

Mobile Security für Android 2.2–3.2 Geräte

1 Swisscom Mobile Security™ für Android 2.2–3.2 Geräte

Dieses Handbuch gilt für mobile Geräte (Smartphones, Tablets), welche mit dem Betriebssystem Android (Version 2.2 bis 3.2) ausgestattet sind. Welche mobilen Geräte mit diesem Betriebssystem mit Swisscom Mobile Security getestet wurden, entnehmen Sie bitte der Webseite www.swisscom.com/f-secure.

2 Installation von Mobile Security

2.1 Android Betriebssystem Geräte mit vorinstalliertem Mobile Security Programm



Ihr Swisscom Mobile Security Programm ist teilweise bereits auf Ihrem bei Swisscom erworbenen mobilen Gerät vorinstalliert. In den meisten Fällen befindet sich die Vor-Installierte Software im *Menu Applikationen (Apps)*. Sie können deshalb direkt zur Aktivierung Ihres Mobile Security Programms gehen, indem Sie das Schlosssymbol mit der Bezeichnung *Mobile Security* auswählen. Anmerkung: je nach Typ des mobilen Gerätes kann die Bezeichnung auch abgekürzt erscheinen. Beim erstmaligen Aufrufen von Mobile Security müssen Sie dieses Programm noch zuerst aktivieren (siehe Kapitel 3), bevor Ihr mobiles Gerät geschützt ist. Das Produkt schützt Ihr Gerät nicht, solange Sie es nicht aktiviert haben. Sie haben die Wahl, das Produkt während 30 Tagen in einem Trial kostenlos zu testen, bevor Sie es bei Swisscom abonnieren können.

2.2 Android Betriebssystem Geräte mit vorinstalliertem Swisscom Security Launcher



Sollten Sie Ihr mobiles Gerät von Swisscom erworben haben, so befindet sich evtl. in Ihrem *Menu Applikationen (Apps)* das Schlosssymbol mit dem Titel *Swisscom Security Launcher* (evtl. ist die Bezeichnung abgekürzt). Hinter diesem Symbol öffnet sich ein dediziertes Download-Programm (Launcher) für das Programm Mobile Security von Swisscom.

Beachten Sie, dass Sie bei der Installation eine Datenmenge in der Grössenordnung von 2 MB herunterladen. Sie sollten also ein Abonnement von Swisscom mit Datenoption haben und sich während des Downloads im Swisscom Netz oder einem privaten WLAN befinden.

Wichtig: Versichern Sie sich zunächst, dass Sie die Freigabe für *Unbekannte Quellen* aktiviert haben. Diese Freigabe können Sie im *Menu Einstellungen → Anwendungen* vornehmen und nach der erfolgreichen Installation von Mobile Security wieder zurücksetzen.

Der Swisscom Security Launcher wird Sie zu dieser Einstellung hinführen, wenn Sie unbekannte Quellen noch nicht freigegeben haben. Nach Abschluss der Installation müssen Sie Mobile Security zuerst aktivieren (siehe Kapitel 3). Das Produkt schützt Ihr Gerät nicht, solange Sie es nicht aktiviert haben. Sie haben die Wahl, das Produkt während 30 Tagen in einem Trial kostenlos zu testen, bevor Sie es bei Swisscom abonnieren können.

2.3 Android Betriebssystem Geräte ohne vorinstalliertes Mobile Security oder Swisscom Security Launcher

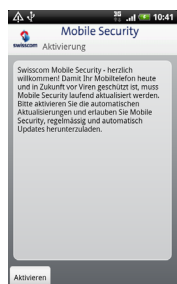
Sollten Sie ein mobiles Gerät erworben haben, das weder ein vorinstalliertes Swisscom Mobile Security Programm noch einen Swisscom Security Launcher hat, dann können Sie trotzdem die Anwendung Swisscom Mobile Security installieren. Das Fehlen der beiden Apps erkennen Sie, dass kein Schlosssymbol von Swisscom im *Menu Applikationen (Apps)* Ihres mobilen Gerätes zu finden ist.

Wichtig: Versichern Sie sich zunächst, dass Sie die Freigabe für *Unbekannte Quellen* aktiviert haben. Diese Freigabe können Sie im *Menu Einstellungen → Anwendungen* vornehmen und nach der erfolgreichen Installation von Mobile Security wieder zurücksetzen.

Öffnen Sie Ihren Internet-Browser und tippen Sie <http://mobile.f-secure.com/swisscom> in die Adresszeile ihres Browsers ein. Auf der sich öffnenden Internet-Seite können Sie nun den Download aufrufen. Wählen Sie den Download von Mobile Security für Android 2.2–3.2 aus. Das fertig herunter geladene Download-Programm finden Sie in den Benachrichtigungen auf Ihrem mobilen Gerät. Aktivieren Sie das herunter geladene Download-Programm Mobile Security und folgen Sie dem Installationsassistenten zur Aktivierung.

3 Aktivierung/Deaktivierung von Mobile Security

3.1 Aktivierung von Mobile Security



Aktivierung des kostenlosen Trials von Mobile Security:

Wenn Sie Mobile Security zum ersten Mal aufrufen, können Sie die Applikation zunächst in einem 30 Tage dauernden kostenlosen Trial testen. Die Trialdauer beginnt mit der ersten Aktivierung von Mobile Security. Drücken Sie auf das Symbol von Mobile Security, danach auf die Auswahl *Aktivieren* und folgen Sie dem Assistenten, der Sie durch die Aktivierung führen wird. Bei der Aktivierung ist auch eine Aktualisierung des Programms bei einem Update Server erforderlich. Benutzen Sie im Mobilfunknetz von Swisscom die Verbindung *Swisscom Services*, um die Updates herunter zu laden. Der Aktivierungsassistent wird Sie danach auch gleich noch bitten, die nötigen Konfigurationen in Mobile Security vorzunehmen und ihr Gerät nach Viren zu scannen. Sie können dies aber jederzeit nachholen.

Wenn Sie Mobile Security erfolgreich aktiviert haben, wird die verbleibende Trialdauer in ihrem Mobile Security Übersichtsfenster angezeigt. Mobile Security besitzt während des Trials den gleichen Funktionsumfang wie das kostenpflichtige Abonnement.

Sie können während der Trialdauer jederzeit direkt ein kostenpflichtiges Abonnement bei Swisscom bestellen. Mobile Security wird Sie 7 bzw. 3 Tage vor Ablauf der Trialdauer daran erinnern, dass ihr Gratis-Trial abläuft. Um ihr mobiles Gerät weiterhin optimal zu schützen, empfehlen wir Ihnen, nun rechtzeitig ein Abonnement bei Swisscom abzuschliessen.



Bestellung des kostenpflichtigen Abonnements Mobile Security (empfohlene Variante):

1. Öffnen Sie die Anwendung *Mobile Security* in ihrem Haupt- oder Programm-Menu. Mobile Security zeigt Ihnen in einer Übersicht, wie viele Tage ihr Trial noch gültig ist.
2. Wählen Sie die Schaltfläche *Kaufen* aus. Sie sehen, wann ihr Trialabonnement ausläuft und wieviel Sie das Abonnement Mobile Security bei Swisscom monatlich kosten wird.
3. Drücken Sie danach auf die oberste Schaltfläche *Fortlaufendes Abonnement*, wenn Sie ein Abonnement bestellen möchten, das Sie bequem auf Ihre eigene Monatsrechnung von Swisscom belasten lassen.
4. Ihr Mobile Security Programm sendet automatisch ein Gratis-SMS mit dem Schlüsselwort *START SECURITY* an die Zielnummer *811*. Sie erhalten danach eine Information, dass Sie eine Bestätigung der Bestellung erhalten werden. In der Übersicht ihres Mobile Security Programms sehen Sie, dass ihre Bestellung erfolgt ist.
5. Gehen Sie nun in die Applikation *Nachricht*, wo Sie SMS empfangen. Sie haben in ihrem Eingangs-Ordner ein SMS erhalten von der Zielnummer *811* mit dem Schlüsselwort *START SECURITY* und einem Hinweis, wie Sie die Bestellung bestätigen können. Sie erhalten ausserdem nochmals die Information, wieviel Sie das Abonnement Mobile Security monatlich kosten wird.
6. **Wichtig:** Beantworten Sie dieses SMS mit einem neuen SMS mit dem Schlüsselwort *START* an dieselbe Zielnummer (*811*). Ohne diese Antwort ist ihre Bestellung nicht abgeschlossen.
7. Sie erhalten darauf erneut ein SMS in ihrem Eingangs-Ordner von der Zielnummer *811*. Dieses SMS enthält die Bestellbestätigung, die Service-Kosten sowie einen Hinweis, wie Sie das Abonnement Mobile Security kündigen können.
8. In ihrem Mobile Security Programm erscheint nun in der Übersichtseite der Hinweis, dass der Dienst abonniert ist.



Alternative Aktivierung des kostenpflichtigen Abonnements Mobile Security:

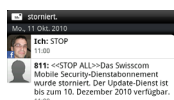
Sie können das Abonnement für Mobile Security auch bestellen, ohne die Trial-Version von Mobile Security zu starten. Dafür senden Sie ein SMS direkt an die Zielnummer *811*. Senden Sie dazu bitte aus ihrer SMS-Applikation ein SMS an die Nummer *811* mit dem folgenden Schlüsselwort: *START*. Sie werden anschliessend per SMS von der Nummer *811* informiert, dass ihr Mobile Security Abonnement bestellt wurde.

3.2 Deaktivierung von Mobile Security (Kündigung)

Abonnementkündigung über die Auswahl «Abbestellen» in Mobile Security (empfohlene Variante):

Wenn Sie Mobile Security nicht mehr nutzen möchten, so finden Sie in ihrem Mobile Security Programm die Auswahl *Abonnement*.

1. Wählen Sie *Fortlaufendes Abonnement* aus.
2. Wählen Sie auf die Schaltfläche *Abbestellen*. Sie finden darauf Informationen zu ihrem Abonnement Mobile Security.
3. Falls Sie Ihr Abonnement bei Swisscom kündigen möchten, so drücken Sie auf die Schaltfläche *Abbrechen*.
4. Im Hintergrund schickt ihr Mobile Security Programm ein Gratis-SMS mit dem Schlüsselwort *STOP SECURITY* an die Zielnummer *811*. Mobile Security zeigt Ihnen an, dass die Kündigungsanforderung abgeschickt wurde und Sie eine Bestätigung per SMS erhalten werden.
5. Sie erhalten darauf ein SMS von der Zielnummer *811* in ihrem Eingangs-Ordner. Dieses enthält die Kündigungsbestätigung sowie einen Hinweis, wie lange das Abonnement Mobile Security noch gültig sein wird.
6. In ihrem Mobile Security Programm erscheint nun in der Übersichtseite der Hinweis, wie lange der Dienst noch abonniert ist.



Alternative Abonnementkündigung per SMS:

Sie haben auch die Möglichkeit, das Abonnement bei Swisscom per SMS an die Zielnummer *811* zu künden. Senden Sie dazu aus ihrer SMS-Applikation ein SMS an die Nummer *811* mit einer der folgenden Texte:

- > STOP, STOPP
- > STOP ALL, STOPP ALL
- > STOP SECURITY

Sie werden anschliessend per SMS von der Nummer *811* informiert, dass ihr Mobile Security Abonnement gekündigt ist und wie lange der Update-Dienst von Mobile Security noch verfügbar ist.

Anmerkung: ein SMS mit den Befehlen *STOP ALL* bzw. *STOPP ALL* löscht auch die Mobile Security Abonnemente von allfälligen Gast-Geräten (siehe Kap. 3.4.2)



3.3 Informationen zu Ihrem Swisscom Abonnement von Mobile Security

Sie können sich jederzeit über Ihr Abonnement Mobile Security per SMS informieren. Mit dem Versenden von SMS mit bestimmten Schlüsselwörtern an die Zielnummer *811* erhalten Sie diverse Informationen per SMS zurück. Folgende Informationen mit den angegebenen Schlüsselwörtern werden Ihnen zurück geschickt.

- > *HELP* oder *INDEX*: Sie erhalten ein SMS mit Angaben zum Service und zu den anfallenden Kosten ihres Abonnements.
- > *INFO*: Sie erhalten ein SMS mit Angaben zu Supportadressen von Swisscom und F-Secure
- > *VIEW*: Sie erhalten ein SMS mit Angaben, ob ihr Abonnement Mobile Security noch aktiv ist oder nicht

3.4 Abonnerung und Kündigung von Mobile Security für ein Gast Gerät

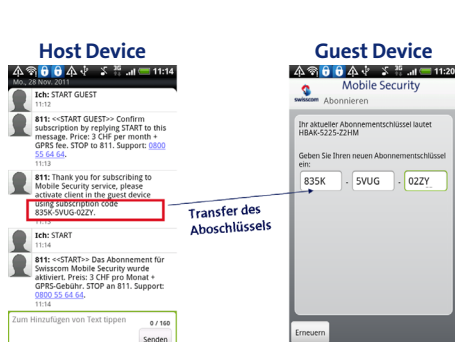
3.4.1 Abonnerung von Mobile Security für ein Gast Gerät (mit oder ohne SIM Karte)

Ab der Version 7.5 von Mobile Security können Sie diese Anwendung auch auf einem mobilen Gerät betreiben,

1. welches permanent ohne SIM-Karte betrieben wird oder
2. welches nicht dauernd mit einer Swisscom SIM Karte betrieben wird oder
3. welches mit einer SIM Karte eines anderen Mobilfunkbetreibers betrieben wird oder
4. dessen monatliche Abo-Kosten für Mobile Security Sie übernehmen möchten

Sie finden die Version von Swisscom Mobile Security im Hauptmenu unter *Info*. Haben Sie eine ältere Version als V7.5, so können Sie die neuste Version herunterladen, indem Sie im Hauptmenu *Aktualisieren* auswählen.

Wenn Ihr kostenloser 30 Tage dauernder Trial abgelaufen ist, werden Sie aufgefordert, Mobile Security zu abonnieren. Im Normalfall abonnieren Sie den Dienst, indem Sie, wie unter Kap. 3.1 beschrieben, den Dienst per SMS über die Nummer *811* auf Ihrem eigenen Abonnement bei Swisscom abonnieren. Wünschen Sie jedoch für die genannten vier Fälle ein mobiles Gerät mit Mobile Security zu betreiben, so können Sie Ihr mobiles Gerät als Gastgerät (*Gast*) deklarieren. Sie brauchen dazu nur ein mobiles Gerät (*Host Gerät*) mit einem Swisscom Abonnement, welches die Kosten für Mobile Security Ihres Gerätes übernimmt. Diese Bezahlmethode eignet sich insbesondere gut, wenn Sie ein *Tablet* ausschliesslich an Ihrem Home WLAN ohne SIM-Karte betreiben möchten und trotzdem gegen die Gefahren im Internet geschützt sein möchten:



1. Senden Sie vom mobilen Gerät (Host Gerät, Bild links), welches die Kosten übernimmt, ein Gratis-SMS mit dem Schlüsselwort *START GUEST* an die Zielnummer *811*.
 2. Ihr Host Gerät erhält danach ein erstes SMS von der Zielnummer *811* mit der Aufforderung, nochmals ein SMS an die Zielnummer *811* zu schicken. Anschliessend sofort ein zweites SMS von der Zielnummer *811* mit einem 12-stelligen *Abonnementsschlüssel*.
 3. Auf dem Host Gerät muss die Abonierung unbedingt nochmals mit einem SMS mit dem Schlüsselwort *START* an die Zielnummer *811* bestätigt werden.
 4. Ihr Host Gerät erhält danach erneut ein SMS von der Zielnummer *811* mit der Mitteilung, dass nun das Abonnement für das Gast-Gerät aktiviert wurde.
 5. Wählen Sie nun auf Ihrem mobilen Gerät (Gastgerät) die Schaltfläche *Kaufen* aus. Danach wählen Sie die zweite Bezahlmethode *Abonnementsschlüssel verwenden* aus. Im folgenden Feld (siehe Bild rechts) können Sie dann den 12-stelligen Abonnementsschlüssel eingeben, welches ihr Host Gerät empfangen hat.
- Anmerkung: Ihr Host Gerät kann die Kosten für mehrere Gast Geräte übernehmen.

3.4.2 Deaktivierung (Kündigung) von Mobile Security für ein Mobiles Gast Gerät

Wenn Ihr Mobile Security Abonnement von einem anderen Mobilen Gerät (Host Gerät) übernommen wird, so muss die Kündigung des Dienstes ebenfalls auf diesem Host Gerät vorgenommen werden.

1. Senden Sie dazu vom mobilen Gerät (Host), welches die Kosten übernimmt ein Gratis-SMS mit dem Schlüsselwort *STOP GUEST* <Gast Abonnementsschlüssel> an die Zielnummer *811*.
2. Das Host Gerät erhält danach ein SMS von der Zielnummer *811* mit einer Kündigungsbestätigung für das Gast Gerät.

Anmerkung: *STOP GUEST* ohne Angabe eines Abonnementsschlüssels wird als ungültiges Schlüsselwort gewertet.

3.4.3 Informationen zu Mobile Security für ein Mobiles Gast Gerät

Sie können sich jederzeit über das Abonnement Mobile Security eines Gast Gerätes per SMS informieren. Mit dem Versenden von SMS mit Hilfe bestimmter Schlüsselwörter vom Host Gerät aus an die Zielnummer 811 erhalten Sie diverse Informationen per SMS zurück. Folgende Informationen mit den angegebenen Schlüsselwörter werden dem Host Gerät zurück geschickt.

- > *HELP GUEST* oder *INDEX GUEST*: das Host Gerät erhält ein SMS mit Angaben zum Service und zu den anfallenden Kosten des Abonnements eines Gast Gerätes.
- > *INFO GUEST*: das Host Gerät erhält ein SMS mit Angaben zu Supportadressen von Swisscom und F-Secure.
- > *VIEW GUEST*: Das Host Gerät erhält ein SMS mit Angaben, ob das Abonnement Mobile Security eines Gast Gerätes noch aktiv ist oder nicht.

Anmerkung: falls das Host Gerät die Kosten für mehrere Gast Geräte übernommen hat, so muss auf dem Host Gerät zur eindeutigen Kennzeichnung eines mobilen Geräts der Abonnementsschlüssel hinter den Schlüsselwörter eingegeben werden. Also z.B. *VIEW GUEST* <Gast Abonnementsschlüssel>.

Anmerkung: falls sie diese SMS vom Gastgerät aus an die Zielnummer 811 senden, bleiben die SMS ohne Wirkung. Die Mobile Security Verwaltung kennt das Gast Gerät nicht über seine Mobiltelefon-Nummer sondern nur über das Host Gerät.

4 Funktionen von Mobile Security

4.1 Diebstahlschutz

Der Diebstahlschutz (Anti-Theft) dient dazu, ihre Daten bei Verlust oder Diebstahl zu schützen, damit diese nicht missbräuchlich genutzt werden. Sie können ausserdem Ihr mobiles Gerät lokalisieren, wenn es sich um ein mobiles Gerät mit GPS Empfänger handelt. Sie benötigen für die Funktionen des Diebstahlschutzes ein weiteres vertrauenswürdigen mobiles Gerät zur Steuerung der Funktionen des Diebstahlschutzes in ihrem mobilen Gerät.

Falls Sie ein mobiles Gerät verwenden, welches keine SMS Funktionen erlaubt, können Sie Anti-Theft nicht nutzen.



Verwenden der Gerätesperre:

Anti-Theft kann Ihr Gerät automatisch sperren, wenn die SIM-Karte im Gerät geändert wurde. Das gesperrte Gerät lässt sich nur mit Ihrem Sperrcode entsperren.

So richten Sie die Gerätesperre ein:

1. Wählen Sie *Einstellungen* im Hauptmenu von Mobile Security.
2. Wählen Sie in der Einstellungsauswahlliste *Anti-Theft* aus.
3. Geben Sie einen *Sicherheitscode* ein. Der Sicherheitscode muss aus mindestens 4 Zeichen bestehen. Bewahren Sie ihn an einem sicheren Ort auf.

Verwenden des ferngesteuerten Diebstahlschutzes:

Der Diebstahlschutz besteht darin, dass Sie mit einem anderen vertrauenswürdigen mobilen Gerät eine SMS-Textnachricht mit Ihrem Sperrcode an Ihr verlorenes oder gestohlenen mobiles Gerät senden können, um dessen Standort zu bestimmen oder um es zu sperren oder dessen Daten zu löschen.

So richten Sie die Remotesperre ein:

1. Öffnen Sie *Einstellungen* im Hauptmenu und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste *Anti-Theft* aus.
3. Wenn Sie in der Lage sein möchten, Ihr Gerät ferngesteuert (remote) zu sperren, befolgen Sie diese Anweisungen:
 - a. Geben Sie einen *Sicherheitscode* (mind. 4 Zeichen, siehe Bild) ein.
 - b. Aktivieren Sie *Remote-Funktionen*, wenn Sie ihr mobiles Gerät ferngesteuert sperren bzw. wenn Sie die Daten auf ihrem mobilen Gerät ferngesteuert löschen möchten. Das gesperrte Gerät lässt sich nur mit Ihrem Sperrcode entsperren.
 - c. Tragen Sie unter *Vertrauenswürdige Nummer* ein vertrauenswürdige mobiles Gerät-Nummer ein, welches eine SMS versenden kann. Dieses mobile Gerät-Nummer benötigen Sie zum Sperren ihres eigenen Gerätes zum Löschen der Daten auf ihrem eigenen Gerät.
 - d. Wählen Sie *Locator aktivieren*, wenn ihr eigenes Gerät von einem anderen Gerät aus lokalisiert werden darf (d.h. die GPS Koordinaten erhalten darf).

So sperren oder reinitialisieren Sie Ihr Gerät aus der Ferne (Remote-Sperrung):

Senden Sie die folgenden SMS-Textnachrichten vom vertrauenswürdigen Gerät an die Nummer Ihres mobilen Gerätes.

> Um ihr mobiles Gerät zu sperren, senden Sie folgende SMS: #LOCK#<Sperrcode> (z. B. #LOCK#abcd1234)

> Um ihr mobiles Gerät zu reinitialisieren, senden Sie folgende SMS: #WIPE#<Sperrcode> (z. B. #WIPE#abcd1234)

Da Speicherkarten mühelos entfernt werden können, speichern Sie Ihre vertraulichen Informationen in den Gerätespeicher. Diesen können Sie mit dem Diebstahlschutz (Anti-Theft) sperren oder löschen.

Der Diebstahlschutz speichert keine Standortdaten. Die einzige Standortinformation befindet sich in der SMS, die an Sie gesendet wird.

So können Sie über das vertrauenswürdige Gerät ihr verlorenes oder gestohlenen mobile Gerät lokalisieren:

- > Um den Standort ihres mobilen Gerätes zu ermitteln, senden Sie folgende SMS mit dem vertrauenswürdigen Gerät an Ihr eigenes mobiles Gerät: #LOCATE#<Sperrcode> (Zum Beispiel): #LOCATE#abcd1234).
- > Das vertrauenswürdige Gerät erhält anschliessend ein SMS von Ihrem mobilen Gerät zurück mit einem Link auf Google Maps. Falls Sie den Aufenthaltsort nicht auf dem vertrauenswürdigen mobilen Gerät anzeigen können, so sehen Sie zumindest in der SMS die GPS-Koordinaten der letzten GPS-Aufzeichnung ihres mobilen Gerätes.

So können Sie den aktuellen Standort ihres mobilen Geräts an Freunde oder Familie schicken:

- > Wählen Sie im Hauptmenu *Diebstahlsicherung* aus
- > Wählen Sie *Standort mitteilen* aus
- > Ihr mobiles Gerät ruft nun die GPS-Daten von ihrem GPS-Empfänger ab und bereitet ein SMS mit einem Google Maps Link ihres Standortes vor.
- > Tragen Sie danach in die Adresszeile des SMS die gewünschte Nummer ein und wählen Sie *Senden* aus.
- > Der Empfänger ihres SMS kann nun ihren Standort über den Link im SMS anschauen oder sieht direkt die GPS-Koordinaten im SMS-Text.

4.2 Auf Viren scannen

Scannen Sie Ihr mobiles Gerät nach der erstmaligen Aktivierung von Mobile Security auf Viren und andere Schadprogramme, um sicherzustellen, dass Ihr Gerät virenfrei ist. Sie sollten Ihr Gerät immer dann scannen, wenn Sie von der Anwendung dazu aufgefordert werden.

Swisscom Mobile Security wird im Hintergrund ausgeführt und scannt Ihre Dateien automatisch.

1. Falls während des Echtzeit-Scans ein Schadprogramm gefunden wird, wird eine Meldung angezeigt. Drücken Sie auf *Ja*, um die infizierte(n) Datei(en) anzuzeigen, oder auf *Nein*, um die Anzeige zu schließen.
2. Die Ansicht *Infizierte Dateien* zeigt eine Liste mit infizierten Dateien, die auf Ihrem mobilen Gerät gefunden wurden, sowie den Status der jeweiligen Datei (unter Quarantäne, freigegeben).

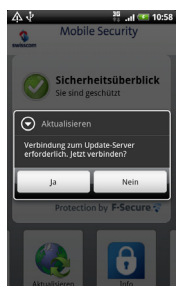
Wenn Sie zusätzliche Details zu einer infizierten Datei anzeigen möchten, gehen Sie folgendermassen vor:

1. Scrollen Sie zu der infizierten Datei und drücken Sie die Auswahl Taste.
2. Wählen Sie *Anzeigen*.
3. Die Anzeige mit den Infektionsdetails zeigt den Pfad und den Namen der infizierten Datei an sowie den Namen des Schadprogramms, mit dem die Datei infiziert wurde.

Zur Verarbeitung infizierter Dateien gehen Sie folgendermassen vor:

1. Scrollen Sie in der Ansicht *Infizierte Dateien* zu der infizierten Datei, die Sie verarbeiten möchten.
2. Drücken Sie auf die Auswahl Taste.
3. Wählen Sie eine der folgenden Aktionen aus:
 - > *Löschen* – Löscht die infizierte Datei. Dies ist die empfohlene Option. Die Datei wird vollständig von Ihrem Gerät entfernt.
 - > *Quarantäne* – Stellt die infizierte Datei unter Quarantäne, falls die Datei noch nicht unter Quarantäne ist. Eine Datei unter Quarantäne ist gesperrt und kann Ihr Gerät nicht schädigen, wenn Mobile Security aktiviert ist.
 - > *Freigeben* – Gibt die unter Quarantäne stehende Datei frei. Wenn Sie eine Datei freigeben, ist sie nicht mehr gesperrt. Sie können auf Ihr eigenes Risiko auf die frei gegebene Datei zugreifen.

4.3 Automatische Updates (Aktualisierungen)



Swisscom Mobile Security enthält einen automatischen Update-Dienst. Damit wird die Virendefinitionsdatenbank der Anwendung regelmäßig aktualisiert. Nur eine aktuelle Virendefinitionsdatenbank schützt Ihr Gerät vor den neuesten Viren und anderen Schadprogrammen. Automatische Updates werden verwendet, nachdem Sie das Produkt aktiviert haben. Die Anwendung benötigt für die Updates eine aktive Internetverbindung. Wenn eine Verbindung mit dem Internet verfügbar ist, prüft Mobile Security, wann die Virendefinitionsdatenbank zuletzt aktualisiert wurde, und lädt ggf. neue Updates herunter. Beachten Sie, dass hier ein Datentransfer stattfindet. Akzeptieren Sie deshalb diese Funktion nur, wenn Sie sich in einem Netz befinden, wo die Kosten für den Datentransfer im Abonnement enthalten sind oder wenn Sie sich in einem privaten WLAN befinden.

4.4 Manuelle Updates

Sie können den Update Dienst auch manuell aktualisieren:

1. Gehen Sie im Mobile Security Hauptmenu zur Auswahl *Aktualisieren*.
2. Beantworten Sie die Frage nach der Verbindung zum Update-Server mit *Ja*.
3. Wählen Sie den Internet-Zugriffspunkt für die Verbindung mit dem Update-Server. Beachten Sie, dass hier ein Datentransfer stattfindet. Nutzen Sie deshalb diese Funktion nur, wenn Sie sich in einem Netz befinden, wo die Kosten für den Datentransfer im Abonnement enthalten ist. Die aktualisierte Virendefinitionsdatenbank wird von der Anwendung heruntergeladen und sofort eingesetzt.
4. Wenn das Update beendet ist, drücken Sie auf *Ja*, um Ihr Gerät auf Viren zu überprüfen, wenn Sie dazu aufgefordert werden. Wenn eine neue Version von Mobile Security verfügbar ist, fordert Sie eine Meldung zum Herunterladen der Version auf. Im Anschluss an die Aktualisierung wird die Anwendung automatisch neu gestartet.

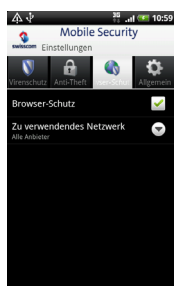
4.5 Sichere Nutzung des Internets mit dem Browser-Schutz

Mobile Security installiert auf Ihrem mobilen Gerät auch automatisch einen weiteren Internet Browser, der als Symbol mit der Bezeichnung Browser-Schutz auf ihrem mobilen Gerät im App Menu erscheint. Benutzen Sie diesen Browser, wenn immer Sie im Internet surfen.

Mithilfe des Browser-Schutzes können Sie die Sicherheit von Websites einschätzen und unabsichtliche Besuche gefährlicher Websites vermeiden. Sobald Sie eine Website besuchen, prüft das Produkt automatisch deren Sicherheit. Ist die Website als verdächtig oder gefährlich eingestuft (Phishing Webseiten oder mit Schadprogrammen infiziert), blockiert Mobile Security

den Zugriff auf diese Website. Die Sicherheitseinstufung einer Website basiert auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partner von F-Secure.

Sie können den Browser-Schutz auch aus Mobile Security heraus aufrufen. Wählen Sie Browser-Schutz im Hauptmenu auf und wählen Sie anschliessend Sicherer Browser aus. Wichtig: der Browser-Schutz ist nur aktiv, wenn Sie mit diesem Browser im Internet surfen. Wenn Sie trotzdem einen anderen Browser auswählen, sind Sie beim Surfen nicht geschützt. Wenn Sie für Ihr Kind die Kindersicherung aktiviert haben, wird das mobiles Gerät immer den Browser-Schutz benutzen, auch wenn Ihr Kind einen anderen Browser aufrufen möchte.



Ändern der Browser-Schutz-Einstellungen:

Wählen Sie aus, wann der Browser-Schutz aktiviert werden soll. Die Aktivierung richtet sich nach dem von Ihnen genutzten Netz. So ändern Sie die Einstellungen des Produkts:

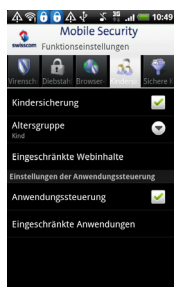
1. Wählen Sie in der Hauptansicht von Mobile Security die Schaltfläche *Einstellungen* und wählen Sie *Browser-Schutz* aus.
2. Aktivieren Sie den Browser-Schutz, indem Sie im Feld *Browser-Schutz* die Eingabe auf *Ein* setzen. Damit läuft Mobile Security im Hintergrund, während Sie das Internet durchsuchen.
3. Wählen Sie aus, wann der Browser-Schutz aktiviert werden soll:
 - > *Alle Anbieter* – Das Produkt prüft die Sicherheit der von Ihnen besuchten Websites unabhängig von dem Netz, das Sie gerade nutzen (siehe Bild).

> *Nur mein Anbieter* – Das Produkt prüft die Sicherheit der von Ihnen besuchten Websites nur, wenn Sie gerade das Netz Ihres eigenen Anbieters nutzen.

Das Produkt wendet die neuen Einstellungen sofort an. Es kann sein, dass Sie Mobile Security auffordert, den Browser als Standard zu verwenden, den der Hersteller Ihres mobilen Gerätes installiert hat. Um einen optimalen Surfschutz zu erhalten, sollten Sie daher auf den von Mobile Security empfohlenen Browser als Standard wechseln.

Den Status des Browser-Schutzes Ihres mobilen Geräts können Sie jederzeit überprüfen, indem Sie im Hauptmenu von Mobile Security die Schaltfläche *Browser-Schutz* auswählen.

4.6 Kindersicherung



Ihr Swisscom Mobile Security ist ab der Version V7.5 mit einer Kindersicherung ausgestattet, die Sie nach Bedarf für Ihre Kinder oder Teenager einschalten können. Sie finden die Version von Swisscom Mobile Security im Hauptmenu unter *Weitere Info*. Haben Sie eine ältere Version als V7.5, so können Sie die neuste Version herunterladen, indem Sie im Hauptmenu *Aktualisieren* auswählen.

Die Kindersicherung erlaubt es Ihnen, die Auswahl an aufrufbaren Webseiten im Internet für Ihr Kind einzuschränken. In der Grundeinstellung, d.h. nach der Aktivierung von Swisscom Mobile Security, ist die Kindersicherung ausgeschaltet.

Die Kindersicherung finden Sie innerhalb von Swisscom Mobile Security im Haupt-Menu unter *Einstellungen* → *Kindersicherung*. oder im Haupt-Menu unter *Kindersicherung* → *Einstellungen* (siehe Bild).

Im Menu Kindersicherung können Sie die Kindersicherung generell mit einem Häkchen ein- oder ausschalten (erster Menüpunkt). Wenn Sie die Kindersicherung ausgeschaltet lassen, dann können Sie weiterhin die verschiedenen Internet Browser, die auf dem mobilen Gerät Ihres Kindes installiert haben, nutzen. Wir empfehlen Ihrem Kind jedoch stets die Benutzung des Browser-Schutzes, damit es gegen die Gefahren von mit schädlichen Programmen infizierten Webseiten bzw. betrügerische (Phishing) Webseiten geschützt bleibt.

Wenn Sie die Kindersicherung einschalten, egal in welcher Stufe, dann kann Ihr Kind nur noch den Browser-Schutz benutzen. Sollte Ihr Kind einen anderen Internet Browser aufrufen, wird Ihrem Kind automatisch der Browser-Schutz geöffnet. Damit wird gewährleistet, dass Ihr Kind nicht nur gegen Schadsoftware auf infizierten Seiten geschützt wird, sondern auch nur noch diejenigen Webseiten einer Kategorie aufrufen kann, die Sie ihm erlauben. Bei allen Änderungen an diesen Einstellungen werden Sie aufgefordert einen *Sicherheitscode* einzugeben, welchen nur Sie (und nicht Ihr Kind) kennen sollten. Sollten Sie diesen Sicherheitscode beim erstmaligen Einrichten von Swisscom Mobile Security noch nicht definiert haben, dann können Sie dies hier nachholen.



Kindersicherung für Jugendliche:

Aktivieren Sie die *Kindersicherung* und wählen Sie unter *Altersgruppe* die Einstellung *Jugendlicher*. In der Auswahl *Eingeschränkte Webinhalte* (dritter Menüpunkt) finden Sie die voreingestellten erlaubten und gesperrten Webseitenkategorien für Jugendliche. Sie können nun je nach Wunsch die Kategorienliste für Ihren Jugendlichen noch korrigieren, indem Sie die entsprechenden Häkchen in der Kolonne *Zulassen* (siehe Bild) setzen oder löschen.

Kindersicherung für Kinder (siehe Bild):

Aktivieren Sie die *Kindersicherung* und wählen Sie unter *Altersgruppe* die Einstellung *Kind*. In der Auswahl *Eingeschränkte Webinhalte* finden Sie die voreingestellten erlaubten und gesperrten Webseitenkategorien für Kinder. Sie können nun je nach Wunsch die Kategorienliste für Ihr Kind noch korrigieren, indem Sie die entsprechenden Häkchen in der Kolonne *Zulassen* setzen oder löschen.

Kindersicherung für Erwachsene:

Diese Stufe können Sie als Erwachsener im Menüpunkt *Altersgruppe* setzen, um entweder temporär die Kindersicherung für Ihr Kind aufzuheben oder Ihrem Jugendlichen ein von Ihnen angepasstes Kategorienprofil wie für Erwachsene geben zu können. Sie können diese Altersgruppe aber auch setzen, um zu verhindern, dass Sie oder Ihr Jugendlicher selber einen anderen Browser benutzen als den Browser-Schutz, der Sie gegen Webseiten mit schädlicher Software schützt.

Was sollten Sie ausserdem wissen: wenn Sie die Kindersicherung auf dem mobilen Gerät Ihres Kindes eingeschaltet haben, egal in welcher Stufe, dann kann Ihr Kind keine anderen Browser nutzen ausser dem Browserschutz. Sie, bzw. Ihr Kind, werden zudem bei bestimmten Applikationen oder administrativen Aufgaben aufgefordert, den Sicherheitscode der Kindersicherung einzugeben. Die Eingabe des Sicherheitscodes schützt davor, dass Ihr Kind die Sicherheitseinstellungen der Kindersicherung umgeht oder z.B. versucht, Swisscom Mobile Security zu stoppen, zu deaktivieren oder zu deinstallieren. Der Sicherheitscode ist identisch mit dem Sicherheitscode, den Sie auch für den Diebstahlschutz verwenden.



Anwendungssteuerung

Die Kindersicherung von Mobile Security ist ausserdem mit einer Anwendungssteuerung ausgestattet. Damit können Sie Ihrem Kind gezielt das Nutzen von bestimmten Applikationen (Apps) sperren. Unter *Eingeschränkte Anwendungen* sucht die Kindersicherung alle installierten Apps ab und zeigt diese zunächst als zugelassen an. Sie können nun die einzelnen Apps sperren, indem Sie das Häkchen unter *Zulassen* (siehe Bild) entfernen. Beachten Sie, dass auch hier die Änderungen die Eingabe des Sicherheitscodes erfordern. Damit wird verhindert, dass Ihr Kind nachträglich die Änderungen wieder rückgängig machen kann. Die von Ihnen gesperrten Apps werden nicht deinstalliert, sondern verbleiben im App Menu des Smartphones Ihres Kindes. Sollte Ihr Kind nun trotzdem die App aufrufen wollen, dann wird ihm in einem Fenster angezeigt, dass Swisscom Mobile Security die App blockiert hat.

Sollte Ihr Kind zu einem späteren Zeitpunkt weitere Apps installieren, so sind diese zunächst automatisch durch die Anwendungssteuerung blockiert. Ihr Kind muss sich dann an Sie wenden, damit Sie ihm diese App in der Anwendungssteuerung der Kindersicherung frei geben können.

4.7 Schutz vor ungewollten Anrufen und Nachrichten

Die Funktion *Sichere Kontakte* schützt Sie vor ungewollten Anrufen und Nachrichten. Mit *Sichere Kontakte* können Sie einstellen, von wem Sie Anrufe und Nachrichten erhalten möchten, und ungewollte Anrufe und Spam-Nachrichten sperren. Sie können die Nummern auswählen, die Sie sperren möchten. *Sichere Kontakte* sperrt alle einkommenden Anrufe und SMS/MMS-Nachrichten von den ausgewählten Nummern. Ausserdem werden ausgehende Anrufe an die Nummern dieser Sperrliste ebenfalls blockiert (editierbar).

Verwenden von Sichere Kontakte

Sichere Kontakte sperrt Anrufe und Nachrichten von Nummern der Sperrliste. Folgen Sie diesen Anweisungen, um Anrufe und Nachrichten von einer neuen Nummer zu sperren:

1. Wählen Sie in der Hauptansicht die Option *Einstellungen*. Die Einstellungsauswahlliste wird geöffnet.
2. Wählen Sie *Sichere Kontakte* aus der Einstellungsauswahlliste aus. Hinweis: Als nächstes stellen Sie Ihren Sicherheitscode ein, wenn Sie dies noch nicht getan haben.
3. Stellen Sie sicher, dass *Sichere Kontakte* aktiviert ist.
4. Wählen Sie *Nummern blockieren* aus. Geben Sie Ihren Sicherheitscode ein, um neue Nummern zu sperren.
Die Liste mit den gesperrten Nummern öffnet sich.
5. Wählen Sie *Geben Sie eine Nummer ein, die blockiert werden soll* aus.
6. Geben Sie zuerst den Namen dann im zweiten Feld die Nummer ein, die Sie sperren möchten.
7. Wählen Sie *Speichern* aus, um die Nummer zur Liste mit den gesperrten Nummern hinzuzufügen.

Wenn *Sichere Kontakte* aktiviert ist, erhalten Sie keine Anrufe oder Nachrichten mehr von den Nummern aus der Liste mit den gesperrten Nummern (Der Anruf wird nur kurz angezeigt und erscheint in Ihrer Telefon-Liste der nicht beantworteten Anrufe). Ausserdem sind alle Anrufe an die gesperrten Nummern ebenfalls blockiert.

Wenn Sie die Blockierung für eingehende und ausgehende Anrufe und Nachrichten unterschiedlich behandeln wollen oder löschen wollen, dann wählen Sie den blockierten Kontakt in der Liste aus. Im aufgehenden Fenster können Sie den Kontakt wieder löschen oder detailliert bearbeiten.

Anzeigen gesperrter Anrufe und Nachrichten

Sie können im Blockierungsverlauf sehen, welche Anrufe und Nachrichten von *Sichere Kontakte* gesperrt wurden.

Folgen Sie diesen Anweisungen, um anzuzeigen, welche Anrufe und Nachrichten von *Sichere Kontakte* gesperrt wurden:

1. Wählen Sie in der Hauptansicht die Option *Einstellungen*. Die Einstellungsauswahlliste wird geöffnet.
2. Wählen Sie *Sichere Kontakte* aus der Einstellungsauswahlliste aus.
3. Wählen Sie *Blockierungsverlauf anzeigen*.

5. Technischer Support

Wenn Sie Fragen zur Anwendung oder zur Installation/Aktivierung/Deaktivierung und zum Trial haben, können Sie sich an die Swisscom Hotline 0800 55 64 64 wenden.

Um weitere Informationen zu den Funktionen von Mobile Security im Internet zu erhalten, können Sie auch bei unserem Security Partner die Supportseiten besuchen http://www.f-secure.com/de_DE/support/

Beachten Sie aber, dass Ihr Mobile Security Programm von Swisscom in Bezug auf Installation, Aktivierung, Deaktivierung und Aussehen vom Standardprodukt von F-Secure abweichen kann.

