

Mobile Security per apparecchi Android 2.2–3.2

1 Swisscom Mobile Security™ per apparecchi Android 2.2–3.2

Questo manuale vale per apparecchi mobili (smartphone, tablet) che hanno il sistema operativo Android (versione da 2.2 a 3.2). Per sapere quali sono gli apparecchi mobili con questo sistema operativo testati da Swisscom Mobile Security, siete pregati di consultare la pagina internet www.swisscom.com/f-secure.

2 Installazione di Mobile Security

2.1 Apparecchi con sistema operativo Android con programma Mobile Security preinstallato



Il programma Mobile Security di Swisscom è in parte già preinstallato sull'apparecchio mobile acquistato da Swisscom. Nella maggior parte dei casi il software preinstallato si trova nel *menu Applicazioni (App)*. Pertanto potete attivare direttamente il programma Mobile Security selezionando il simbolo con il lucchetto denominato *Mobile Security*. Osservazione: a seconda del tipo di apparecchio mobile, la designazione può figurare anche in forma abbreviata. Quando richiamate Mobile Security per la prima volta dovete innanzitutto attivare detto programma (vedi capitolo 3) affinché il vostro apparecchio sia protetto. Il prodotto non protegge l'apparecchio fintanto che non l'avete attivato. Potete scegliere di testare gratuitamente il prodotto per un periodo di 30 giorni prima di stipulare l'abbonamento con Swisscom.

2.2 Apparecchi con sistema operativo Android con Swisscom Security Launcher preinstallato



In caso abbiate acquistato l'apparecchio mobile presso Swisscom, è possibile che nel *menu Applicazioni (app)* si trovi il simbolo con il lucchetto denominato Swisscom Security Launcher (ev. con denominazione abbreviata). Selezionando questo simbolo si apre un programma di download dedicato (launcher) per il programma Mobile Security di Swisscom. Tenete presente che durante l'installazione state scaricando una quantità di dati dell'ordine di grandezza di 2 MB. Dovreste quindi avere un abbonamento di Swisscom con l'opzione dati e, durante il download, trovarvi nella rete Swisscom o in un WLAN privata. Importante: assicuratevi innanzitutto di aver attivato l'abilitazione per *Origini sconosciute*. Potete effettuare questa attivazione nel menu *Impostazioni* → *Applicazioni* e ripristinare il blocco ad installazione di Mobile Security avvenuta. Lo Swisscom Security Launcher vi condurrà a tale impostazione, in caso non aveste ancora abilitato l'opzione Origini sconosciute. Al termine dell'installazione dovete dapprima attivare Mobile Security (vedi capitolo 3). Il prodotto non protegge l'apparecchio fintanto che non l'avete attivato. Potete scegliere di testare gratuitamente il prodotto per un periodo di 30 giorni prima di stipulare l'abbonamento con Swisscom.

2.3 Apparecchi con sistema operativo Android senza Mobile Security o Swisscom Security Launcher preinstallati

Potete installare l'applicazione Swisscom Mobile Security anche in caso abbiate acquistato un apparecchio mobile senza il programma Swisscom Mobile Security né lo Swisscom Security Launcher preinstallati. Vi accorgete dell'assenza delle due app dal fatto che nel *menu Applicazioni (app)* del vostro apparecchio mobile non c'è il simbolo con il lucchetto di Swisscom. *Importante:* assicuratevi innanzitutto di aver attivato l'abilitazione per *Origini sconosciute*. Potete effettuare questa attivazione nel menu *Impostazioni* → *Applicazioni* e ripristinare il blocco ad installazione di Mobile Security avvenuta. Aprite il browser e scrivete l'indirizzo <http://mobile.f-secure.com/swisscom> nell'apposito campo. Ora avviate il download dalla pagina internet che si è aperta. Selezionate il download di Mobile Security per Android 2.2–3.2. Una volta scaricato, il programma si trova nelle Benachrichtigungen sull'apparecchio mobile. Attivate il programma Mobile Security scaricato e seguite le istruzioni dell'assistente d'installazione.

3 Attivazione/disattivazione di Mobile Security

3.1 Attivazione di Mobile Security



Attivazione della demo gratuita di Mobile Security:

Se avviate Mobile Security per la prima volta, potete innanzitutto testare gratuitamente l'applicazione per un periodo di prova di 30 giorni. La durata della prova inizia con la prima attivazione di Mobile Security. Premete sul simbolo di Mobile Security, successivamente sull'opzione *Attiva* e seguite le istruzioni dell'assistente, che vi indicherà come effettuare l'attivazione. Durante l'attivazione è auspicabile anche aggiornare il programma presso un server di aggiornamenti. Utilizzate nella rete mobile di Swisscom il collegamento *Swisscom Services* per scaricare gli aggiornamenti. L'assistente di attivazione vi pregherà poi di effettuare le configurazioni necessarie in Mobile Security e di scansionare l'apparecchio alla ricerca di virus. Potete però anche farlo in un secondo tempo. Se avete attivato Mobile Security correttamente, la durata rimanente del periodo di prova verrà segnalata nella panoramica di Mobile Security. Nel periodo di prova, Mobile Security possiede le stesse funzioni della versione in

abbonamento.

Tuttavia durante il periodo di prova potete in qualsiasi momento ordinare direttamente un abbonamento a pagamento presso Swisscom. Mobile Security vi rammenterà con un anticipo tra 7 e 3 giorni che il periodo di prova gratuito sta per scadere. Per continuare a proteggere l'apparecchio mobile in modo ottimale, a questo punto vi consigliamo di stipulare tempestivamente un abbonamento con Swisscom.



Ordinazione dell'abbonamento Mobile Security a pagamento (variante consigliata):

1. Aprite l'applicazione *Mobile Security* nel menu principale o nel menu programmi. Mobile Security indica la panoramica dei giorni di prova rimanenti.
2. Selezionate l'icona *Acquista*. Vedrete la scadenza dell'abbonamento di prova e il costo mensile dell'abbonamento a Swisscom Mobile Security.
3. Premete poi l'icona *Abbonamento continuo* se desiderate ordinare un abbonamento che potrete comodamente far addebitare sulla vostra fattura mensile di Swisscom.
4. Il programma Mobile Security invia automaticamente un SMS gratuito con la parola chiave *START SECURITY* al numero *811*. Successivamente sarete informati che riceverete una conferma dell'ordine. Nella panoramica del programma Mobile Security vedrete che l'ordine è andato a buon esito.
5. Andate ora nell'applicazione *Messaggi* dove ricevete gli SMS. Nella cartella della posta in arrivo figura l'SMS ricevuto dal numero *811* con la parola chiave *START SECURITY* e l'indicazione di come confermare l'ordine. Inoltre riceverete una seconda notifica di quanto vi costerà mensilmente l'abbonamento a Mobile Security.
6. **Importante:** rispondete a questo SMS con un nuovo SMS con la parola chiave *START* allo stesso numero (*811*). Senza questa risposta l'ordine non è concluso.
7. Riceverete un altro SMS nella cartella della posta in arrivo dal numero *811* contenente la conferma dell'ordine, i costi di servizio come pure un'indicazione di come disdire l'abbonamento Mobile Security.
8. A questo punto nella panoramica del programma Mobile Security appare il messaggio di avvenuta attivazione del servizio.



Attivazione alternativa dell'abbonamento Mobile Security a pagamento:

Potete ordinare l'abbonamento a Mobile Security anche senza avviare la versione di prova di Mobile Security. Per farlo inviate direttamente un SMS al numero *811*.

Inviare dunque dall'applicazione SMS un SMS al numero *811* con la seguente parola chiave: *START*.

Successivamente sarete informati via SMS dal numero *811* che l'abbonamento a Mobile Security è stato ordinato.

3.2 Disattivazione di Mobile Security (disdetta)

Disdetta dell'abbonamento tramite l'opzione «Disdici» di Mobile Security (variante consigliata):

Se non desiderate più il servizio Mobile Security trovate nel programma Mobile Security l'opzione *Abbonamento*.

1. Selezionate *Abbonamento continuo*.
2. Premete l'icona *Disdici*. Qui trovate informazioni sull'abbonamento Mobile Security.
3. Se volete disdire l'abbonamento presso Swisscom premete l'icona *Annulla abbonamento*.
4. Il programma Mobile Security invia automaticamente un SMS gratuito con la parola chiave *STOP SECURITY* al numero *811*. Mobile Security vi indica che la richiesta di disdetta è stata spedita e che riceverete un SMS di conferma.
5. Nella cartella di posta in arrivo ricevete quindi dal numero 811 un SMS contenente la conferma della disdetta come pure l'indicazione della rimanente validità dell'abbonamento a Mobile Security.
6. Nella panoramica del programma Mobile Security appare ora l'indicazione della rimanente durata del servizio in abbonamento.



Disdetta alternativa dell'abbonamento via SMS:

Potete anche disdire l'abbonamento presso Swisscom con un SMS al numero 811.

Per farlo inviate dall'applicazione SMS un SMS al numero 811 con uno dei testi seguenti:

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

Successivamente sarete informati con un SMS dal numero 811 dell'avvenuta disdetta dell'abbonamento Mobile Security e del tempo rimanente in cui sarà disponibile il servizio aggiornamenti di Mobile Security.

Osservazione: un SMS con gli ordini STOP e/o STOP ALL cancella anche gli abbonamenti Mobile Security di eventuali apparecchi ospiti (vedi cap. 3.4.2)



3.3 Informazioni sull'abbonamento Swisscom Mobile Security

Potete informarvi in qualsiasi momento via SMS sull'abbonamento Mobile Security. Inviando degli SMS con determinate parole chiave al numero *811* ricevete varie informazioni, sempre via SMS. Ecco le informazioni con le rispettive parole chiave che potete ricevere.

- > *HELP* oppure *INDEX*: ricevete un SMS con informazioni sul servizio e sui costi dell'abbonamento.
- > *INFO*: ricevete un SMS che vi indica gli indirizzi di supporto di Swisscom ed F-Secure
- > *VIEW*: ricevete un SMS che vi indica se l'abbonamento Mobile Security è ancora attivo oppure no

3.4 Abbonamento e disdetta di Mobile Security per un apparecchio ospite

3.4.1 Abbonamento a Mobile Security di un apparecchio ospite (con o senza scheda SIM)

A partire dalla versione 7.5 di Mobile Security, potete utilizzare questa applicazione anche su un apparecchio mobile,

1. gestito permanentemente senza scheda SIM oppure
2. non sempre gestito con una scheda SIM di Swisscom oppure
3. gestito con una scheda SIM di un altro operatore di rete mobile oppure
4. di cui voi desiderate assumere le spese mensili di abbonamento a Mobile Security

Trovate la versione di Swisscom Mobile Security nel menu principale sotto *Informazioni* su. Se possedete una versione anteriore a V7.5 potete scaricare la versione più recente selezionando *Aggiorna* nel menu principale.

Una volta scaduto il periodo di prova di 30 giorni, sarete sollecitati ad abbonarvi a Mobile Security. Di norma l'abbonamento al servizio si sottoscrive, come descritto al cap. 3.1., abbonando il servizio tramite SMS al numero 811 sul vostro abbonamento Swisscom personale. Se tuttavia, per i quattro casi summenzionati, desiderate gestire un apparecchio mobile con Mobile Security, potete dichiarare il vostro apparecchio mobile come apparecchio ospite (ospite). A tal fine vi serve unicamente un apparecchio mobile (apparecchio host) con un abbonamento Swisscom, sul quale addebitare le spese di Mobile Security del vostro apparecchio. Questa modalità di pagamento è particolarmente indicata se desiderate gestire un tablet esclusivamente nello WLAN privato senza scheda SIM, ma tuttavia essere protetti dai pericoli di internet:



Trasferimento della chiave d'abbonamento

1. Dall'apparecchio mobile (apparecchio host, immagine a sinistra) sul quale addebitare le spese, inviate un SMS gratuito con la parola chiave *START GUEST* al numero *811*.
 2. L'apparecchio host riceve poi un primo SMS dal numero *811* con l'invito a spedire di nuovo un SMS al numero *811*. Ricevete immediatamente un secondo SMS dal numero *811* con un *codice di abbonamento* a 12 caratteri.
 3. La sottoscrizione dell'abbonamento sull'apparecchio host va imperativamente confermata di nuovo inviando un SMS con la parola chiave *START* al numero *811*.
 4. Successivamente l'apparecchio host riceve di nuovo un SMS dal numero *811* con la comunicazione dell'avvenuta attivazione dell'abbonamento per l'apparecchio ospite.
 5. Selezionate ora sul vostro apparecchio mobile (apparecchio ospite) l'icona *Acquista*. Selezionate poi la seconda modalità di pagamento *Utilizza codice abbonamento*. Nel campo seguente (vedi immagine a destra) potete poi inserire il codice di abbonamento di 12 caratteri ricevuto sul vostro apparecchio host.
- Osservazione: sul vostro apparecchio host possono essere addebitate le spese di vari apparecchi ospiti.

3.4.2 Disattivazione (disdetta) di Mobile Security per un apparecchio mobile ospite

Se le spese del vostro abbonamento a Mobile Security vengono addebitate a un altro apparecchio mobile (apparecchio host), anche la disdetta del servizio va effettuata su questo apparecchio host.

1. A tal fine inviate dall'apparecchio mobile (host) che si assume le spese un SMS gratuito con la parola chiave *STOP GUEST* <codice di abbonamento ospite> al numero *811*.
2. L'apparecchio host riceve poi un SMS dal numero *811* con la conferma della disdetta per l'apparecchio ospite.

Osservazione: la parola chiave *STOP GUEST* senza l'indicazione del codice di abbonamento è considerata nulla.

3.4.3 Informazioni su Mobile Security per un apparecchio mobile ospite

Potete in qualsiasi momento richiedere tramite SMS informazioni sull'abbonamento Mobile Security di un apparecchio mobile. Inviando degli SMS abbinati a determinate parole chiave dall'apparecchio host al numero *811* ricevete varie informazioni via SMS. L'apparecchio host riceve le seguenti informazioni con le parole chiave indicate di seguito.

- > *HELP GUEST* oppure *INDEX GUEST*: l'apparecchio host riceve un SMS con indicazioni riguardanti il servizio e i costi maturati per l'abbonamento di un apparecchio ospite.
- > *INFO GUEST*: l'apparecchio host riceve un SMS con indicazioni in merito agli indirizzi di supporto di Swisscom e di F-Secure.
- > *VIEW GUEST*: l'apparecchio host riceve un SMS con l'indicazione se l'abbonamento Mobile Security di un apparecchio ospite è ancora attivo oppure no.

Osservazione: nel caso in cui l'apparecchio host si è assunto le spese di abbonamento di vari apparecchi ospiti, sull'apparecchio host occorre, ai fini dell'identificazione inequivocabile di un apparecchio mobile, inserire, dopo le parole chiave, anche il codice di abbonamento dell'apparecchio in questione. Cioè, ad es., *VIEW GUEST* <codice di abbonamento ospite>.

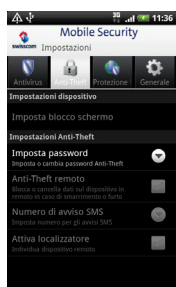
Osservazione: se inviate tali SMS dall'apparecchio ospite al numero *811*, essi saranno inefficaci. L'amministrazione di Mobile Security infatti non riconosce l'apparecchio ospite attraverso il suo numero di cellulare, ma solo attraverso l'apparecchio ospite.

4 Funzioni di Mobile Security

4.1 Protezione antifurto

La protezione antifurto (Anti-Theft) serve a proteggere i vostri dati in caso di smarrimento o furto, in modo che non vengano usati impropriamente. Potete inoltre localizzare l'apparecchio mobile, purché sia dotato del dispositivo GPS. Per poter gestire le funzioni di protezione antifurto del vostro cellulare avete bisogno di un altro apparecchio mobile fidato.

Se utilizzate un apparecchio mobile che non consente le funzioni SMS non potete usare Anti-Theft.



Utilizzo del blocco dell'apparecchio

Anti-Theft può bloccare automaticamente il vostro apparecchio se la carta SIM dello stesso è stata cambiata. L'apparecchio bloccato può essere sbloccato solo tramite il vostro codice di blocco.

Come effettuare il blocco dell'apparecchio:

1. selezionate Impostazioni nel menu principale di Mobile Security;
2. selezionate Anti-Theft nella lista delle Impostazioni;
3. premete Configura codice di sicurezza. Il codice di sicurezza deve essere composto da un minimo di 4 caratteri. Conservatelo in un luogo sicuro.

Utilizzo della protezione antifurto in modalità remota

La protezione antifurto consiste nell'invviare con un altro apparecchio mobile fidato un SMS contenente il codice di blocco all'apparecchio mobile smarrito o rubato per determinarne la posizione o per bloccarlo o per cancellare i dati ivi contenuti.

Come effettuare il blocco remoto:

1. Aprite le *Impostazioni* nel menu principale e premete il tasto Opzioni.
2. Nelle impostazioni selezionate l'opzione *Anti-Theft*.
3. Se volete essere in grado di bloccare l'apparecchio a distanza (remote), seguite le istruzioni:
 - a. premete *configura codice di sicurezza* (minimo 4 caratteri, vedi immagine);
 - b. attivate *Anti-Theft remoto*, se volete bloccare l'apparecchio mobile a distanza oppure cancellarne i dati a distanza. L'apparecchio bloccato può essere sbloccato solo con il vostro codice di blocco;
 - c. inserite sotto *Numero attendibile* il numero di un apparecchio mobile fidato dal quale inviare un SMS. Questo numero di apparecchio mobile serve a bloccare il vostro apparecchio o a cancellarne i dati;
 - d. selezionate *Attiva localizzatore*, in modo da consentire a un altro apparecchio di localizzare il vostro (ovvero se gli concedete di ricevere le coordinate GPS).

Come bloccare o reiniziare il vostro apparecchio a distanza (blocco remoto):

Inviare i seguenti messaggi SMS dall'apparecchio mobile fidato al vostro.

> Per bloccare l'apparecchio mobile inviate il seguente SMS: #LOCK#<codice di blocco> (p.es. #LOCK#abcd1234)

> Per reiniziare l'apparecchio mobile inviate il seguente SMS: #WIPE#<codice di blocco> (p.es. #WIPE#abcd1234)

Dato che le schede di memoria possono essere rimosse con facilità, salvate le informazioni confidenziali nella memoria dell'apparecchio. Quest'ultima può essere bloccata o cancellata tramite la protezione antifurto (Anti-Theft).

La protezione antifurto non salva nessun dato relativo alla posizione. L'unica informazione riguardante la posizione si trova nell'SMS inviato a voi.

Come localizzare l'apparecchio smarrito o rubato attraverso l'apparecchio mobile fidato:

- > Per determinare la posizione del vostro apparecchio mobile, inviate al vostro numero il seguente SMS con l'apparecchio mobile fidato: #LOCATE#<codice di blocco> (per esempio): #LOCATE#abcd1234).
- > Successivamente l'apparecchio fidato riceve un SMS dal vostro apparecchio mobile con un link a Google Maps. Anche se l'apparecchio mobile fidato non vi consente di visualizzare il luogo in cui si trova il vostro apparecchio, nell'SMS vedete almeno le coordinate dell'ultima registrazione GPS del vostro apparecchio mobile.

Come inviare la posizione aggiornata del vostro apparecchio mobile ad amici o parenti:

- > Selezionate Antifurto nel menu principale;
- > Selezionate Condivisione posizione.
- > Il vostro apparecchio mobile richiama ora i dati del GPS e prepara un SMS con un link a Google Maps che illustra la vostra posizione.
- > Immettete ora il numero desiderato nel campo dell'indirizzo SMS e selezionate Invia.
- > Il destinatario può ora guardare la vostra posizione attraverso il link nell'SMS oppure vedere direttamente le coordinate GPS nel testo dell'SMS.

4.2 Scansione antivirus

Effettuate una scansione dell'apparecchio contro virus e altri programmi dannosi dopo la prima attivazione di Mobile Security, per verificare che sia privo di virus. Effettuate la scansione ogni qualvolta l'applicazione lo richiede.

Swisscom Mobile Security viene eseguito in background ed esegue automaticamente la scansione dei file.

1. Se durante la scansione in tempo reale viene rilevato un programma dannoso, verrà visualizzato un messaggio. Premete *Sì* per visualizzare il/i file infetto/i o *No* per chiudere la schermata.
2. La schermata *File infetti* riporta un elenco dei file infetti trovati sull'apparecchio mobile nonché lo stato dei relativi file (in quarantena, ripristinato).

Se desiderate visualizzare ulteriori dettagli su un file infetto, procedete nel modo seguente:

1. Scorrete l'elenco fino al file infetto e premete il tasto di selezione.
2. Selezionate *Visualizza*.
3. La schermata con i dettagli dell'infezione consente di visualizzare il nome del file infetto e il relativo percorso, nonché il nome del programma dannoso che ha infettato il file.

Per l'elaborazione dei file infetti procedete nel modo seguente:

1. Nella schermata *File infetti*, scorrete fino al file infetto che desiderate elaborare.
2. Premete il tasto di selezione.
3. Selezionate una delle seguenti azioni:
 - > *cancella* – elimina il file infetto. Questa è l'azione consigliata. Il file viene eliminato completamente dall'apparecchio.
 - > *quarantena* – mette in quarantena il file infetto, se non lo è già. Un file in quarantena risulta bloccato e non può danneggiare l'apparecchio finché Mobile Security è attivato.
 - > *rilascia* – libera il file in quarantena. Se rilasciate un file, non è più bloccato e potete accedervi a vostro rischio e pericolo.

4.3 Aggiornamento automatico (update)



Swisscom Mobile Security include un servizio di aggiornamento automatico che consente di aggiornare regolarmente la banca dati delle definizioni dei virus dell'applicazione. Solo una banca dati delle definizioni antivirus aggiornata protegge il vostro cellulare dalle ultime minacce di virus o di programmi dannosi. L'aggiornamento automatico entra in funzione dopo l'attivazione del prodotto. Per eseguire gli aggiornamenti è necessario un collegamento a internet attivo. Quando un collegamento a internet è disponibile, Mobile Security verifica l'ultimo aggiornamento della banca dati delle definizioni dei virus e, se necessario, scarica gli ultimi aggiornamenti. Tenete presente che in questo caso avviene un trasferimento di dati. Pertanto accettate questa funzione solo se vi trovate su una rete in cui i costi per il trasferimento dati siano inclusi nell'abbonamento oppure se vi trovate in un WLAN privato.

4.4 Aggiornamento manuale

Potete aggiornare l'applicazione anche manualmente:

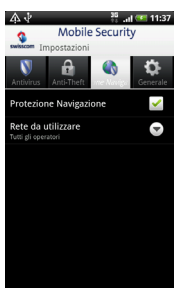
1. Navigate nel menu principale di Mobile Security fino ad *Aggiorna*.
2. Rispondete *Sì* alla domanda di collegarvi con il server d'aggiornamento.
3. Selezionate il punto di accesso a internet per stabilire il collegamento con un server d'aggiornamento. Tenete presente che in questo caso avviene un trasferimento di dati. Pertanto accettate questa funzione solo se vi trovate su una rete in cui i costi per il trasferimento dati siano inclusi nell'abbonamento. L'ultima banca dati delle definizioni dei virus viene scaricata dall'applicazione e subito attivata.
4. Al termine dell'aggiornamento, premete *Sì*, quando richiesto, per verificare la presenza di virus. Quando è disponibile una nuova versione di Mobile Security, un avviso vi richiede di effettuarne il download. Al termine dell'aggiornamento, l'applicazione viene riavviata automaticamente.

4.5 Utilizzo sicuro di internet con la protezione di navigazione

Mobile Security installa sul vostro apparecchio mobile automaticamente anche un altro browser, che compare come simbolo con la denominazione *Protez. Navigazione* nel menu Applicazioni dell'apparecchio mobile. Utilizzate questo browser ogni qualvolta navigate in internet.

Con l'aiuto della protezione di navigazione potete valutare la sicurezza delle pagine web ed evitare di visitare pagine pericolose. Appena visitate una pagina, il prodotto ne verifica automaticamente la sicurezza. Se la pagina web viene classificata come sospetta o pericolosa (pagine web infettate con phishing o con programmi dannosi), Mobile Security ne blocca l'accesso. La classificazione della sicurezza di una pagina internet si basa su informazioni provenienti da varie fonti, come analisti di malware e partner di F-Secure.

Potete attivare la protezione di navigazione anche da Mobile Security. Selezionate *Protez. Navigazione* nel menu principale e successivamente selezionate *Browser sicuro*. *Importante*: la protezione di navigazione è attiva solo se navigate in internet con questo browser. Se lo stesso ne scegliete un altro, durante la navigazione non sarete protetti. Se per vostro figlio avete attivato il Controllo genitori, l'apparecchio mobile utilizzerà sempre la protezione del browser, anche se vostro figlio desidera richiamare un altro browser.



Modificare le impostazioni della protezione di navigazione:

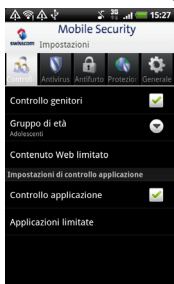
Scegliete quando attivare la protezione di navigazione. L'attivazione dipende dalla rete che usate. Ecco come modificare le impostazioni del prodotto:

1. Nel menu principale di Mobile Security selezionate *Impostazioni* e poi *Protez. Navigazione*.
2. Attivate la protezione di navigazione, selezionando il campo *Protez. Navigazione*. In tal modo Mobile Security è attivo in background mentre consultate internet.
3. Scegliete quando attivare la protezione di navigazione:
 - > *Tutti gli operatori* – Il prodotto verifica la sicurezza delle pagine internet che visitate indipendentemente dalla rete che state usando (vedi immagine).
 - > *Solo il mio operatore* – Il prodotto verifica la sicurezza delle pagine internet che visitate solo se state usando la rete del vostro operatore.

Il prodotto applica subito le nuove impostazioni. È possibile che Mobile Security richieda di utilizzare per default il browser che ha installato il fabbricante del vostro apparecchio mobile. Per godere di una protezione di navigazione ottimale, dovrete impostare come browser standard quello consigliato da Mobile Security.

Potete verificare lo stato della protezione del browser dell'apparecchio mobile in qualsiasi momento, selezionando l'icona *Protez. Navigazione* nel menu principale di Mobile Security.

4.6 Controllo genitori



Dalla versione V7.5 il vostro Swisscom Mobile Security è dotato di un controllo genitori che potete attivare a piacimento per i vostri bambini o adolescenti. Trovate la versione di Swisscom Mobile Security sul menu principale, alla voce *Ulteriori informazioni*. Se avete una versione antecedente alla versione V7.5, potete scaricare la nuova versione dal menu *Aggiorna*.

Il controllo genitori vi consente di scegliere le pagine internet alle quali i vostri figli non possono accedere. Nelle impostazioni di base, ossia dopo l'attivazione di Swisscom Mobile Security, la funzione Controllo genitori è disattivata.

All'interno di Swisscom Mobile Security, il Controllo genitori si trova nel menu principale, alla voce *Impostazioni* → *Controllo genitori* oppure nel menu principale sotto *Controllo genitori* → *Impostazioni* (cfr. immagine).

Nel menu Controllo genitori potete in generale attivare o disattivare tale funzione con un visto (primo punto del menu). Se lasciate il controllo genitori disattivato, potete continuare ad utilizzare i diversi browser internet installati sull'apparecchio mobile di vostro figlio.

Vi consigliamo tuttavia di attivare la protezione del browser, affinché siate protetti da programmi nocivi, da pagine web infettate da virus o da pagine truffaldine (ad esempio Phishing).

Se attivate il Controllo genitori, indipendentemente dal livello, vostro figlio può unicamente utilizzare il browser protetto. Se vostro figlio dovesse consultare un browser internet diverso, viene automaticamente aperta la protezione del browser. In tal modo vi assicurate non solo che vostro figlio sia protetto contro software pericolosi che si trovano su pagine infette, ma fate anche in modo che possa accedere unicamente alle pagine web, conformemente alle categorie che gli consentite di consultare. Per effettuare tutte le modifiche di queste impostazioni vi si chiederà di inserire un *Codice di sicurezza* che dovrete conoscere solo voi (e non i vostri figli). Se al momento della prima impostazione di Swisscom Mobile Security non avete ancora definito tale codice di sicurezza, lo potete fare anche in seguito.



Controllo genitori per giovani :

Attivate il *Controllo genitori* e alla voce *Gruppo di età*, selezionate l'impostazione *Adolescenti*. Alla voce *Contenuto Web limitato* (terza voce del menu) trovate le categorie di siti web predefinite ammesse e quelle bloccate. In funzione dei vostri desideri potete correggere l'elenco di categorie per gli adolescenti, attivando o eliminando i relativi visti nella colonna *Consenti* (cfr. immagine).

Controllo genitori per bambini (cfr. immagine):

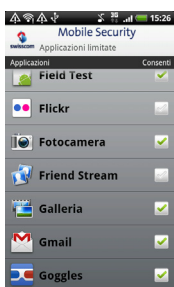
Attivate il *Controllo genitori* e alla voce *Gruppo di età*, selezionate l'impostazione *Bambini*. Alla voce *Contenuto Web limitato* (terza voce del menu) trovate le categorie di siti web predefinite ammesse e quelle bloccate.

In funzione dei vostri desideri potete correggere l'elenco di categorie per i bambini, attivando o eliminando i relativi visti nella colonna *Consenti* (cfr. immagine).

Controlli genitori per adulti:

Questo livello vi consente di selezionare la voce adulto nel menu *Gruppo di età*, sia per eliminare provvisoriamente il Controllo genitori per i vostri bambini o per assegnare a un figlio adolescente un profilo di categorie creato da voi, simile a quello di un adulto. Potete anche attivare questo Gruppo di età per impedire che voi o i vostri adolescenti possiate utilizzare un browser diverso dal browser protetto, che vi protegge contro siti web che contengono software dannosi.

Ciò che dovrete inoltre sapere: se attivate il Controllo genitori sull'apparecchio mobile di vostro figlio, indipendentemente dal livello, vostro figlio può utilizzare unicamente il browser protetto. A voi o a vostro figlio verrà chiesto di inserire il *codice di sicurezza* del controllo genitori quando utilizzate determinate applicazioni o dovete inserire dati amministrativi. L'inserimento del codice di sicurezza impedisce a vostro figlio di bypassare le impostazioni di sicurezza del Controllo genitori o di bloccare, disattivare o disinstallare Swisscom Mobile Security. Tale codice di sicurezza è identico al codice di sicurezza che utilizzate contro il furto.



Controllo applicazione

Il controllo genitori di Mobile Security è dotato inoltre di un controllo delle applicazioni. Ciò vi consente di bloccare in modo mirato l'utilizzo di determinate applicazioni (apps). Sotto *Applicazioni limitate* il controllo genitori cerca tutte le app installate e le indica inizialmente come ammesse. Potete ora bloccare le singole app, togliendo il visto da *Consenti* (cfr. immagine). Anche per queste modifiche è richiesto il codice di sicurezza. In tal modo si toglie al bambino la possibilità di ripristinare le modifiche. Le app che avete bloccato non vengono disinstallate, ma rimangono nel menu dello smartphone di vostro figlio. Se vostro figlio dovesse tentare di utilizzarle, appare una finestra che indica che Swisscom Mobile Security ha bloccato la app in questione.

Se vostro figlio dovesse installare in seguito altre app, anche questo vengono inizialmente automaticamente bloccate dal controllo applicazione. Vostro figlio deve rivolgersi a voi per sbloccarla attraverso il controllo applicazione.

4.7 Protezione da chiamate e messaggi non desiderati

La funzione *Contatti sicuri* vi protegge da chiamate e messaggi non desiderati. Con *Contatti sicuri* potete definire da chi volete ricevere chiamate e messaggi nonché bloccare chiamate non desiderate e messaggi spam.

Potete selezionare i numeri che desiderate bloccare. *Contatti sicuri* blocca tutte le chiamate e i messaggi SMS/MMS in entrata dei numeri selezionati. Inoltre vengono bloccate anche le chiamate in uscita ai numeri della lista di blocco da voi definita (editabile).

Utilizzate Contatti sicuri

Contatti sicuri blocca le chiamate e i messaggi della lista di blocco. Seguite le seguenti istruzioni per bloccare chiamate e messaggi di un nuovo numero:

1. nella videata principale selezionate l'opzione *Impostazioni*. Viene aperta la lista delle possibili impostazioni.
2. Selezionate *Contatti sicuri* dalle impostazioni. Nota: se non lo avete ancora fatto, inserite il vostro codice di sicurezza.
3. Assicuratevi che *Contatti sicuri* sia attivato.
4. Selezionate *Numeri blocco*. Inserite il codice di sicurezza per bloccare nuovi numeri. Si aprirà la lista con i numeri bloccati.
5. Selezionate *Immettere un numero da bloccare*.
6. Inserite dapprima il nome e nel secondo campo il numero che volete bloccare.
7. Selezionate *Salva* per aggiungere il numero alla lista dei numeri bloccati.

Dopo aver attivato *Contatti sicuri*, non riceverete più chiamate né messaggi dalla lista dei numeri bloccati. (La chiamata viene solo rapidamente visualizzata e nell'elenco del telefono appare la chiamata non risposta). Non potete ovviamente effettuare chiamate ai numeri bloccati.

Se volete gestire il blocco delle chiamate e dei messaggi in entrata e in uscita in modo differenziato o desiderate cancellare un blocco, selezionate il contatto bloccato dalla lista. Sulla lista che appare potete o cancellare il contatto o gestirlo in modo più dettagliato.

Visualizzazione di chiamate e messaggi bloccati

Nella cronologia blocchi potete vedere quali chiamate e messaggi sono stati bloccati da *Contatti sicuri*.

Seguite queste istruzioni per visualizzare quali chiamate e messaggi sono stati bloccati da *Contatti sicuri*:

1. Nel menu principale selezionate l'opzione *Impostazioni*. Si apre l'elenco di selezione delle impostazioni.
2. Selezionate *Contatti sicuri* nella lista di selezione delle impostazioni.
3. Selezionate *Mostra cronologia blocchi*.

5. Supporto tecnico

In caso di domande sull'applicazione oppure su installazione/attivazione/Disattivazione e sulla demo di prova, siete pregati di contattare la hotline di Swisscom 0800 55 64 64.

Per ricevere altre informazioni sulle funzioni di Mobile Security in internet potete anche consultare le pagine di supporto presso il nostro partner per la sicurezza http://www.f-secure.com/de_DE/support/

Tuttavia, tenete presente che il programma Mobile Security di Swisscom può differire dal prodotto standard di F-Secure riguardo a installazione/attivazione/disattivazione e aspetto.

