه‌ی نصب شده بر روی دستگاه خود را به لیست مطمئن بیفزایید. اگر برنامه‌ای را به لیست مطمئن بیفزایید، در هنگام اجرای ویژگی **Kill Running Apps**، اجرای این برنامه متوقف نخواهد شد. هرچند تنها برای برنامه‌های موردنیاز از این ویژگی استفاده کنید.

برای افزودن برنامه به لیست مطمئن گام‌های زیر را دنبال نمایید:

۱. برنامه **Quick Heal Total Security** را اجرا کنید.

۲. در داشبورد، بر روی منوی **Optimize Device** ضربه بزنید.

۳. بر روی **Apps Safe List** ضربه بزنید.

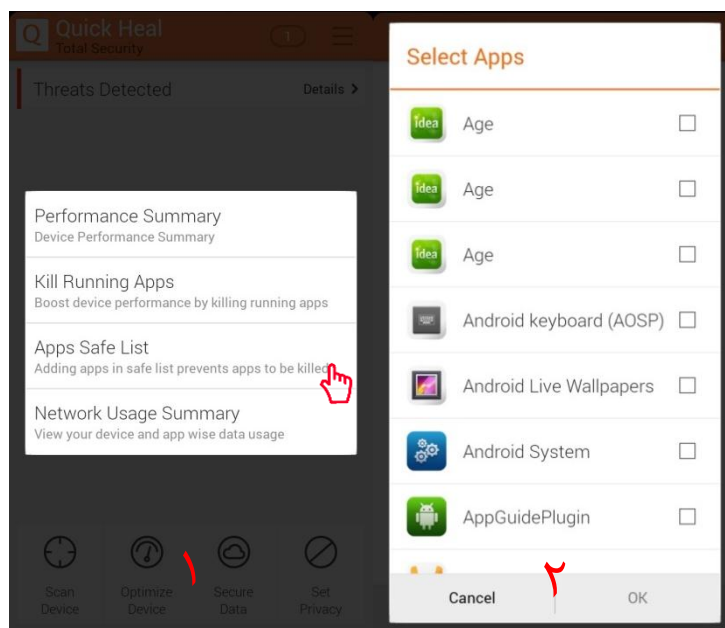
صفحه **App Safe List** (لیست برنامه‌های مطمئن)، برنامه‌هایی که از قبل به لیست مطمئن افزودید را نمایش می‌دهد.

۴. برای افزودن یک برنامه بر روی دکمه **Add apps to safe list** ضربه بزنید.

همه برنامه‌های نصب شده دستگاه شما در زیر **Select Apps** لیست می‌شوند.

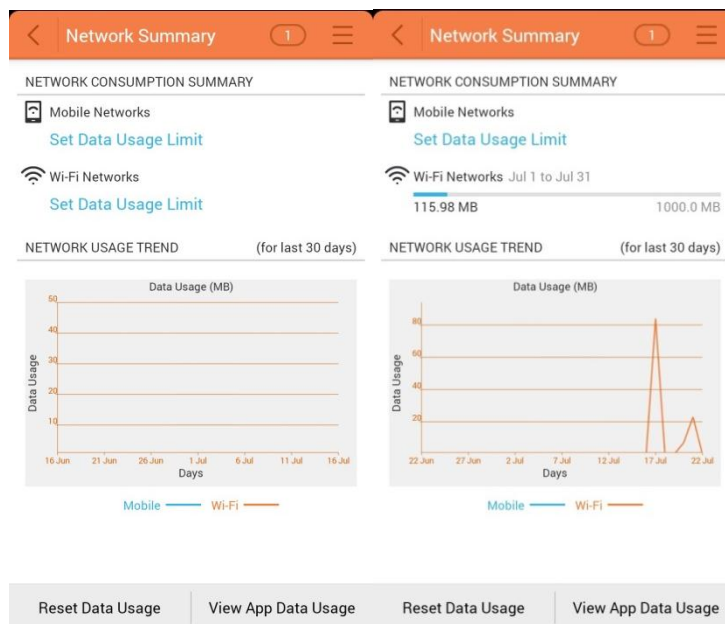
۵. هر برنامه‌ای که می‌خواهید آنرا به لیست برنامه‌های مطمئن بیفزایید، گزینه سمت راست نام برنامه را تیک کرده سپس بر روی **OK** ضربه بزنید.

اگر می‌خواهید برنامه‌ای در زمان افزایش سرعت دستگاه، بسته شود، می‌توانید آنرا انتخاب و بر روی دکمه **X** کلیک کنید تا آن برنامه از لیست مطمئن خارج شود.



Network Usage Summary (خلاصه استفاده از شبکه)

با این گزینه، شما می‌توانید اطلاعات کلی تنظیمات شبکه را به صورت گرافیکی مشاهده نمایید. صفحه Network Summary اطلاعات جاری میزان مصرف شبکه و تنظیمات آن را نشان می‌دهد. اگر اولین بار به این صفحه وارد می‌شوید، لینک Set Data Usage برای پیکربندی محدودیت میزان مصرف داده نشان داده می‌شود. پس از تعیین محدودیت داده، این لینک نمایش داده نخواهد شد.



Set Data Usage Limit (تعیین محدودیت میزان مصرف داده)

با استفاده از این ویژگی شما می‌توانید برای استفاده از داده خود محدودیت استفاده قرار دهید. به عنوان مثال شما یک طرح تشویقی به میزان ۲ گیگابایت خریداری کرده‌اید. ممکن است در صورت اتمام حجم ۲ گیگ، به صورت خودکار با هزینه‌ای بالا از شارژ موبایل شما مصرف شود (یا بر روی قبض موبایل اعمال شود).

برای تغییر محدودیت میزان استفاده داده بر روی **link Set Data Usage Limit** ضربه بزنید. بر روی هر یک از انواع شبکه که می‌خواهید بر روی آن محدودیت قائل شوید ضربه بزنید: **Mobile Network** (شبکه موبایل) یا شبکه‌های **WiFi**. (مثلاً شبکه‌های **Mobile**).

بر اساس انتخاب نوع شبکه، صفحه **Mobile Network Monitor** یا **Wi-Fi Network Monitor** نمایش داده می‌شود.

فرایند برای هر دو نوع شبکه یکسان است.

گزینه‌ها را براساس نیاز خودتان پیکربندی کنید:

Billing Date: تاریخ شروع طرح (یا صورتحساب) را وارد نمایید تا از آن تاریخ به مدت یک‌ماه مانیتورینگ و کنترل صورت پذیرد. (مثلاً اگر طرح از امروز سوم مرداد شروع شده، تاریخ روز را ۳ قرار می‌دهید)

Set data usage limit: برای فعال شدن بقیه گزینه‌ها و اعمال محدودیت حجم مصرفی این گزینه را تیک کنید.

Max data usage limit: یک میزان محدودیت حداکثری برای کنترل میزان مصرف قرار دهید. (مثلاً ۲۰۰۰ مگابایت)

Notify if data usage reaches: می‌توانید یک میزانی از مصرف را تعیین نمایید تا هنگام رسید مصرف داده به آن حجم، یک پیام هشدار به شما نمایش داده شود. (مثلاً ۱۸۰۰ مگابایت)

Disconnect after max limit is reached: اگر این گزینه فعال باشد، به محض اینکه میزان مصرف داده‌ی شما به حداکثر تعیین شده (مثلاً ۲۰۰۰ مگابایت) برسد، شبکه داده به صورت خودکار قطع خواهد شد.

Already used data from max limit: اگر قبل از تنظیم این ویژگی، شما از شبکه خود مقداری استفاده کرده‌اید (مثلاً ۲۰۰ مگابایت)، آن مقدار را در این بخش وارد نمایید تا در محاسبات لحاظ گردد.

Reset Data Usage (بازنشانی مصرف داده)

با استفاده از این گزینه می‌توانید خلاصه اطلاعات مصرف داده را پاکسازی کرده و ثبت مصرف را مجدداً از صفر آغاز کنید.

View App Data Usage (نمایش مصرف داده‌ی برنامه)

با استفاده از این گزینه می‌توانید میزان مصرف داده‌ی هر برنامه را به صورت جداگانه مشاهده نمایید. همچنین می‌توانید با ضربه بر روی نام برنامه خاص، جزئیات بیشتری از مصرف داده توسط یک برنامه دریافت نمایید. این قابلیت به شما کمک می‌کند تا متوجه شوید که چه برنامه‌ای مصرف غیرضروری داده دارد و موجب اتلاف حجم اینترنت شما می‌شود. برای کنترل چنین برنامه‌هایی، می‌توانید اقدامات مناسب زیر را انجام دهید:

Add to Safe List: می‌توانید یک برنامه را به لیست برنامه‌های مطمئن بیفزایید تا اجرای آن متوقف نشود.

Uninstall: اگر فکر می‌کنید برنامه، استفاده غیرضروری از داده و اینترنت دارد، می‌توانید آن را حذف نمایید.

Kill App: با این دکمه می‌توانید اجرای برنامه را متوقف سازید.

Secure Data (امن سازی داده)

با استفاده از این گزینه شما می‌توانید با ذخیره اطلاعات خود در فضای ابری و امن کوپیک هیل آنها را امن سازید. در صورت نیاز می‌توانید اطلاعات خود را از فضای ابری بر روی گوشی برگردانید و یا آن را حذف نمایید.

برای استفاده از ویژگی امن سازی داده گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. در داشبورد، بر روی منوی *Secure Data* ضربه بزنید.

Backup data to Cloud

با استفاده از این ویژگی می‌توانید اطلاعات با ارزش خود مانند لیست مخاطبین (Contacts)، تقویم رویدادها (Calendar Events)، پیام‌ها (SMS/ Messages)، و حتی در صورت تمایل تصاویر و موسیقی را بر روی فضای ابری و امن کوپیک هیل ذخیره سازید. در این صورت اطلاعات شما در جایی امن نگهداری خواهد شد و هر زمان که به آن نیاز داشته باشید (مثلاً تعویض یا خراب شدن یا گم شدن گوشی یا برگرداندن گوشی به حالت کارخانه (factory reset)، حذف ناخواسته (به اشتباه یا توسط بدافزارها) اطلاعات از روی گوشی) می‌توانید آن را به گوشی بازگردانید.

برای گرفتن پشتیبان اطلاعات بر روی فضای ابری کوپیک هیل گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. در داشبورد، بر روی منوی *Secure Data* ضربه بزنید.

۳. بر روی گزینه *Backup data to cloud* ضربه بزنید.

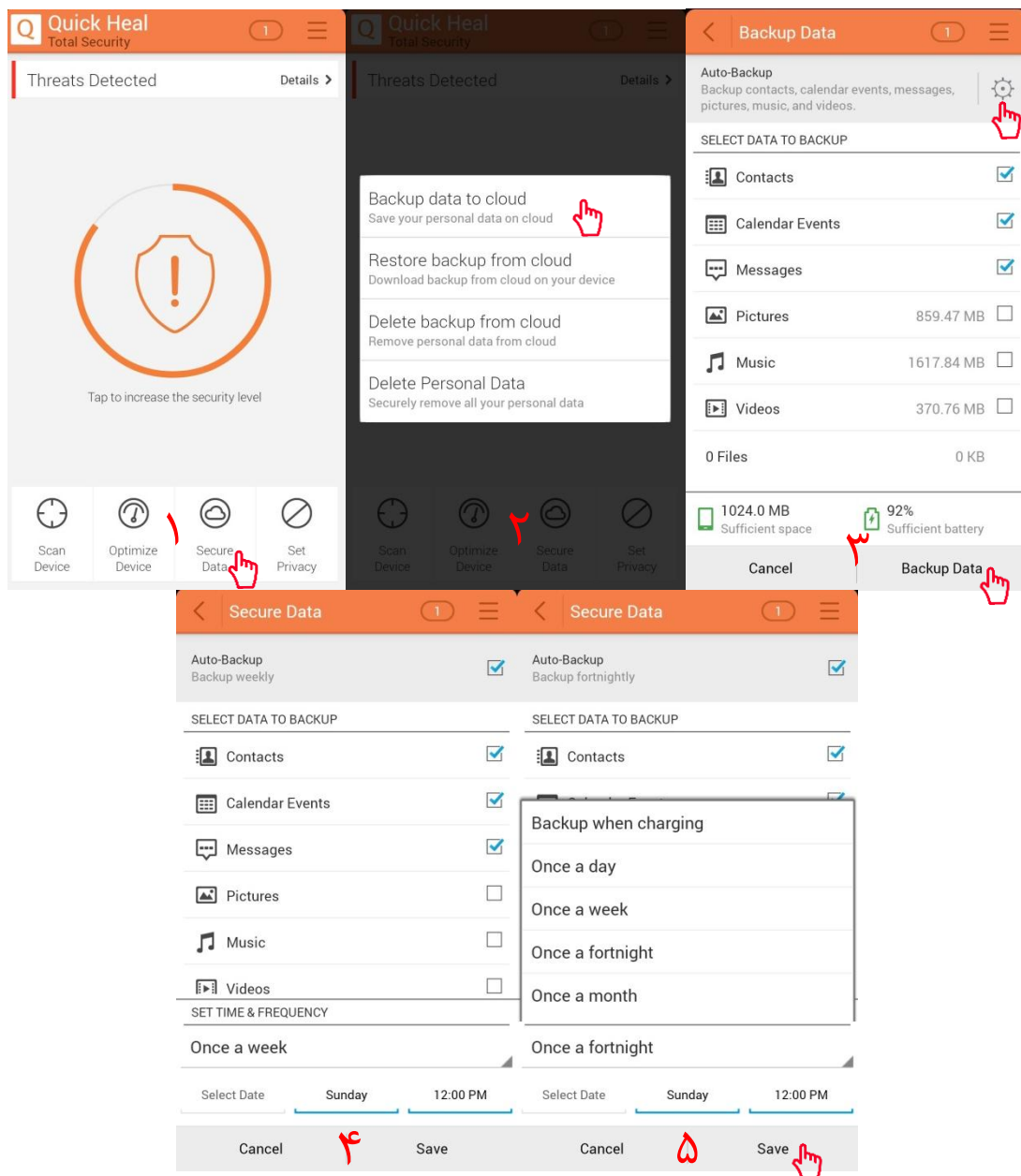
۴. در صفحه‌ی Backup Data، اطلاعاتی که می‌خواهید از آن پشتیبان تهیه کنید، را انتخاب کنید.

۵. برای پشتیبان‌گیری خودکار اطلاعات بر روی فضای ابری کوپیک هیل در زمان‌های مشخص، می‌توانید گزینه *Auto-Backup* را فعال کنید.

همچنین می‌توانید گزینه پشتیبان‌گیری خودکار را از منوی *Dashboard < Backup data to cloud* *Auto-Backup* فعال نمایید.

۶. زمان (time) و تکرار (frequency) را تعیین نمایید.

۷. بر روی *Save* ضربه بزنید.

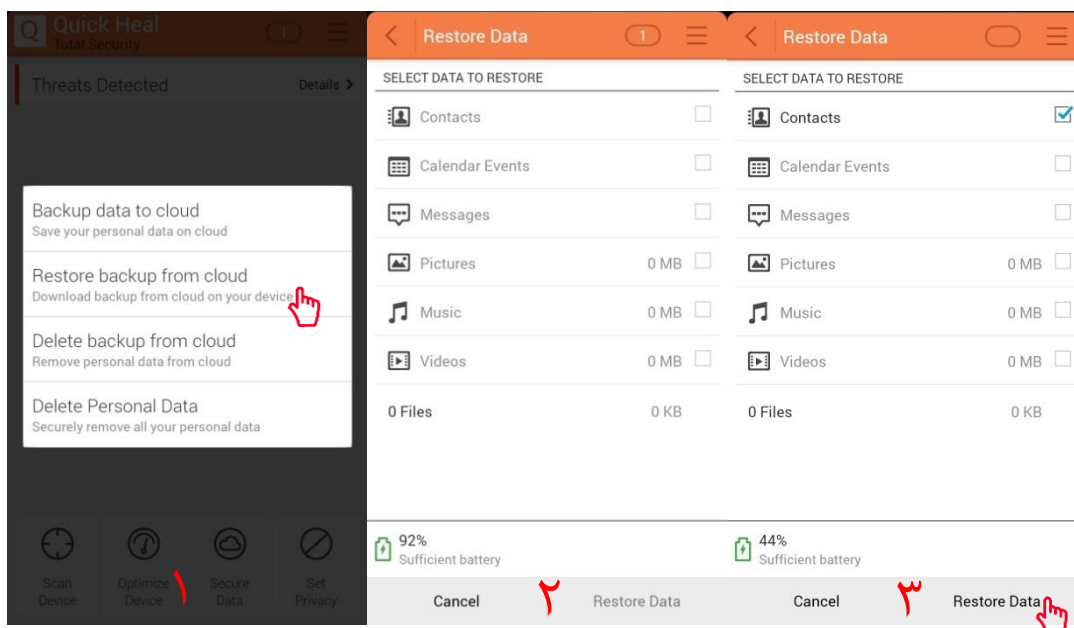


Restore Backup from Cloud

با استفاده از این گزینه می‌توانید اطلاعات خود را از فضای ابری به گوشی خود برگردانید. آخرین اطلاعات ذخیره شده در فضای ابری، به دستگاه برگردانده خواهد شد.

برای بازیابی اطلاعات پشتیبان بر روی دستگاه، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی *Secure Data* ضربه بزنید.
۳. بر روی گزینه *Restore backup from cloud* ضربه بزنید.
۴. در صفحه *Restore Data*، نوع اطلاعاتی که می‌خواهید بر روی دستگاه شما بازیابی شود، را انتخاب کنید.
۵. بر روی *Restore* ضربه بزنید.



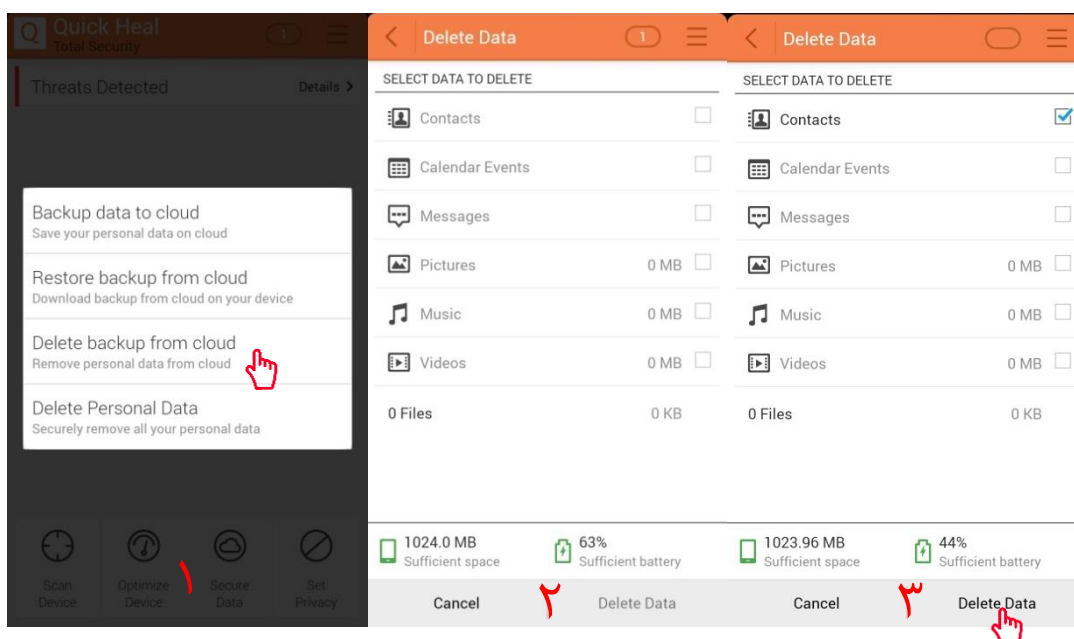
توجه: اطلاعات چندرسانه‌ای (صوتی / تصویری) ممکن است بر روی دستگاه‌هایی با سیستم عامل KitKat بر روی کارت‌های SD بازیابی نشوند.

Delete Backup from Cloud

همه اطلاعات شما بر روی بستر ابری حذف خواهد شد. پیش از حذف، مطمئن شوید که دیگر به این اطلاعات نیازی ندارید، زیرا حذف به صورت دائمی بوده و امکان بازیابی اطلاعات وجود ندارد.

برای حذف اطلاعات پشتیبان بر روی فضای ابری، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی *Secure Data* ضربه بزنید.
۳. بر روی گزینه *Delete backup from cloud* ضربه بزنید.
۴. در صفحه *Delete Data*، نوع اطلاعاتی که می‌خواهید حذف شود را انتخاب کنید.
۵. بر روی *Delete* ضربه بزنید.

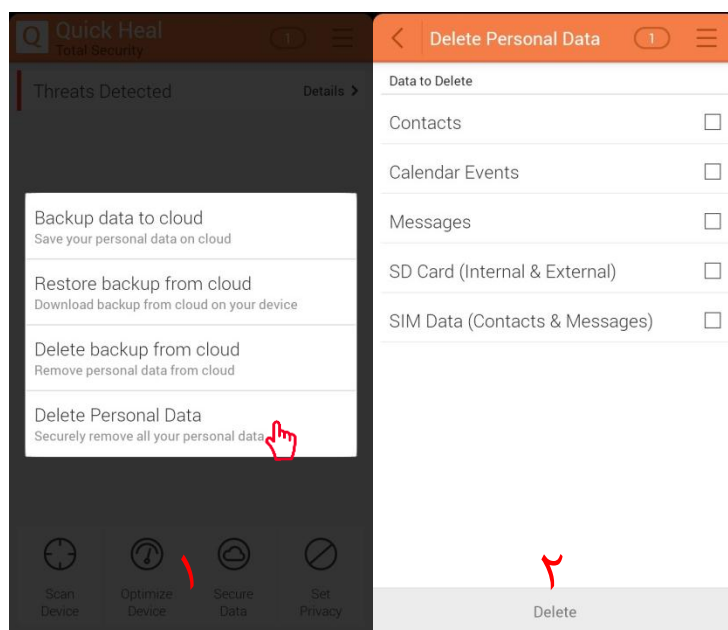


Delete Personal Data

این گزینه کلیه اطلاعات شخصی شما را از روی گوشی حذف می‌کند. (مثلاً زمانی که می‌خواهید گوشی خود را بفروشید.) پیش از حذف، مطمئن شوید که دیگر به این اطلاعات نیازی ندارید، زیرا حذف به صورت دائمی بوده و امکان بازیابی اطلاعات وجود ندارد.

برای حذف اطلاعات شخصی از روی گوشی، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی *Secure Data* ضربه بزنید.
۳. بر روی گزینه *Delete Personal Data* ضربه بزنید.
۴. اطلاعاتی که می‌خواهید حذف شود را انتخاب کنید.
اطلاعاتی که می‌توانند حذف شوند شامل: **Contacts** (لیست مخاطبین)، **Calendar Events** (رویدادهای تقویم)، پیام‌ها (**Messages**)، کارت حافظه **SD** (داخلی و خارجی)، اطلاعات سیم‌کارت (مخاطبین و پیام‌ها) می‌باشند.
- توجه:** اطلاعات کارت‌های **SD** ممکن است بر روی دستگاه‌هایی با سیستم عامل **KitKat** (اندروید ۴.۴) حذف نشوند. اطلاعات سیم‌کارت در بعضی از دستگاه‌ها ممکن است حذف نشود.
۵. بر روی *Delete* ضربه بزنید.



Set Privacy (تنظیم حفظ حریم خصوصی)

با استفاده از این ویژگی شما می‌توانید تماس‌ها و پیامک‌های مزاحم را مسدود کرده، یک لیست مخاطبین خصوصی ایجاد نموده و اطلاعات مهم تاریخچه‌ی تماس‌ها و پیامک‌های مخاطبین خصوصی خود را امن کرده و از دسترس دیگران حفظ نمایید. همچنین می‌توانید با استفاده از کنترل خانواده (Parental Control) دسترسی فرزندان به اینترنت را محدود و کنترل نمایید.

برای تنظیم حفظ حریم خصوصی، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. در داشبورد، بر روی منوی Set Privacy ضربه بزنید.

۳. یکی از گزینه‌های زیر را انتخاب نمایید:

Call & Message Filter (فیلتر تماس و پیام)

با استفاده از این گزینه می‌توانید تماس‌ها و پیامک‌های یک مخاطب را مسدود نمایید. مسدود کردن می‌تواند بر اساس یک شماره خاص، یا شماره‌هایی که با ارقام خاص شروع یا پایان می‌پذیرند، و یا بر اساس یک کلمات کلیدی که در متن پیامک قرار دارد (مثلاً کلمه «جشنواره») صورت پذیرد.

اگر دوسیم‌کارت در یک موبایل دارید، ممکن است رفتار تماس در دستگاه‌های مختلف با توجه به تنظیمات سیم‌کارت دستگاه متفاوت باشد. به همین خاطر در دستگاه دوسیم‌کارته، برای برقراری تماس، انتخاب سیم‌کارت از کاربر سوال نشده و تماس از سیم‌کارت اصلی صورت می‌گیرد.

اگر تنها سیم‌کارت دوم در دستگاه باشد، تماس با سیم‌کارت دوم صورت می‌پذیرد.

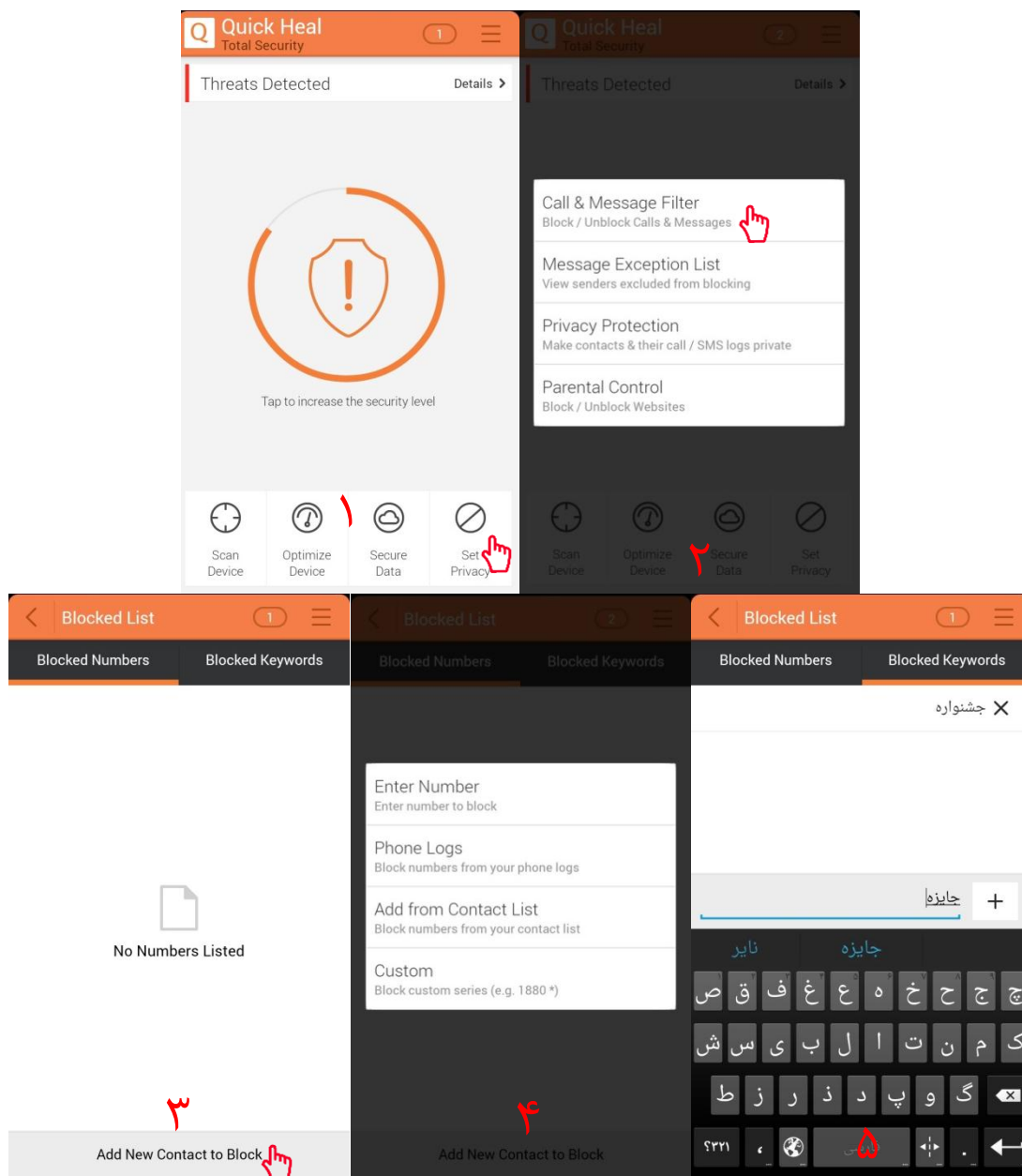
Set Privacy	
CALL & MESSAGE FILTER	
Nonnumeric Senders Nonnumeric senders blocked	☒
Notifications Notify blocked calls & SMS	☒
Alert on Call Rejection Alert on call rejection enabled	☒
Alert on SMS Delete Alert on SMS delete disabled	☐
International Calls Block all unknown international calls	☐
PRIVACY PROTECTION	
Privacy Protection Privacy Protection enabled	☒
Notifications Notify private SMS	☒
PARENTAL CONTROL	
Parental Control Block unwanted content and websites enabled	☒
Browsing Protection Block infected and malicious websites enabled	☒
Phishing Protection Block fraudulent and phishing websites enabled	☒

برای فیلترینگ تماس و پیام گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. در داشبورد، بر روی منوی Set Privacy ضربه بزنید.

۳. بر روی گزینه Call & Message Filter ضربه بزنید.



لیست مسدود شده‌ها (*Blocked List*) شامل موارد زیر است:

- **Blocked Numbers** – همه شماره‌های مسدود شده را نمایش می‌دهد.

- **Blocked Keywords** – همه کلمات کلیدی مسدود شده را نمایش می‌دهد.

۴. برای مسدود کردن یک شماره، بر روی **Add New Contact to Block** ضربه زده و یکی از گزینه‌های زیر را انتخاب نمایید:

- **Enter Number**: شما می‌توانید، شماره تلفن را تایپ کرده و یکی یا هر دو گزینه **Block**

Calls (مسدود کردن تماس) و **Block Messages** (مسدود کردن پیامک‌ها) را انتخاب نمایید.

بر روی **Add to Blocked Numbers List** ضربه بزنید.

- **Phone Logs**: می‌توانید از تاریخچه تماس‌های تلفن خود، یک شماره (مخاطب) را انتخاب

کنید تا یکی یا هر دو گزینه مسدود کردن تماس و مسدود کردن پیامک‌ها بر روی آن صورت

پذیرد. بر روی **Add to Blocked List** ضربه بزنید.

- **Add from Contact List:** می‌توانید از دفترچه تلفن خود، یک شماره (مخاطب) را انتخاب کنید تا یکی یا هر دو گزینه مسدود کردن تماس و مسدود کردن پیامک‌ها بر روی آن صورت پذیرد. بر روی **Add to Blocked List** ضربه بزنید.
- **Custom:** شما می‌توانید همه تماس‌ها و پیام‌ها از یک سری شماره‌ها یا حروف مشخص مسدود کنید (مثلاً **Jazireh** یا شماره‌هایی که با 205 آغاز می‌شوند). همچنین می‌توانید مشخص کنید که شماره تلفن‌هایی که با شماره یا عبارت مشخصه شروع یا پایان می‌پذیرند، مسدود شوند.

توجه ۱: سیستم عامل KitKat از مسدود کردن پیامک پشتیبانی نمی‌کند.

توجه ۲: این ویژگی شماره‌های مطمئن که در ویژگی ضد-سرقت یا در زمان ثبت نام وارد کرده‌اید را مسدود نمی‌کند.

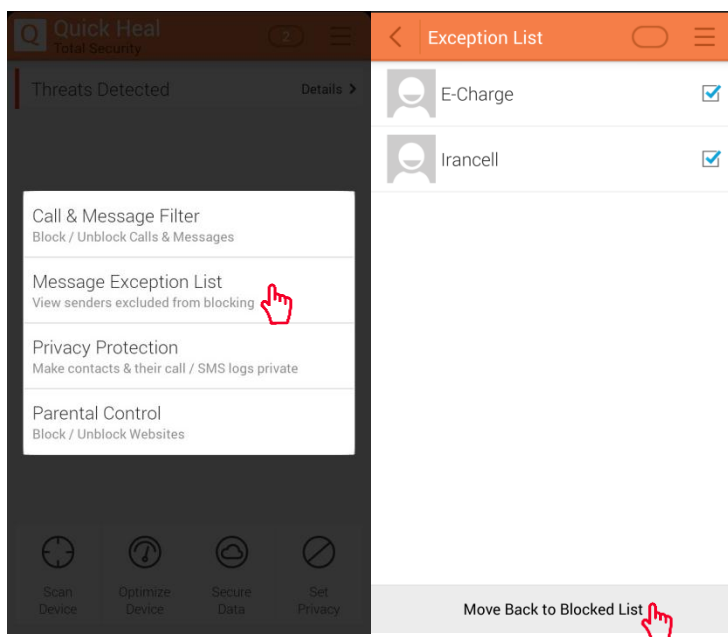
۵. برای مسدود کردن یک کلیدواژه، بر روی **Blocked Keywords** کلیک نمایید. اگر می‌خواهید پیامک‌های حاوی کلیدواژه‌های خاص، مسدود شوند، آن کلمه را نوشته و بر روی علامت بعلاوه + کلیک کنید. اگر پیامی حاوی چنین کلیدواژه‌هایی باشد، مسدود خواهد شد. این ویژگی در مسدود کردن هرزنامه‌ها، پیام‌های ناخواسته و تبلیغاتی مفید است. برای حذف کلیدواژه بر روی علامت منفی جلوی گذرواژه ضربه بزنید.

Message Exception List (لیست استثنای پیام)

اگر می‌خواهید پیام‌های این مخاطبین را دریافت کنید، می‌توانید یک ارسال کننده غیرشماره‌ای مسدود شده را به این لیست انتقال دهید.

برای انتقال یک مخاطب به این لیست، گام‌های زیر را دنبال کنید:

۱. برنامه **Quick Heal Total Security** را اجرا کنید.
 ۲. در داشبورد، بر روی منوی **Set Privacy** ضربه بزنید.
 ۳. بر روی گزینه **Message Exception List** ضربه بزنید.
 ۴. بر روی علامت منفی کنار ارسال کننده‌های غیرشماره‌ای ضربه بزنید.
- ارسال کننده به لیست استثنای پیام افزوده شده است.

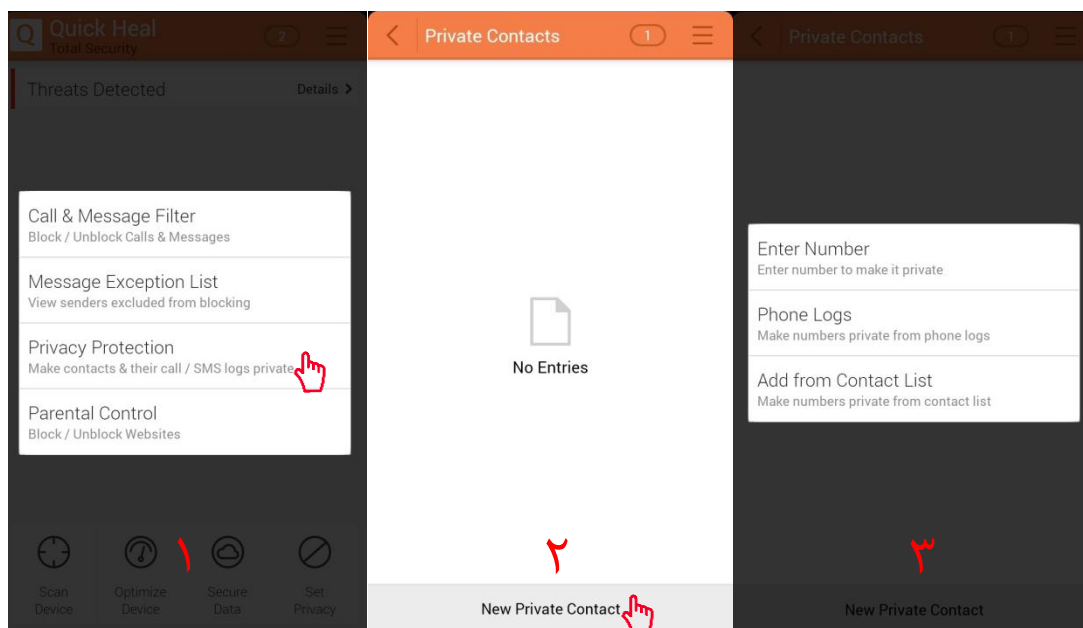


Privacy Protection (محافظة از حریم خصوصی)

ویژگی Privacy Protection می‌تواند لیست مخاطبین خصوصی ایجاد کرده و تاریخچه تماس‌ها و پیام‌های آنها را امن سازد تا با رمز کردن آن هم از دسترس دیگران دور باشد و هم این اطلاعات از گوشی حذف نشود. شما می‌توانید تعیین کنید که مخاطبین، تاریخچه تماس‌ها یا تاریخچه پیامک‌ها و یا هر دو را خصوصی سازید. اگر موبایل شما دو سیم‌کارت دارد، ممکن است رفتار تماس در دستگاه‌های مختلف با توجه به تنظیمات سیم‌کارت دستگاه متفاوت باشد.

برای انتقال یک مخاطب به این لیست، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی Set Privacy ضربه بزنید.
۳. بر روی گزینه Privacy Protection ضربه بزنید.
۴. برای خصوصی کردن یک مخاطب، بر روی New Private Contact ضربه بزنید.
۵. مخاطب را با یکی از روش‌های زیر درج کنید:
 - Enter Number: می‌توانید مستقیماً یک شماره را وارد نمایید. (مثلاً ۰۹۱۱۱۱۱۱۱۱)
 - Phone Log: می‌توانید یک مخاطب/شماره را از تاریخچه تماس گوشی انتخاب نمایید.
 - Add from Contact List: می‌توانید یک مخاطب را از دفترچه تلفن گوشی انتخاب نمایید.
۶. زمانی که می‌خواهید یک شماره را به لیست بیفزایید، بر اساس انتخاب شما، گزینه‌های زیر ظاهر می‌شوند. یکی، یا ترکیبی از این گزینه‌های زیر را انتخاب کنید:
 - Contact (مخاطب)
 - Call Logs (تاریخچه تماس)
 - SMS (پیامک)



توجه ۱: اگر گزینه **contact** را انتخاب کنید، اطلاعات آن مخاطب (مثل نام و شماره تلفن) فقط در لیست مخاطبین خصوصی کوپیک هیل قرار خواهد گرفت. اگر این گزینه را انتخاب نکنید، آن مخاطب در هر دو لیست مخاطبین غیرخصوصی (**nonprivate contact**) و لیست مخاطبین خصوصی (**private contact**) وجود خواهد داشت.

توجه ۲: همچنین اگر شما گزینه **Call Logs** و **SMS** را انتخاب کنید، علاوه بر خصوصی (رمز) کردن تاریخچه تماس‌ها و پیامک‌های قبلی، تماس‌ها و پیامک‌های آینده را نیز خصوصی می‌کند.

توجه ۳: اگر تیک گزینه **Call Logs** و **SMS** را بردارید، تاریخچه تماس‌ها و پیامک‌ها تنها در تاریخچه دستگاه (موبایل) در دسترس خواهد بود. هرچند تماس‌ها و پیامک‌های آینده خصوصی خواهند شد.

شرایط خصوصی کردن مخاطبین به شرح زیر می‌باشد:

- اگر یک مخاطب دارای چندین شماره را خصوصی نمایید، همه شماره‌ها و تاریخچه تماس‌ها و پیامک‌های او خصوصی خواهند شد.
- اگر می‌خواهید هنگام دریافت پیامک از یک مخاطب خصوصی، به شما اطلاع‌رسانی شود، مطمئن شوید که گزینه **Notification** در بخش **Privacy Protection** تنظیمات انتخاب شده باشد.
(Notification < Set Privacy < Settings < main menu < Dashboard)
- ویژگی **Backup**، هیچ‌گونه پشتیبانی از اطلاعات خصوصی تهیه نمی‌کند.
- شماره‌های لیست سیاه (**blacklisted**) نمی‌توانند خصوصی شوند. برای اینکه یک اطلاعات شماره لیست سیاه را خصوصی کنید، ابتدا آن را از لیست سیاه حذف کنید.

غیرخصوصی کردن یک مخاطب خصوصی شده:

هر زمان که بخواستید می‌توانید یک مخاطب خصوصی شده را به دفترچه تلفن خود برگردانید.

برای بازگرداندن یک مخاطب خصوصی به مخاطبان غیر خصوصی (عادی) گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. در داشبورد، بر روی منوی Set Privacy ضربه بزنید.

۳. بر روی گزینه Privacy Protection ضربه بزنید.

۴. برای خصوصی کردن یک مخاطب، بر روی آیکن منفی (-) کنار مخاطب ضربه بزنید.

بر اساس اطلاعات موجود در گوشی شما گزینه‌های زیر ممکن است نمایش داده شوند:

- Contact (مخاطب)
- Call Logs (تاریخچه تماس)
- SMS (پیامک)

۵. گزینه‌ای که می‌خواهید اطلاعات آن به دستگاه شما برگردد را انتخاب کنید.

هر گزینه‌ای که می‌خواهید اطلاعات به صورت دائم حذف شوند، انتخاب (تیک) نکنید.

۶. بر روی OK ضربه بزنید.

اکنون مخاطب (نام و شماره تماس) به همراه اطلاعات آن (مثلاً پیامک‌ها) با موفقیت بازیابی شده‌اند.

اگر یک مخاطب دارای چندین شماره را غیرخصوصی نمایید، همه شماره‌ها و تاریخچه تماس‌ها و پیامک‌های آنها به گوشی باز خواهند گشت.

توجه ۱: اگر می‌خواهید برنامه کوپیک هیل را از روی گوشی خود حذف نمایید، توصیه می‌شود پیش از حذف، اطلاعات خصوصی خود را بازیابی نمایید تا آنها را از دست ندهید.

توجه ۲: اگر یک شماره‌ی غیر-مخاطب (در دفترچه تلفن ذخیره نکردید) که پیامک و تاریخچه تماس ندارد را بازیابی کنید، آن شماره غیر-مخاطبی به طور دائم حذف می‌شود.

محافظت از حریم خصوصی (Privacy Protection) پس از انقضای لایسنس کوپیک هیل:

- پس از انقضای لایسنس، همه تاریخچه تماس‌ها و پیامک‌های مخاطبین خصوصی جدید به جای قرار گرفتن در لیست مخاطبین خصوصی، به تاریخچه دستگاه، مسیریابی و منتقل می‌شوند.
- امکان افزودن مخاطب جدید به لیست مخاطبین خصوصی (Private Contact list)، وجود ندارد.
- نمی‌توانید پیامک‌ها و دیگر اطلاعات مخاطبین خصوصی را مشاهده نمایید، اما می‌توانید آنها را به دستگاه بازیابی کرده و آنها را مشاهده نمایید.

حقایق مربوط به تماس‌ها و پیامک‌های خصوصی

برخی از موارد مهم مربوط به تماس‌ها و پیامک‌های خصوصی به شرح زیر است:

تماس‌ها (Calls)

- می‌توانید تاریخچه تماس‌های خصوصی را مشاهده کرده و تماس با آنها برقرار کنید، تاریخچه آن تماس‌ها را حذف کنید، یا به آنها پیام بفرستید.
- تنها ۲۰۰ تاریخچه تماس آخر در بخش تاریخچه تماس خصوصی ذخیره می‌شوند. اطلاعات تماس‌های بیش از این بدون اطلاع شما حذف خواهند شد.

پیامک‌ها (SMS)

- می‌توانید تاریخچه پیامک‌های خصوصی را مشاهده کرده و متن پیامک را کپی، حذف و یا به هر مخاطب دیگری ارسال نمایید.
- تنها ۵۰۰ پیامک در بخش تاریخچه پیامک خصوصی ذخیره می‌شوند. پیامک‌های بیش از این بدون اطلاع شما حذف خواهند شد.

سازگاری به سیستم عامل KitKat

- محافظت از حریم شخصی از مسدود کردن پیامک در سیستم عامل KitKat پشتیبانی نمی‌کند.

تاثیر استفاده از گزینه حذف اطلاعات شخصی بر محافظت از حریم خصوصی

استفاده از گزینه حذف اطلاعات شخصی (Delete Personal Data) اثرات زیر را به دنبال دارد:

مخاطبین (Contacts)

- اگر شما با استفاده از گزینه Delete Personal Data option، مخاطبین خود را حذف نمایید، جزئیات مخاطبین خصوصی مانند نام مخاطب، آدرس، عکس، آدرس ایمیل و جزئیات دیگر نیز حذف خواهند شد. اگرچه شماره‌های مخاطبین در لیست مخاطبین خصوصی باقی خواهد ماند.
- تاریخچه تماس همه مخاطبین خصوصی به طور دائم حذف خواهد شد و امکان بازیابی آنها وجود ندارد.

پیام (Messages)

- اگر شما با استفاده از گزینه Delete Personal Data option، پیام‌های خود را حذف نمایید، همه پیامک‌های مخاطبین خصوصی به طور دائم حذف خواهند شد. هرچند شماره‌های مخاطبین در لیست مخاطبین خصوصی باقی خواهد ماند.
- امکان بازیابی پیامک‌های مخاطبین خصوصی حذف شده وجود ندارد.

استفاده از پاک کردن اطلاعات (Wipe) در محافظت از حریم خصوصی

با استفاده از دستور پاک کردن اطلاعات (Wipe) شما می‌توانید اطلاعات خود را در زمان گم شدن یا دزدیده شدن دستگاه حذف نمایید. زمانی که شما دستور پاک کردن اطلاعات را ارسال کردید، همه اطلاعات مخاطبین خصوصی و غیرخصوصی شما به طور دائم حذف خواهند شد.

شما می‌توانید دستور Wipe را از روی هر موبایلی به دستگاه گم شده خود ارسال نمایید. همچنین می‌توانید دستور پاک کردن اطلاعات (WIPE) را از پورتال تحت وب مدیریت از راه دور کوپیک هیل (RDM) نیز ارسال نمایید.

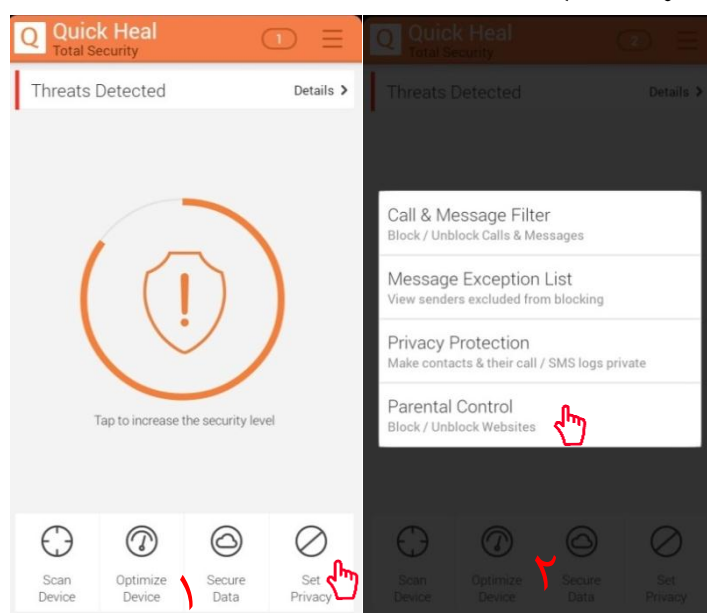
اطلاعاتی که حذف می‌شوند شامل مخاطبین (دفترچه تلفن)، پیامک‌ها، رویدادهای تقویم و اطلاعات حافظه‌ی داخلی و خارجی می‌باشند.

Parental Control (کنترل خانواده)

با استفاده از ویژگی Parental Control می‌توانید وبسایت‌های آلوده، ویروسی و کلاهبردارانه را مسدود نمایید. این ویژگی از دسترسی شما به سایت‌های ناخواسته که ممکن است اطلاعات محرمانه شما (مثلاً اطلاعات بانکی) را به سرقت ببرند جلوگیری می‌کند. همچنین می‌توانید فعالیت‌های آنلاین فرزندان یا دیگر کاربران را کنترل کنید.

برای پیکربندی کنترل خانواده، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی Set Privacy ضربه بزنید.
۳. بر روی گزینه Parental Control ضربه بزنید.
۴. یکی از گزینه‌های زیر را انتخاب کنید:



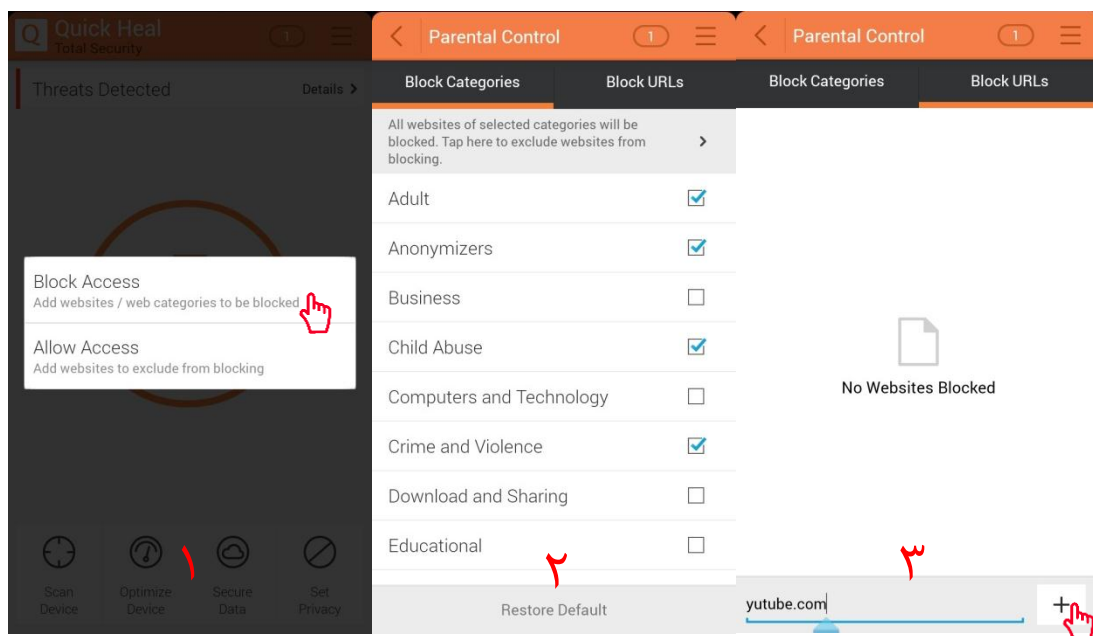
- **Block Access** (مسدود کردن دسترسی): می‌توانید دسترسی به وبسایت‌های خاص را مسدود نمایید. شما می‌توانید وبسایت‌ها را بر اساس طبقه‌بندی (مثلاً با مسدود کردن طبقه‌بندی Games کلیه سایت‌های بازی ایرانی و خارجی مسدود می‌شوند) و نیز آدرس‌های اینترنتی (مثلاً دسترسی به سایت yahoo.com را مسدود کنید) قابل مسدود شدن می‌باشند.
- **Allow Access** (مجاز کردن دسترسی): می‌توانید دسترسی به یک یا چند وبسایت خاص را مجاز کنید. (مثلاً گروه News را مسدود کردید، کلیه سایت‌های خبری جهان مسدود خواهند شد، در اینجا می‌توانید دسترسی به سایت خبری farsnews.com را مجاز کنید).

Block Access (مسدود کردن دسترسی)

شما می‌توانید دسترسی به وبسایت‌ها را بر اساس اولویت و نظر خود محدود نمایید. ممکن است بخواهید به فرزندان اجازه دسترسی به گروه خاصی از وبسایت‌ها (مثلاً بازی) و یا وبسایت‌های مشکوک را ندهید. می‌توانید وبسایت‌ها را بر اساس طبقه‌بندی و همچنین آدرس‌های اینترنتی مسدود نمایید.

برای مسدود کردن دسترسی به وبسایت‌ها، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
 ۲. در داشبورد، بر روی منوی *Set Privacy* ضربه بزنید.
 ۳. بر روی گزینه *Parental Control* ضربه بزنید.
 ۴. بر روی *Block Access* ضربه بزنید.
- صفحه *Parental Control* با دو گزینه *Block Categories* (مسدود کردن طبقه بندی) و *Block URLs* (مسدود کردن آدرس‌های اینترنتی) ظاهر می‌شود.
۵. در صورت انتخاب *Block Categories*، گروه‌هایی که می‌خواهید دسترسی به آنها مسدود شوند را انتخاب کنید.
 ۶. در صورت انتخاب *Block URLs*، آدرس وبسایت‌هایی که می‌خواهید دسترسی به آنها مسدود شوند را تایپ کرده و بر روی علامت به‌اضافه (+) ضربه بزنید.



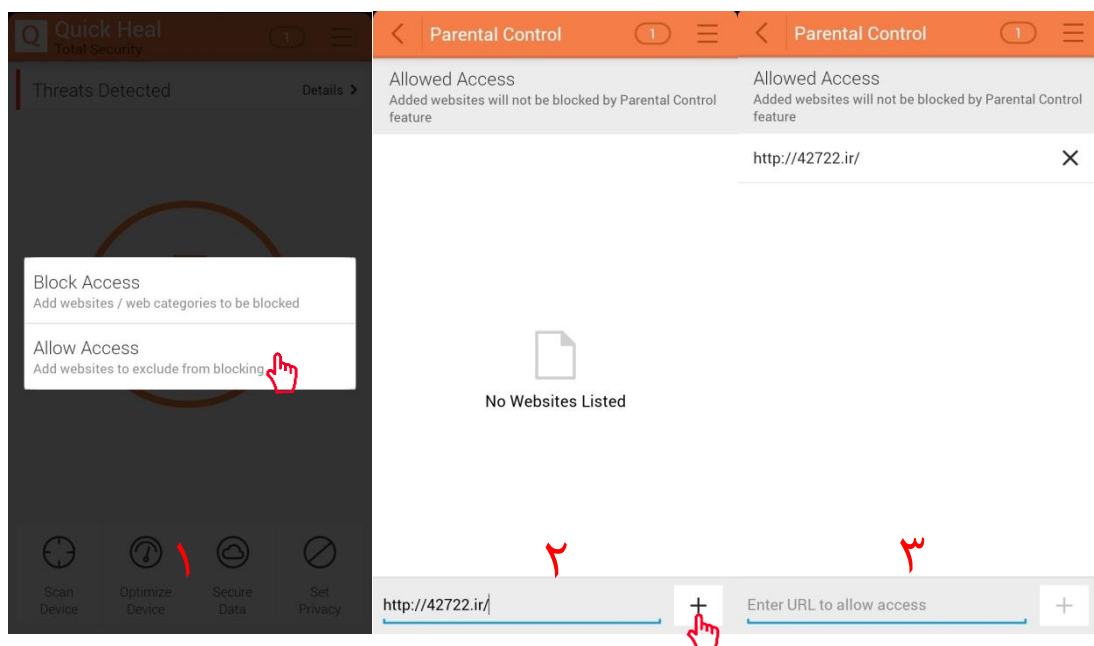
Allow Access (مجاز کردن دسترسی)

اگر یک گروه از وبسایت‌ها را مسدود کردید (مثلاً *News*) اما می‌خواهید دسترسی به یک وبسایت عضو آن گروه (مثلاً *Farsnews.com*) را مجاز کنید این گزینه مفید است.

برای مجاز کردن دسترسی به وبسایت‌های خاص، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. در داشبورد، بر روی منوی *Set Privacy* ضربه بزنید.
۳. بر روی گزینه *Parental Control* ضربه بزنید.
۴. بر روی *Allow Access* ضربه بزنید.

در صفحه Parental Control بر روی کادر *Enter URL to allow access* ضربه زده و آدرس وبسایت موردنظر خود را (مثلاً 42722.ir) وارد نمایید. بر روی علامت به اضافه (+) ضربه بزنید.



توجه ۱: ویژگی مدیریت خانواده، از مرورگر پیش فرض اندروید و نیز مرورگر کروم (Chrome) نسخه ۲۵ و بالاتر پشتیبانی می کند.

توجه ۲: ویژگی مدیریت خانواده، ممکن است بر روی مرورگر پیش فرض اندروید ۴.۰ و بالاتر به خوبی پشتیبانی نکند.

توجه ۳: ویژگی مدیریت خانواده، از نسخه های آزمایشی (beta) کروم پشتیبانی نمی کند.

ج) منوهای اصلی

منوهای اصلی یا سراسری برنامه شامل موارد زیر است:

Home (صفحه اصلی)

با ضربه به این منو شما به صفحه اصلی یا داشبورد کوپیک هیل توتال سکیوریتی منتقل می شوید.

Settings (تنظیمات)

تنظیمات شامل ویژگی های مربوط به تنظیمات برنامه کوپیک هیل مانند، تنظیمات رمز عبور، جلوگیری از حذف غیرمجاز برنامه کوپیک هیل، گزینه های تنظیمات اسکن، تنظیمات حفظ حریم خصوصی و ضد-سرقت می باشد. با ضربه به این منو شما به صفحه اصلی یا داشبورد کوپیک هیل توتال سکیوریتی منتقل می شوید.

برای دسترسی به تنظیمات، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ) در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. رمز عبور خود را در کادر Enter your password تایپ کرده و بر روی Submit ضربه بزنید.
۴. بر روی Allow Access ضربه بزنید.

فراموشی رمز عبور (Using Forgot Password)

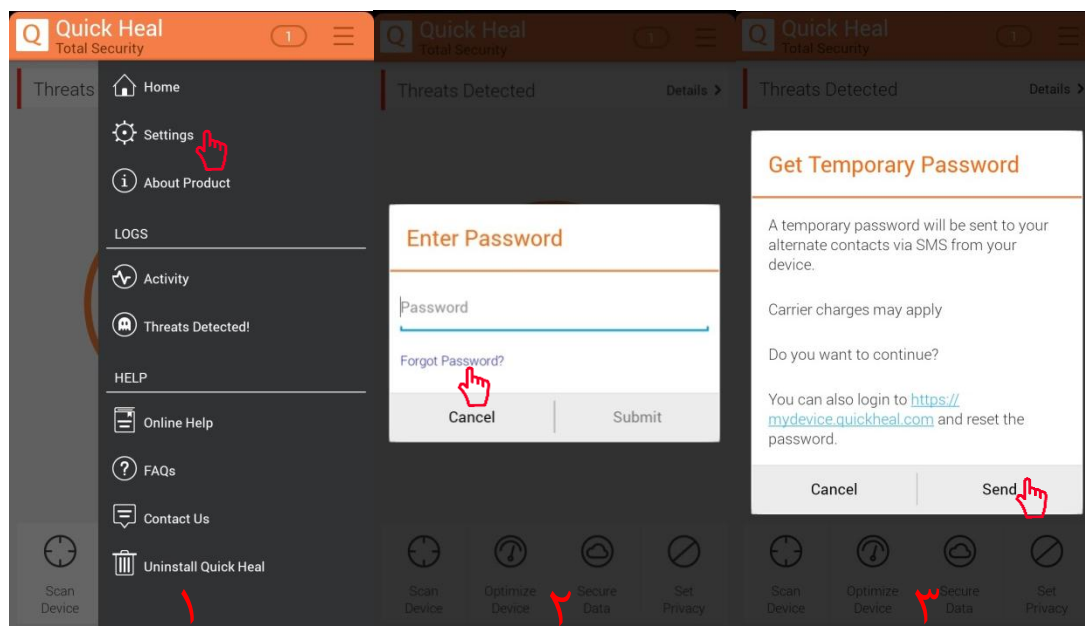
اگر رمز عبور خود را فراموش کردید، می‌توانید آن را بازنشانی یا ریست نمایید.

برای بازنشانی رمز عبور، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. بر روی Forgot Password ضربه بزنید.
۴. صفحه Get Temporary Password نمایش داده می‌شود.

این صفحه چگونگی بازنشانی رمز عبور را شرح می‌دهد. یک رمز عبور موقت به شماره‌های موبایل مخاطبین جایگزین (شماره اعضای خانواده یا دوستان که در هنگام نصب معرفی کردید) ارسال می‌شود. همچنین می‌توانید رمز عبور خود را با استفاده از پورتال تحت وب مدیریت از راه دور کوپیک هیل (RDM) نیز بازنشانی نمایید. آدرس اینترنت پورتال RDM در صفحه دریافت رمز عبور موقت نمایش داده می‌شود.

توجه ۱: ممکن است ارسال پیامک به شماره‌های جایگزین از طرف اپراتور هزینه دربردارد.



۵. بر روی Send ضربه بزنید.

۶. یک پیامک حاوی رمز عبور به شماره موبایل جایگزین (دوست یا اعضای خانواده که در زمان نصب معرفی کردید) ارسال می‌شود. رمز عبور موقت ارسالی را در صفحه نمایش دستگاه خود وارد نمایید.
۷. رمز عبور جدید را وارد و سپس در فیلد **Confirm password** مجدداً رمز عبور را وارد نمایید.
۸. بر روی **Submit** ضربه بزنید.

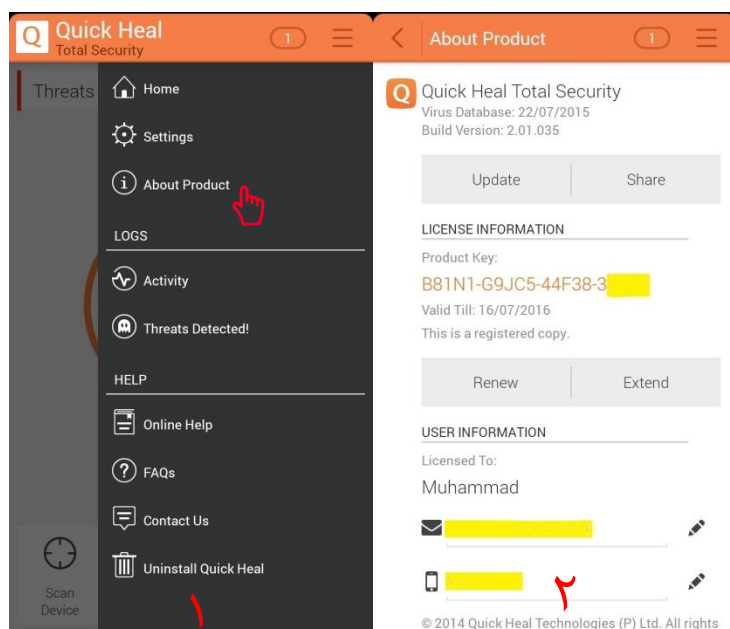
اگر دستگاه شما قفل (Block) شده و رمز عبور خود را فراموش کرده‌اید، باید همین گام‌ها را برای بازگشایی قفل دستگاه دنبال کنید.

برای اطلاعات بیشتر درباره ویژگی‌های **Settings** به بخش **Settings** مراجعه فرمایید.

About Product (درباره محصول)

- در این صفحه شما می‌توانید به جزئیات لایسنس، محصول و دیگر اطلاعات دسترسی یابید.
- با ضربه به این منو شما به صفحه اصلی یا داشبورد کوپیک هیل توتال سکیوریتی منتقل می‌شوید.
- برای رفتن به صفحه درباره محصول، گام‌های زیر را دنبال کنید:
۱. برنامه **Quick Heal Total Security** را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **About Product** ضربه بزنید.

صفحه **About Product** کوپیک هیل توتال سکیوریتی شامل اطلاعات زیر می‌باشد:



Product details (جزئیات محصول):

در بخش اول صفحه «درباره محصول» نام محصول (**Quick Heal Total Security**) و تاریخ بروزرسانی محصول (**Virus Database**)، نسخه ساخت (**Build Version**) نمایش داده می‌شود.

این بخش دو دکمه دارد:

- **Update** (بروزرسانی): با ضربه به این دکمه، آنتی‌ویروس (پایگاه داده ویروس‌ها) و نیز جزئیات اشتراک لایسنس آپدیت می‌شود.
- **Share** (به اشتراک گذاری): شما می‌توانید با استفاده از این ویژگی لینک دانلود آنتی‌ویروس کوپیک‌هیل را به دوستان خود ارسال کنید.

License Information (اطلاعات لایسنس):

در این بخش اطلاعات مربوط به لایسنس و مجوز استفاده از محصول نمایش داده می‌شود. این اطلاعات شامل کلید محصول یا لایسنس (Product key) و تاریخ انقضای لایسنس (License expiry date) می‌باشد.

این بخش دو دکمه دارد:

- **Renew** (تمدید): با استفاده از این گزینه می‌توانید لایسنس خود را تمدید کنید. برای اطلاعات بیشتر می‌توانید با نماینده انحصاری کوپیک‌هیل در ایران، شرکت فناوری ارتباطات و اطلاعات فانوس تماس بگیرید.
- **Extend** (به اشتراک گذاری): شما می‌توانید با معرفی برنامه کوپیک‌هیل به دوستان خود، اعتبار لایسنس خود را افزایش دهید. هرچند اگر یکبار از آن استفاده کنید یا در بعضی از نسخه‌ها، این دکمه دیگر نمایش داده نخواهد شد.

User Information (اطلاعات کاربری):

در این بخش اطلاعات مربوط به کاربر ثبت کننده و استفاده کننده از لایسنس کوپیک‌هیل نمایش داده می‌شود. لایسنس هر شخص به نام او و در سرور جهانی کوپیک‌هیل ثبت می‌شود. این اطلاعات شامل نام کاربری (Username)، آدرس ایمیل (Email Address) و شماره موبایل (Mobile Number) کاربر می‌باشد.

بروزرسانی اطلاعات کاربر: این بخش دو دکمه (به شکل قلم) جهت ویرایش آدرس ایمیل و موبایل در کنار ایمیل و موبایل دارد. با ضربه به هر کدام می‌توانید اطلاعات خود را ویرایش نمایید.
توجه: توجه داشته باشید، پس از اینکه یکبار شماره موبایل با موفقیت راستی‌آزمایی شد (successfully verified)، شما نمی‌توانید مجدداً آن را راستی‌آزمایی و یا شماره موبایل خود را تغییر دهید.

News (اخبار)

با این گزینه، می‌توانید اخبار مرتبط با تهدیدات ویروس‌ها، بدافزارهای جدید در حال گسترش و هرنوع هشدار امنیت دیجیتالی را مشاهده نمایید. اخبار به صورت منظم توسط کوپیک‌هیل به شما ارسال می‌شود. ده پیام خبری آخر در این صفحه نمایش داده می‌شود.

Logs (تاریخچه)

تاریخچه (لاگ) شامل گزارش فعالیت‌ها و اطلاعاتی راجع به شناسایی تهدیدات می‌باشد.

Activity (فعالیت)

با استفاده از این گزینه می‌توانید گزارش فعالیت ویژگی‌های مختلف کوپیک‌هیل مانند ضد-سرقت، اسکن، اسکن پس‌زمینه، کنترل خانواده، و بروزرسانی‌ها را مشاهده نمایید. همچنین می‌توانید گزارش‌ها را بر اساس روز و ویژگی امنیتی فیلتر نمایید.

Threats Detected (تهدیدات شناسایی شده)

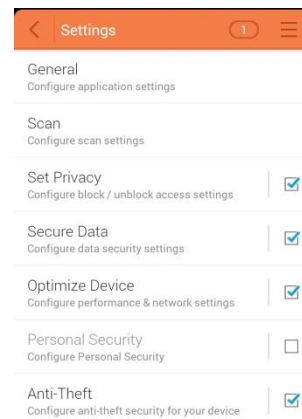
با استفاده از این گزینه می‌توانید وضعیت آلودگی فایل‌ها و برنامه‌ها را بررسی نمایید. همچنین می‌توانید در برابر یک برنامه آلوده لیست شده در این بخش، اقدام مناسب انجام داده (مثلاً **Uninstall** / حذف کردن یا **Skipp** / صرف‌نظر کردن از برنامه آلوده) یا حتی فایل‌های آلوده قرنطینه شده که فکر می‌کنید برای شما مفید هستند را بازبینی کنید.

Help (راهنما)

کوپیک‌هیل روش‌های مختلفی را برای کمک به حل مشکلات و مسائل شما ارائه می‌دهد. برای اطلاعات بیشتر به بخش **Help** مراجعه نمایید.

Settings (منوی تنظیمات)

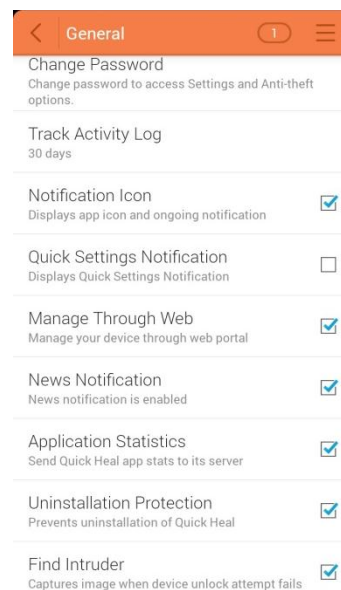
منوی Settings شامل موارد زیر است:



General (عمومی)

گزینه General به شما کمک می‌کند تا گزینه‌های مربوط به برنامه کوپیک هیل را پیکربندی نمایید. این گزینه

شامل موارد زیر است:



Change Password (تغییر رمز عبور)

با استفاده از این گزینه می‌توانید رمز عبور خود را تغییر دهید. برای دسترسی به منوی Settings (تنظیمات)

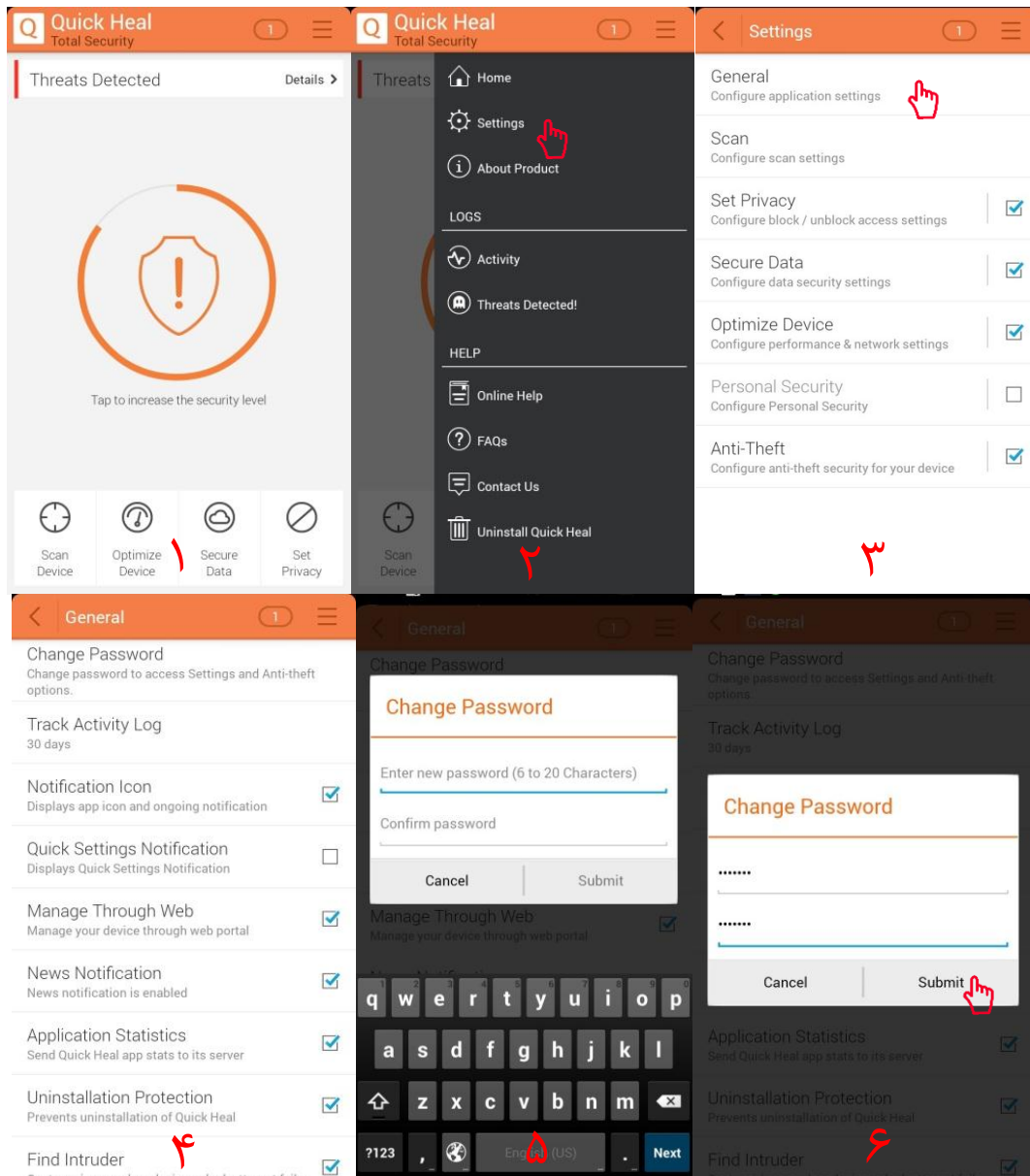
و Anti-Theft (ضد-سرقت) شما نیاز دارید تا رمز عبور داشته باشید.

برای تغییر رمز عبور، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.

۳. بر روی **General** و سپس **Change Password** ضربه بزنید.
۴. رمز عبور صحیح را وارد کرده و سپس مجدداً رمز عبور را در فیلد **Confirm Password** نیز وارد کنید.
توجه: رمز عبور باید حداقل ۶ کاراکتر که می تواند عدد، حرف، علامت و یا ترکیبی از آنها باشد.
۵. بر روی **Submit** ضربه بزنید.



Track Activity Log (ردیابی گزارش فعالیت)

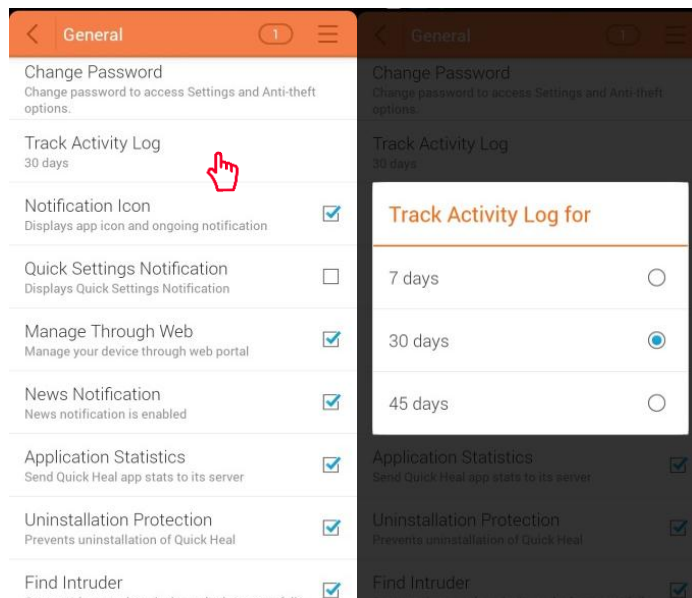
با استفاده از این گزینه می توانید مدت زمانی که تاریخچه فعالیت نگهداری می شود را تعیین نمایید.

برای پیکربندی ردیابی فعالیت، گام های زیر را دنبال کنید:

۱. برنامه **Quick Heal Total Security** را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ) در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. بر روی **General** و سپس **Track Activity** ضربه بزنید.

۴. یکی از گزینه‌های زیر را انتخاب کنید:

- 7 days: گزارش فعالیت ۷ روز اخیر را نگه می‌دارد.
- 30 days: گزارش فعالیت ۳۰ روز اخیر را نگه می‌دارد.
- 45 days: گزارش فعالیت ۴۵ روز اخیر را نگه می‌دارد.



Notification Icon (آیکن اطلاع‌رسانی)

اگر گزینه آیکن اطلاع‌رسانی را فعال کنید، آیکن برنامه کوپیک‌هیل و وضعیت فعلی آن در بخش notification دستگاه شما نمایش داده می‌شود.

برای فعال کردن آیکن اطلاع‌رسانی، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ≡ در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. بر روی **General** ضربه زده و سپس گزینه **Notification Icon** را انتخاب (تیک) کنید.

Quick Settings Notification (هشدار تنظیمات سریع)

برای اینکه دسترسی سریع به گزینه‌های تنظیمات دستگاه خود داشته باشید، گزینه **Quick Settings Notification** را انتخاب کنید. این گزینه‌ها دستگاه شامل: Wi-Fi (شبکه بی‌سیم وای‌فای)، Bluetooth (بلوتوث)، Mobile Data (دیتا یا اینترنت اپراتور موبایل)، Brightness (درخشندگی صفحه نمایش)، و Torch (چراغ قوه گوشی) می‌شود.

برای فعال کردن هشدار تنظیمات سریع، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ≡ در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. بر روی **General** ضربه زده و سپس گزینه **Quick Setting Notification Icon** را انتخاب (تیک) کنید.

Manage Through Web (مدیریت از طریق وب)

شما می‌توانید کوپیک‌هیل توتال سکیوریتی بر روی موبایل خود را از طریق پورتال مدیریت دستگاه راه دور کوپیک‌هیل (Quick Heal RDM) مدیریت کنید. شما می‌توانید کارهای متنوعی مانند پشتیبان‌گیری اطلاعات بر روی فضای ابری، بازیابی اطلاعات از فضای ابری به دستگاه (موبایل)، مکان‌یابی و رهگیری دستگاه در صورت مفقود شدن یا به سرقت رفتن، و بسیاری کارهای دیگر جهت کنترل و امن کردن اطلاعات، را از طریق این پورتال مبتنی بر فناوری ابری و از بستر اینترنت انجام دهید. امکان کنترل دستگاه از طریق پورتال RDM کوپیک‌هیل زمانی ممکن است که شما همواره گزینه Manage Through Web را فعال نگه دارید.

برای فعال کردن گزینه‌ی مدیریت از طریق وب، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
 ۳. بر روی General ضربه زده و سپس گزینه Manage Through Web را انتخاب کنید.
- برای اطلاعات بیشتر به بخش معرفی پورتال مدیریت راه دور دستگاه کوپیک هیل (Quick Heal RDM) مراجعه نمایید.

News Notification (اطلاع‌رسانی اخبار)

آخرین اخبار تهدیدات ویروس‌ها، بدافزارهای جدید و هرنوع هشدار مربوط به امنیت دیجیتالی به صورت منظم توسط کوپیک‌هیل به شما ارسال می‌شود. همه‌ی خبرها در Message Center (مرکز پیام) لیست خواهند شد. همچنین اخبار جدید به محض دریافت در نوار اطلاع‌رسانی دستگاه (notification bar) نیز نمایش داده خواهد شد. اما اگر گزینه News Notification را غیرفعال کنید، هیچ خبری در بخش نوار اطلاع‌رسانی و نیز مرکز پیام دریافت نخواهد شد.

توصیه می‌شود این گزینه را فعال نگه دارید تا از آخرین اخبار امنیت IT جهان مطلع شوید.

برای فعال کردن گزینه اطلاع‌رسانی اخبار، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. بر روی General ضربه زده و سپس گزینه News Notification را انتخاب کنید.

Application Statistics (آمار برنامه)

کوپیک‌هیل توتال سکیوریتی اندروید، بر روی انواع مختلفی از دستگاه‌ها مانند موبایل، تبلت، و دیگر دستگاه‌های با سیم‌کارت یا بدون سیم‌کارت قابل نصب و استفاده است. تلاش می‌کنیم تا برنامه‌ی خود را با آخرین دستگاه‌ها بیشتر و بیشتر سازگار کنیم. برای سازگاری بیشتر برنامه، به طور پیوسته در حال تحقیق و پژوهش بر روی ویژگی‌ها و برنامه کوپیک‌هیل هستیم. برای انجام این امر، آمارها را از منابع مختلف جمع‌آوری می‌کنیم که یکی از این منابع، جامعه کاربران می‌باشد.

با فعال‌سازی این گزینه، شما به برنامه اجازه می‌دهید تا آمارها را با سرور کوپیک‌هیل به اشتراک گذارد. هرچند اگر تمایل ندارید، می‌توانید این گزینه را غیرفعال کنید.

برای فعال کردن گزینه آمارهای برنامه، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. بر روی **General** ضربه زده و سپس گزینه **Application Statistics** را انتخاب کنید.

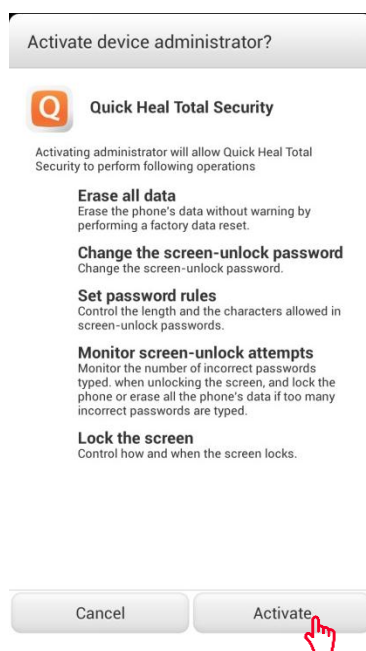
Uninstallation Protection (محافظت در برابر حذف)

با استفاده از این گزینه می‌توانید از حذف برنامه کوپیک‌هیل توسط افراد غیرمجاز جلوگیری کنید. اگر شما یک نسخه لایسنس‌دار (خریداری شده) در اختیار دارید، این گزینه به صورت پیش فرض فعال است. توصیه می‌شود این گزینه را همواره فعال نگه دارید.

اگر دستگاه شما به سرقت رود یا مفقود شود، هیچ کس نمی‌تواند برنامه کوپیک‌هیل را از دستگاه شما حذف کند. این کار موجب می‌شود شما بتوانید با دستگاه خود ارتباط داشته و آن را ردیابی نمایید.

برای فعال کردن گزینه محافظت در برابر حذف، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. بر روی **General** ضربه زده و سپس گزینه **Uninstallation Protection** را انتخاب کنید.
۴. پس از انتخاب این گزینه، صفحه **Activate device administrator (ADA)** نمایش داده می‌شود. شرایط و توافقنامه را خوانده و بر روی **Activate** ضربه بزنید.



Find Intruder (یافتن مزاحم)

اگر شخص غیرمجازی بخواهد بدون اطلاع شما به دستگاهتان دسترسی یابد، گزینه یافتن مزاحم، آنرا شناسایی می‌کند. اگر شخصی دوبار پسورد (یا الگوی ورودی موبایل) را برای باز کردن قفل دستگاه به صورت نادرست وارد کند، کوپیک‌هیل با استفاده از دوربین جلوی دستگاه یک عکس از فرد غیرمجاز تهیه کرده و بعداً به شما نمایش می‌دهد. اگر دستگاه شما دوربین جلو نداشته باشد، عکسی از آن گرفته نمی‌شود. اگر باز کردن قفل برای ویژگی ضد-سرقت تلاش کند، عکس به حساب کاربری ابری (RDM) شما نیز ارسال خواهد شد. اگر شخص بخواهد فقط صفحه نمایش دستگاه شما را باز کند، عکس در پوشه نفوذ غیرمجاز کوپیک‌هیل در حافظه جانبی به نشانی `/sdcard/QhDeviceIntruder` ذخیره می‌شود.

برای فعال کردن گزینه یافتن مزاحم، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. بر روی General ضربه زده و سپس گزینه Find Intruder را انتخاب کنید.

Virus Statistics (آمار ویروس)

هرگاه یک ویروس در دستگاه شما شناسایی شود، آمار آن نیز ساخته خواهد شد. این آمار برای آنالیز و پژوهش بیشتر به لابراتوار ویروس‌شناسی کوپیک‌هیل ارسال خواهد شد. این کار به ما در توسعه راهکار برای آن نوع ویروس کمک می‌کند. تنها با فعال کردن این گزینه، اجازه ارسال آمار ویروس به سرور کوپیک‌هیل را می‌دهید. توصیه می‌شود این گزینه را فعال نگه دارید.

برای فعال کردن گزینه آمار ویروس، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. بر روی General ضربه زده و سپس گزینه Virus Statistics را انتخاب کنید.

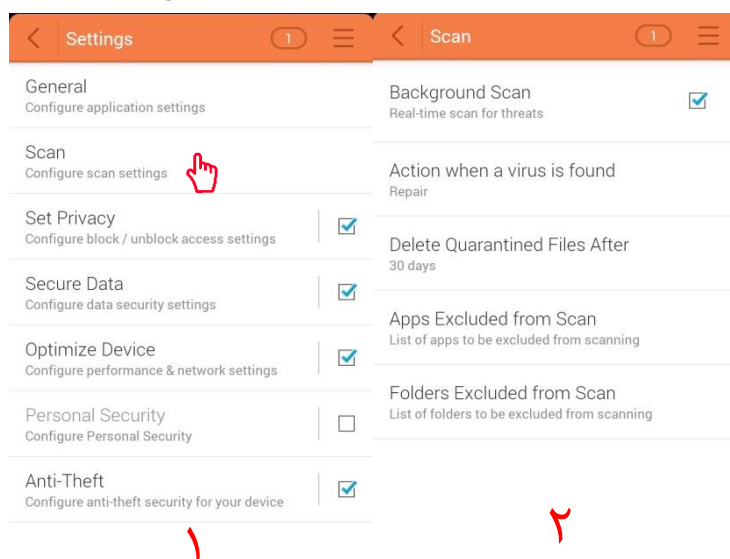
Scan (اسکن / ویروس‌یابی)

با استفاده از این گزینه، می‌توانید گزینه‌های مختلف اسکن را پیکربندی نمایید: برای پیکربندی گزینه اسکن، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.

۳. بر روی **Scan** ضربه زده و پیکربندی‌های زیر را انجام دهید:

- **Background Scan** (اسکن پس‌زمینه): این گزینه دستگاه را به صورت بلادرنگ و پیشگیرانه اسکن می‌کند. همه برنامه‌ها، فایل‌ها یا پوشه‌ها به محض دسترسی (مشاهده یا انتخاب برای کپی یا اجرا) پیش از هر گونه اقدام به صورت پس‌زمینه اسکن می‌شوند. اگر تهدید شناسایی شد، اقدامی که تعیین کرده‌اید، فوراً بر روی فایل یا برنامه آلوده اعمال خواهد شد. برای فعال کردن اسکن پس‌زمینه گزینه **Background Scan** را تیک کنید.
- **Action on Detected Virus** (اقدام بر روی ویروس شناسایی شده): می‌توانید تعیین کنید هنگام شناسایی یک ویروس در دستگاه شما، چه اقدامی روی آن انجام شود. اقدامات شامل: **Repair** (تعمیر)، **Delete** (حذف) و **Skip** (پرش یا عدم اقدام) می‌باشند. اقدام انتخاب شده، به صورت خودکار در زمان شناسایی یک ویروس عمل خواهد کرد.
- **Delete Quarantined Files After** (حذف فایل‌ها پس از قرنطینه): همه فایل‌های آلوده پس از شناسایی حذف نشده بلکه قرنطینه می‌شوند. شما می‌توانید در این بخش مدت زمانی که فایل‌های آلوده نگهداری می‌شوند را تعیین نمایید. پس از سپری شدن آن مدت، فایل‌های آلوده به صورت خودکار حذف می‌شوند. دوره‌های زمانی شامل **7 Days**، **30 Days** و **45 Days** (۷، ۳۰، ۴۵ روز) می‌باشد.
- **Apps Excluded from Scan** (استثنا کردن برنامه از اسکن): می‌توانید برنامه‌ها را از اسکن استثنا کنید تا ویروسیابی نشوند. توصیه می‌شود تنها برنامه‌هایی را استثنا کنید که به آنها اطمینان دارید. این کار باعث کاهش مصرف حافظه می‌گردد.
- **Folders Excluded from Scan** (استثنا کردن پوشه‌ها از اسکن): می‌توانید تعدادی از پوشه‌ها را از اسکن استثنا کنید تا ویروسیابی نشوند. توصیه می‌شود تنها پوشه‌هایی را استثنا کنید که از فایل‌های داخل آن اطمینان دارید. این کار باعث کاهش مصرف حافظه می‌گردد.

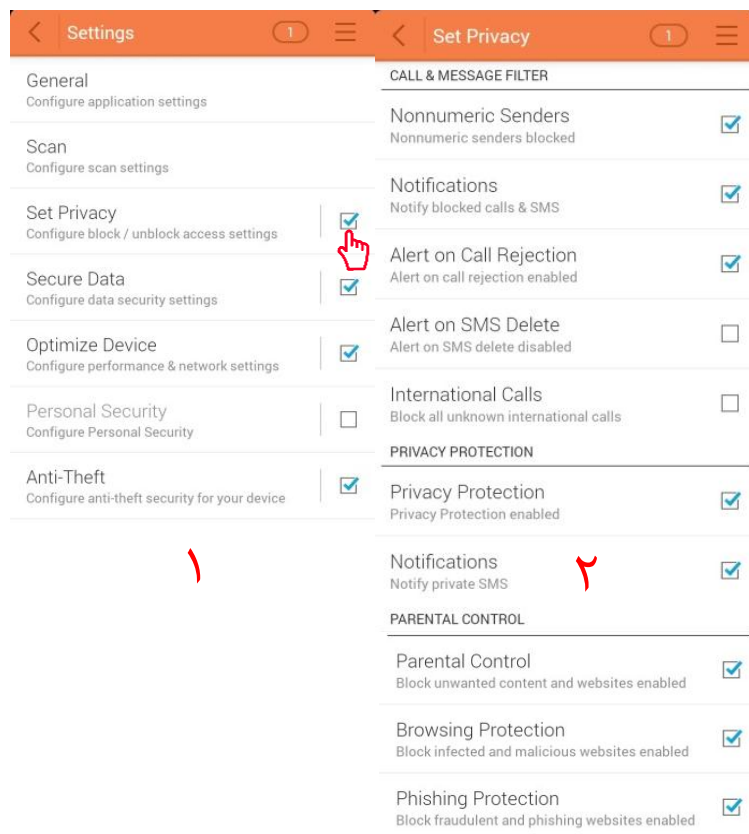


Set Privacy (تنظیم حفظ حریم خصوصی)

با استفاده از این گزینه می‌توانید پیامک‌های غیرشماره‌ای و تماس‌های بین‌المللی را مسدود کرده، هنگام رد تماس یا مسدود کردن پیامک هشدار دریافت نمایید. همچنین محافظت از حریم خصوصی، کنترل خانواده و دیگر ویژگی‌ها را فعال نمایید.

برای پیکربندی تنظیم حفظ حریم خصوصی، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. گزینه **Set Privacy** را تیک کنید تا فعال شود.



۴. بر روی عبارت **Set Privacy** ضربه بزنید تا بتوانید تنظیمات زیر را انجام دهید:

- **Nonnumeric Senders:** اگر این گزینه را فعال کنید، همه پیامک‌ها و تماس‌ها از افراد غیرشماره‌ای (مثل Jashnvareh) مسدود خواهند شد. علاوه بر آن، این گزینه پیام‌های فوری (Flash) و WAP Push که از سوی اپراتورها ارسال می‌شوند (و مستقیماً بر روی صفحه نمایش موبایل نشان داده می‌شوند) را نیز مسدود می‌کند.
- **Notifications:** اگر می‌خواهید هنگام مسدود شدن پیام‌ها، در قسمت اطلاع‌رسانی (notification) صفحه اول دستگاه، اعلان درج گردد، این گزینه را انتخاب کنید.

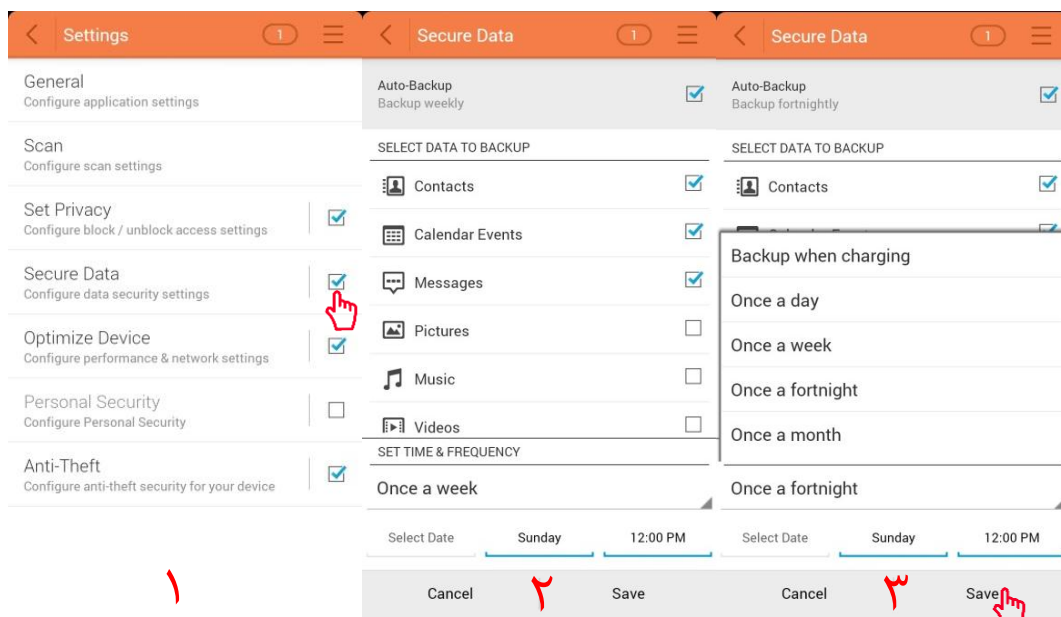
- **Alert on Call Rejection:** برای دریافت هشدار هنگام رد (reject) یک تماس، این گزینه را فعال کنید. اگر شما یک تماس ناخواسته را رد کنید، به مدت ۲۰ ثانیه پیامی به شما نشان داده خواهد شد تا بتوانید شماره تماس رد شده را به لیست مسدودی‌ها (Blocked List) اضافه کنید.
- **Alert on SMS Delete:** اگر این گزینه فعال باشد، هنگام حذف کردن یک پیامک، صفحه‌ای به شما نشان داده می‌شود تا بتوانید شماره (یا ارسال کننده‌های غیرشماره‌ای) پیامک ناخواسته را وارد لیست مسدودی‌ها (Blocked List) کنید تا از این پس پیامک آن شماره مسدود شود. این اعلان به مدت ۲۰ ثانیه پس از حذف یک پیامک نشان داده می‌شود.
- **International Calls:** برای مسدود کردن همه تماس‌های بین‌المللی ناخواسته این گزینه را فعال کنید.
- **Privacy Protection:** برای فعال کردن محافظت از حریم خصوصی این گزینه را تیک بزنید. برای اطلاعات بیشتر در مورد ویژگی حفظ حریم خصوصی به بخش تنظیم حفظ حریم خصوصی مراجعه نمایید.
- **Notification:** اگر این گزینه فعال باشد، هنگام دریافت پیامک از سوی مخاطبین خصوصی، یک پیغام اطلاع‌رسانی در بخش notification صفحه اصلی دستگاه نمایش داده می‌شود.
- **Parental Control:** برای فعال کردن ویژگی کنترل خانواده این گزینه را تیک کنید. برای مسدود کردن همه تماس‌های بین‌المللی ناخواسته این گزینه را فعال کنید. برای اطلاعات بیشتر در مورد ویژگی کنترل خانواده به بخش ویژگی کنترل خانواده مراجعه نمایید.
- **Browsing Protection:** برای فعال شدن محافظت مرور اینترنتی این گزینه را فعال نمایید.
- **Phishing Protection:** برای فعال شدن محافظت فیشینگ (سایت‌های کلاهبردار) این گزینه را فعال نمایید.

Secure Data (امن‌سازی اطلاعات)

با استفاده از این گزینه می‌توانید اطلاعات مهم خود را با ذخیره آنها در فضای ابری کوپیک هیل امن سازید. در زمان‌های دلخواه می‌توانید از اطلاعات خود پشتیبان تهیه کرده، آنها را به گوشی خود بازیابی نمایید، یا اطلاعات پشتیبان را از فضای ابری خود حذف نمایید.

برای استفاده از امن‌سازی اطلاعات پیکربندی، گام‌های زیر را دنبال کنید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. گزینه Secure Data را تیک کنید تا فعال شود.



۴. بر روی عبارت **Secure Data** ضربه بزنید تا بتوانید تنظیمات زیر را انجام دهید:

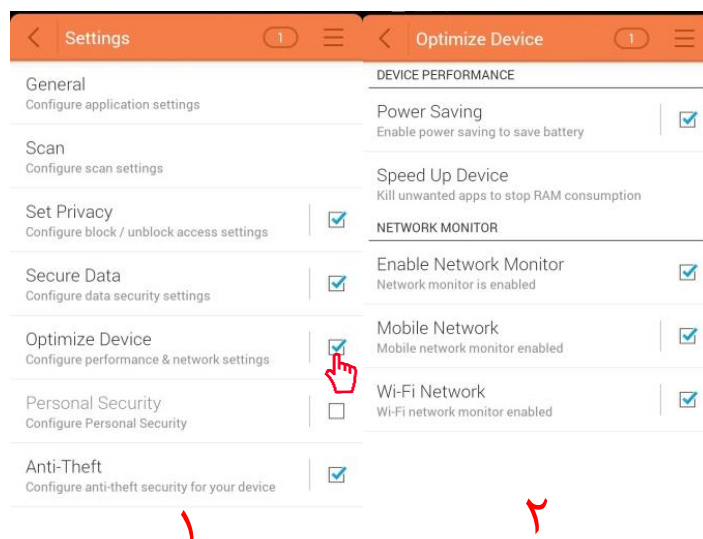
- **Auto-Backup**: برای تهیه پشتیبان به صورت خودکار، این گزینه را فعال نمایید. اگر این گزینه را تیک کنید، گزینه‌های بعدی در بخش **Select Data to Backup** فعال و قابل پیکربندی می‌گردند.
 - **Select Data to Backup**: اطلاعاتی که می‌خواهید از آن پشتیبان تهیه شود را در این بخش انتخاب می‌کنید.
 - **Set Time & Frequency**: زمان و تکراری که پشتیبان باید تهیه شود را در این بخش تعیین می‌نمایید. **Frequency** (تکرار) شامل: **Backup while charging** (پشتیبان‌گیری در زمان داشتن شارژ بالای ۵۰٪)، **Once a day** (یکبار در روز)، **Once a week** (یکبار در هفته)، **Once a fortnight** (یکبار در هر دو هفته) و **Once a month** (یکبار در ماه) می‌باشد.
۵. بر روی **Save** ضربه بزنید.

Optimize Device (بهینه‌سازی دستگاه)

با استفاده از این گزینه می‌توانید کارایی دستگاه خود را بررسی، سرعت دستگاه را افزایش و تنظیمات و کنترل شبکه (اینترنت) را اعمال نمایید.

برای پیکربندی بهینه‌سازی دستگاه، گام‌های زیر را دنبال کنید:

۱. برنامه **Quick Heal Total Security** را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. به طور پیش‌فرض گزینه **Optimize Device** فعال است. اگر فعال نبود، گزینه **Optimize Device** را تیک نمایید.
۴. بر روی عبارت **Optimize Device** ضربه بزنید تا بتوانید تنظیمات زیر را انجام دهید:

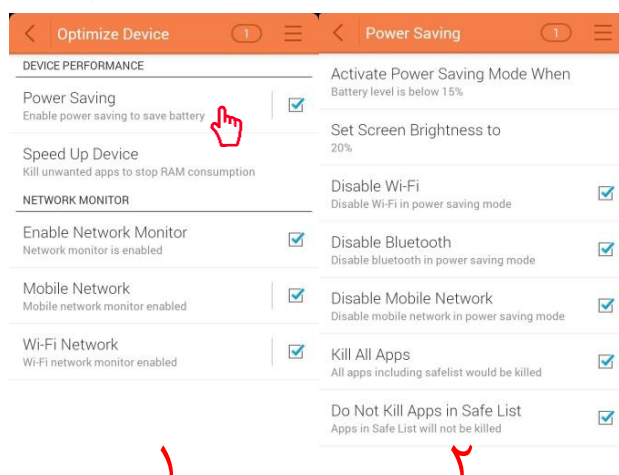


Power Saving (صرفه‌جویی در انرژی)

با استفاده از این گزینه می‌توانید با پیکربندی تنظیمات بر اساس نیاز خود مصرف انرژی (باتری) دستگاه خود را کاهش دهید.

برای پیکربندی صرفه‌جویی در انرژی، گام‌های زیر را دنبال نمایید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
۳. به طور پیش‌فرض گزینه **Optimize Device** فعال است. اگر فعال نبود، گزینه **Optimize Device** را تیک نمایید.
۴. بر روی عبارت **Optimize Device** ضربه بزنید تا بتوانید تنظیمات را پیکربندی نمایید.
۵. بر روی عبارت **Power Saving** ضربه بزنید تا بتوانید تنظیمات زیر را پیکربندی نمایید:

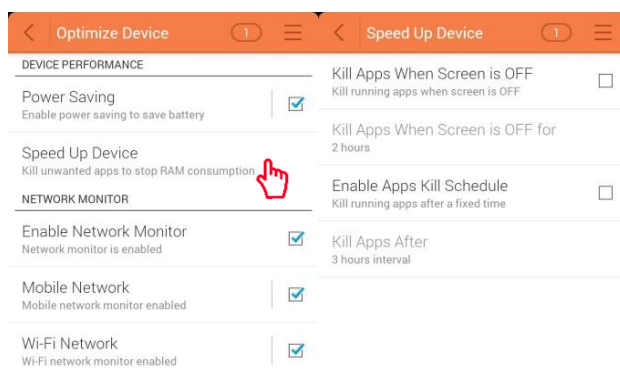


- **Activate Power Saving Mode When:** در این بخش تعیین می‌کنید که چه زمانی (رسیدن باتری به سطح مشخص) حالت صرفه‌جویی آغاز شود. (مثلاً وقتی که سطح باتری دستگاه به ۱۵٪ رسید، حالت صرفه‌جویی فعال شود)

- **Set Screen Brightness to**: میزان نور صفحه نمایش در هنگام آغاز حالت صرفه‌جویی را تعیین کنید.
- **Disable Wi-Fi**: اگر این گزینه را انتخاب کنید، هنگام فعال شدن حالت صرفه‌جویی، شبکه بی‌سیم Wi-Fi به صورت خودکار غیرفعال می‌شود.
- **Disable Bluetooth**: اگر این گزینه را انتخاب کنید، هنگام فعال شدن حالت صرفه‌جویی، شبکه بلوتوث به صورت خودکار غیرفعال می‌شود.
- **Disable Mobile Network**: اگر این گزینه را انتخاب کنید، هنگام فعال شدن حالت صرفه‌جویی، شبکه (اینترنت) موبایل به صورت خودکار غیرفعال می‌شود.
- **Kill all Apps**: برای توقف اجرای (بستن) همه برنامه‌های در حال اجرا هنگام آغاز حالت صرفه‌جویی این گزینه را فعال کنید. این گزینه کمک می‌کند تا در مصرف انرژی صرفه‌جویی شود.
- **Do not Kill Apps in Safe List**: اگر نمی‌خواهید در زمان بسته شدن همه برنامه‌ها (Kill all Apps)، برنامه‌های لیست مطمئن (Safe List) نیز بسته نشوند، این گزینه را فعال نمایید.

Speed Up Device (افزایش سرعت دستگاه)

- با استفاده از این گزینه می‌توانید سرعت دستگاه خود را افزایش دهید.
- برای افزایش سرعت دستگاه، گام‌های زیر را دنبال نمایید:
۱. برنامه **Quick Heal Total Security** را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن ) در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.
 ۳. به طور پیش‌فرض گزینه **Optimize Device** فعال است. اگر فعال نبود، گزینه **Optimize Device** را تیک نمایید.
 ۴. بر روی عبارت **Optimize Device** ضربه بزنید تا بتوانید تنظیمات را پیکربندی نمایید.
 ۵. بر روی عبارت **Speed Up Device** ضربه بزنید تا بتوانید تنظیمات زیر را پیکربندی نمایید:



- **Kill Apps When Screen is OFF**: اگر می‌خواهید هنگام خاموش شدن صفحه نمایش همه‌ی برنامه‌ها بسته شوند، این گزینه را فعال نمایید.
- **Kill Apps When Screen is OFF for**: یک دوره زمانی برای اجرای برنامه‌ها تعیین نمایید. برنامه‌ها پس از طی شدن مدت زمان مشخص شده در این قسمت، بعد از خاموش شدن صفحه نمایش، بسته خواهند شد. دوره‌های زمانی شامل 30 minutes و 1 hour, 2 hours, 4 hours و 3 hours (۱، ۲، ۴ و نیم ساعت) می‌باشد.
- **Enable Apps Kill Schedule**: در این بخش می‌توانید یک بازه زمانی تعیین نمایید تا پس از آن برنامه‌ها به صورت خودکار بسته شوند.
- **Kill Apps After**: یک دوره زمانی تعیین نمایید تا بستن برنامه‌ها (Kill Apps) هر بار به صورت متناوب (مثلاً هر ۳ ساعت) اعمال شود. دوره‌های زمانی شامل 6 hours, 9 hours, 12 hours و 3 hours (۳، ۶، ۹ و ۱۲ ساعت) می‌باشد.

Enable Network Monitor (فعال کردن نظارت بر شبکه)

- با استفاده از این گزینه می‌توانید بر شبکه داده (اینترنت) نظارت داشته و میزان مصرف داده (اینترنت) شبکه موبایل و شبکه بی‌سیم Wi-Fi را کنترل و مدیریت نمایید. (مثلاً یک طرح تشویقی همراه اول اینترنت ۱ ماهه ۲ گیگابایتی خریداری کرده‌اید، می‌خواهید هنگام رسیدن مصرف به ۲ گیگابایت، اینترنت موبایل به صورت خودکار قطع شده و از مصرف خارج از طرح و گران خودداری نمایید)
- برای فعال کردن نظارت بر شبکه، گام‌های زیر را دنبال نمایید:
۱. برنامه Quick Heal Total Security را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
 ۳. به طور پیش‌فرض گزینه Optimize Device فعال است. اگر فعال نبود، گزینه Optimize Device را تیک نمایید.
 ۴. بر روی عبارت Optimize Device ضربه بزنید تا بتوانید تنظیمات را پیکربندی نمایید.
 ۵. گزینه Enable Network Monitor را تیک کنید تا بتوانید شبکه موبایل و شبکه Wi-Fi را پیکربندی نمایید.

Mobile Network (شبکه داده موبایل)

- با استفاده از این گزینه می‌توانید محدودیت استفاده از داده برای شبکه‌ی موبایل را پیکربندی نمایید.
- برای پیکربندی محدودیت استفاده از داده، گام‌های زیر را دنبال نمایید:
۱. برنامه Quick Heal Total Security را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
 ۳. به طور پیش‌فرض گزینه Optimize Device فعال است. اگر فعال نبود، گزینه Optimize Device را تیک نمایید.

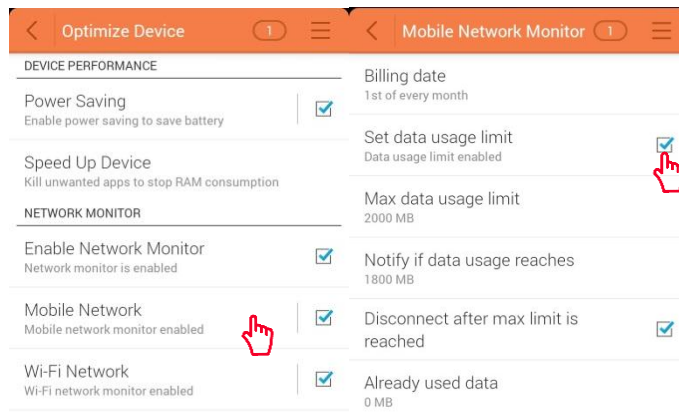
۴. بر روی عبارت *Optimize Device* ضربه بزنید.

۵. بر روی عبارت *Mobile Network* ضربه بزنید.

توجه: اگر گزینه *Mobile Network* فعال نیست، ابتدا گزینه *Enable Network Monitor* را تیک کنید.

۶. گزینه *Set data usage limit* را انتخاب نمایید تا بتوانید سایر تنظیمات اعمال محدودیت مصرف داده را پیکربندی کنید.

برای دریافت اطلاعات بیشتر به بخش تعیین محدودیت میزان مصرف داده مراجعه نمایید.



Wi-Fi Network (شبکه بی سیم Wi-Fi)

با استفاده از این گزینه می توانید محدودیت میزان استفاده از شبکه ی *Wi-Fi* را پیکربندی نمایید.
برای پیکربندی محدودیت استفاده از شبکه *Wi-Fi*، گام های زیر را دنبال نمایید:

۱. برنامه *Quick Heal Total Security* را اجرا کنید.

۲. بر روی منوی اصلی (آیکن ≡ در بالا سمت راست) ضربه زده سپس بر روی *Settings* ضربه بزنید.

۳. به طور پیش فرض گزینه *Optimize Device* فعال است. اگر فعال نبود، گزینه *Optimize Device* را تیک نمایید.

۴. بر روی عبارت *Optimize Device* ضربه بزنید تا بتوانید تنظیمات شبکه *Wi-Fi* را پیکربندی نمایید.

۵. بر روی عبارت *Wi-Fi Network* ضربه بزنید.

مطمئن شوید که گزینه *Enable Network Monitor* انتخاب شده باشد.

برای دریافت اطلاعات بیشتر به بخش تعیین محدودیت میزان مصرف داده مراجعه نمایید.

Personal Security (امنیت شخصی)

با استفاده از این گزینه می‌توانید در مواقع اورژانسی یا خطر، با فشردن ۷ تا ۱۰ باره دکمه خاموش-روشن (Power) دستگاه و کشیدن فلش دکمه **Slide to Activate** به سمت راست می‌توانید پیامک درخواست کمک را به همراه موقعیت جغرافیایی خود (نقشه) به شماره‌های جایگزین ارسال نمایید. (به عنوان مثال فرزند خانواده در موقعیت اورژانسی امکان تماس با والدین را نداشته و تنها با فشردن ۷-۱۰ بار کلید خاموش-روشن دستگاه، یک پیام درخواست کمک به همراه موقعیت خود در نقشه (لینک صفحه ای از کوپیک هیل که موقعیت فرد بر روی نقشه را نشان می‌دهد) به والدین خود ارسال می‌کند).

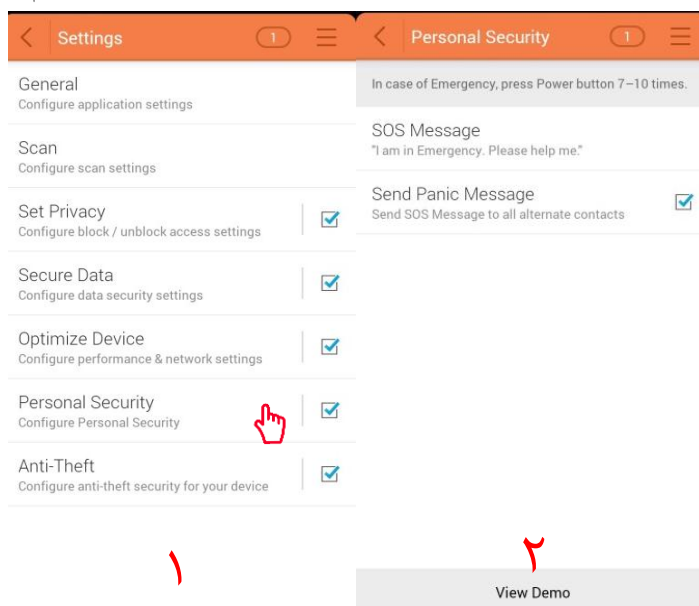
برای پیکربندی امنیت شخصی، گام‌های زیر را دنبال کنید:

۱. برنامه **Quick Heal Total Security** را اجرا کنید.

۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.

۳. گزینه **Personal Security** را تیک نمایید تا ویژگی امنیت شخصی فعال شود.

۴. بر روی عبارت **Personal Security** ضربه بزنید تا بتوانید تنظیمات زیر را انجام دهید:



- **SOS Message**: می‌توانید متن پیامی که در مواقع اورژانسی به شماره‌های جایگزین (و سایت‌های شبکه اجتماعی) شما ارسال می‌شود را تغییر دهید. شماره‌های جایگزین همان شماره‌هایی هستند که در زمان ثبت نام نرم‌افزار کوپیک هیل وارد کردید. هرچند می‌توانید در هر زمانی با مراجعه به تنظیمات **Anti-Theft** (ضدسرقت) این شماره‌ها را تغییر دهید.
- **Send Panic Message**: اگر می‌خواهید هنگامی که در شرایط اضطراری هستید، پیام کمک ارسال شود، این گزینه را انتخاب کنید. اگر این گزینه غیرفعال باشد، پیام درخواست کمک ارسال نخواهد شد.

توجه: بلافاصله پس از ورود به حالت اورژانسی، یک پیام اطلاع‌رسانی غیرفعال کردن حالت اورژانسی (**Deactivate Emergency**) در نوار اطلاع‌رسانی کوپیک هیل (**Quick Heal Notification bar**) نمایش داده می‌شود. برای غیرفعال کردن حالت اورژانسی، باید رمزعبور خود را وارد نمایید.

Anti-Theft (ضد-سرقت)

با استفاده از این ویژگی ضد-سرقت، می‌توانید دسترسی به سیم‌کارت‌های خاص را مجاز یا غیرمجاز کرده؛ در صورت تعویض سیم‌کارت، دستگاه شما به صورت خودکار قفل می‌گردد. همچنین می‌توانید در صورت به سرقت رفتن یا گم شدن دستگاه، آن را از راه دور مسیریابی و کنترل کرده و مکان گوشی را از طریق پیامک به اطلاع شماره‌های جایگزین (یکی از اعضای خانواده یا دوست) برسد.

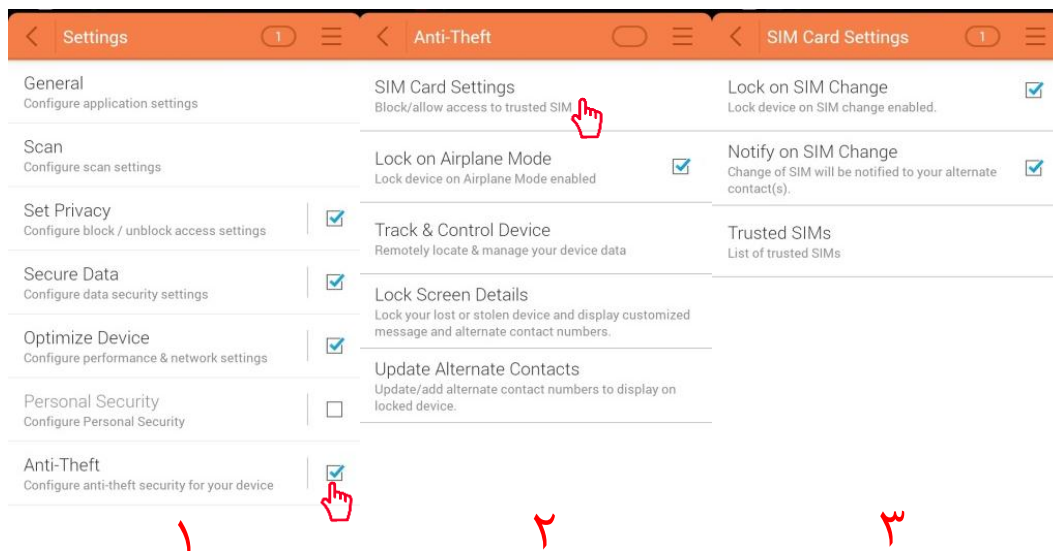
SIM Card Settings (تنظیمات سیم‌کارت)

با استفاده از این گزینه می‌توانید دسترسی به سیم‌کارت‌ها را مسدود یا مجاز کرده، یا دستگاه را به صورتی پیکربندی نمایید تا به محض تغییر سیم‌کارت، گوشی قفل شود و نیز یک لیست از سیم‌کارت‌های مورد اطمینان بسازید.

برای پیکربندی تنظیمات سیم‌کارت، گام‌های زیر را دنبال نمایید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
 ۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
 ۳. اگر گزینه ضد-سرقت فعال نبود، گزینه Anti-Theft را تیک نمایید تا ویژگی امنیت شخصی فعال شود.
 ۴. بر روی عبارت Anti-Theft ضربه بزنید تا بتوانید تنظیمات سیم‌کارت را پیکربندی کنید.
 ۵. بر روی عبارت SIM Card Settings ضربه بزنید و تنظیمات زیر را پیکربندی نمایید:
 - Lock on SIM Change: اگر می‌خواهید به محض تغییر سیم‌کارت (توسط سارق)، دستگاه شما قفل شود، این گزینه را فعال کنید. این گزینه دستگاه را امن کرده، و تنها با استفاده از رمز عبور معتبر قابل بازگشایی می‌باشد.
 - Notify on SIM Change: اگر می‌خواهید در زمان تغییر سیم‌کارت، پیامک اطلاع‌رسانی دریافت کنید، این گزینه را فعال کنید. این گزینه کمک می‌کند تا از علت تغییر سیم‌کارت و کاری که نیاز است بر روی آن انجام شود اطلاع یابید.
 - Trusted SIMs: می‌توانید یک لیست از سیم‌کارت‌های مورد اطمینان بسازید. اگر از چندین سیم‌کارت استفاده می‌کنید و به طور متناوب سیم‌کارت‌ها را تغییر می‌دهید، می‌توانید همه‌ی سیم‌کارت‌ها را وارد لیست نمایید. در این حالت، در صورت تعویض سیم‌کارت‌های شما، گوشی شما قفل نخواهد شد.
- ممکن است به دلایل شغلی و یا دسترسی به شبکه‌های مختلف موبایل، بخواهید از چندین سیم‌کارت استفاده نمایید. برای مثال ممکن است به مکان‌های جغرافیایی مختلف (مثلاً کشورهای خارجی) سفر کنید و بخواهید از سیم‌کارت‌های محلی (همان کشور) برای ارتباط استفاده کنید، بنابراین نیاز به تعویض سیم‌کارت دارید.

برای افزودن سیم کارت به لیست سیم کارت‌های مورد اطمینان، پس از خاموش کردن دستگاه، سیم کارت جدید را درون گوشی قرار داده و سپس آن را مجدداً روشن نمایید تا پیغام افزودن به لیست سیم کارت‌های مورد اطمینان (Trusted SIMs list) نمایش داده شود، سپس سیم کارت را به لیست add (اضافه) کنید.



Lock on Airplane Mode (قفل شدن در حالت هواپیما)

با استفاده از این گزینه به محض فعال شدن حالت پرواز (flight) یا هواپیما (Airplane)، دستگاه به صورت خودکار قفل می‌شود. این ویژگی امنیت را هنگام سرقت یا گم شدن این گوشی (در صورت فعال کردن حالت هواپیما برای قطع ارتباط)، تامین می‌کند.

برای پیکربندی قفل شدن در حالت هواپیما، گام‌های زیر را دنبال نمایید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی Settings ضربه بزنید.
۳. اگر گزینه ضد-سرقت فعال نبود، گزینه Anti-Theft را تیک نمایید تا ویژگی امنیت شخصی فعال شود.
۴. بر روی عبارت Anti-Theft ضربه بزنید تا بتوانید ویژگی قفل شدن در حالت هواپیما را فعال کنید.
۵. بر روی عبارت Lock on Airplane Mode ضربه بزنید تا این گزینه فعال شود.

Track & Control Device (ردیابی و کنترل دستگاه)

با استفاده از این گزینه می‌توانید در صورت به سرقت رفتن و یا گم شدن دستگاه خود، آنرا ردیابی و کنترل کنید. امکان مکان‌یابی جغرافیایی (موقعیت موبایل بر روی نقشه)، قفل کردن و نیز پاک کردن کلیه اطلاعات شخصی از راه دور برای امنیت بیشتر وجود دارد. این ویژگی کمک می‌کند تا دوباره به دستگاه گم شده یا به سرقت رفته خود دست یابید.

برای تنظیم ردیابی و کنترل دستگاه، گام‌های زیر را دنبال نمایید:

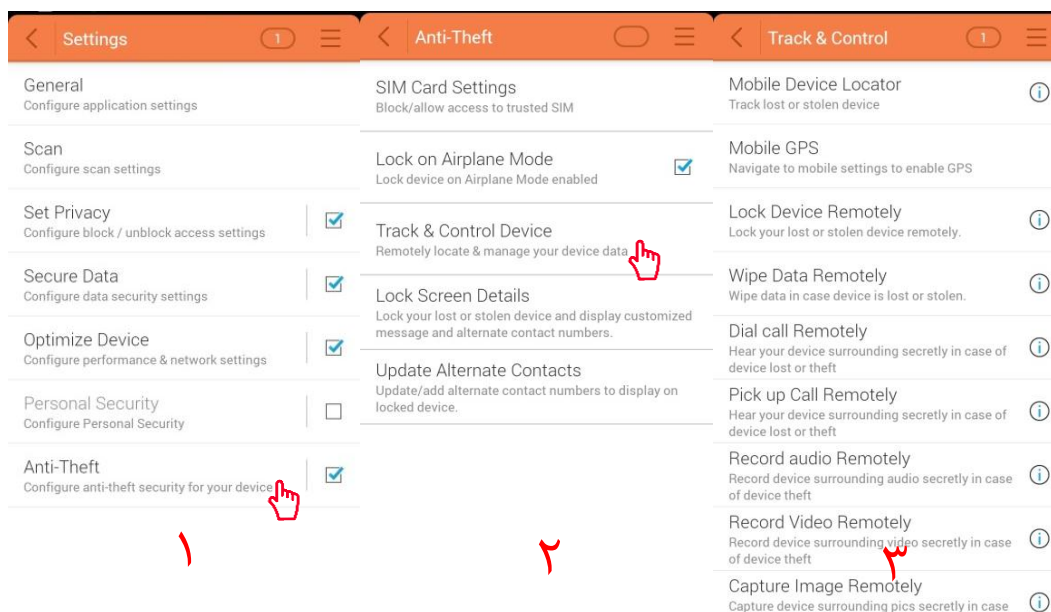
۱. برنامه Quick Heal Total Security را اجرا کنید.

۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه زده سپس بر روی **Settings** ضربه بزنید.

۳. اگر گزینه ضد-سرقت فعال نبود، گزینه **Anti-Theft** را تیک نمایید تا ویژگی امنیت شخصی فعال شود.

۴. بر روی عبارت **Anti-Theft** و سپس بر روی عبارت **Track & Control Device** ضربه بزنید.

شما می‌توانید با ارسال یک پیامک از گوشی دیگر، به شماره سیم‌کارت خود و با ارسال دستور به قالب شرح داده شده، اقدامات مختلفی را بر روی گوشی از راه دور انجام دهید. علاوه بر پیامک، ویژگی‌های جالبی از طریق پورتال مدیریت ابزار راه دور کوپیک هیل (RDM) نیز از طریق اینترنت بر روی هر دستگاهی (رایانه، موبایل ...) قابل اعمال می‌باشد. ویژگی‌های زیر ظاهر می‌شوند: در این بخش می‌توانید دستوراتی که برای اقدامات مختلف باید ارسال (SMS) شوند را مشاهده نمایید.



- **Mobile Device Locator**: می‌توانید موقعیت جغرافیایی دستگاه گم شده خود را رهگیری کنید. برای دریافت موقعیت مکانی دستگاه دستور زیر ارسال نمایید:

TRACE password

مثلاً اگر رمز عبور گوشی 123456 باشد یک پیامک به صورت زیر به موبایل گم شده ارسال می‌کنید:

TRACE 123456

- **Mobile GPS**: با استفاده از این گزینه می‌توانید GPS موبایل خود را روشن نمایید تا بتوانید موقعیت مکانی گوشی خود را رهگیری نمایید.

- **Lock Device Remotely**: کمک می‌کند تا در صورت مفقود شدن و یا دزدیده شدن دستگاه شما، آن را از راه دور قفل نمایید. همچنین این دستور مکان دستگاه و عکس‌هایی را از اطراف گوشی ارسال می‌کند. برای قفل کردن دستگاه دستور زیر ارسال نمایید:

BLOCK password

مثلاً: **BLOCK 123456**

اگر به اشتباه دستگاه را مسدود کردید و می‌خواهید قفل آن را باز کنید دستور زیر را ارسال کنید:

UNBLOCK password

مثلاً: UNBLOCK 123456

- **Wipe Data Remotely**: می‌توانید اطلاعات دستگاه مفقود شده خود را از راه دور پاک نمایید.

برای حذف کردن اطلاعات، دستور زیر را ارسال نمایید:

WIPE password

مثلاً: WIPE 123456

- **Dial Call Remotely**: با استفاده از این ویژگی می‌توانید به صورت مخفیانه و بی‌صدا از موبایل

مفقود شده خود به تلفن دیگری تماس برقرار نمایید. این گزینه به شما کمک می‌کند تا به

مکالمات و صداهای اطراف دستگاه مفقود شده خود گوش دهید. برای برقراری تماس از راه دور

دستور زیر ارسال نمایید:

CALL password

مثلاً: CALL 123456

- **Pickup Call Remotely**: با استفاده از این ویژگی می‌توانید به صورت مخفیانه و بی‌صدا به

محض برقراری تماس با موبایل مفقود شده خود، تماس پاسخ داده شود. این گزینه به شما کمک

می‌کند تا به مکالمات و صداهای اطراف دستگاه مفقود شده خود گوش دهید. برای پاسخ خودکار

به تماس از راه دور دستور زیر ارسال نمایید:

PICKUP password

مثلاً: PICKUP 123456

- **Record audio Remotely**: با استفاده از این ویژگی یک دقیقه از صدای اطراف دستگاه خود

به صورت مخفیانه ضبط شده و به فضای ابری (RDM) و ایمیل شما ارسال خواهد شد. این

گزینه به شما کمک می‌کند تا مکالمات و صداهای اطراف دستگاه مفقود شده خود را ضبط کنید.

برای ضبط از راه دور صدا دستور زیر ارسال نمایید:

AUDIO password

مثلاً: AUDIO 123456

- **Record Video Remotely**: با استفاده از این ویژگی یک دقیقه فیلم از اطراف دستگاه خود به

صورت مخفیانه ضبط شده و به فضای ابری (RDM) و ایمیل شما ارسال خواهد شد. این گزینه

به شما کمک می‌کند تا تصاویر و فیلم اطراف دستگاه مفقود شده خود را ضبط کنید. برای ضبط فیلم از راه دور دستور زیر ارسال نمایید:

VIDEO password

مثلاً: VIDEO 123456

- **Capture Image Remotely**. با استفاده از این ویژگی می‌توانید از اطراف دستگاه خود به صورت مخفیانه عکس گرفته و آنها را به فضای ابری (RDM) و ایمیل خود ارسال خواهد کنید. برای گرفتن عکس از راه دور دستور زیر ارسال نمایید:

PHOTO password

مثلاً: PHOTO 123456

- **Ring Device Remotely**. اگر فکر می‌کنید موبایل یا تبلت در نزدیکی شماست، می‌توانید مکان آن را با استفاده از پخش صدای زنگ (آژیر) بیابید. برای پخش از راه دور صدای زنگ دستگاه دستور زیر ارسال نمایید:

RING password

مثلاً: RING 123456

Lock Screen Details (اطلاعات صفحه نمایش در زمان قفل شدن)

زمانی که دستگاه شما قفل شد یک پیغام و شماره مخاطبین جایگزین (شماره دوست یا اعضای خانواده شما) بر روی صفحه نمایش دستگاه قفل شده نمایش داده می‌شود. یک پیغام پیش‌فرض از قبل بر روی کوپیک‌هیل وجود دارد اما شما می‌توانید آن را به صورت دلخواه تغییر دهید. مطمئن شوید که شماره‌های مخاطبین جایگزین را فعال کرده باشید تا بتوانید همه فعالیت‌هایی که بر روی دستگاه شما انجام می‌شود، با موفقیت ردیابی کنید.

Update Alternate Contacts (تغییر مخاطبین جایگزین)

شما می‌توانید شماره‌های مخاطبین جایگزین (شماره دوست یا اعضای خانواده شما) خود را تغییر داده و یا شماره تلفن جدیدی را به لیست مخاطبین جایگزین اضافه کنید تا در زمان قفل شدن بر روی صفحه نمایش دستگاه نشان داده شده و پیام‌هایی را از دستگاه گم (دزدیده) شده بر روی آن موبایل‌ها دریافت کنید. از ذخیره شدن شماره‌های مخاطبین جایگزین فعال مطمئن شوید.

راهنما (Help)

با استفاده از این گزینه، شما می‌توانید پرسش‌های متداول (FAQ) را خوانده، اطلاعات و شماره‌های تماس ما را مشاهده و در صورت نیاز کوپیک‌هیل را حذف نمایید.

برای مشاهده راهنما، گام‌های زیر را دنبال نمایید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن ) در بالا سمت راست ضربه بزنید.
۳. در بخش Help، می‌توانید بر روی هر یکی از گزینه‌های زیر ضربه بزنید:

Online Help (راهنمای آنلاین)

این بخش حاوی راهنمای آنلاین کوپیک‌هیل توتال سکیوریتی می‌باشد. اگر می‌خواهید اطلاعات بیشتری از ویژگی‌ها و نحوه پیکربندی تنظیمات برنامه کوپیک‌هیل داشته باشید این گزینه را انتخاب نمایید. ضربه بر روی Online Help شما را به وب‌سایت کوپیک‌هیل بخش راهنما هدایت خواهد کرد. (نیاز به اینترنت بر روی گوشی دارید).

FAQs (سوالات متداول)

این بخش حاوی پرسش‌های پرتکرار مربوط به کوپیک‌هیل توتال سکیوریتی می‌باشد. برای مشاهده سوالات متداول شما به وب‌سایت کوپیک‌هیل بخش سوالات متداول هدایت خواهد کرد. (نیاز به اینترنت بر روی گوشی دارید).

Contact Us (تماس با ما)

انواع روش‌ها جهت دریافت پشتیبانی در این بخش نشان داده می‌شود:

Live Chat (گفتگوی زنده)

برای دریافت پشتیبانی فنی آنلاین یا پاسخ به مسائل خود می‌توانید با کارشناسان فنی کوپیک‌هیل گفتگو نمایید. امکان گفتگوی زنده و فارسی با کارشناسان فنی شرکت فناوری ارتباطات و اطلاعات فانوس با مراجعه به وب‌سایت www.quickheal.co.ir و یا مشترکین جزیره امن www.42722.ir و کلیک بر روی گفتگوی زنده وجود دارد.

Web Support (گفتگوی زنده)

اگر سوال یا مشکلی دارید و می‌خواهید از طریق تیکت (ارسال پیام به سامانه پشتیبانی) ارتباط برقرار کنید، می‌توانید از سامانه پشتیبانی تحت وب دیدن نمایید. کارشناسان ما پاسخ مناسب را در کوتاه‌ترین زمان به شما ارائه می‌دهند.

همچنین امکان ایجاد تیکت و دریافت پشتیبانی فنی از طریق سامانه پشتیبانی شرکت فناوری ارتباطات و اطلاعات فانوس از طریق وبسایت support.quickheal.co.ir و برای مشترکین جزیره امن از طریق support.42722.ir نیز وجود دارد.

همچنین می‌توانید سوالات و مشکلات خود را از طریق ارسال ایمیل به آدرس support@quickheal.co.ir و یا مشترکین جزیره امن support@42722.ir مطرح نمایید تا در کوتاه‌ترین زمان، پاسخ به زبان فارسی برای شما ارسال گردد.

Support Center (مرکز پشتیبانی)

شما می‌توانید سوالات خود را با تماس شماره تلفن‌های درج شده در نرم‌افزار کوپیک هیل مطرح نمایید.
 مشتریان کوپیک هیل در ایران:

تماس با شماره ۰۱۱-۴۲۰۴۹۳۰۰ در ساعات ۹ تا ۱۶ روزهای شنبه تا پنج شنبه

مشتریان طرح جزیره امن کوپیک هیل:

تماس با شماره ۰۱۱-۴۲۷۲۲ در ساعات ۹ تا ۱۶ روزهای شنبه تا پنج شنبه

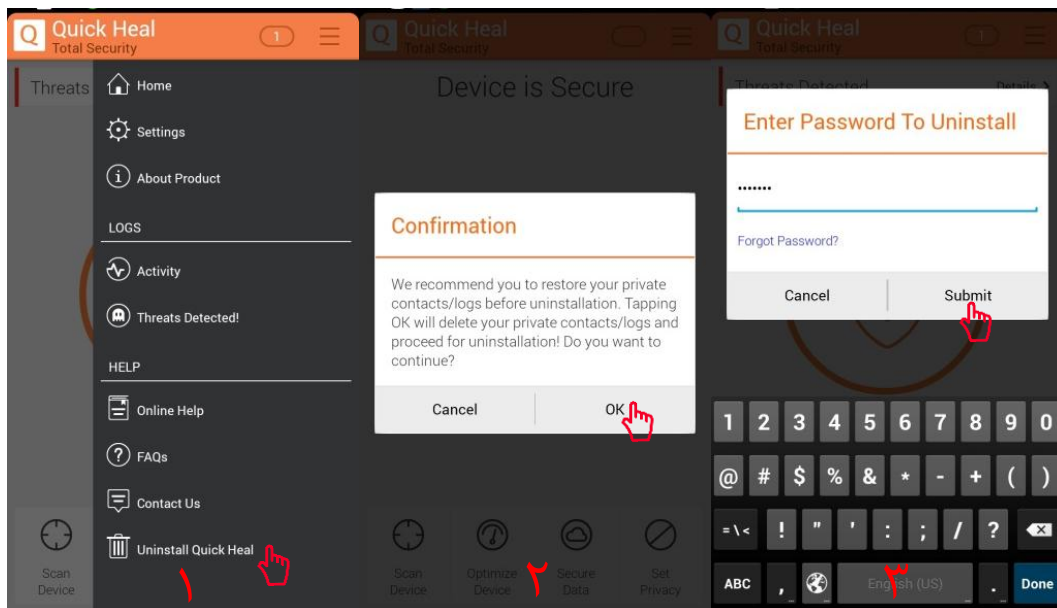
Uninstall Quick Heal Total Security (حذف کوپیک هیل توتال سکیوریتی)

حذف برنامه جامع امنیتی کوپیک هیل توتال سکیوریتی، دستگاه شما را در معرض تهدیدات ویروسی قرار می‌دهد. هرچند در مواردی اگر بخواهید دستگاه خود را تعویض کنید و یا آن را فرمت کنید، نیاز دارید تا کوپیک هیل را حذف نمایید.

برای حذف کوپیک هیل توتال سکیوریتی، گام‌های زیر را دنبال نمایید:

۱. برنامه Quick Heal Total Security را اجرا کنید.
۲. بر روی منوی اصلی (آیکن  در بالا سمت راست) ضربه بزنید.
۳. بر روی **Uninstall Quick Heal** ضربه بزنید.
- یک پیغام تایید حذف برنامه نمایش داده می‌شود.
۴. بر روی **OK** ضربه بزنید.
۵. رمز عبور کوپیک هیل را وارد کرده و بر روی **Submit** ضربه بزنید.

ابتدا لایسنس شما غیرفعال شده و سپس از شما تایید حذف (uninstallation) سوال می‌شود. اگر شما حذف برنامه را لغو کنید، آنتی‌ویروس شما غیرفعال خواهد شد اما از روی دستگاه شما حذف نخواهد شد. اگر بعداً به برنامه کوپیک‌هیل دسترسی داشتید، باید ابتدا آنرا فعال نمایید.



خاتمه

در کنار سه شعار اصلی هوشمندتر، سبک‌تر و سریع‌تر (smarter, lighter, faster) کوپیک‌هیل، که نمایانگر استفاده حداکثری از منابع می‌باشد، رعایت اصول سادگی، کاربرپسند در نصب، راه‌اندازی و مدیریت اندپوینت سکیوریتی کوپیک‌هیل یکی دیگر از مزایای کلیدی این آنتی‌ویروس نسبت به سایرین می‌باشد.

راه‌اندازی Update Server رسمی و Honeypot در ایران (ظرف عسل جهت جذب و آنالیز ویروس‌های منطقه‌ای ایران برای افزایش قدرت ویروس شناسی در ایران)، به همراه لابراتوارهای مجازی مستقر در انجین DNAScan در همه کلاینت‌ها از دیگر قابلیت‌های انحصاری این شرکت برای کاربران ایرانی جهت افزایش قدرت ویروس‌شناسی می‌باشد.

ارتباط مستقیم و مستمر و بدون واسطه تیم فنی و پشتیبانی شرکت تکنولوژی‌های کوپیک‌هیل هند با کاربران نهایی و نیز شرکت فناوری ارتباطات و اطلاعات فانوس به عنوان نماینده رسمی محصولات امنیتی در ایران موجب اطمینان خاطر کاربران از پشتیبانی بدون وقفه کوپیک‌هیل می‌گردد.

برای دریافت اطلاعات بیشتر از جوایز، تاییدیه‌ها، سایر محصولات و توانمندی‌های کوپیک‌هیل به وب‌سایت شرکت به نشانی www.quickheal.co.ir مراجعه و یا با شماره ۰۲۱-۷۷۱۴۲۵۲۶ تماس حاصل فرمایید.