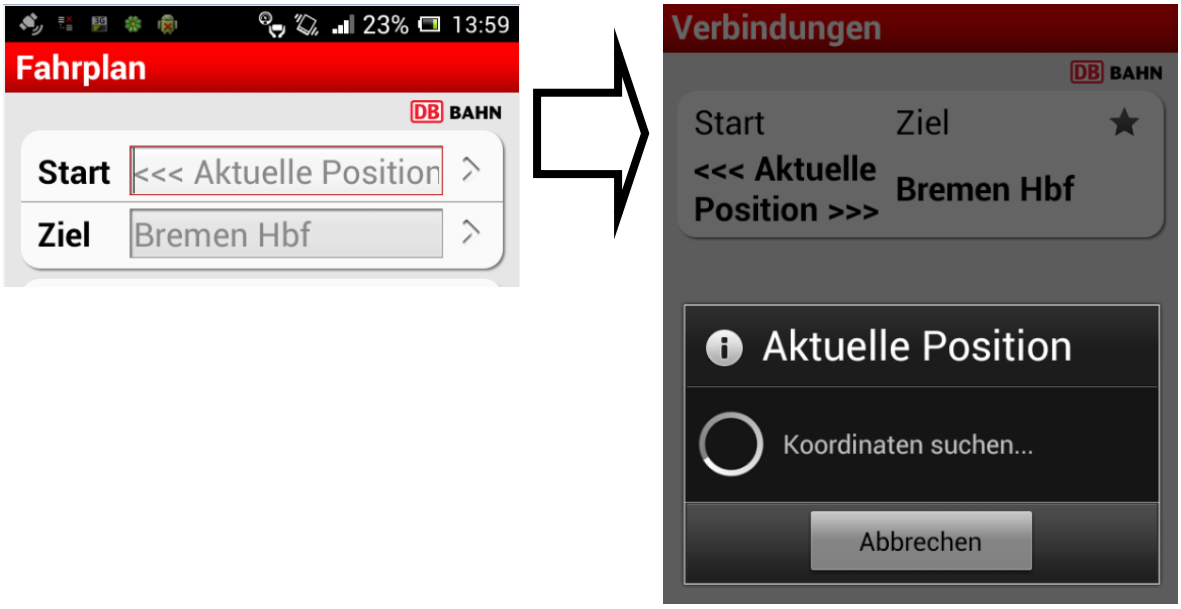
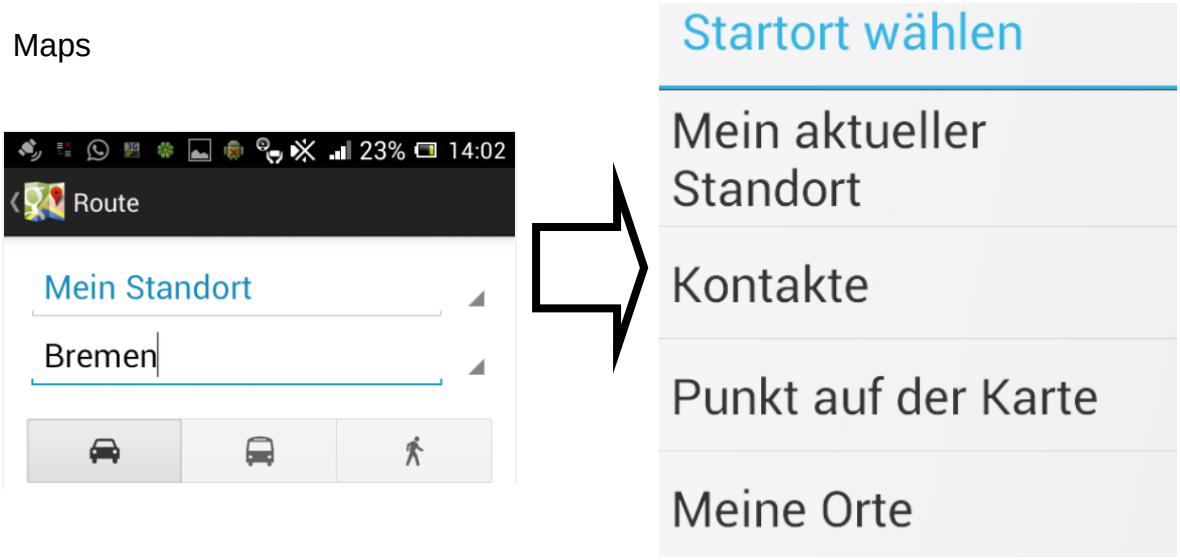
Ortungsdienst

Dieser Dienst hat Vor- als auch Nachteile. Zum einen kann der Standort bestimmt werden und somit eine einfache Navigation vom „Aktuellen Standort“ zu einem beliebigen Ort ermöglicht werden.

DB Navigator



Maps

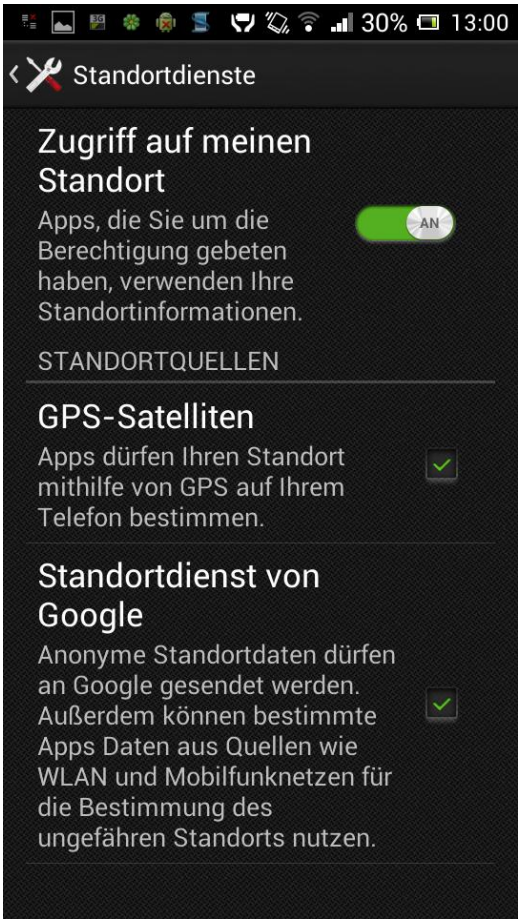


Andere Programme benutzen den Standort um einen Beitrag mit aktueller Zeit und Ortsangabe zu veröffentlichen. Dabei ist immer fraglich, inwiefern entsprechende Programme / Anbieter diese Daten nachträglich speichern. Bestimmte Programme zeichnen sogar ein Bewegungsprofil auf, ohne vorher eine Frage / Mitteilung an den Benutzer zu geben.

Ein großer Vorteil des Ortungsdiensts ist das Aufspüren verlorener Smartphones. Dies geschieht über spezielle Programme, wie F-Secure Anti-Theft for Mobile

Norton Mobile Security oder GadgetTrak.

Somit muss der Benutzer letztlich selbst abwägen, inwiefern der Ortungsdienst und die damit verbundenen Datenspeicherung hinnehmbar ist.



Aktiviert bzw. Deaktiviert werden kann die Funktion Rund um den Ortungsdienst unter den Einstellungen → Standortdienste.

(Einschränkung von bestimmten Programmfunktionalitäten möglich)

Durch Antippen des Reglers oder der Kasten werden die Funktionen aktiviert oder deaktiviert.

Allgemein

Sicherheitsanwendungen und Virenschutz:
Das Smartphone, dient wie der PC, als Speicherort für persönliche Daten. Das wissen auch Kriminelle, die es auf die eigenen Daten und das Geld abgesehen haben. Auf dem Smartphone werden Log-In Daten von verschiedenen Internetanbietern gespeichert, unter anderem Mail –Konten, Online – Banking,…

Für das Google System steigt die Zahl neuer Viren am stärksten, im Gegensatz zum iPhone, wo es in „freier" Wildbahn nicht vorkommt.

Verbreitung eines Virus:
Um eine entsprechende Schadsoftware auf dem Mobiltelefon zu verbreiten, müssen Kriminelle nur wenige Schritte vollziehen. Zuerst wird ein entsprechender Code programmiert, dieser wird dann in eine bestehende App integriert und unter ähnlichem Namen in den Play Store eingestellt. Virenprogrammierer können somit Handy komplett fernsteuern und beliebig neue Schädlinge nachladen.

Verbreitung durch mangelhafte Überwachung:
Eine entsprechende App wurde auf ihre Manifestdatei (beschreibt welche Rechte der App gewährt werden) überprüft und der damit verbunden Anwendung (Quellcode Abgleich durch einen Computer). Bei erfolgreicher Übereinstimmung passiert die Applikation die Sicherheitsbarriere und wird im Play Store eingestellt. Eine Plausibilitätskontrolle, bei Apple üblich, gibt es für Android nicht.

Beispiel Flashlight no add:
Eigentlich: Einschalten des Blitzlichts oder Displays
Stattdessen: Internet, Kamera, Mikrofon, persönliche Daten

Beispiel Mania.A
Versendet SMS – Nachrichten an teure Premium-Nummern. Antworten auf SMS werden auf andere Nummern umgeleitet damit kein Verdacht geschöpft wird.

ZitMo & SpitMo
Späht Bankdaten in Spanien und Polen aus.

➔ Kriminelle tarnen Apps als nützliche Anwendungen!
➔ Hauptsächlich sind Viren in Russland und Asien verbreitet!

Aufgrund eines ersten größeren Virus (200.000 Betroffene) entschloss sich Google zu einer Fernlöschung der App auf den Smartphones der Opfer. Google hatte somit Zugriff auf rund 200.000 Handys. Bisher war nicht bekannt das Android eine solche Fernlöschung überhaupt unterstützt.

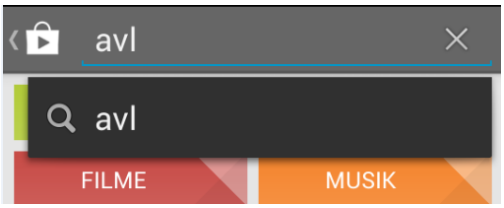
Unterschiede bei den Virenprogrammen
Empfehlenswerte Programme kommen von großen Anbietern, die bereits Antivieren Programme für den PC hergestellt haben.
Durch ständige Weiterentwicklung ist es mittlerweile auch möglich Apps vor der Installation zu Prüfen. Weitere Funktionen von Viren Programmen für das Androidsystem sind:

- Internetseitenfilter: Blockiert virenverseuchte Internetseiten

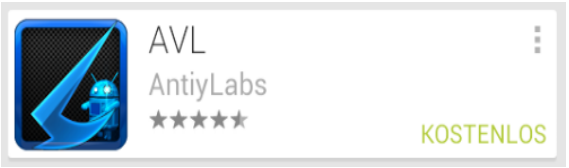
- Lokalisierung: Das Smartphone lässt sich über eine Internetseite orten
- Fernsteuerfunktion: Sperrfunktion, nach Verlust
- App – Kontrolle: App Berechtigungen einsehen
- Backup: Speicherung persönlicher Daten auf SD Karte, PC oder Online

Virenprogramm – kostenlos

Von AV-Test wurde das kostenlose Virenprogramm AVL von Antiylabs mit einer Sehr guten Erkennungsrate abgesegnet.

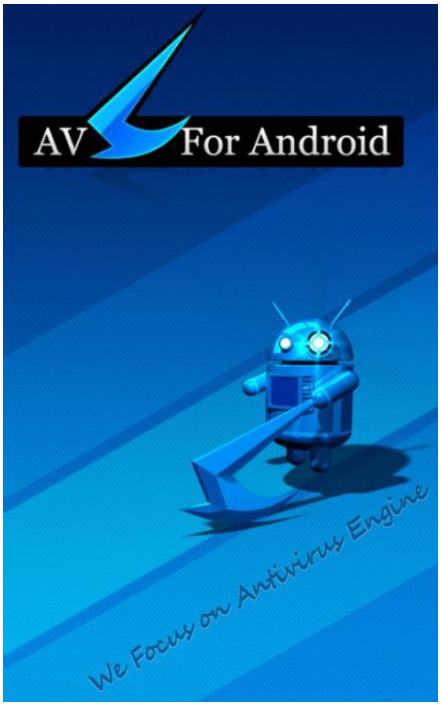


Über den Play Store kann AVL heruntergeladen werden.
Mit Hilfe der Suchfunktion geht dies schnell.



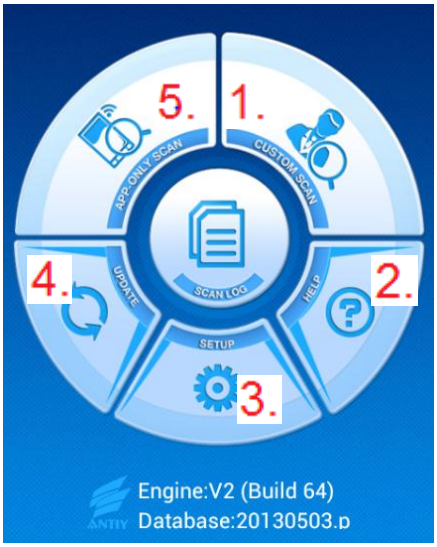
Durch das Anwählen des Suchergebnisses wird zur Produktseite weiter gleitet.

Wie gewohnt wird die Anwendung durch Antippen auf „Installieren“ auf dem Gerät heruntergeladen und installiert.



Das Programm benötigt beim ersten Start ein wenig Zeit bis die benutzerfreundliche Bedienfläche erscheint.

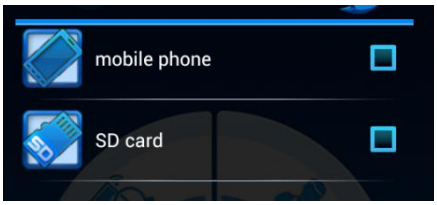
Als Übergang wird ein Startbildschirm angezeigt.



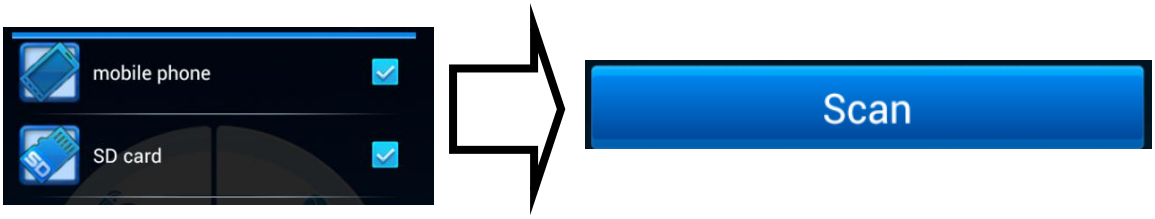
Nachdem Start kann der Benutzer Bedienflächen antippen:

1. Custom Scan
2. Help
3. Setup
4. Update
5. App Only Scan

Custom Scan

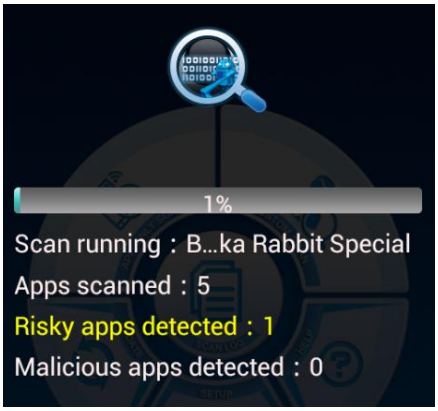


Bei Custom Scan kann ausgewählt werden, welche Bereiche gescannt werden sollen.
Durch Antippen den gewünschten Haken setzen auf Scan tippen.



Die Überprüfung beginnt.

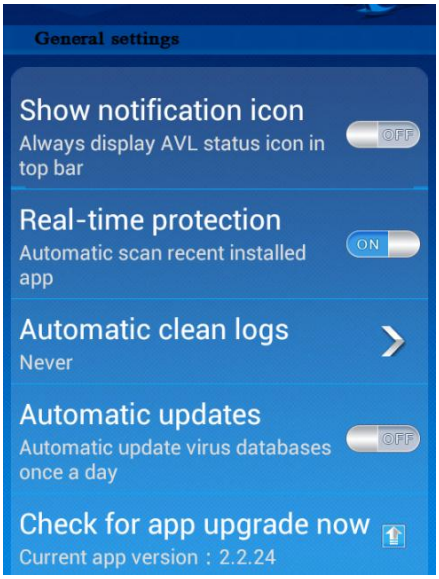
Es werden die bereits gescannten Apps angezeigt, potenziell risikoreiche sowie tatsächliche Malware
(=schädliche Software alias Viren).



Help

Wie bei jedem Programm kann unter „Help“ Lizenzvereinbarungen und ein FAQ aufgerufen werden.

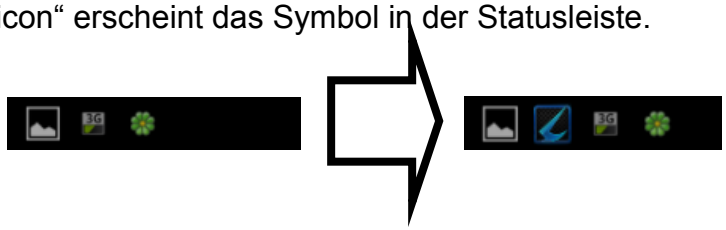
Setup



Hier können verschiedene Einstellungen vorgenommen werden. Standardgemäß sind „Real – time protection“ (=Echtzeitschutz) eingeschaltet und dringend empfehlenswert.

Automatische Updates sind ebenfalls sinnvoll.

Mit dem Setzen des Reiters bei „Show notification icon“ erscheint das Symbol in der Statusleiste.



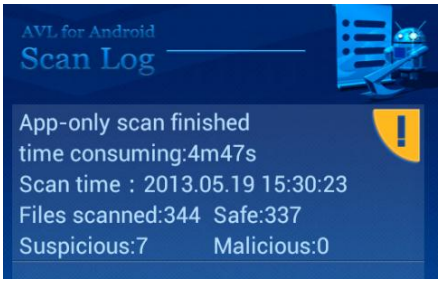
Update

Durch Antippen auf Update wird nochmals auf die aktuellste Virendatenbank aktualisiert, sofern vorhanden.

APP - Only scan

Es werden NUR Anwendungen, die auf dem Telefon installiert sind, gescannt. Keine Dokumente, Bilder,…

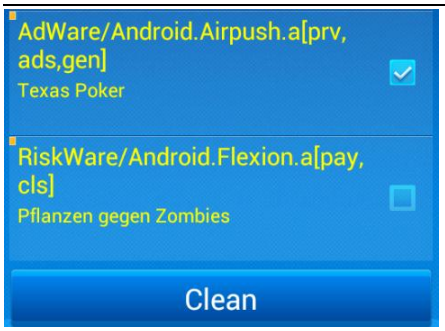
Scan Log



Der Scan Log zeigt die Scans in einer Übersicht an, hier werden aufgelistet alle gescannten Anwendungen, darunter auch potentiell gefährliche und entdeckte Malware.

Durch Antippen erscheint eine Detailansicht.

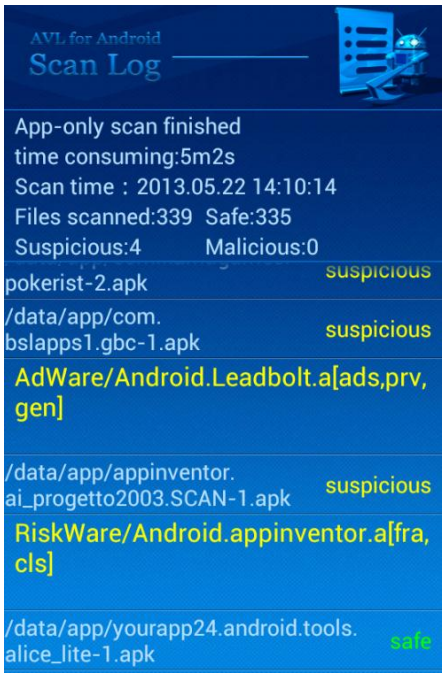
Mit Clear werden die Logdateien gelöscht.
Durch Resolve können potentiell gefährdete / unerwünschte Programme entfernt werden.



Dafür im neu erschienen Menü Haken in die zu löschenden Einträge setzen und auf „Clean“ tippen.

Das Programm filtert die Art der Viren und zeigt diese dem Benutzer.

„AdWare“ und „RiskWare“ im Bild links.



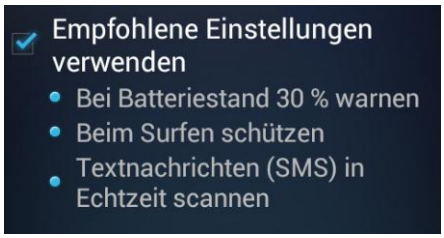
Der geöffnete Scan Log gibt Auskunft über die durchsuchten Daten, das Datum an dem der Scan ausgeführt wurde sowie die gefunden „Sicheren“, „Verdächtigen“ und „Bösartige“ Dateien.

„suspicious“	Verdächtig (Gelb)
„malcious“	Bösartig (Rot)
„safe“	Sicher (Grün)

Virenprogramm – kostenpflichtig

Als kostenpflichtiges Programm wird Antivirus Pro für Mobilgeräte aus dem Hause AVG Mobile Technologies vorgestellt.

Nachdem das Programm aus dem Play Store heruntergeladen und installiert wurde, kann es mit einem Druck auf die Verknüpfung gestartet werden. 

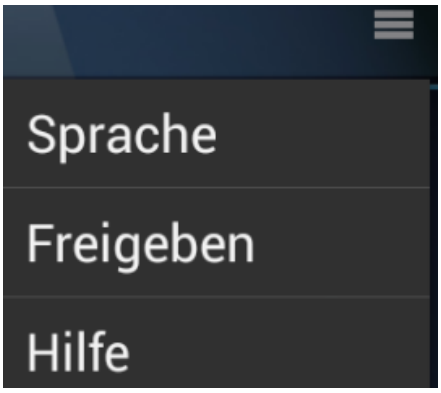


Der erste Programmstart dient als Schnellkonfiguration.

Mit „Aktivieren“ fortfahren, andernfalls den Haken entfernen und fortsetzen.

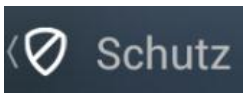
Ähnlich wie das kostenlose Programm, ist die Oberfläche angenehm einfach gehalten.

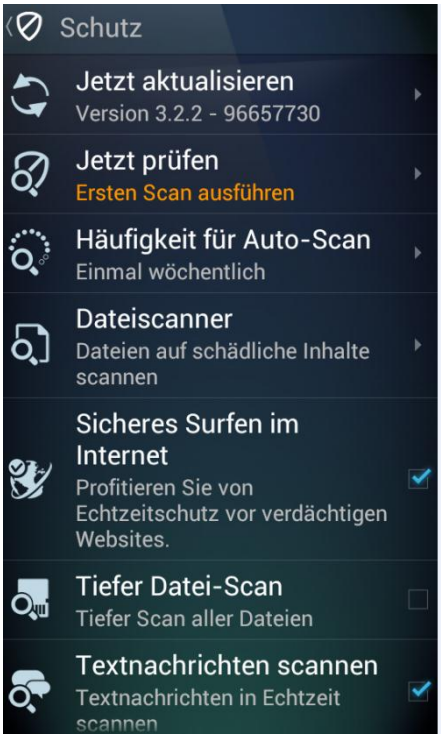
Eine Navigation zu den einzelnen Bereichen erweist sich als einfach.



Oben rechts in der Ecke befindet sich das erweiterte Einstellungssymbol.

Es kann die Sprache angepasst werden, Freigegeben werden sowie die Hilfe aufgerufen werden.

Schutz 

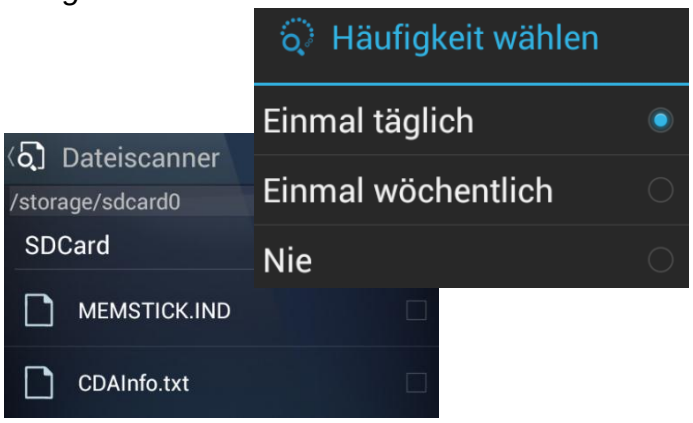


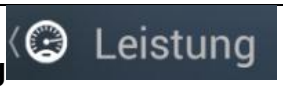
Durch Antippen auf Schutz erscheinen Einstellungen rund um den Schutz.

Dabei ist es sinnvoll die Häufigkeit für Auto-Scan auf „einmal täglich“ zu stellen.

Der Dateiscanner scannt nur bestimme, vom Benutzer, vorher festgelegte Bereiche.

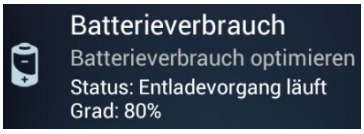
Sicheres Surfen im Internet, Tiefer Datei Scan, Textnachrichten scannen sowie PUP aktivieren Erkennen sollten aktiv gesetzt sein um einen bestmöglichen Schutz zu haben.



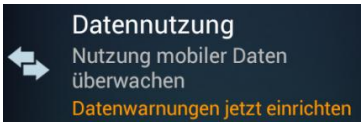
Leistung 

Leistung bietet dem Benutzer zusätzliche Funktionen.

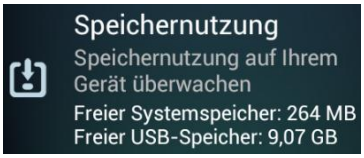
Aufgaben – Killer stellt dabei den typischen Task Manager dar.



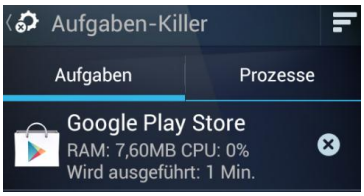
Batterieverbrauch zeigt an, welche Aktion des Telefons, wie lange ausgeführt wird.

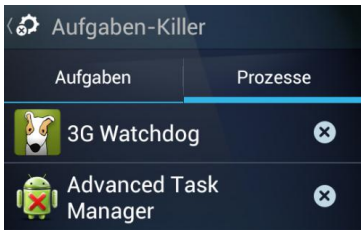


Datennutzung zeigt an welches Programm wie viele Upload und Download hat. Wenn der Nutzungszähler eingestellt wird, kann ein statistikführendes Programm aktiviert werden.



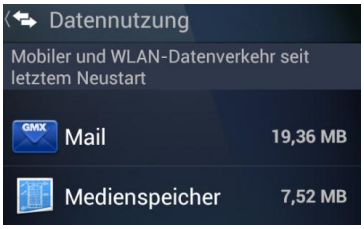
Speichernutzung gibt eine Übersicht des Systemspeichers und ermöglicht es Programme zu verschieben (SD Karte) oder zu Löschen.





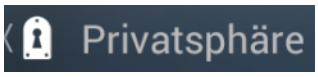
Es können Prozesse mit einem Tipp auf das „X“ geschlossen werden.

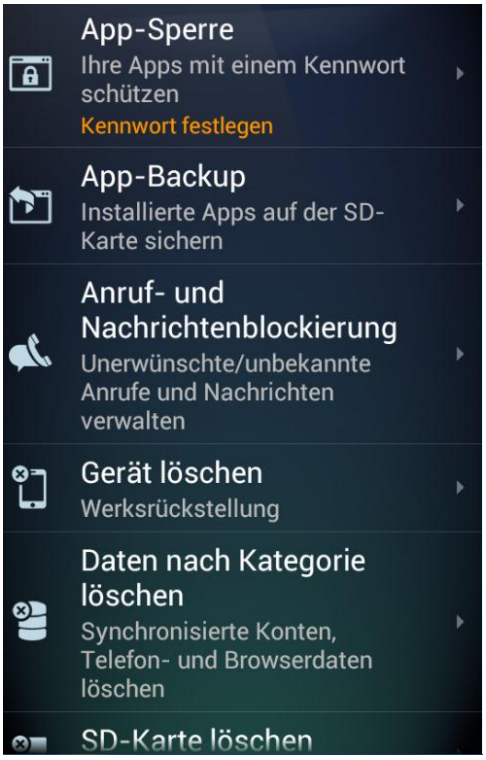
Wenn sich im Batterieverbrauchbefunden wird, kann über die Menütaste weitere Stromsparmaßnahmen einschalten.



Durch einschalten des „Nutzungszählers“ kann das statistikführende Programm aktiviert und eingerichtet werden.

Speichernutzung ist leicht zu bedienen (löschen und verschieben einer Anwendung) und ermöglicht einen genauen Überblick über die installierten Anwendungen.

Privatsphäre 



Die App – Sperre ermöglicht dem Anwender, alle oder einzelne Apps mit einem Passwort zu schützen.

App – Backup dient als Sicherung installierter Apps und deren Einstellungen.

Anruf- und Nachrichtenblockierung kann bestimmte Rufnummern sperren, sodass keine anrufe und / oder Nachrichten von bestimmten Nummern mehr erhalten werden.

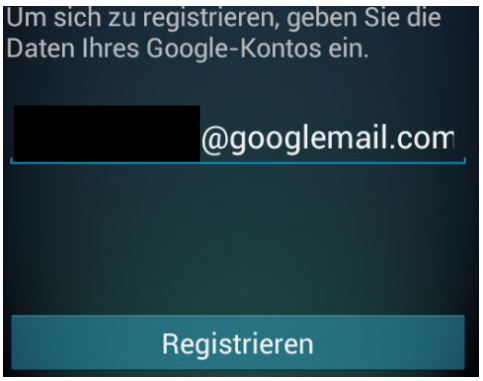
Gerät löschen setzt dies auf die Werkseinstellung.

Daten nach Kategorie löschen, gibt dem Benutzer die Möglichkeit nur einen bestimmten Bereich, der sich auf dem Telefon befindenden Daten, zu löschen.

SD – Karte löschen – alle Daten werden gelöscht.

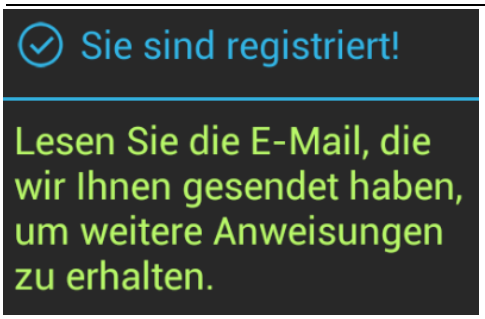
Antidiebstahl 

Dient zum Orten und Sperren des Telefons.



Zuerst muss das Telefon registriert werden.

Dies geschieht mit der Google Kennung.

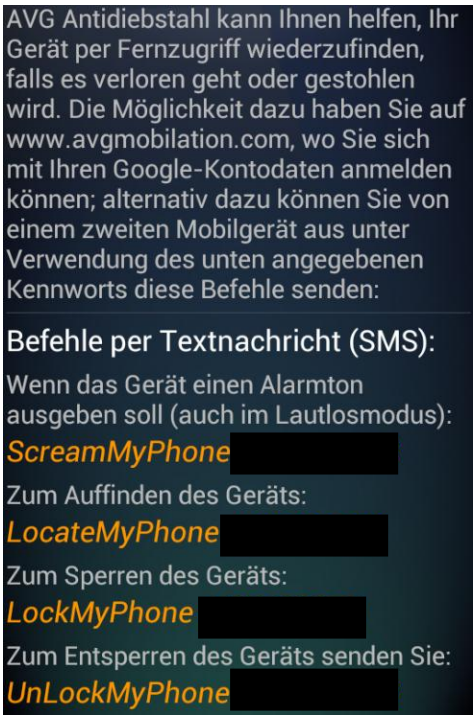


Sofern die Registrierung erfolgreich war, teilt das Programm Benutzer dies mit.

Es wird das Registrierte Konto aufgeführt, welches auch geändert werden kann.

Darunter wird erklärt wie die Funktion bedient werden kann.

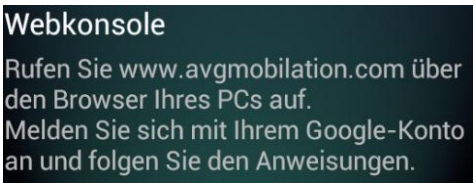
- Über das Internet
- Über ein anderes Mobiltelefon



Die Erklärung ist verständlich und leicht auszuführen.

Darüber hinaus bekommt jeder registrierte Nutzer eine Funktionsanleitung an die Googlemailadresse, (für Internet und Telefon), um im Falle des Verlusts sofort Schritte in die Wege zu leiten.

Um eine Ortung zu versuchen.

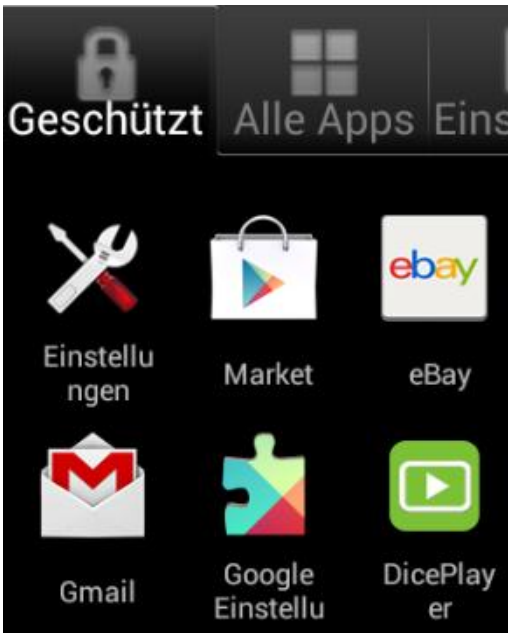


Sicherheitsapps  

Es lässt sich jede beliebige Anwendung mit einem Passwort sperren: SMS, E-Mail, Fotos, Kamera, USB-Verbindungen, Kalender, Messenger – darunter auch jene die gerne vor unbefugtem Zugriff geschützt sein soll, im schlimmsten Fall bei Verlust des Telefons oder wenn das Handy aus der Hand gegeben wurde. Mit entsprechenden Sicherheitsapps ist dies kein Problem mehr.
Bevor eine gesperrte App geöffnet werden kann (wird nicht angezeigt), erfolgt die Abfrage eines Passwort oder Muster.

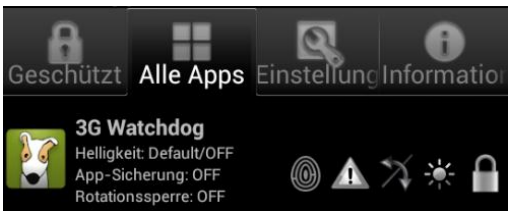
Perfect App Protector hat den Vorteil, dass lediglich Werbung eingeblendet wird, jedoch der Funktionsumfang der gleiche wie bei der Bezahlversion ist.

Es werden 4 Registerkarten unterteilt.



„Geschützt“ zeigt alle Anwendungen an, die von dem Programm geschützt werden.

Wenn das Programm zum ersten Mal startet, sind keine Einträge zu finden.



„Alle Apps“ listet alle auf dem Gerät installierten Anwendungen auf.

Diese können dann auf verschiedene Arten geschützt werden.

Fake Finger Print 

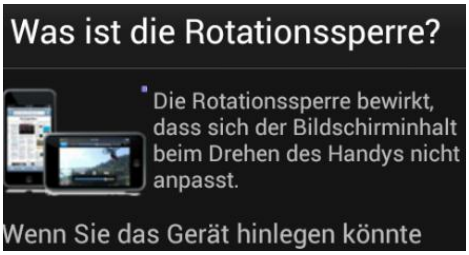
Der Benutzer wird aufgefordert einen korrekten Fingerabdruck zu identifizieren.

Jedoch wird die App trotzdem noch über ein Passwort geschützt.

Fake Pop – Up 

Das Programm startet nicht und es erscheint die Meldung, dass die Anwendung nicht mehr funktioniert.

Rotationssperre 



Die App wird nicht mehr gedreht, auch wenn es in den Einstellungen aktiv ist.

Bildschirmfilter 

Beim Öffnen der entsprechenden Anwendung wird die Bildschirmhelligkeit (wie eingestellt) gedimmt oder aufgehellt.

Passwort geschützt 

Bevor eine Anwendung geöffnet wird muss ein Pin oder Muster eingegeben werden.

Bei vergessen des Musters / Pins kann über eine Sicherheitsfrage die App trotzdem geöffnet werden.

Hilfreich beim Öffnen der Sicherheitsapp.

Die Einstellungen ermöglichen dem Benutzer verschiedene Personalisierungsmöglichkeiten vorzunehmen.

Darunter den Pin zu ändern, den Geheim Modus zu aktivieren (die Anwendungsverknüpfung verschwindet), Benachrichtigungssymbole zu deaktivieren uvm. .

Der Reiter Informationen zeigt die Programmversion an und gibt die Möglichkeit den Support zu kontaktieren.