



## نرم افزار

# SHATEL ANDROID SECURITY

راهکار امنیتی شاتل برای سیستم عامل اندروید



تاریخ تنظیم: آبان ۱۳۹۵

گروه شرکتهای شاتل

## فهرست مطالب

درباره نرم افزار SHATEL ANDROID SECURITY

راهنمای نصب نرم افزار

راهنمای استفاده از نرم افزار SHATEL ANDROID SECURITY

نحوه پاکسازی دستگاه از عوامل مخرب

بررسی تنظیمات مربوط به Monitoring

به روز رسانی نرم افزار

بررسی تنظیمات مربوط به PRIVAY CONTROL

بررسی تنظیمات مربوط به Theft protection

تغییر پسورد SHATEL ANDROID SECUEITY

بررسی تنظیمات URL FILTER

اطلاعات مربوط به SHATEL ANDROID SECURITY

به دست آوردن LOG از عملکرد نرم افزار

نصب و راه اندازی مجدد SHATEL ANDROID SECURITY

حذف SHATEL ANDROID SECURITY

پرسش های متداول در مورد نرم افزار

## درباره نرم افزار SHATEL ANDROID SECURITY

نرم افزار امنیتی SHATEL ANDROID SECURITY یک راهکار امنیتی قابل اطمینان برای استفاده بر روی دستگاه های اندرویدی است که با استفاده از آن می توانید دستگاه خود را از حملات احتمالی بدافزارها در فضای وب و در اپلیکیشن هایی که بر روی دستگاه خود نصب می کنید، محفوظ نگاه دارید.

در حال حاضر تلفن های همراه و تبلت ها به یکی از پرکاربردترین ابزارها برای استفاده کنندگان از دستگاه های دیجیتال تبدیل شده اند. این دستگاه ها حاوی مهم ترین و محرمانه ترین اطلاعات کاربران هستند که به سادگی می توانند مورد

دستبرد و سواستفاده و تهدید قرار گیرند. از همین رو حفاظت از اطلاعات موجود بر روی دستگاه های یاد شده به یکی از بزرگ ترین دغدغه های صاحبان آن ها تبدیل شده است

اگر در جست و جوی آخرین راه حل امنیتی برای دستگاه های اندرویدی خود (همچون موبایل و تبلت) هستید، نرم افزار حاضر مناسب ترین پاسخ برای نیازهای امنیتی شماست.

با استفاده از این نرم افزار می توانید با آسودگی خاطر از مرور صفحات وب بر روی دستگاه خود لذت ببرید و از اپلیکیشن های نصب شده با اطمینان بیش تری استفاده کنید.

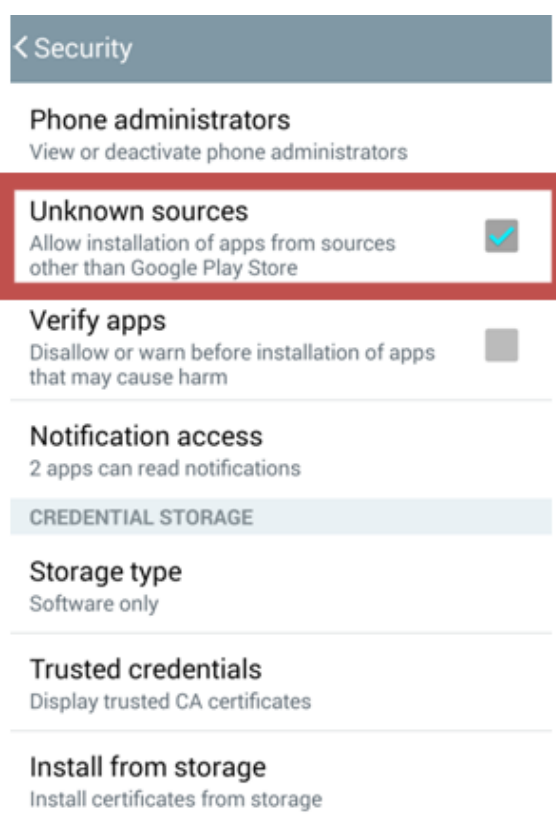
SHATEL ANDROID SECURITY هر آن چه را که برای حفاظت از اطلاعات و امنیت دستگاه اندرویدی خود نیاز دارید، در اختیارتان می گذارد و با پیچیده ترین بدافزارها و تهدیدهای اینترنتی مقابله می کند.

راهکار نرم افزاری SHATEL ANDROID SECURITY بدون تاثیر قابل توجه بر روی باتری و حافظه دستگاه، انواع بدافزارها و ویروس ها را شناسایی و از روی دستگاه حذف می کند. شما با خرید اشتراک یک ساله این نرم افزار، می توانید از همه امکانات آن شامل: شناسایی و حذف بدافزارها، حفاظت در مقابل دست بردهای اینترنتی، فیلترینگ وب و ... استفاده کنید.

## راهنمای نصب

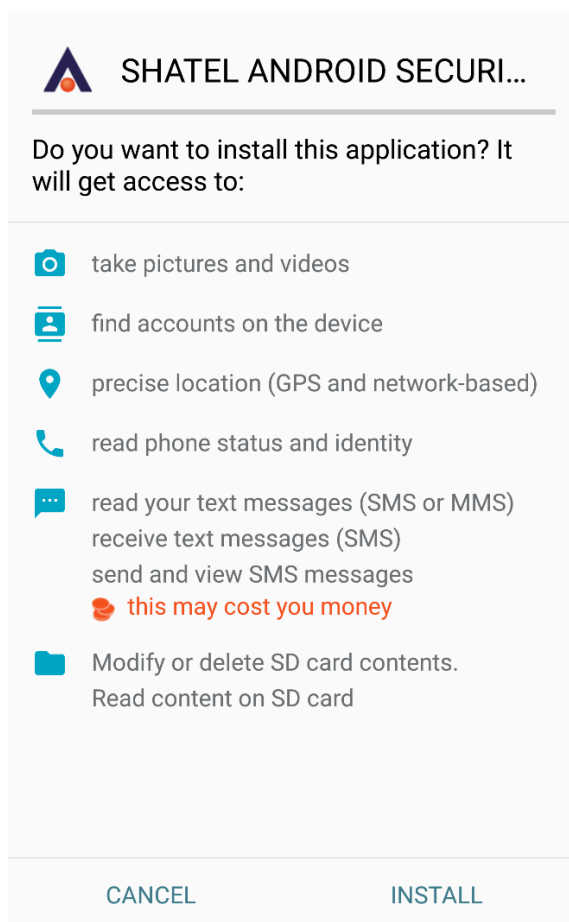
راهنمای پیش رو برای نصب و اجرای راهکار نرم افزاری SHATEL ANDROID SECURITY بر روی دستگاه‌های اندرویدی همچون موبایل و تبلت تهیه شده است. در صورت بروز هر گونه مشکل در اجرای برنامه می‌توانید با بخش پشتیبانی فنی این نرم افزار با شماره تلفن: ۲۳۰۸۹ تماس حاصل فرمایید و یا پرسش خود را با ارسال ایمیل به نشانی av@shatel.ir مطرح سازید.

نرم افزار SHATEL ANDROID SECURITY را از سایت مای شاتل [my.shatel.ir](http://my.shatel.ir) دریافت کنید، پیش از نصب نرم‌افزار، نیاز است وارد قسمت تنظیمات دستگاه خود شده و در قسمت Security گزینه Unknown Sources را فعال کنید تا نصب نرم‌افزار جدید بر روی دستگاه امکان‌پذیر شود.



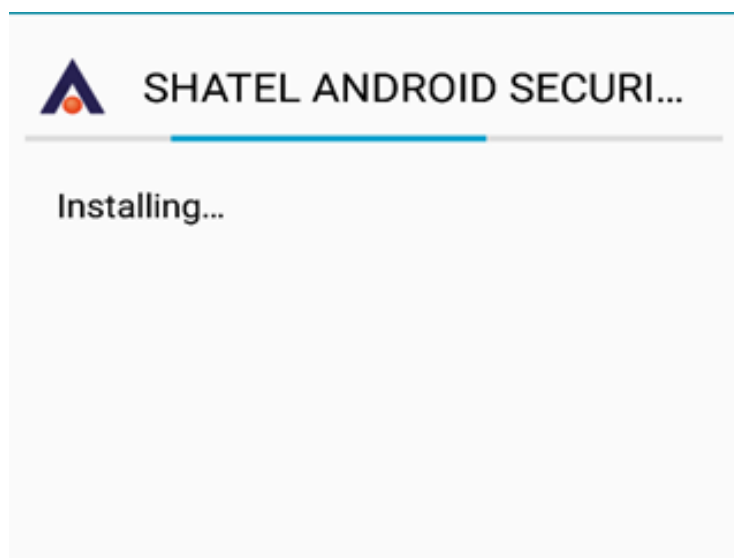
شکل ۱

بعد از دریافت فایل و اجرای آن، مطابق تصویر زیر صفحه ای نمایش داده می شود، برای نصب نرم افزار بر روی کلید Install کلیک کنید.



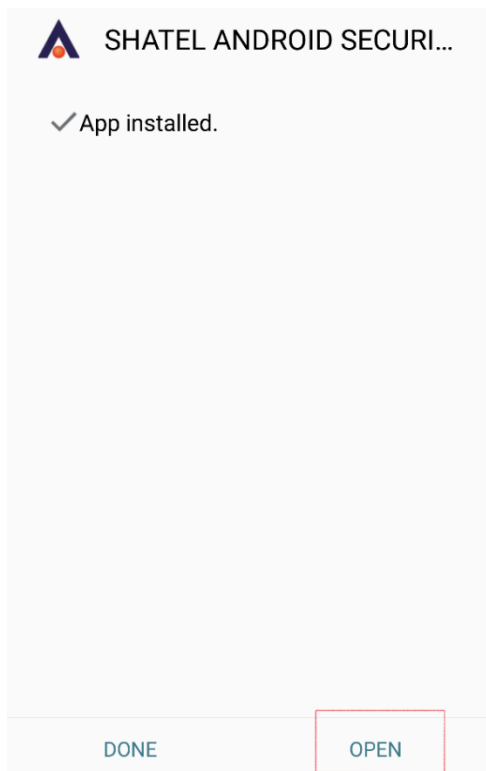
شکل ۲

با کلیک بر روی INSTALL نصب نرم افزار شروع شده و در حین نصب تصویر زیر نمایش داده خواهد شد



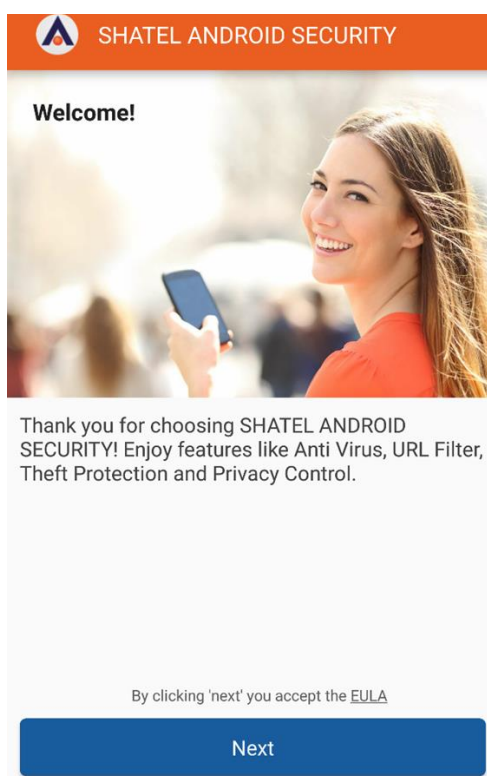
شکل ۳

بعد از نصب نرم افزار با کلیک بر روی OPEN نرم افزار اجرا خواهد شد.



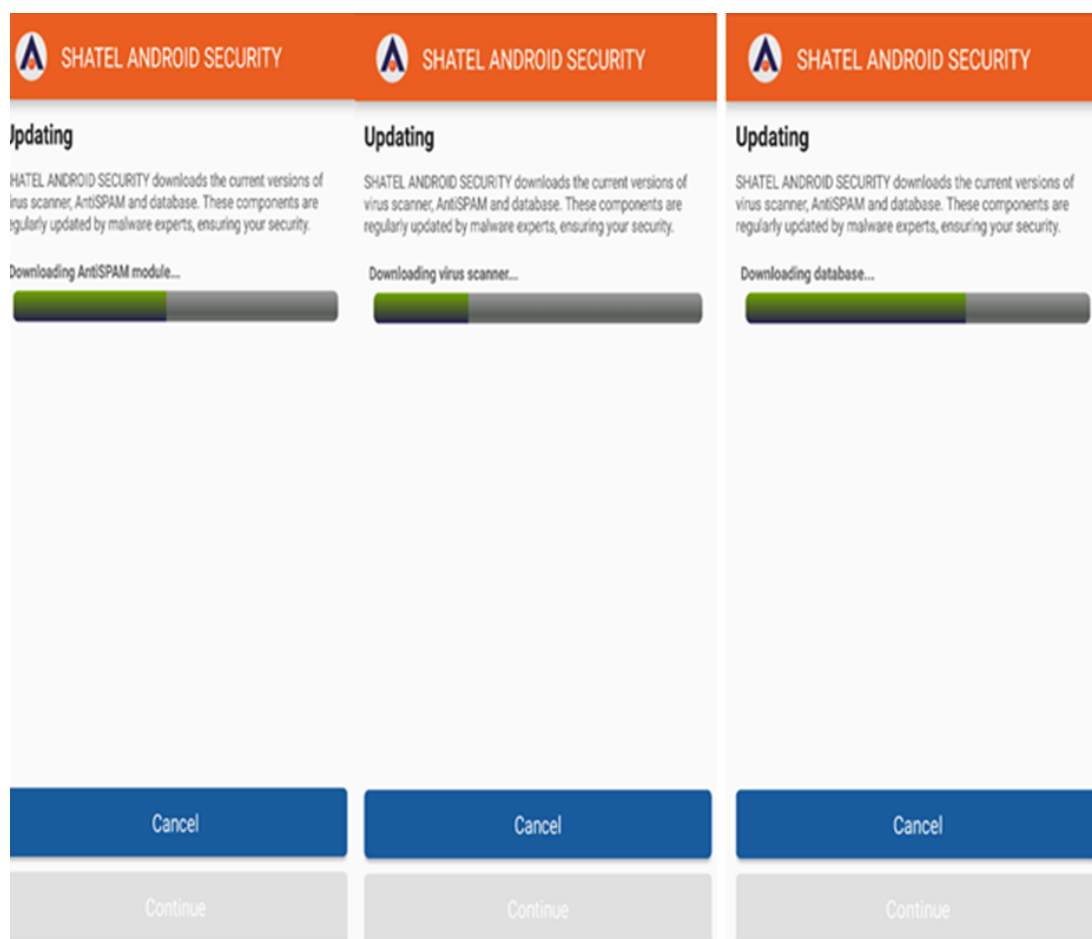
شکل ۴

سپس صفحه خوشامدگویی مطابق تصویر نمایش داده خواهد شد. بر روی Next کلیک کنید.



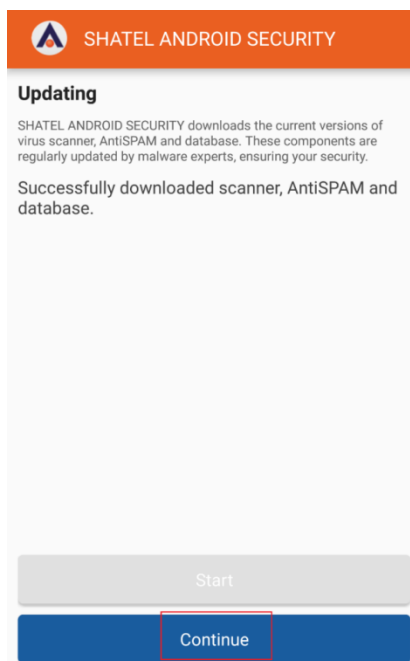
شکل ۵

در این مرحله پایگاه داده شناسایی ویروس‌ها و سایر بخش‌های نرم افزار مانند مازول های Anti spam و Virus scanner به روز رسانی می‌شود. توجه داشته باشید در این مرحله دستگاه شما باید به اینترنت وصل باشد. سرعت به روزرسانی به سرعت اینترنت شما بستگی خواهد داشت



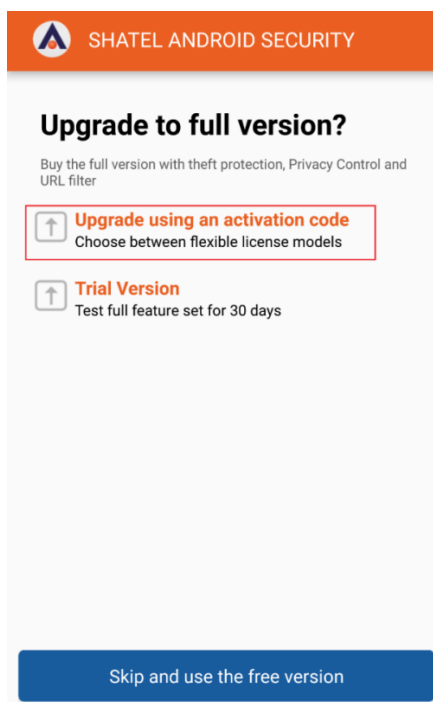
شکل ۶

پس از پایان یافتن به روز رسانی نرم افزار پیامی با مضمون موفقیت آمیز بودن عملیات نمایش داده می شود. با کلیک بر روی Continue وارد مرحله بعد شوید.



شکل ۷

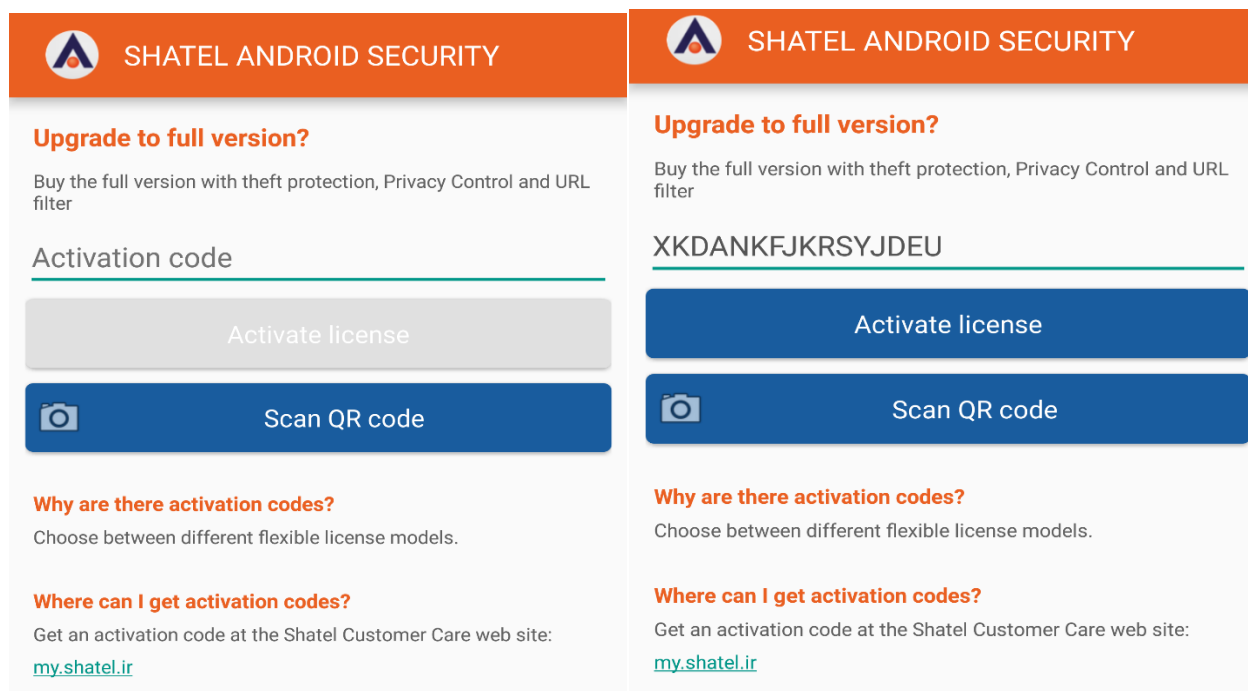
پس از خرید محصول از سایت [my.shatel.ir](http://my.shatel.ir) یک کد فعال سازی در اختیار شما قرار می گیرد، در این مرحله باید این کد را وارد کنید تا نسخه اشتراکی نرم افزار در اختیار شما قرار گیرد. برای وارد کردن این کد بر روی گزینه Upgrade using an activation code کلیک کنید.



شکل ۸

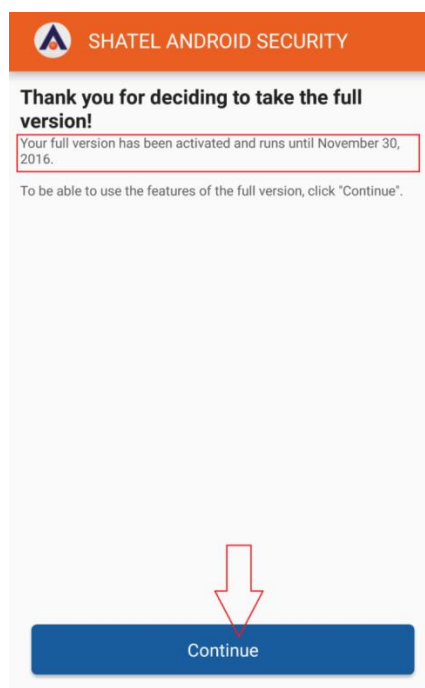


سپس مطابق تصویر با وارد کردن کد فعال سازی که با خرید نرم افزار به آدرس ایمیل شما ارسال می شود Activate license فعال شده و بر روی آن کلیک کنید.



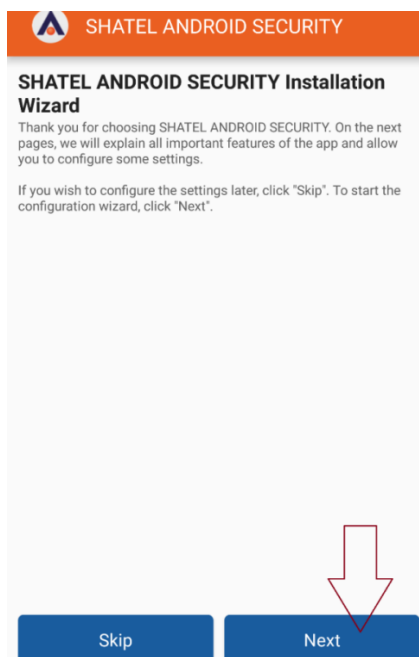
شکل ۹

پس از وارد کردن کد فعال سازی و کلیک بر روی Activate License نرم افزار فعال شده و تاریخی که اشتراک خریداری شده تا آن زمان اعتبار خواهد داشت، نمایش داده می شود. سپس بر روی Continue کلیک کنید.



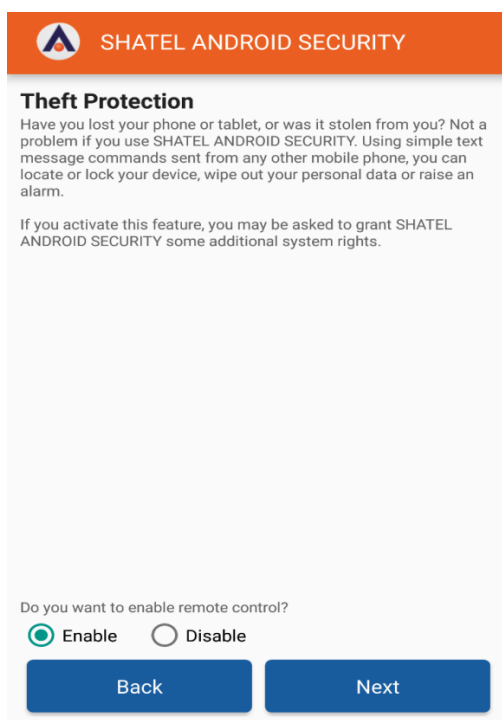
شکل ۱۰

با ورود به این مرحله شما قادر خواهید بود قابلیت های نرم افزار را مدیریت و برخی از آنها را فعال و یا غیر فعال کنید. برای شروع بر روی دکمه Next کلیک کنید.



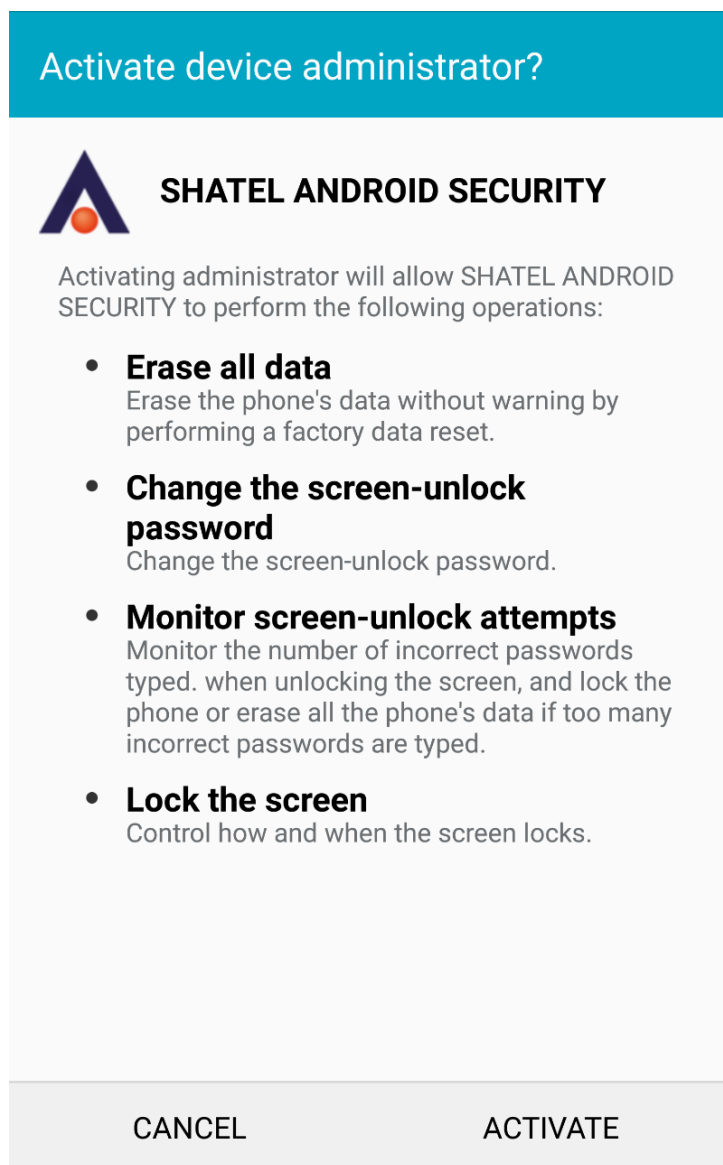
شکل ۱۱

در صورتی که مایل باشید از قابلیت محافظت در برابر سرقت دستگاه استفاده کنید، گزینه Enable را در این صفحه فعال سازید. توجه داشته باشید، با فعال کردن این قابلیت، شما قادر خواهید بود در صورت گم شدن یا دزدیده شدن دستگاه با ارسال پیامک به سیم کارت خود دستگاه را قفل کرده، اطلاعات شخصی خود را پاک کرده و یا از موقعیت مکانی دستگاه خود با خبر شوید.



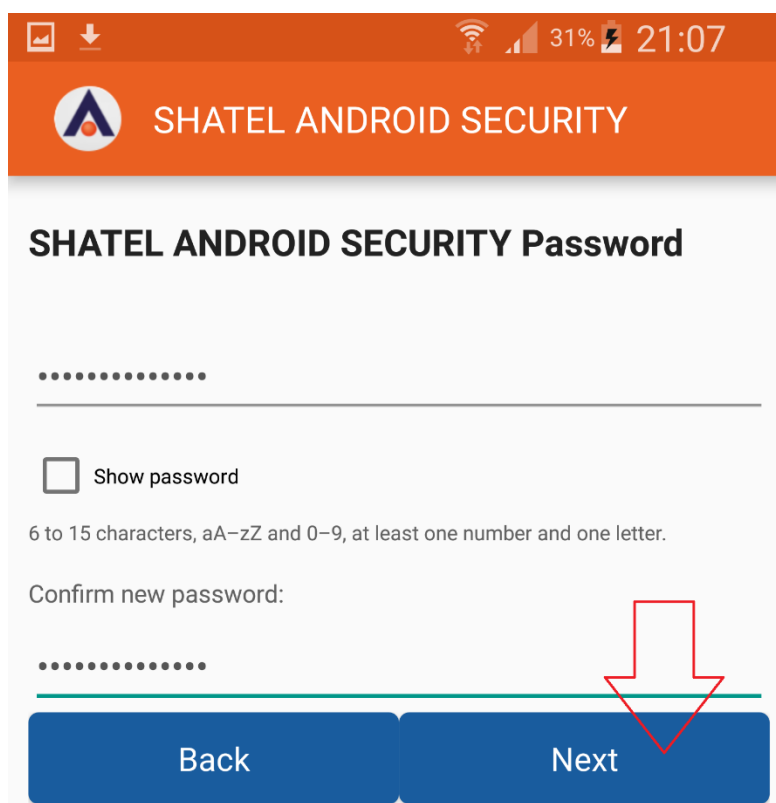
شکل ۱۲

پس از فعال کردن قابلیت Theft Protection باید به اپلیکیشن SHATEL ANDROID SECURITY ، دسترسی Phone Administrators داده شود و با توجه به تصویر زیر کافی است که بر روی گزینه Activate کلیک کنید.



شکل ۱۳

در این قسمت باید کلمه عبوری دلخواه بین ۶ تا ۱۵ کاراکتر شامل حرف و عدد وارد کنید، کوچک و بزرگ بودن حروف تاثیری ندارد ولی امکان استفاده از علائم برای تعریف کلمه عبور وجود ندارد. در نظر داشته باشید که در متن پیامک‌های ارسالی برای قفل کردن دستگاه، آگاه شدن از مکان دستگاه، پاک کردن اطلاعات دستگاه و یا ایجاد زنگ هشدار، هم چنین پاک کردن SHATEL ANDROID SECURITY از روی دستگاه خود از این کلمه عبور استفاده می کنید. در بخش Confirm Password بار دیگر پسورد را وارد و بر روی Next کلیک کنید.



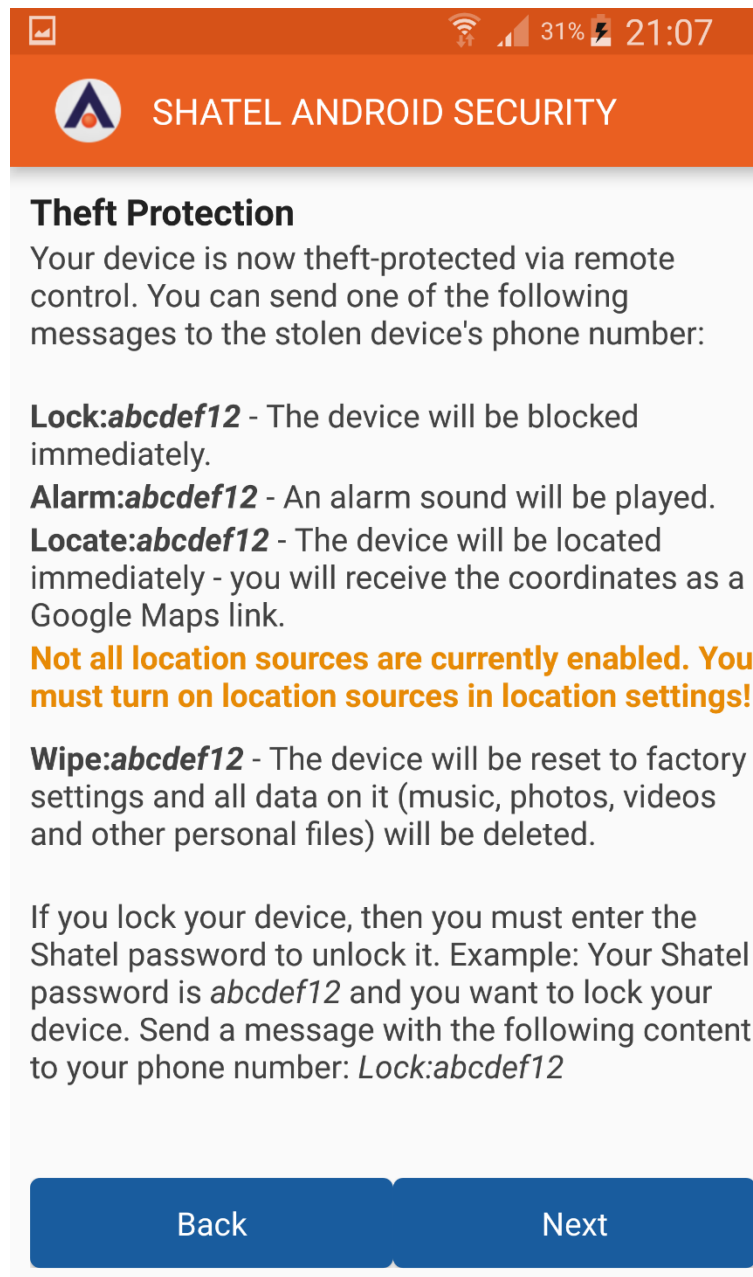
شکل ۱۴

اکنون قابلیت محافظت در برابر سرقت بر روی گوشی شما فعال شده است. برای مثال اگر پسوردی که شما در مرحله قبل وارد کردید abcdef12 باشد با ارسال هر کدام از متن‌های زیر به شماره تلفن همراه خود می‌توانید عملیات شرح داده شده در مقابل آن را انجام دهید:

- Lock:abcdef12: با ارسال این متن، دستگاه شما بی‌درنگ قفل می‌شود.
- Alarm:abcdef12: با ارسال این متن، آلام دستگاه شما پخش خواهد شد.
- Locate:abcdef12: با ارسال این متن موقعیت مکانی دستگاه شما بر روی Google Maps نمایش داده خواهد شد.

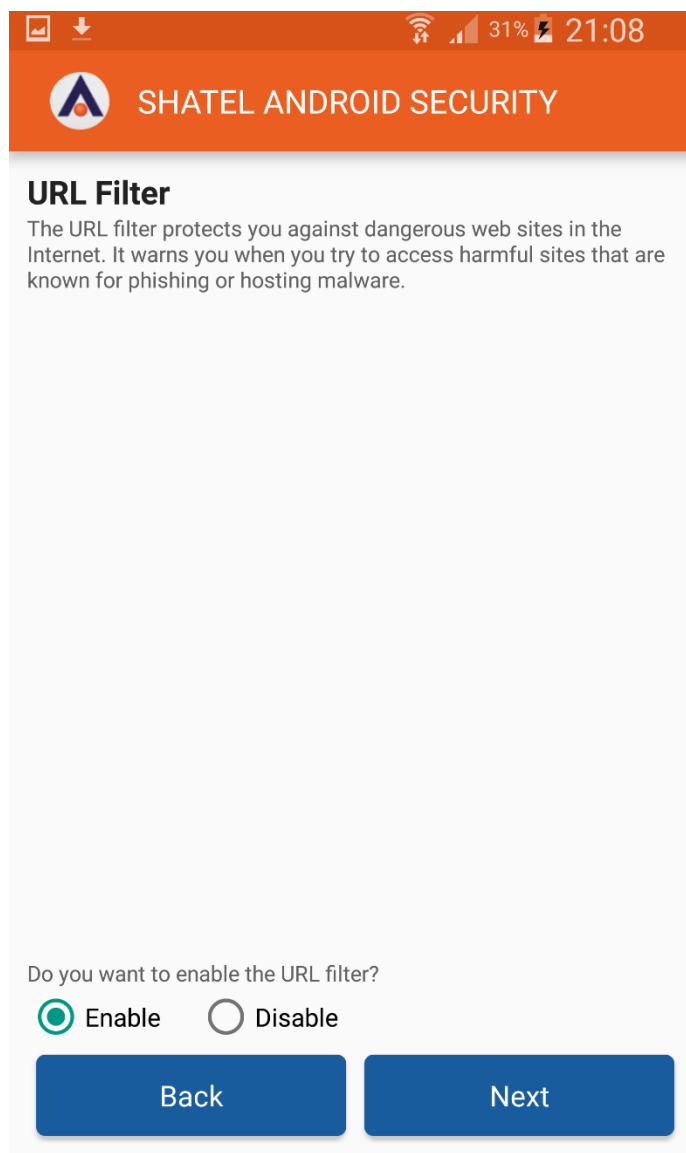
**نکته:** توجه داشته باشید که برای استفاده از این ویژگی باید GPS دستگاه فعال باشد.

- Wipe:abcdef12: در صورتی که این متن را ارسال کنید، دستگاه شما به تنظیمات اولیه ریست خواهد شد و تمامی عکس‌ها، ویدیوها و فایل‌های شخصی شما پاک خواهد شد.



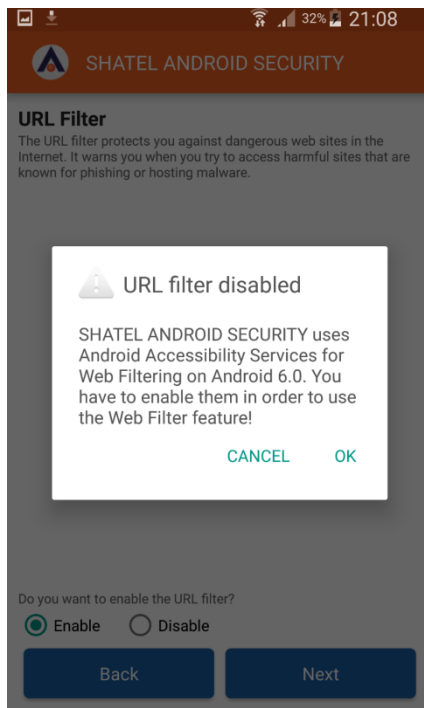
شکل ۱۵

برای استفاده از قابلیت URL Filter، Enable را فعال و سپس بر روی Next کلیک کنید. توجه داشته باشید در صورت فعال سازی این قابلیت دستگاه شما در مقابل سایت های آلوده و مخرب اینترنتی محفوظ می ماند و در صورتی که شما بخواهید سایتی آلوده به ویروس ها و تروجان ها را باز کنید به شما هشدار داده می شود.



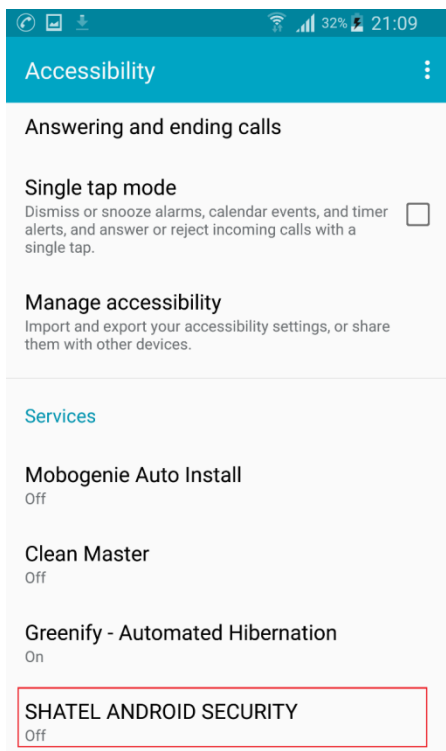
شکل ۱۶

در صورتی که دستگاه شما از اندروید نسخه 6.0 استفاده می کند هنگام فعال سازی قابلیت URL Filter با تصویر زیر مواجه خواهید شد.



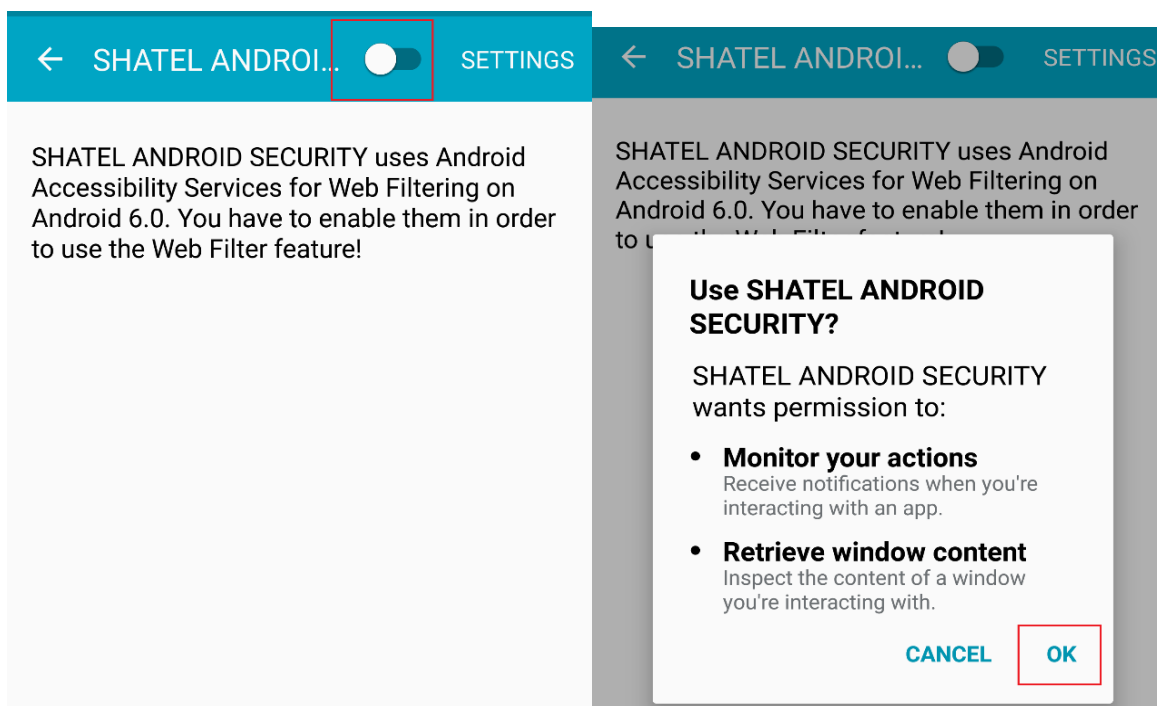
شکل ۱۷

با کلیک بر روی OK ، صفحه دسترسی بر روی دستگاه شما باز می شود. از قسمت سرویس ها، مطابق تصویر بر روی SHATEL ANDROID SECURITY کلیک کنید.



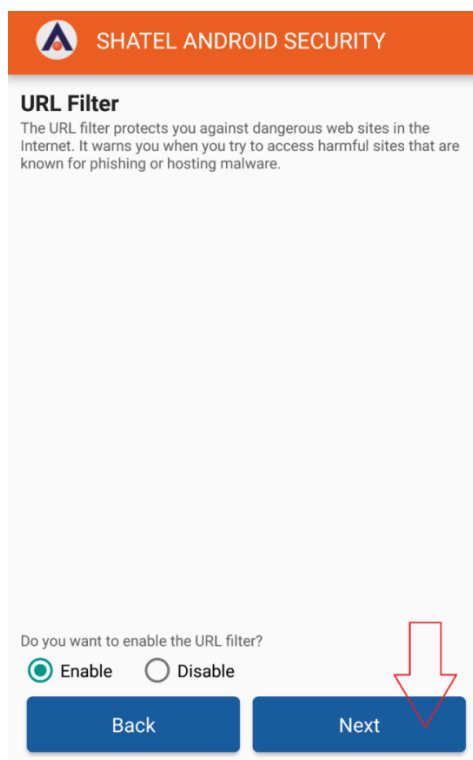
شکل ۱۸

با کشیدن دایره نشان داده شده در تصویر به سمت راست، و پس از آن کلیک بر روی **Ok**، دسترسی های لازم به SHATEL ANDROID SECURITY را برای فعال کردن قابلیت URL filter خواهید داد.



شکل ۱۹

سپس بر روی **Next** کلیک کنید.



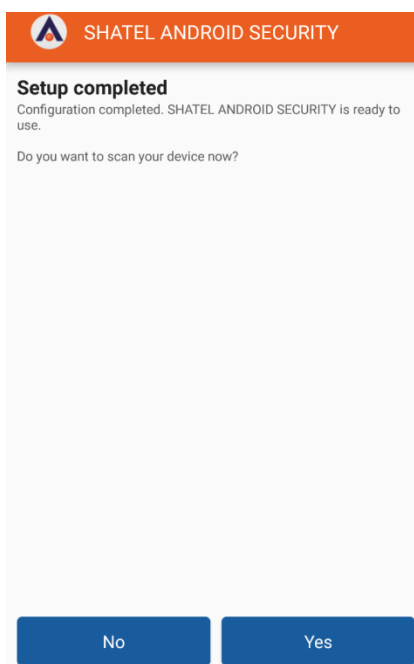
شکل ۲۰



## راهنمای استفاده از نرم افزار SHATEL ANDROID SECURITY

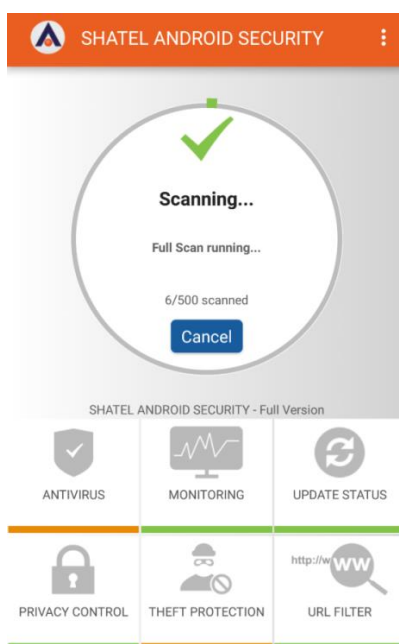
### نحوه پاکسازی دستگاه از عوامل مخرب:

اکنون نصب نرم افزار به پایان رسیده است و در صورتی که می‌خواهید دستگاه خود را برای پیدا کردن فایل‌ها و برنامه‌های مخرب اسکن کنید گزینه Yes را انتخاب کنید.



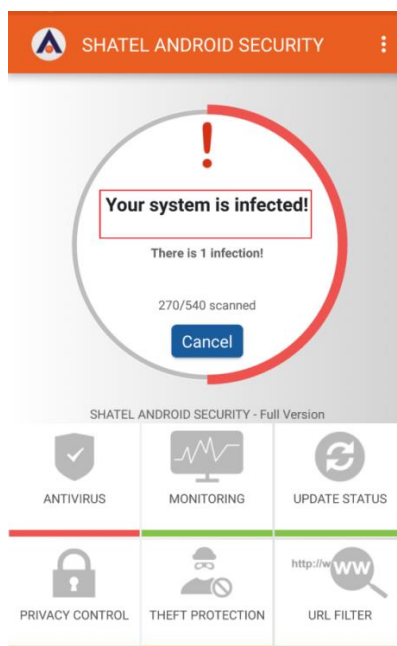
شکل ۲۱

بعد از کلیک بر روی Yes صفحه ای به شکل زیر نمایش داده می‌شود کمی صبر کنید تا اسکن دستگاه شما کامل شود.



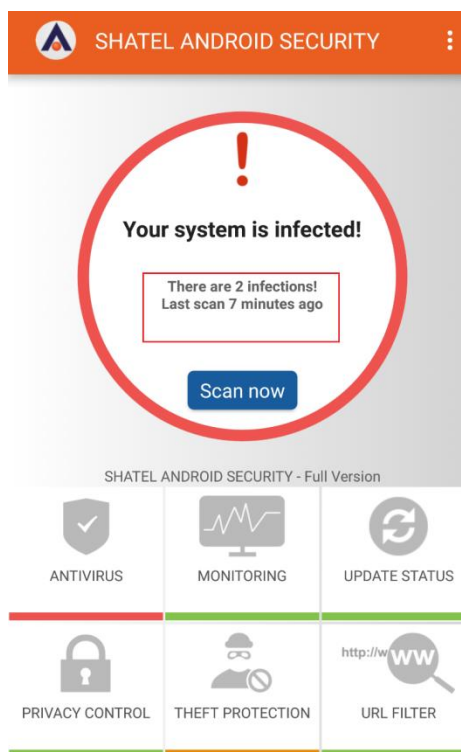
شکل ۲۲

در صورتی که دستگاه شما آلوده به ویروس و برنامه های مخرب باشد، پیغام **Your system is infected!** نمایش داده می شود.



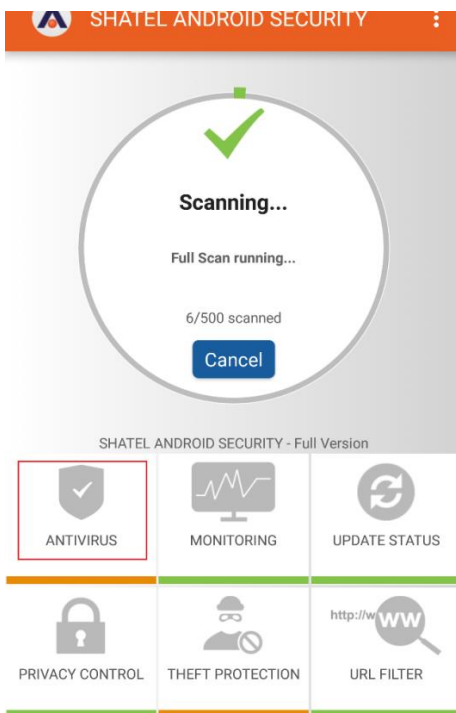
شکل ۲۳

پس از این که اسکن دستگاه کامل شد، تعداد برنامه های مخرب و ویروس هایی را که روی دستگاه شما شناسایی شده اند و هم چنین آخرین زمانی را که دستگاه اسکن شده است، مطابق تصویر مشاهده خواهید کرد.



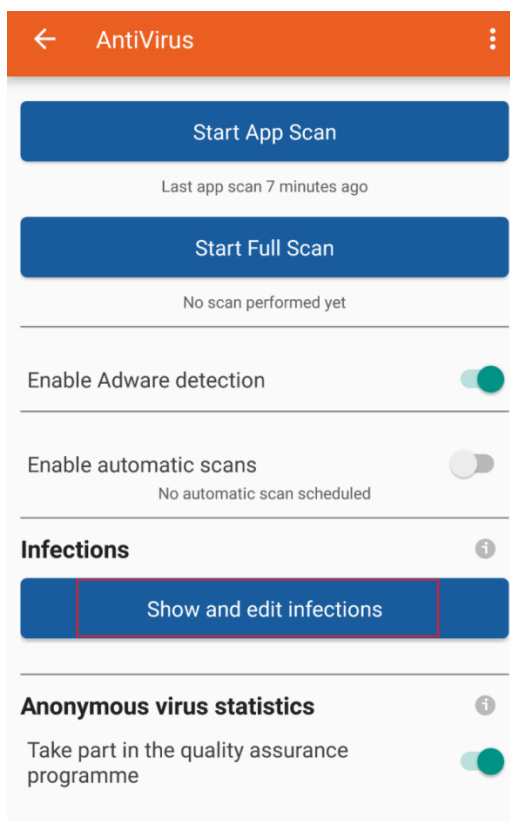
شکل ۲۴

سپس بر روی ANTIVIRUS کلیک کنید.



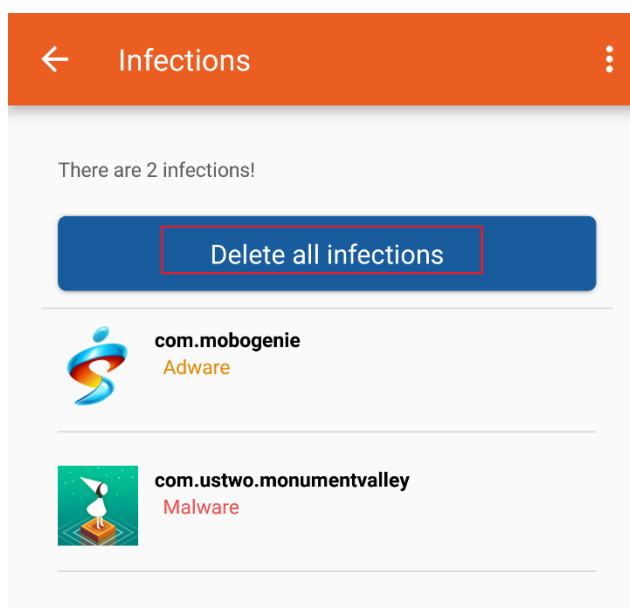
شکل ۲۵

در صفحه باز شده بر روی Show and edit infections کلیک کنید.



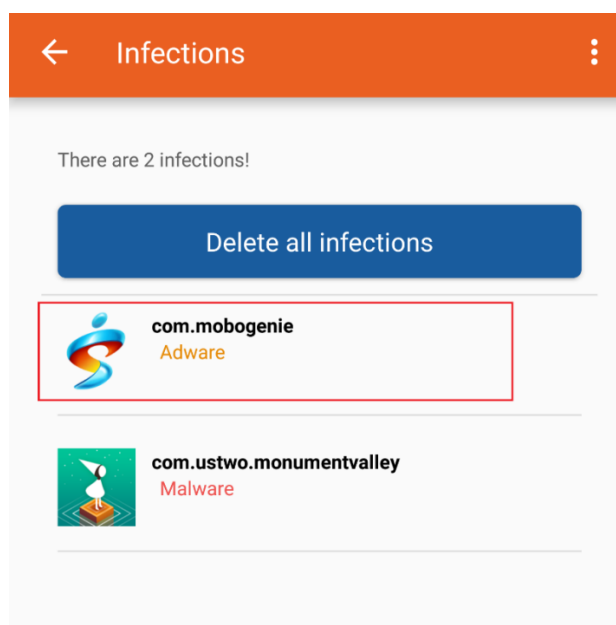
شکل ۲۶

مطابق تصویر لیستی از برنامه های مخرب نمایش داده می شود. توجه داشته باشید که SHATEL ANDROID SECURITY قادر به پاکسازی برنامه ها نمی باشد و در صورتی که مایل باشید دستگاه خود را از ویروس ها و عوامل مخرب پاکسازی کنید، باید برنامه های آلوده را پاک کرده و آنها را از یک منبع معتبر مانند Google play دانلود کنید. مطابق تصویر با کلیک بر روی Delete all infections تمام برنامه های آلوده که در لیست نمایش داده شده است از دستگاه شما حذف خواهد شد.



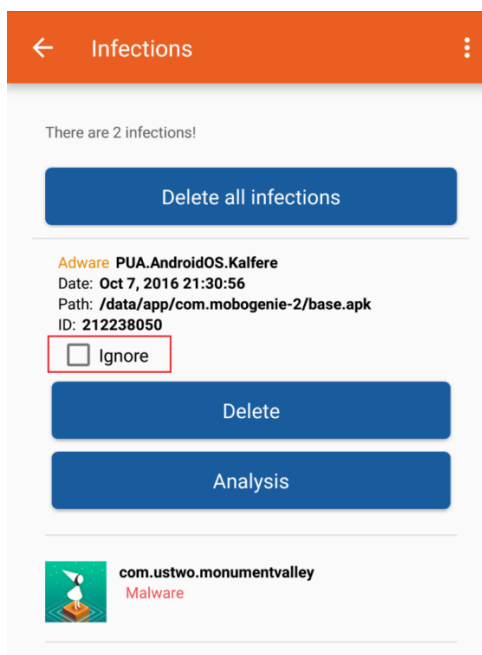
شکل ۲۷

در صورتی که تمایل داشته باشید برای هر برنامه ی مخرب شناسایی شده به صورت جداگانه تصمیم گیری کنید بر روی برنامه ی مورد نظر کلیک کنید



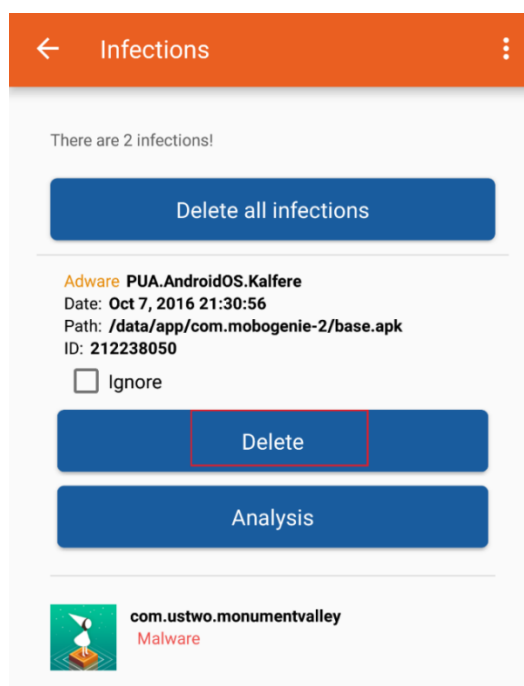
شکل ۲۸

در صورتی که بر روی Ignore کلیک کنید، SHATEL ANDROID SECURITY مخرب بودن آن را نادیده گرفته و درمورد این برنامه هشدار نمی دهد.



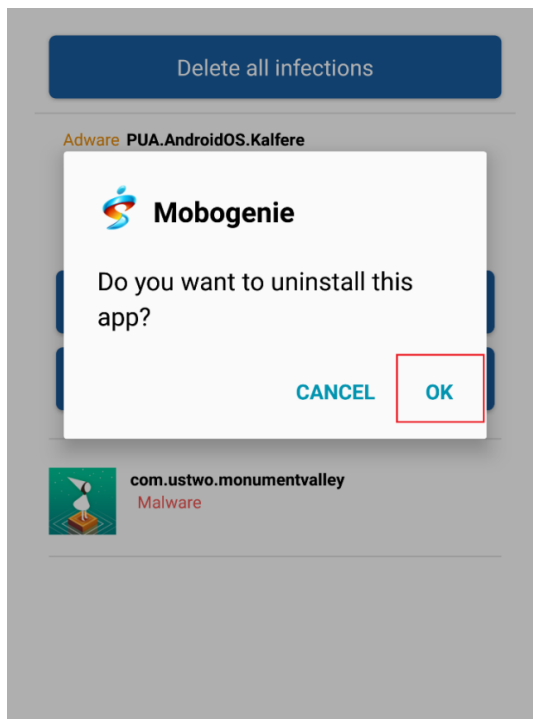
شکل ۲۹

در صورتی که بخواهید یکی از برنامه های مخرب را پاک کنید پس از کلیک بر روی برنامه، در صفحه باز شده بر روی Delete کلیک کنید.



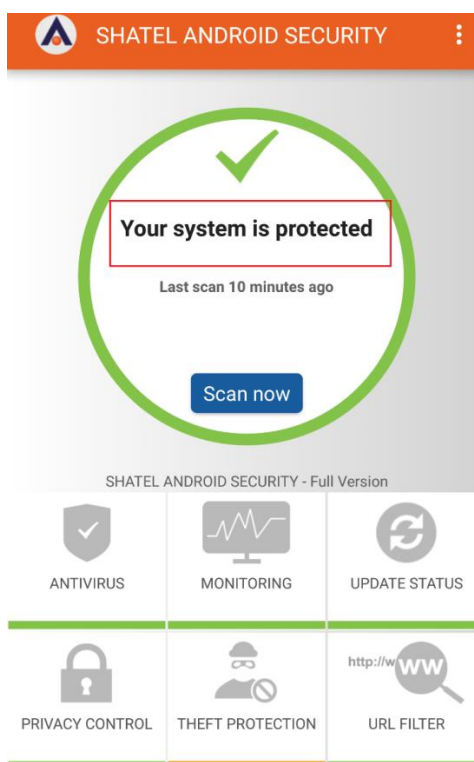
شکل ۳۰

سپس بر روی ok کلیک کنید.



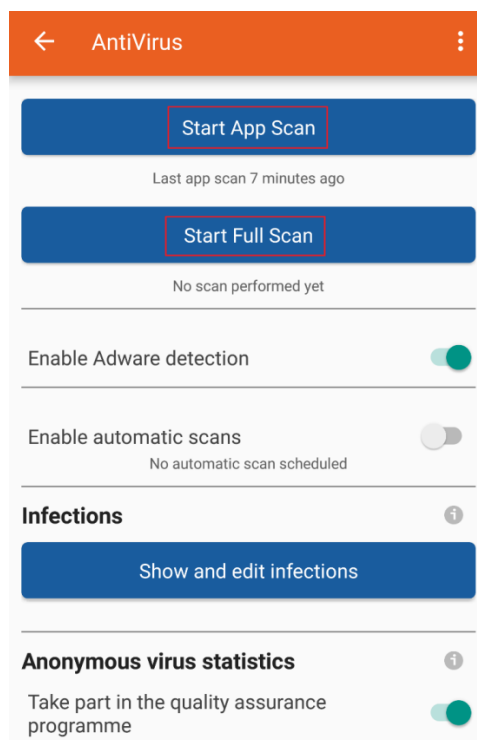
شکل ۳۱

در صورتی که دستگاه شما از برنامه های مخرب و ویروس ها پاکسازی شود یا بعد از اسکن هیچ گونه تهدید و یا عامل مخربی پیدا نشود، پیغام Your system is protected نمایش داده می شود.



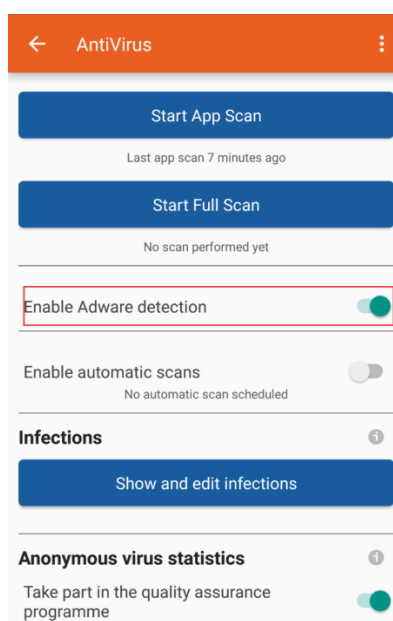
شکل ۳۲

هم چنین توجه داشته باشید هر زمان که نیاز به اسکن دستگاه خود دارید، می توانید پس از باز کردن SHATEL ANDROID SECURITY بر روی ANTIVIRUS کلیک کنید سپس با کلیک بر Start app scan می توانید برنامه های نصب شده بر روی دستگاه خود و یا با کلیک بر روی Start full scan تمامی فایل ها، برنامه و ... را اسکن نمایید.



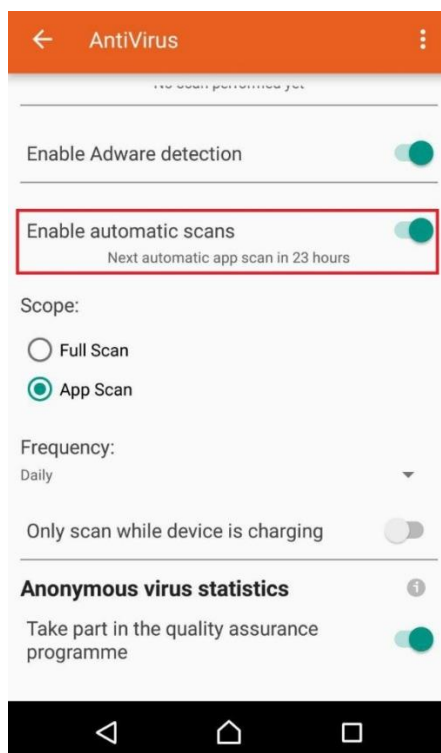
شکل ۳۳

در صورتی که مطابق تصویر Enable Adware detection فعال باشد، برنامه های تبلیغاتی نیز شناسایی می شوند.



شکل ۳۴

در نظر داشته باشید با فعال کردن Enable automatic scans و مشخص کردن محدوده اسکن دستگاه و بازه زمانی می‌توانید دستگاه خود را به صورت اتوماتیک اسکن کنید. در قسمت Scope محدوده اسکن دستگاه و در قسمت Frequency محدوده زمانی مشخص می‌شود. با توجه به تصویر زیر فقط برنامه‌های نصب شده بر روی دستگاه شما به صورت روزانه اسکن می‌شوند.

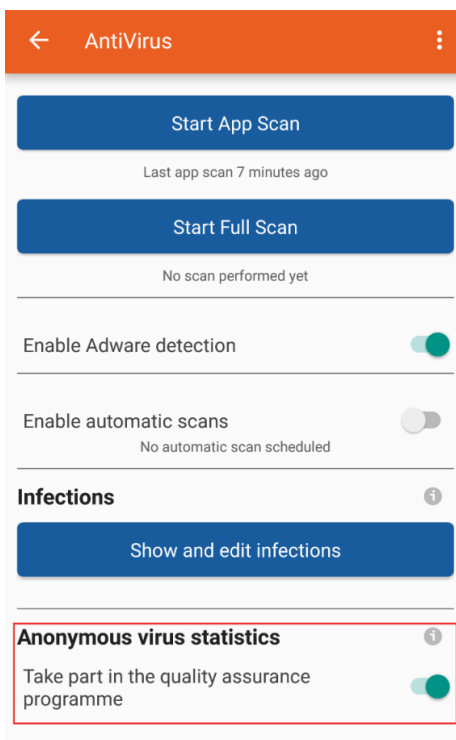


شکل ۳۵

در صورتی که Anonymous virus statistics اطلاعات مربوط به ویروس‌های ناشناخته که روی دستگاه شما شناسایی می‌شود به شرکت سازنده SHATEL ANDROID SECURITY ارسال شده و از این طریق شما در کارآمد کردن این نرم افزار مشارکت خواهید داشت.

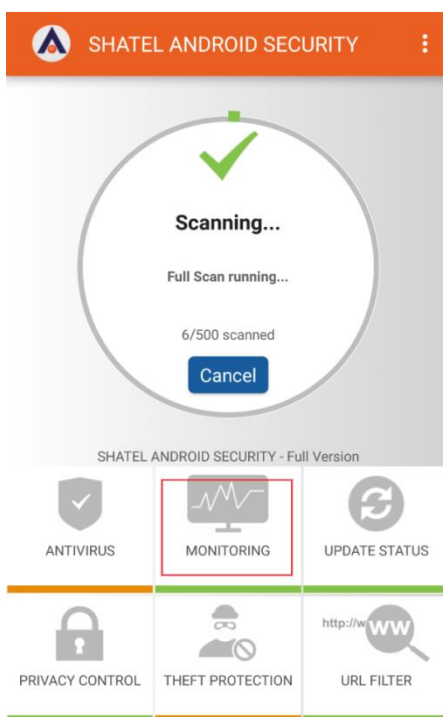


## بررسی تنظیمات مربوط به Monitoring :



شکل ۳۶

در صورتی که تمایل داشته باشید برنامه ها و یا فایل های موجود بر روی دستگاه شما به صورت لحظه ای مانیتور و بررسی شوند پس از باز کردن SHATEL ANDROID SECURITY بر روی Monitoring کلیک کنید.

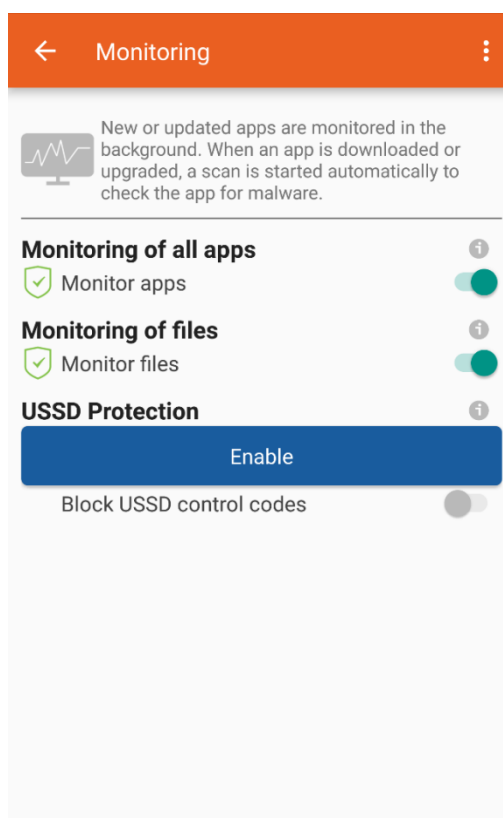


شکل ۳۷

مطابق تصویر زیر با فعال سازی **Monitoring of all apps** ، تنها برنامه ها در لحظه و پس از هر تغییر به عنوان مثال بعد از دانلود و یا به روز رسانی ، اسکن و بررسی می شوند.

در صورت فعال کردن **Monitoring of files** نیز ، فایل های موجود بر روی کارت حافظه یا حافظه داخلی دستگاه به عنوان مثال فایل هایی که از اینترنت دریافت می کنید، به صورت لحظه ای مانیتور و بررسی خواهند شد.

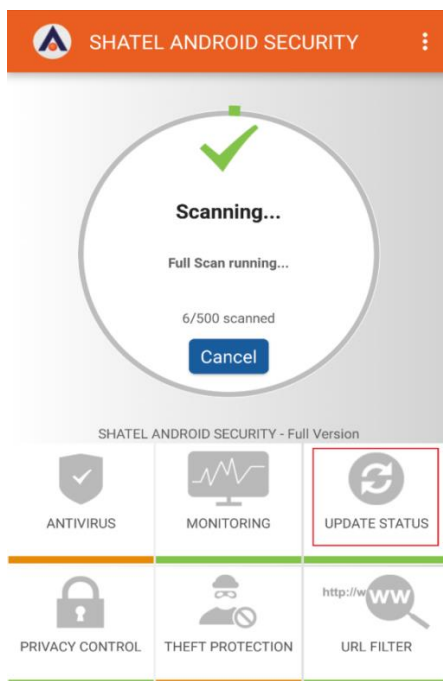
هم چنین با فعال سازی **USSD protection** دستگاه شما از کدهای اجرایی (کدهایی که با × شروع و به # ختم می شوند) که مخرب هستند و یا باعث آسیب رساندن به دستگاه شما می شود محافظت می شود.



شکل ۳۸

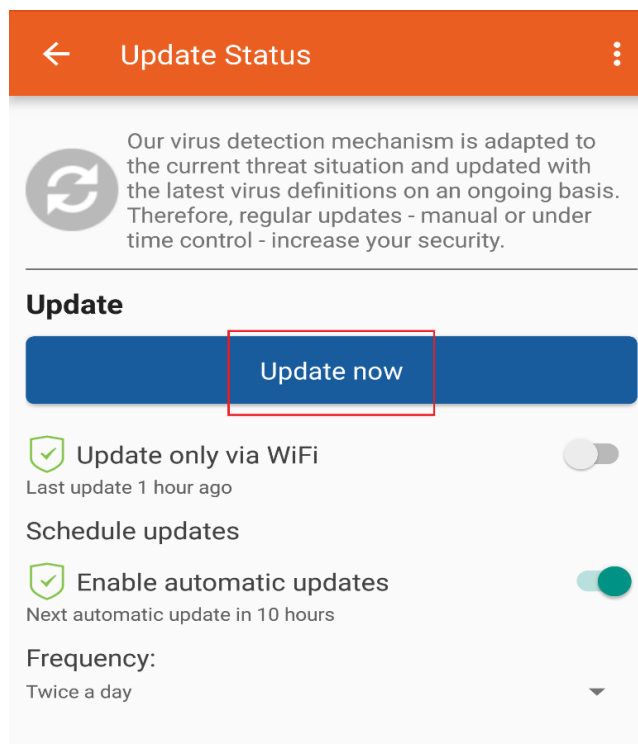
### به روز رسانی نرم افزار:

برای بررسی تنظیمات مربوط به بروز رسانی نرم افزار پس از باز کردن آن، بر روی UPDATE STATUS کلیک کنید.



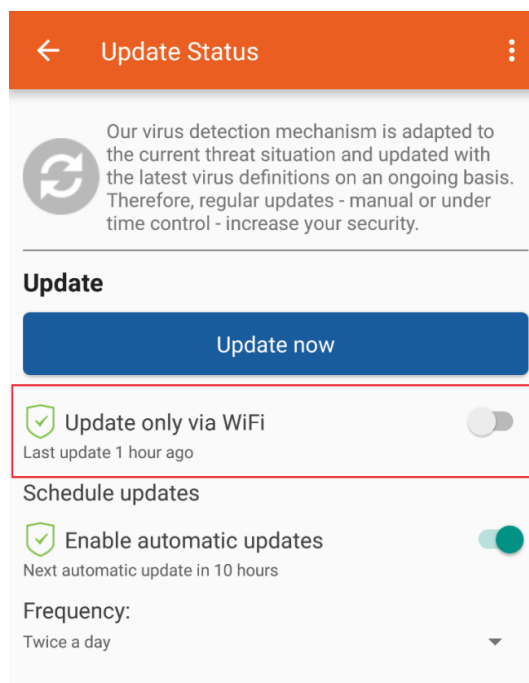
شکل ۳۹

در صورتی که بر روی کلید Update now کلیک کنید نرم افزار شروع به بروز رسانی می کند.



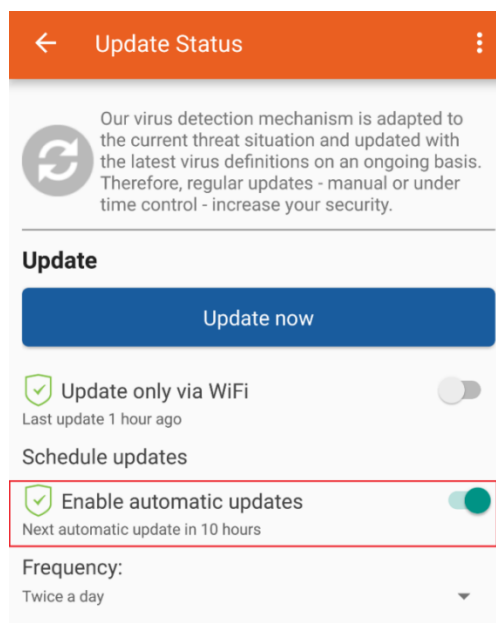
شکل ۴۰

توجه داشته باشید اگر گزینه Update only via WiFi روشن باشد، تنها در زمانی که دستگاه شما به WiFi متصل باشد نرم افزار بروز رسانی می شود. به صورت پیش فرض این گزینه خاموش می باشد، به این معنا که هر زمان دستگاه به اینترنت متصل باشد (WiFi, 4G, ...) فایل های مورد نیاز جهت بروز رسانی دریافت می شود.



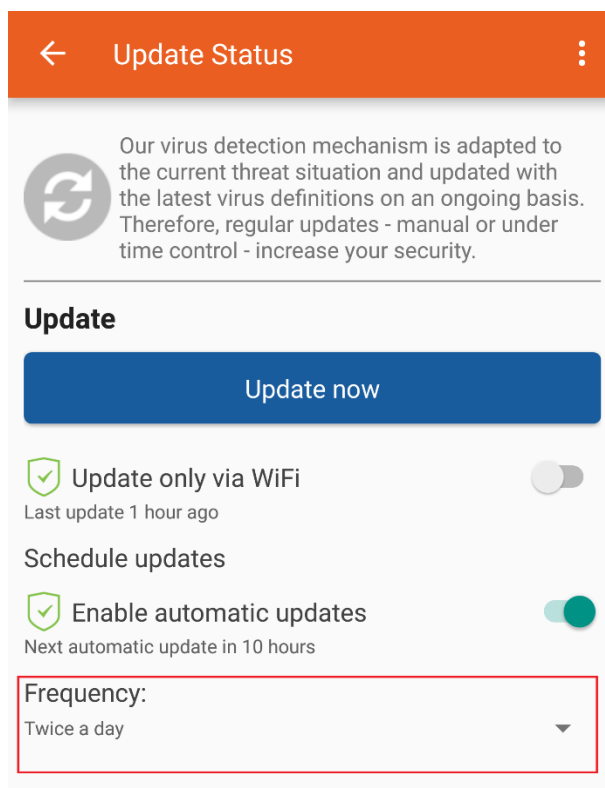
شکل ۴۱

با فعال کردن گزینه Enable automatic updates و مشخص کردن محدوده زمانی، بروز رسانی نرم افزار به صورت اتوماتیک انجام خواهد گرفت.



شکل ۴۲

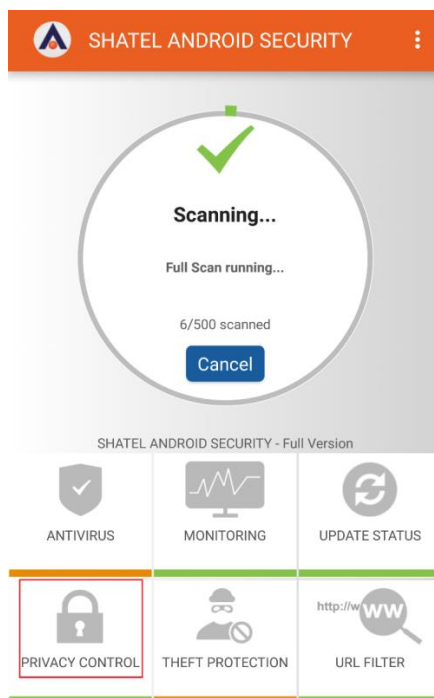
در قسمت Frequency می توان محدوده زمانی را برای بروز رسانی کردن نرم افزار ، مشخص کرد. مطابق تصویر زیر نرم افزار به صورت اتوماتیک روزی دوبار آپدیت خواهد شد.



شکل ۴۳

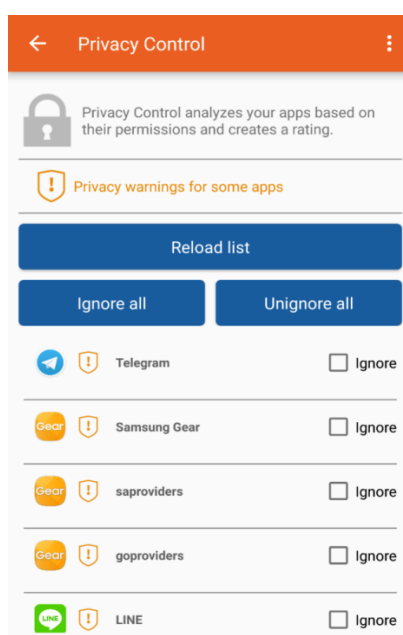
## بررسی تنظیمات مربوط به PRIVACY CONTROL:

قابلیت PRIVACY CONTROL در نرم افزار SHATEL ANDROID SECURITY این امکان را فراهم می کند تا دسترسی های مربوط به برنامه های نصب شده را روی دستگاه خود مشاهده کنید. برای استفاده از این قابلیت پس از باز کردن نرم افزار بر روی PRIVACY CONTROL کلیک کنید.



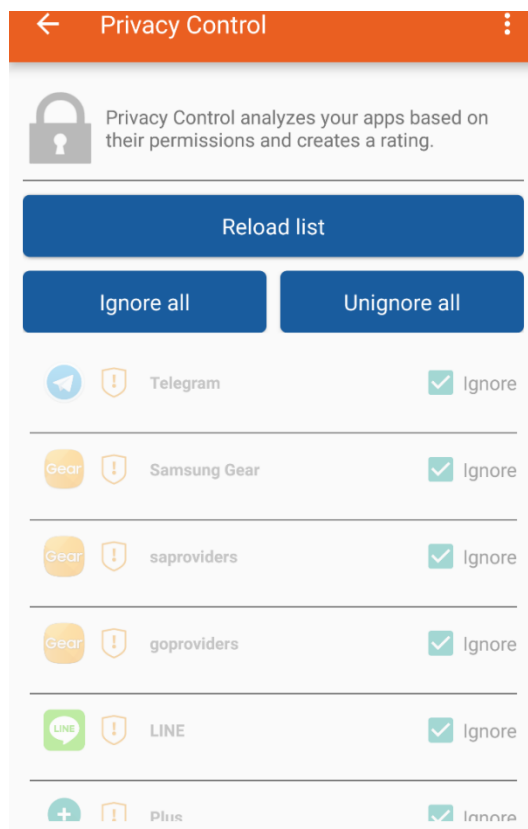
شکل ۴۴

مطابق تصویر لیست برنامه های نصب شده را بر اساس دسترسی های آن ها مشاهده خواهید کرد.



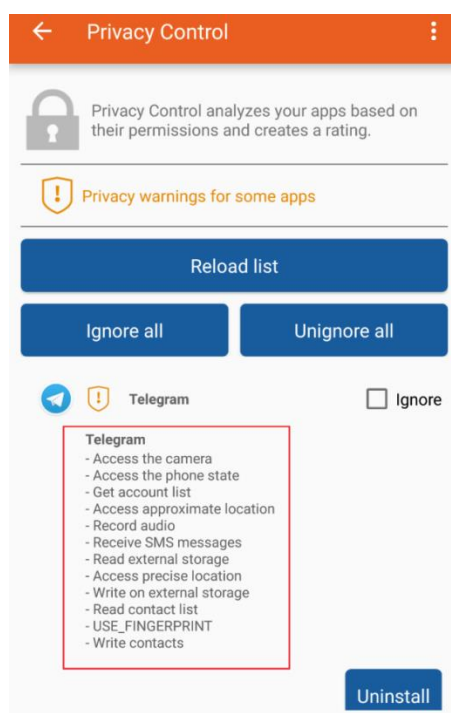
شکل ۴۵

اگر بر روی Ignore all کلیک کنید همه ی دسترسی های مربوط برنامه های لیست شده نادیده در نظر گرفته می شوند.



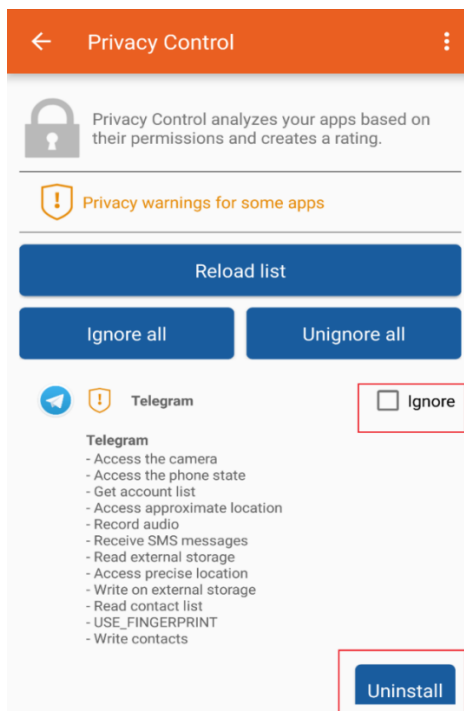
شکل ۴۶

برای مشاهده دسترسی هایی که یک برنامه خاص موجود در لیست دارد بر روی آن کلیک کنید، در این جا با کلیک بر روی برنامه تلگرام دسترسی های مربوط به آن را مشاهده خواهید کرد .



شکل ۴۷

در صورتی که بر روی Ignore کلیک کنید فقط دسترسی های مربوط به این برنامه نادیده گرفته می شود و با کلیک بر روی Uninstall این برنامه به صورت کلی از روی دستگاه شما پاک می شود.

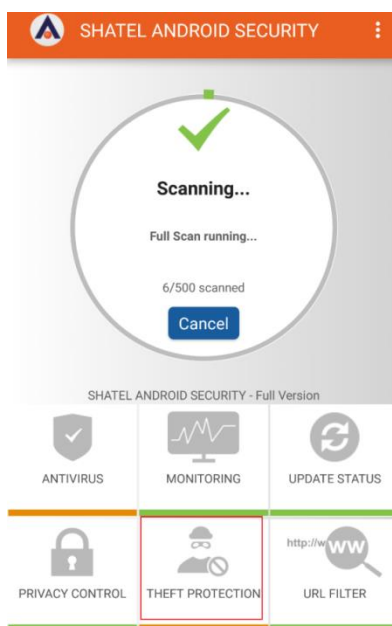


شکل ۴۸



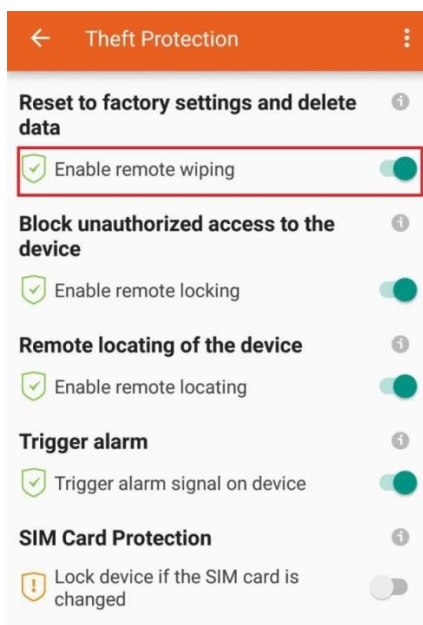
## بررسی تنظیمات مربوط به Theft protection :

برای بررسی تنظیمات مربوط به قابلیت Theft Protection و تغییر پسورد SHATEL ANDROID SECURITY، پس از باز کردن نرم افزار بر روی THEFT PROTECTION کلیک کنید. همانطور که می دانید از جمله امکاناتی که قابلیت PROTECTION THEFT در اختیار شما می گذارد قفل کردن دستگاه و ایجاد صدای هشدار و پاک کردن اطلاعات ذخیره شده درون دستگاه شما از راه دور ، و هم چنین قفل شدن دستگاه در صورت تعویض سیم کارت می باشد.



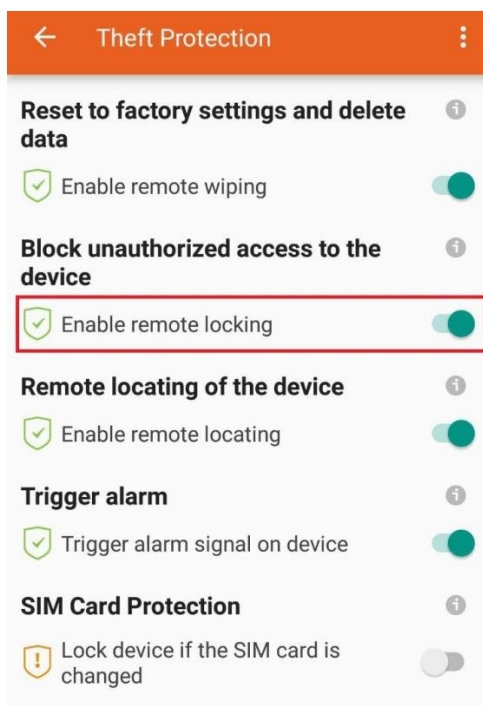
شکل ۴۹

با فعال کردن Enable remote wiping این امکان را خواهید داشت که از راه دور دستگاه خود را به تنظیمات کارخانه ریست کرده و تمام اطلاعات شخصی خود را که بر روی حافظه دستگاه ذخیره شده اند پاک کنید



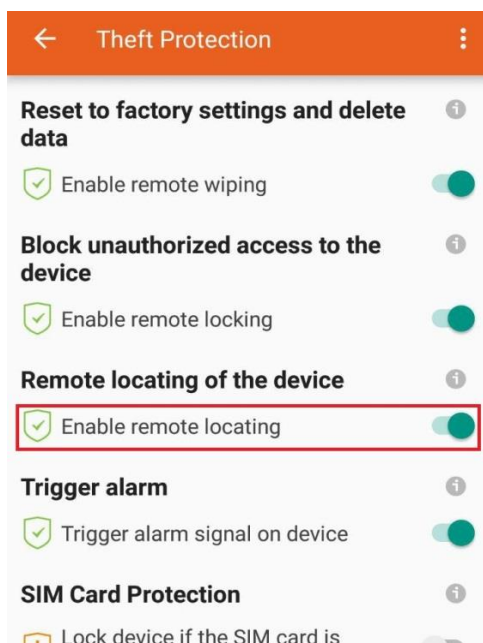
شکل ۵۰

با فعال کردن Enable remote locking، می توانید دستگاه خود را از راه دور قفل کرده و مانع دسترسی افراد ناخواسته شوید.



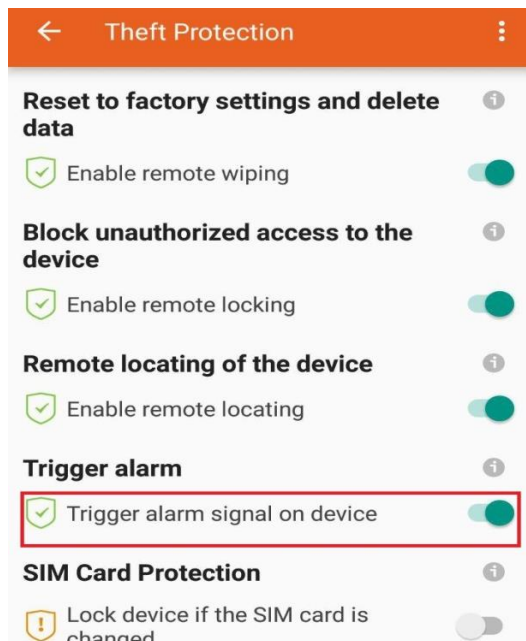
شکل ۵۱

در صورتی که Enable remote locking را فعال کنید می توانید از مکان دستگاه خود آگاه شوید، همان طور که قبلا اشاره شد لازم است حتما Gps دستگاه خود را روشن کرده باشید.



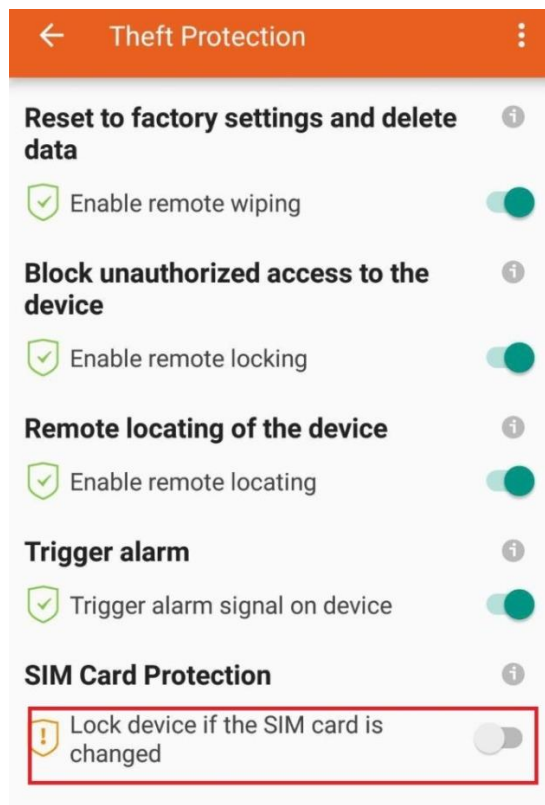
شکل ۵۲

فعال بودن Trigger alarm امکان هشدار دادن دستگاه را از راه دور فراهم می کند.



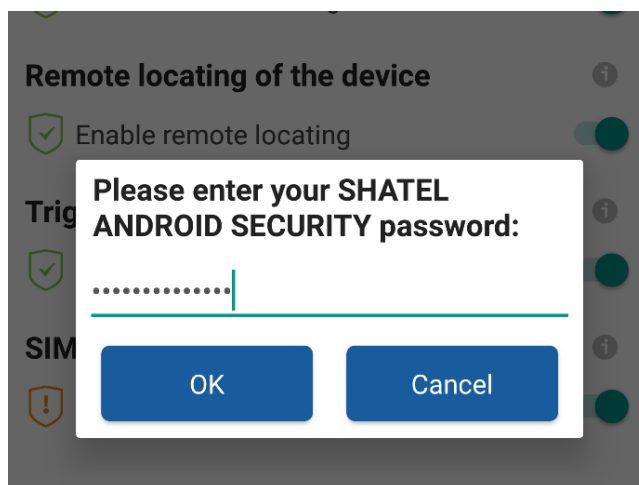
شکل ۵۳

با فعال سازی SIM Card protection در صورت تغییر سیم کارت دستگاه شما قفل می شود.



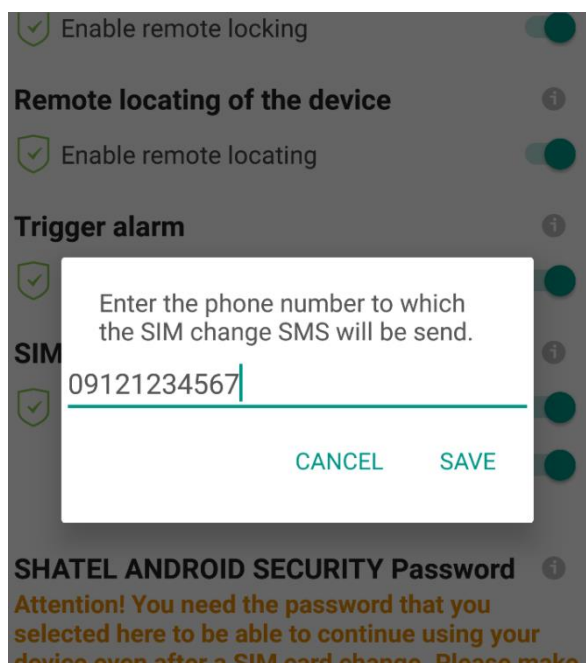
شکل ۵۴

برای فعال سازی SIM CARD Protection ابتدا لازم است پسورد SHATEL ANDROID SECURITY را وارد کنید.



شکل ۵۵

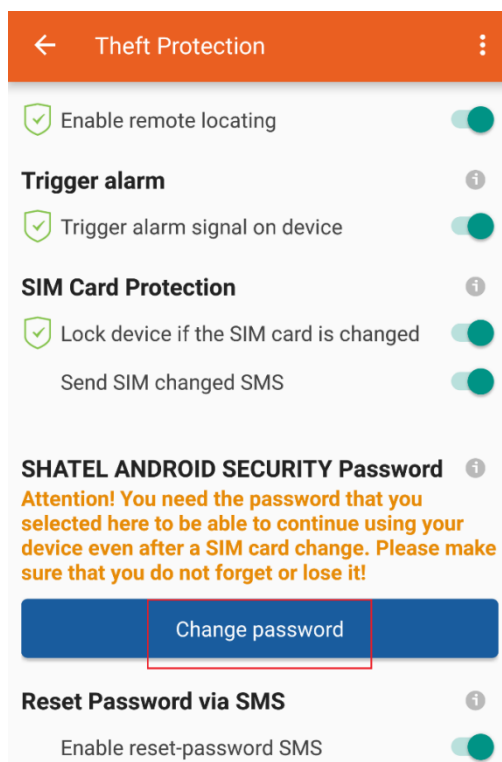
سپس شماره ای را که قصد دارید تغییرات مربوط به سیم کارت به آن پیامک زده شود، وارد کنید.



شکل ۵۶

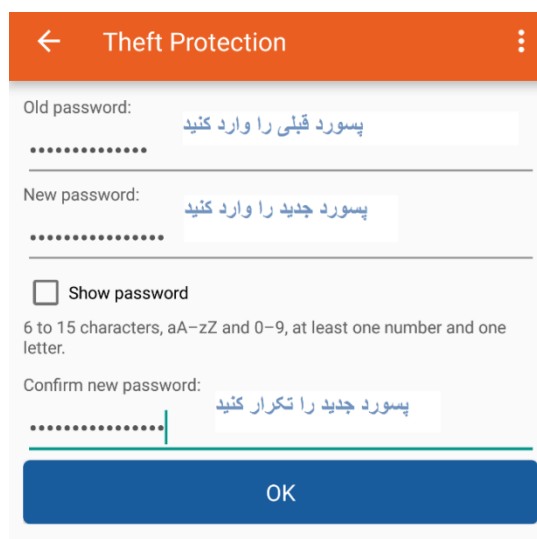
## تغییر پسورد SHATEL ANDROID SECURITY :

در صورتی که تمایل داشته باشید پسورد SHATEL ANDROID SECURITY را تغییر دهید، پس از باز کردن نرم افزار و کلیک بر روی Theft Protection و سپس Change password کلیک کنید.



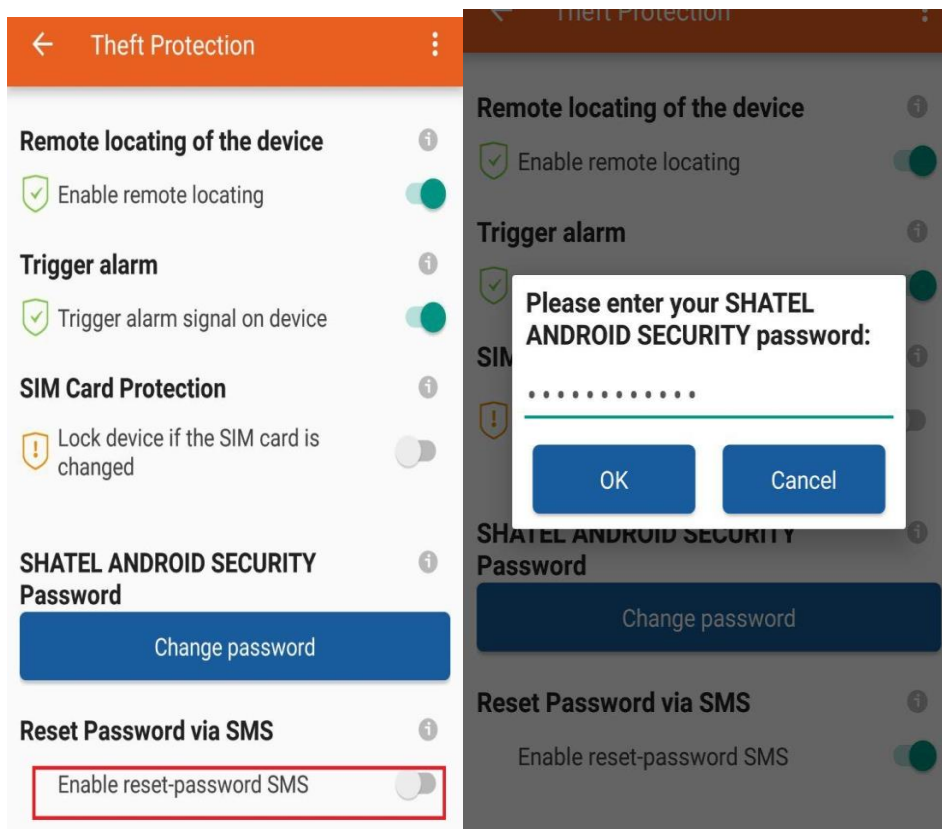
شکل ۵۷

سپس مطابق شکل زیر جهت تغییر پسورد اقدام کنید.



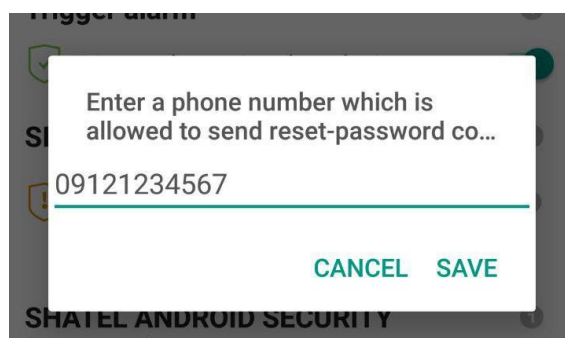
شکل ۵۸

اگر دستگاه شما گم شده و یا به سرقت برود و شما پسورد مربوط به SHATEL ANDROID SECURITY را فراموش کرده باشید دیگر قادر به استفاده از قابلیت های Theft protection که با ارسال پیامک های شامل رمز مربوطه امکان پذیر می شود، نخواهید بود. اما اگر قبلاً Reset Password Via SMS را فعال کرده باشید می توانید پسورد خود را باز یابی کنید. قبل از فعال کردن Reset Password Via SMS از شما رمز عبور نرم افزار را پرسیده می شود.



شکل ۵۹

در این جا شماره دیگری غیر از شماره خود به نرم افزار معرفی کنید.

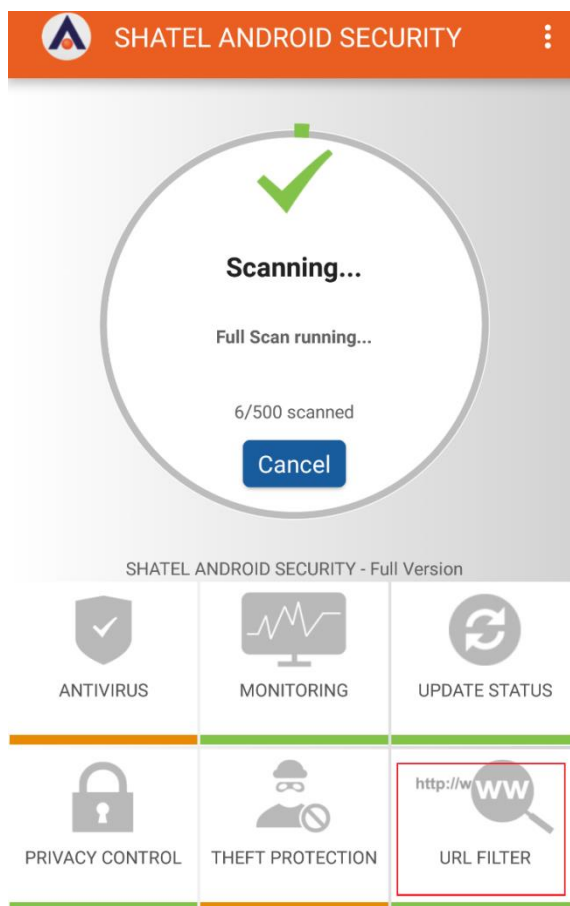


شکل ۶۰

اگر بخواهید رمز خود را باز یابی کنید یک پیامک شامل reset-password از شماره ای که در این قسمت به نرم افزار معرفی می کنید به شماره خود ارسال نمایید تا پیامک شامل پسورد به شماره معرفی شده ارسال شود.

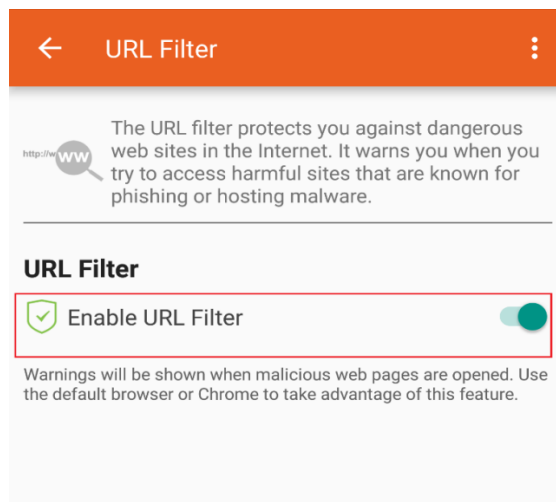
## بررسی تنظیمات URL FILTER :

برای ایجاد تغییر در تنظیمات مربوط به URL FILTER پس از باز کردن نرم افزار، بر روی URL FILTER کلیک کنید.



شکل ۶۱

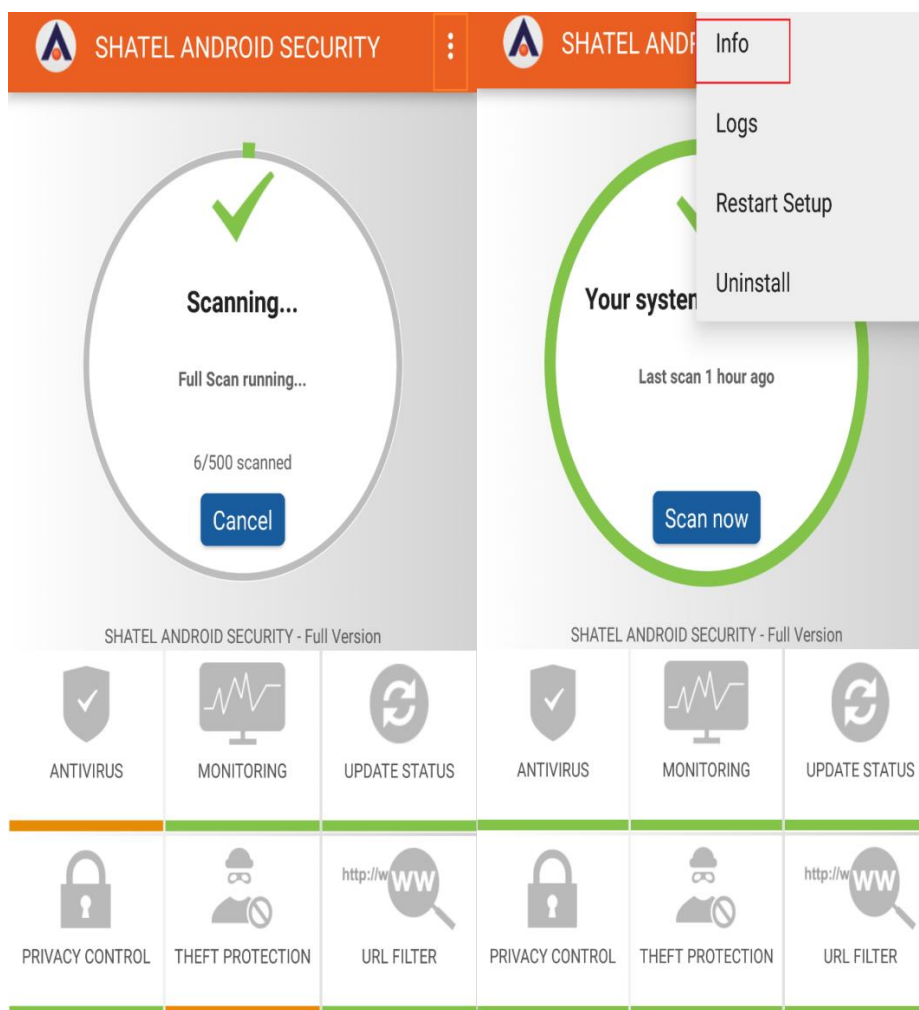
مطابق تصویر، می توانید این قابلیت را فعال یا غیر فعال کنید.



شکل ۶۲

## اطلاعات مربوط به SHATEL ANDROID SECURITY :

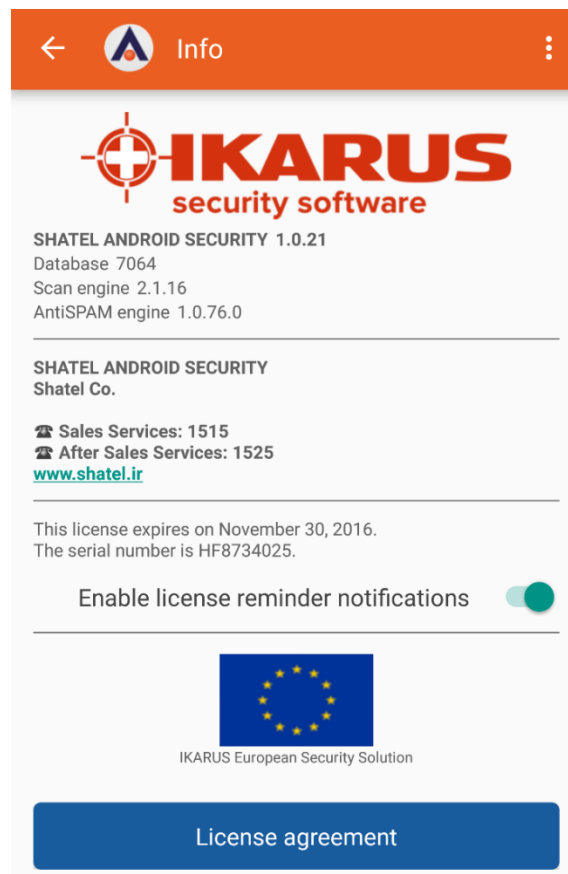
در صورتی که تمایل داشته باشید اطلاعات مربوط به نرم افزار SHATEL ANDROID SECURITY را مشاهده کنید بر روی سه نقطه در بالای نرم افزار کلیک کرده و سپس **info** را انتخاب کنید.



شکل ۶۳



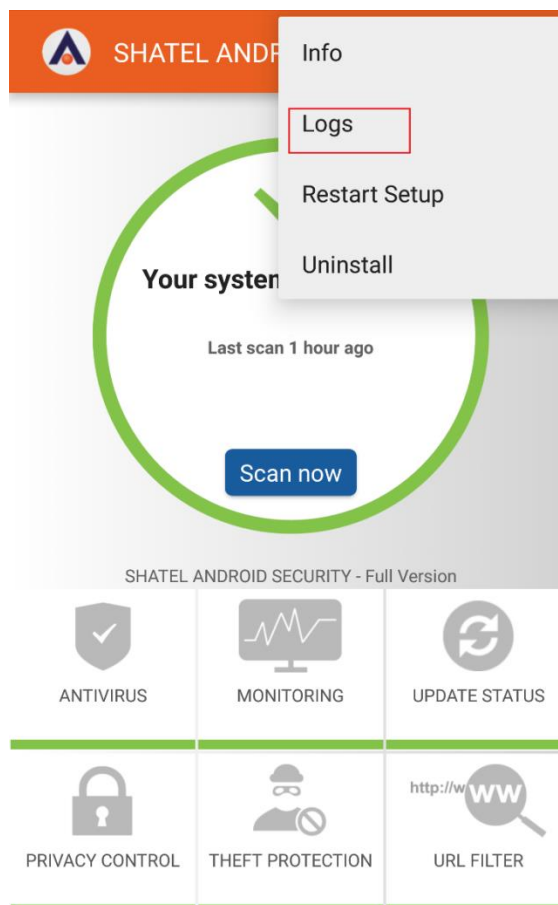
سپس صفحه ای مطابق تصویر باز شده که اطلاعات مربوط به نرم افزار و شرکت سازنده آن را نمایش می دهد.



شکل ۶۴

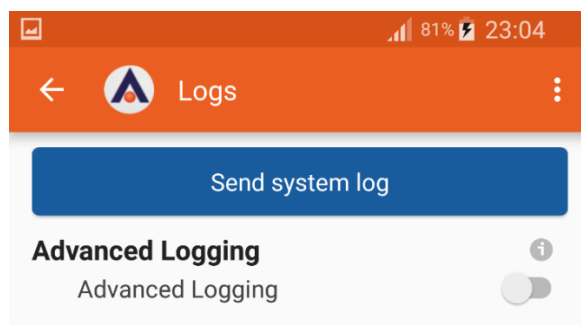
## به دست آوردن LOG از عملکرد نرم افزار:

اگر بخواهید اطلاعاتی را از فعالیت های نرم افزار ذخیره کنید، مطابق تصویر Logs را انتخاب کنید.



شکل ۶۵

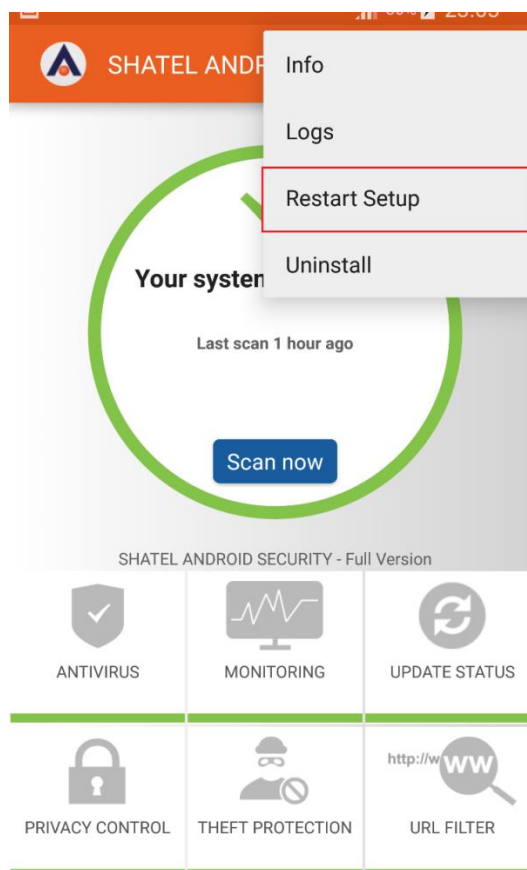
توجه داشته باشید برای ذخیره این اطلاعات نیاز است تا فضای کافی بر روی دستگاه شما وجود داشته باشد، این ویژگی را زمانی که نرم افزار با مشکل مواجه شده و بنا به توصیه گروه پشتیبانی، برای مشخص شدن جزئیات فعال کنید. هم چنین پس از اتمام گزارش گیری با کلیک بر روی Send system log فایل محتوای گزارش ضمیمه ایمیل خواهد شد



شکل ۶۶

## نصب و راه اندازی مجدد SHATEL ANDROID SECURITY :

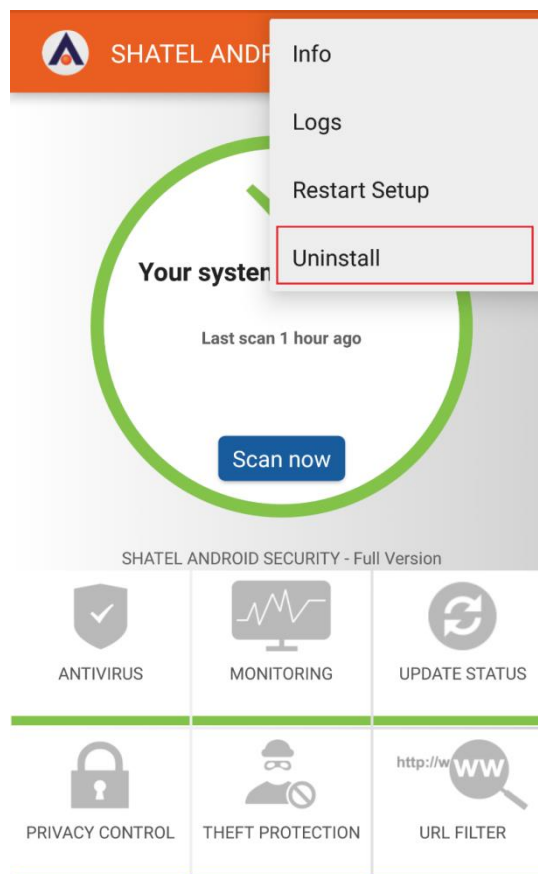
برای نصب و راه اندازی مجدد نرم افزار مطابق تصویر بر روی Restart Setup کلیک کنید توجه داشته باشید تمامی تنظیمات انجام شده بر روی قابلیت های مختلف SHATEL ANDROID SECURITY پاک خواهد شد.هم چنین برای انجام این کار ابتدا باید پسورد نرم افزار را وارد کنید.



شکل ۶۷

## حذف SHATEL ANDROID SECURITY :

برای حذف و پاک کردن نرم افزار SHATEL ANDROID SECURITY از روی دستگاه خود، مانند تصویر بر روی Uninstall کلیک کنید. قبل از انجام این کار پسورد نرم افزار از شما پرسیده خواهد شد.



شکل ۶۸

## پرسش های متداول در مورد نرم افزار SHATEL ANDROID SECURITY

در این بخش سعی شده است مشکلات و سوالات متداولی که ممکن است در هنگام نصب و راه اندازی و یا در زمان استفاده از نرم افزار ممکن است با آنها مواجه شوید بررسی و راهنمایی برای برطرف شدن هرکدام انجام شود.

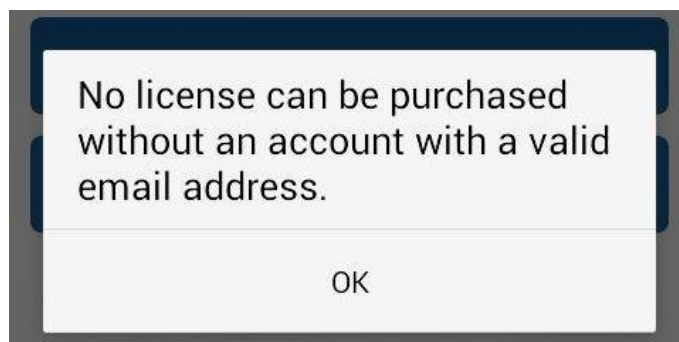
۱- در صورتیکه در مراحل اولیه نصب نرم افزار با پیغام زیر مواجه شدید :



شکل ۶۹

به این علت است که ارتباط تلفن همراه شما با شبکه جهانی اینترنت قطع است . برای نصب حتما باید ارتباط شما با شبکه اینترنت برقرار باشد تا فایل های اولیه مورد نیاز دریافت و بروی گوشی شما نصب شود .

۲- در صورتیکه در زمان وارد کردن کد فعال سازی با پیغام زیر مواجه شدید:

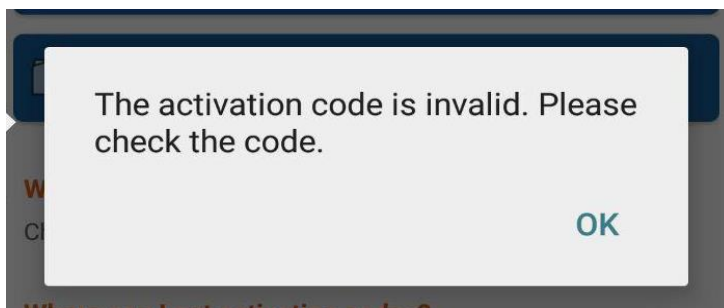


شکل ۷۰

به این علت است که بر روی تلفن همراه خود اکانت ایمیل ثبت نکرده اید. برای حل این مورد از نرم افزار خارج شده، وارد تنظیمات تلفن همراه خود شده و در قسمت Gmail Account یک اکانت Gmail ثبت کنید.

بعد از آن، وارد تنظیمات نرم افزار SHATEL ANDROID SECURITY شده و مجدد کد فعال سازی را وارد کرده و به نصب نرم افزار ادامه دهید.

۳- در صورتیکه در هنگام نصب نرم افزار با پیغام زیر مواجه شدید:



شکل ۷۱

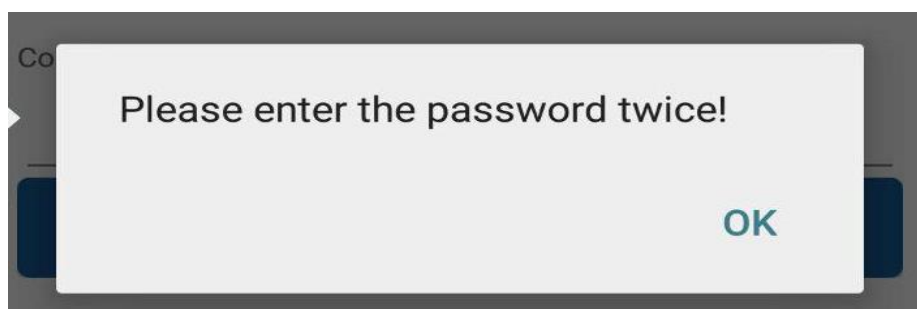
نرم افزار کد فعال سازی را شما را قبول نکرده است، که میتواند دو علت داشته باشد:

- کد فعال سازی اشتباه وارد شده است: کد فعال سازی را مجدد چک کنید و از صحت درست وارد شدن آن اطمینان حاصل کنید.
- کد فعال سازی قبلا بر روی دستگاه دیگری با اکانت ایمیل دیگری ثبت شده است و مورد استفاده قرار گرفته است.

نکته ۱: کد فعال سازی SHATEL ANDROID SECURITY فقط یکبار قابلیت فعال سازی دارد و پس از آن و در صورت ریست کردن تلفن همراه امکان نصب مجدد و فعال سازی در صورت قرار داشتن ایمیلی که با آن برای اولین بار فعال سازی انجام شده وجود خواهد داشت.

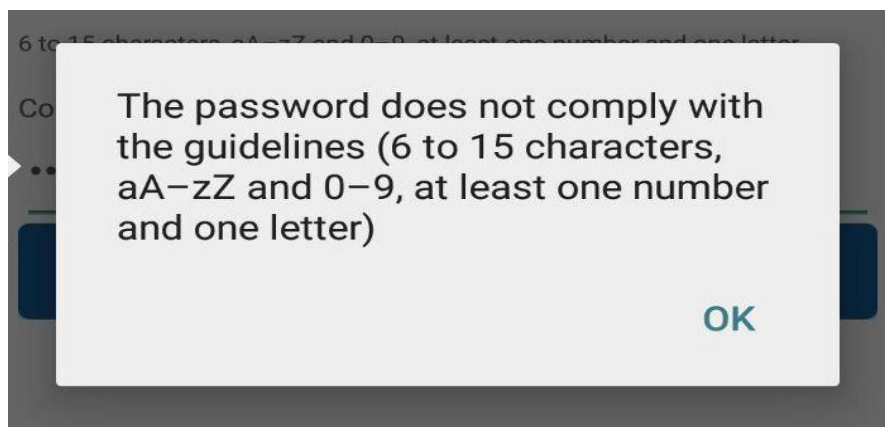
نکته ۲: لزوما نباید ایمیلی که در گوشی خود برای اولین بار ست میکنید با ایمیل وارد شده در پنل سایت یکسان باشد. ولی ایمیل وارد شده در پنل کاربری شاتل برای دریافت کد فعال سازی باید حتما معتبر باشد.

۴- در صورتیکه در هنگام وارد کردن پسونددلخواه خود برای SHATEL ANDROID SECURITY با پیغام زیر مواجه شدید. به این علت است که در کادر دیگری که در بالای گزینه Next وجود دارد نیز باید مجدد پسوندد انتخابی خود را وارد کنید و سپس بر روی گزینه Next کلیک کنید.



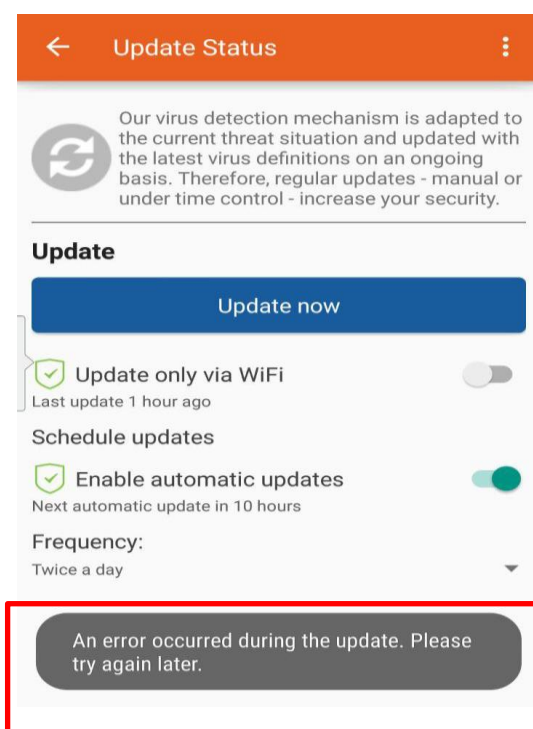
شکل ۷۲

۵- در صورتیکه با وارد کردن پسورد برای نرم افزار SHATEL ANDROID SECURITY با پیغام زیر مواجه شدید :  
 باید پسورد انتخابی شما حداقل ۶ الی ۱۵ کاراکتر داشته باشد و در این کاراکترها حداقل یک عدد نیز وجود داشته باشد  
 . ( ترکیبی از اعداد و حروف باشد )



شکل ۷۳

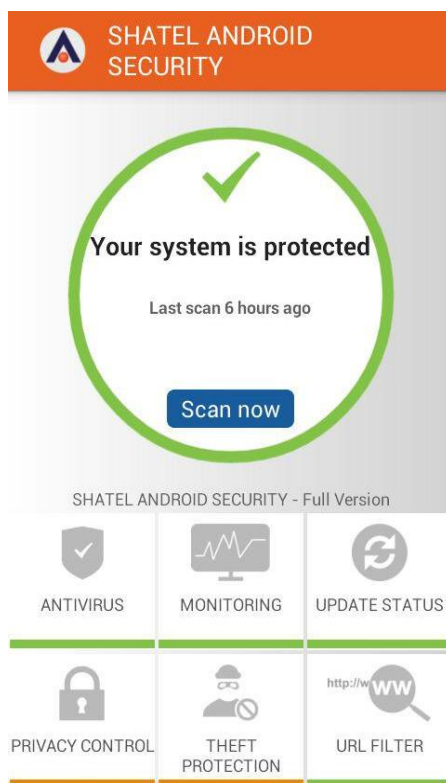
۶- در صورتیکه بعد از نصب نرم افزار بر روی تلفن همراه خود ، نیاز به آپدیت آن داشتید و با کلیک بر روی گزینه Update now با پیغام زیر مواجه شدید :



شکل ۷۴

احتمالا ارتباط شما با شبکه جهانی اینترنت برقرار نیست و امکان متصل شدن به سرور وجود ندارد . لطفا اینترنت تلفن همراه خود را بررسی کنید .

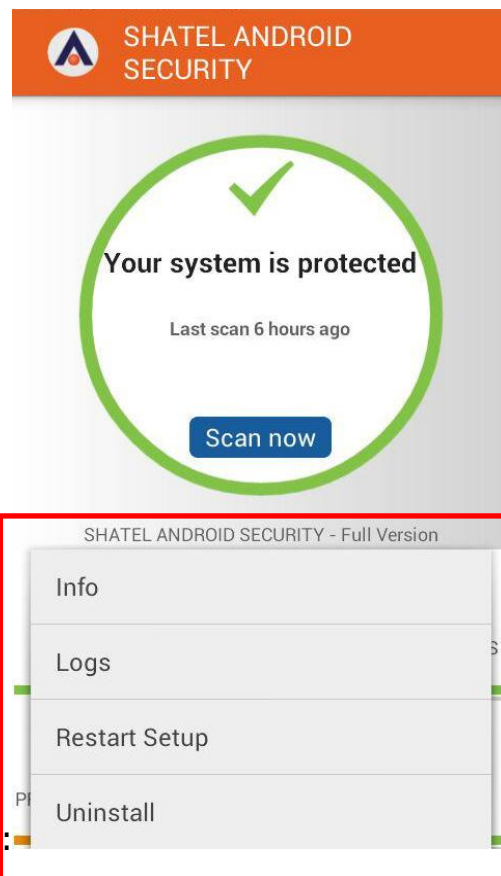
۷- بر روی برخی از گوشی ها ممکن است سه نقطه بالا سمت راست قایل مشاهده نباشد مانند شکل زیر :



شکل ۷۵

در این صورت با زدن دکمه تنظیمات خود تلفن همراهتان قادر به مشاهده این منو در پایین صفحه خواهید بود:





شکل ۷۶