



THEFT AWARE 2.00



für Android™

BENUTZER HANDBUCH

<http://www.avast.com>
<http://www.theftaware.com>

Inhaltsverzeichnis

Theft Aware Übersicht.....	5
NEU IN VERSION 2.00.....	5
THEFT AWARE GRUNDLAGEN	5
Decken Sie die Identität des Diebes auf	5
Steuern Sie Ihr Telefon fern	6
Der unsichtbare Modus	7
Theft Aware 2.00 runterladen	8
THEFT AWARE RUNTERLADEN UND/ODER ERWERBEN	8
INSTALLATIONSVORGANG	8
Theft Aware 2.00 bedienen	9
System aktivieren.....	9
GRUNDEINSTELLUNGEN	10
Besitzer.....	10
Zugangscode	10
Benachrichtigung 1	10
ERWEITERTE EINSTELLUNGEN	10
Benachrichtigung 2	10
Einstellungen sperren	10
SMS Befehle erlauben.....	11
Telefonsperrung.....	11
Eigener Sperrtext	11
Sirene bei Sperrung.....	11
Sirenton.....	11
GPS autom. aktivieren.....	11
SMS Kartentyp	12
Zeitlimit GPS Abfrage	12
SMS bei leerem Akku	12
Gründliches Löschen	12
USB-Debugging sperren	12
Datenverbindung erzwingen.....	13

Einstellungen sichern	13
THEFT AWARE LIZENZIEREN.....	14
Auf Webseite kaufen.....	14
Android Market Kauf.....	15
Lizenz aktivieren.....	15
Gutschein einlösen.....	15
BENUTZEROBERFLÄCHE IM UNSICHTBAREN MODUS ÖFFNEN	16
VERTRAUENSWÜRDIGE SIM KARTE HINZUFÜGEN	16
THEFT AWARE 2.00 SMS-FERNSTEUER-KOMMANDOS.....	17
Autorisierung der SMS-Fernsteuer-Kommandos.....	17
Das Mobiltelefon als Gestohlen markieren	18
Das Mobiltelefon als Gefunden markieren	18
Das Mobiltelefon sperren	18
Das Mobiltelefon entsperren.....	18
Die Sirene aktivieren	18
Die Sirene deaktivieren	19
Aktualisierung der Telefoninformation (einmalig)	19
Aktualisierung der Telefoninformation (in Zeitintervallen)	19
Anruf veranlassen	19
Das Mobiltelefon löschen	19
SMS-Weiterleitung.....	20
SMS Carbon Copy.....	20
Anruf Carbon Copy.....	20
Anruf und SMS Carbon Copy.....	21
Wichtige SMS sichern.....	21
Kontakte sichern	22
Kürzliche Protokoll-Einträge abrufen.....	22
Theft Aware Einstellungen ändern	22
Starten und Beenden der Theft Aware Oberfläche	25
Neustart des Telefons	25
Fernsteuer-Entwicklungs-Schnittstelle	25
ERWEITERTE OPTIONEN.....	26

Test SMS senden	26
Diebstahl simulieren	26
Sperre simulieren	26
SIM-Liste löschen	26
Anhang A – Unterstützte Geräte	27
Anhang B - Sprachen.....	27
Anhang C - Kundendienst	27
Anhang D - Partnerprogramm	27

Theft Aware Übersicht

Theft Aware stellt Ihnen Diebstahlsicherheit und Datenschutz für Mobiltelefone zur Verfügung. Wenn Sie Ihr Telefon verlieren oder es gestohlen wird, können Sie es mit Theft Aware wiederfinden oder fernsteuern.

"A mobile phone gets stolen in the UK every 45 seconds. Thats nearly 800,000 handsets a year." (uknetguide.co.uk)

"Wenn Ihr Mobiltelefon gestohlen wird und ein Dieb die SIM Karte wechselt, ist das Telefon üblicherweise verloren da es im selben Augenblick seine Identität wechselt... Theft Aware ermöglicht es Ihnen auch nach diesem Ereignis noch mit dem Telefon in Kontakt zu bleiben." (Reinhard Holzner, Managing Director AVAST)

NEU IN VERSION 2.00

Neuigkeiten zu Theft Aware 2.00 sind unter http://www.theftaware.com/?step=whats_new verfügbar.

THEFT AWARE GRUNDLAGEN

Decken Sie die Identität des Diebes auf

Als Basis für die Kommunikation konfigurieren Sie Theft Aware mit bis zu zwei Empfänger-Rufnummern (zB. Freunde von Ihnen, oder Ihr Zweit-Telefon). Diese Freunde werden dann für Sie alle Theft Aware Mitteilungen von Ihrem Telefon erhalten. Wird nun die SIM Karte des Telefons getauscht, sendet Theft Aware die *Telefonnummer des Diebes* unsichtbar an diese Rufnummern. Dadurch können Sie mit Ihrem Mobiltelefon in Kontakt bleiben.

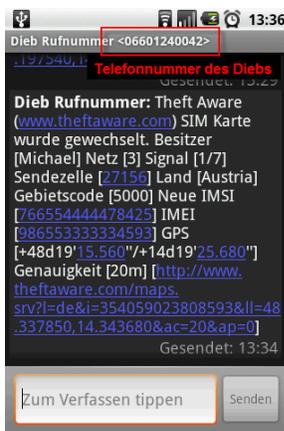


Figure 1: Beispiel einer Benachrichtigungs-SMS

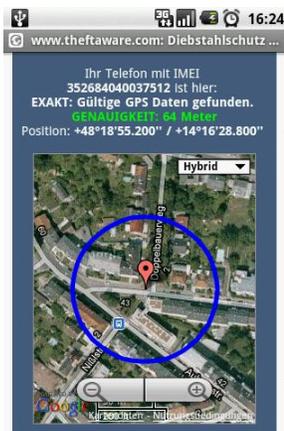


Figure 2: Link zu Online Kartenservice

Die Benachrichtigungs-SMS enthält:

- Die Telefonnummer des Diebes
- Netzwerkspezifische Informationen
- GPS Koordinaten, falls verfügbar
- Einen Link zu einem Online Kartenservice:



Kontaktieren Sie dann die Polizei oder steuern Sie das Telefon fern um Ihre Daten zu schützen.

Steuern Sie Ihr Telefon fern

Theft Aware kann mittels SMS Befehlen ferngesteuert werden:

Momentane Position des Telefons bestimmen: Wenn GPS Koordinaten verfügbar sind wird Ihr Mobiltelefon diese Koordinaten an Sie übermitteln. Sie können diese Benachrichtigung auch in bestimmten Zeitintervallen anfordern.

Telefon sperren: Wenn Sie das Telefon sperren, wird der Bildschirm von Theft Aware blockiert. Das Gerät ist dann nutzlos. Sie können diese Sperrung auch bei jedem SIM Karten Wechsel veranlassen.

Aktivieren Sie ein lautes Sirengeräusch: Das Mobiltelefon beginnt, einen lauten Sirenton wiederzugeben welcher nur durch einen autorisierten Benutzer wieder deaktiviert werden kann. Sie können diesen Sirenton sogar an Ihre eigenen Vorstellungen anpassen indem Sie eine eigene Tondatei angeben oder einen eigenen Sirenton aufnehmen.

Löschen Sie sämtliche privaten Daten: Entfernen Sie Kontakte, Anrufliste, Sms/MMS, Mediendateien, Kalendareinträge und Browser-Verlauf vom Telefon. Löschen Sie die Dateien auf der Speicherkarte um Ihre Daten zu schützen.

Senden Sie Ihre Kontakte: Bevor Sie das Telefon löschen, können Sie alle Ihre Kontakte sichern. Die Kontakte werden dann via SMS zu einem Empfängergerät übertragen.

SMS-Weiterleitung (neu seit Build 1710): Theft Aware kann auf Wunsch SMS unsichtbar an ein anderes Telefon weiterleiten.

Anruf-Weiterleitung (neu seit Build 1710): Theft Aware kann Sie nun per Textnachricht über eingehende Anrufe informieren. *Notiz: Wir haben auf eine direkte Weiterleitung von Anrufen verzichtet da diese je nach Netz unterschiedlich konfiguriert werden müssen. Weiters können Weiterleitungseinstellungen nicht unsichtbar für den Dieb installiert werden.*

Sichern Sie SMS die wichtig für Sie sind: Teilen Sie Theft Aware mit welche SMS Sie sichern wollen. Dieses SMS werden dann zu einem Empfängergerät weitergeleitet.

Ihr Telefon kann heimlich zurückrufen oder andere Nummern anrufen: Ihr Telefon kann nach Befehl selbstständig telefonieren. Dabei wird der Anruf bestmöglich versteckt. So können Sie heimlich mithören was auf der anderen Seite der Leitung passiert.

Fragen Sie Anruf- und SMS-Protokolldaten ab: Mittels Befehl können Anrufs- und SMS-Protokolldaten vom Telefon abgefragt werden.

Ändern Sie Theft Aware Einstellungen: die Einstellungen von Theft Aware können mittels SMS geändert werden.

Fernsteuer-Erweiterungs-Schnittstelle: Schreiben Sie Ihre eigenen SMS Befehle.

Der unsichtbare Modus

Nach einem Diebstahl überprüft ein Dieb üblicherweise das gestohlene Gerät sofort auf *Anwendungen, die dessen Identität aufdecken könnten*. Der Dieb wird sich nach *Anwendungs-Logos* umsehen und die Liste der *installierten Anwendungen* überprüfen. Stößt der Dieb auf eine Spur ist es sehr wahrscheinlich dass dieser das Telefon ausschaltet und entsorgt. Damit ist das Telefon *für immer verloren*.

Alle Hersteller von Anti-Diebstahls-Lösungen für Handies haben versucht dieses Problem zu lösen. In deren Lösungen existieren aber sichtbaren Spuren die ein Dieb sofort sieht, mit oben genannten Folgen.

Wir haben die perfekte Lösung: Theft Aware ist das **einzigste Tool auf dem Markt** das **vollständig unsichtbar** gemacht werden kann. *Dies gibt Ihnen maximale Chancen den Dieb zu schnappen oder Ihr Telefon zurückzubekommen.*

Theft Aware 2.00 runterladen

THEFT AWARE RUNTERLADEN UND/ODER ERWERBEN

Theft Aware ist entweder über unsere Website (<http://www.theftaware.com>) oder über Google's Android Market verfügbar.

INSTALLATIONSVORGANG

Wenn Sie Ihr Installationspaket heruntergeladen haben können Sie das Theft Aware Installationsprogramm starten. Dies ist das Logo des Theft Aware Installationsprogramms:



Abbildung 1: Theft Aware Installationsprogramm Logo

Starten Sie das Installationsprogramm. Dieses überprüft Ihr System nun auf Voraussetzungen die nötig sind um die Theft Aware Stealth Mode Technologie zu verwenden. Folgen Sie den Anweisungen. Im nächsten Schritt können Sie nun einen Anwendungsnamen für Ihre Theft Aware Installation vergeben:



Abbildung 2: Wählen Sie einen Anwendungsnamen

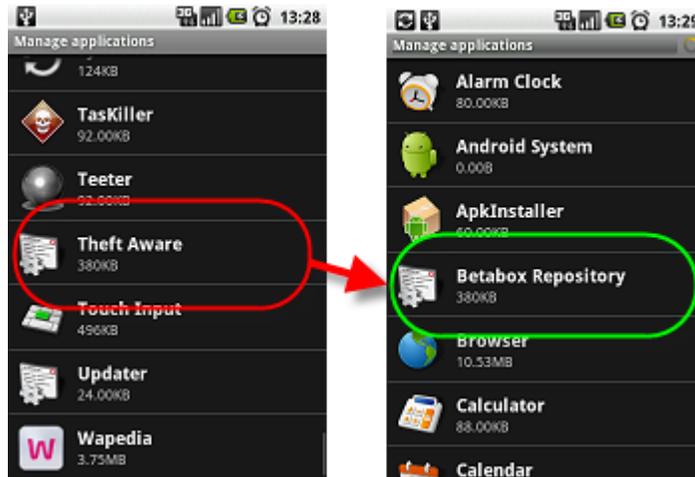


Abbildung 3: Name wurde geändert

In Android ist es **nicht möglich** den Anwendungseintrag im Anwendungs-Manager zu verstecken. Während andere Hersteller dies ignorieren und deren Anwendungen deshalb im Anwendungs-Manager einfach aufzufinden sind, stellen wir Ihnen ein persönliches Installationspaket zusammen, welches mit dem Namen versehen ist den Sie hier angeben. **Damit wird es für Diebe sehr schwer herauszufinden ob Theft Aware auf Ihrem Telefon installiert ist oder nicht** – da der Anwendungsname unauffällig ist.

Das Installationsprogramm wird Ihnen dann helfen Ihr persönliches Installationspaket runterzuladen und zu installieren. Nach Abschluss können Sie das Installationspaket bedenkenlos vom Telefon entfernen und damit fortsetzen, Theft Aware richtig einzustellen.

THEFT AWARE STARTEN

Sie haben Theft Aware nun erfolgreich installiert. Starten Sie das Programm im Anwendungsmenü.



Bild 4: Theft Aware Logo

Theft Aware 2.00 bedienen

Wenn Sie Theft Aware starten, wird die Hauptmenü-Seite geöffnet. Um Theft Aware für den Betrieb vorzubereiten müssen Sie hier die entsprechenden Einstellungen angeben.



Bild 5: Einstellungs-Seite

System aktivieren

Wollen Sie den kompletten Theft Aware Schutz ein- oder ausschalten? **Bitte beachten Sie dass der komplette Diebstahls-Schutz deaktiviert ist wenn die System-Einstellung ausgeschaltet ist.** In diesem Fall können auch keine SMS-Fernsteuer-Kommandos verarbeitet werden.

Wird der Theft Aware Schutz eingeschaltet, wechselt Theft Aware automatisch in den *unsichtbaren Modus*. Dabei wird das Theft Aware Logo in der Anwendungsliste versteckt.

Sobald Sie den Schutz wieder ausschalten kehrt Theft Aware in den *sichtbaren Modus* zurück. Danach wird das Theft Aware Logo in der Anwendungsliste wieder angezeigt.

GRUNDEINSTELLUNGEN

Um Theft Aware für den Einsatz vorzubereiten, **MÜSSEN** Sie die Theft Aware Grundeinstellungen angeben:

Besitzer

Bitte geben Sie hier Ihren Namen ein.

Zugangscode

Bitte geben Sie hier einen Zugangscode ein. Dieser Zugangscode wird verwendet um den Zugriff auf das Theft Aware Programm zu kontrollieren. **Vergessen Sie diesen Code nicht!** Es ist nicht möglich Theft Aware Einstellungen zu verändern ohne den Zugangscode zu kennen. Der Standard-Zugangscode ist **0000**. Sie müssen den Code aber auf einen anderen Wert ändern bevor Sie das Theft Aware System einschalten können.

Benachrichtigung 1

Bitte wählen Sie hier einen Ihrer Kontakte mit einer internationalen Telefonnummer aus. Jede Theft Aware SMS wird zu diesem Kontakt übermittelt.

Aktualisierungen

Mit dieser Einstellung können Sie Theft Aware veranlassen, wöchentlich automatisch nach Programm-Updates zu suchen. Ist ein Update verfügbar, wird eine Benachrichtigung am Telefon angezeigt. Die Überprüfung erfolgt nur wenn eine vertrauenswürdige SIM-Karte im Telefon eingelegt ist.

ERWEITERTE EINSTELLUNGEN

Die erweiterten Einstellungen sind bereits voreingestellt und **KÖNNEN** bei Bedarf angepasst werden:

Benachrichtigung 2

Sie *können* hier einen zweiten Kontakt auswählen. Kopien aller Theft Aware SMS werden zur Sicherheit auch an diesen Kontakt gesendet.

Einstellungen sperren

Theft Aware kann den Zugriff von Anwendern auf die Telefoneinstellungen und/oder den Programm-Manager sperren. Wenn ein Dieb dann die entsprechenden Einstellungen öffnen möchte werden diese sofort und ohne Hinweise wieder beendet. Damit kann Theft Aware über den Anwendungsmanager nicht mehr deinstalliert werden. Diese Option erhöht den Akku-Verbrauch von Theft Aware, verbessert aber den Telefonschutz signifikant.

Wenn Sie diese Option aktiviert haben aber selbst die Einstellungen ändern möchten schalten Sie bitte Theft Aware aus, führen Sie die Änderungen durch und schalten Sie dann Theft Aware wieder ein.

SMS Befehle erlauben

Theft Aware erlaubt es Ihnen Ihr Telefon mittels SMS von der Ferne aus zu steuern. Sie können diese Funktionalität hier deaktivieren. Wenn Sie die Option auf *Von Benachrichtigungsnummern* setzen werden SMS Kommandos nur von Rufnummern akzeptiert die in den Benachrichtigungsnummern vorkommen. Die Option *Von allen Nummern* hebt diese Einschränkung auf.

Telefonsperrung

Wenn diese Option auf *SIM Wechsel, SMS Befehl* gesetzt ist, wird das Telefon bei einem SIM Wechsel automatisch gesperrt. Weiters kann das Telefon durch ein SMS-Fernsteuer-Kommando gesperrt werden. Ist die Option auf *Nur durch SMS Befehl* gesetzt, kann das Telefon nur durch ein SMS-Fernsteuer-Kommando gesperrt werden. Sie können das Telefon entsperren indem Sie während der Sperrung einen gültigen Zugangscode eingeben.

Eigener Sperrtext

Hier können Sie einen Text angeben der bei einer Telefonsperrung am Bildschirm angezeigt wird. Wenn der Text nicht angegeben wird, wird ein Standardtext angezeigt.

Sirene bei Sperrung

Ist diese Option aktiviert, ertönt bei Telefonsperrung ein lauter Sirenenton, der erst durch Entsperrung des Telefons deaktiviert wird. Die Sirene kann auch durch ein SMS-Fernsteuer-Kommando ein- oder ausgeschaltet werden.

Sirenenton

Theft Aware erlaubt Ihnen, den Sirenenton anzupassen. Sie können die Option *Sounddatei auswählen* benutzen um eine bereits existierende Tondatei auszuwählen. Weiters können Sie mittels *Sirenenton aufnehmen* eine neue Aufnahme erstellen. Mit der Option *Sirenenton abspielen* können Sie den momentanen Sirenenton abspielen. *Sirene auf Standard* setzt die Sirene auf den Standard-Ton zurück.

- ⇒ Auf manchen Handies (zB. dem Samsung Galaxy S) ist das Standard-Sound-Aufnahme Werkzeug (Sound Recorder) nicht installiert. Deshalb kann auf diesen Handies kein eigener Sirenenton aufgenommen werden.

GPS autom. aktivieren

Hier können Sie einstellen ob Theft Aware versuchen soll, bei einer GPS-Abfrage das GPS auf nicht-grooteten Handies einzuschalten wenn dieses in den Einstellungen ausgeschaltet. Dies funktioniert nur auf Handies *von Android 1.6 bis Android 2.2 (ab Android 2.3 hat Google diese Funktionalität gesperrt)*

und kann je nach Modell unerwünschte Dialoge verursachen. Wenn Theft Aware als System-Anwendung installiert ist wird GPS in jedem Fall automatisch aktiviert.

Nachdem Sie diese Einstellung aktiviert haben sollten Sie das GPS in den Einstellungen ausschalten und testen ob dies geschieht (zB. mittels *Menü-Taste -> Erweitert -> Diebstahl simulieren*). Falls das Ergebnis negativ ausfällt wird empfohlen die Einstellung wieder zu deaktivieren.

SMS Kartentyp

Die Theft Aware Benachrichtigungs-SMS enthält einen Link damit in einem Online-Kartensystem angezeigt werden kann wo sich das Telefon momentan befindet. Hier können Sie auswählen welches Online-Kartensystem verwendet werden soll (Theft Aware, Google Maps, Yahoo! Maps, Microsoft Bing Maps). Theft Aware Maps ist ein neuer Kartentyp in Version 2.0. Die dabei erzeugten Kartenlinks leiten Sie an unsere Server weiter, wo Sie erweiterte Kartenfunktionalität zur Verfügung haben (der Link funktioniert auch auf Mobilgeräten und ermöglicht auch Ortung anhand der Sendezellen-Nummer wenn keine GPS Daten verfügbar sind).

Ortung bei SIM Wechsel

Diese Option wurde mit Build 1652 entfernt, da durch Android-Bedingte Umstände eine vertrauenswürdige SIM Karte als nicht vertrauenswürdige erkannt werden kann und damit eventuell eine größere Menge an ungewollten SMS versandt wird. Wir bitten um Ihr Verständnis.

Zeitlimit GPS Abfrage

Hier können Sie das Zeitlimit für GPS Positionsabfragen angeben.

SMS bei leerem Akku

Setzen Sie den Wert auf *Immer* damit Sie informiert werden falls der Akku im Handy bald leer ist. Wenn die Option auf *Bei SIM Wechsel* gesetzt ist wird die Nachricht nur gesendet wenn eine fremde SIM eingesetzt ist. Eine Benachrichtigung bedeutet dass das Telefon bald nicht mehr verfügbar sein könnte.

Gründliches Löschen

Wenn diese Option gesetzt ist, wird beim Löschen des Geräts die SD-Karte mit Zufallsdaten überschrieben. Dies verhindert dass Daten wiederhergestellt werden können, verlängert die Löschzeit aber um bis zu 10 Minuten.

USB-Debugging sperren

(Nur für gerootete Geräte, neu seit Build 1732)

Wenn diese Option gesetzt ist wird das USB-Debugging am Gerät gesperrt wenn eine nicht vertrauenswürdige SIM Karte ins Gerät eingesetzt wird. Die Sperre wird auch aktiviert sobald das Telefon als VERLOREN markiert wurde. Der Dieb kann danach über Spezialwerkzeuge nicht mehr auf das Telefon zugreifen.

Datenverbindung erzwingen

(Nur für gerootete Geräte, neu seit Build 1795)

Wenn diese Option gesetzt ist, kann die Datenverbindung nicht mehr ausgeschaltet werden wenn eine nicht vertrauenswürdige SIM Karte ins Gerät eingesetzt wird. Die Funktion wird auch aktiviert sobald das Telefon als VERLOREN markiert wurde.

Einstellungen sichern

(Nur für gerootete Geräte)

Dies speichert die Theft Aware Einstellungen an einen Ort an dem diese sogar eine Rücksetzung des Gerätes auf Fabrikseinstellungen überstehen. Dies macht nur Sinn wenn Sie Theft Aware als Systemprogramm installiert haben. Wenn Sie ein Superuser-Whitelist Programm installiert haben wird im Zuge der Sicherung um Genehmigung für Superuser-Berechtigungen ersucht.

- ⇒ Wenn Sie Theft Aware als Systemprogramm installiert haben, dies aber wieder rückgängig machen wollen, folgen Sie bitte [dieser Anleitung](#).

HILFE-SEITE

Das Hilfesystem enthält auch System-Status Informationen (*Copyright, Systemstatus*):

Eigenschaft	Beschreibung
System-Anwendung	Zeigt an ob Theft Aware als Systemprogramm installiert ist (auf „gerooteten“ Handies)
Netz Verfügbar	Zeigt an ob ein Mobilnetz verfügbar ist (Ja / Nein)
Netz	Wenn ein Mobilnetz verfügbar ist, sehen Sie hier den Namen des Netzes
Sendezelle	Wenn ein Mobilnetz verfügbar ist, sehen Sie hier die Kennnummer der Sendezelle zu der Ihr Telefon momentan verbunden ist
Land	Wenn ein Mobilnetz verfügbar ist, sehen Sie hier den Namen des Landes in dem Sie sich gerade befinden
Ländercode	Wenn ein Mobilnetz verfügbar ist, sehen Sie hier die Kennnummer des Landes in dem Sie sich gerade befinden
Gebietscode	Wenn ein Mobilnetz verfügbar ist, sehen Sie hier den Gebietscode zu dem Sie momentan zugeordnet sind
IMSI	Die IMSI (<i>International Mobile Subscriber Identity</i>) Nummer ist die weltweit eindeutige Kenn-Nummer der SIM Karte in Ihrem Mobiltelefon
IMEI	Die IMEI (<i>International Mobile Equipment Identity</i>) Nummer (oder Seriennummer) ist die weltweit eindeutige Kenn-Nummer Ihrer Mobiltelefon-Hardware
Ortung	Zeigt an ob GPS Daten verfügbar sind
Internet Fernsteuerung	Zeigt an ob die Internet Fernsteuerung richtig konfiguriert wurde. Für weitere Anleitung hierzu besuchen Sie bitte https://internet.theftaware.com

THEFT AWARE LIZENZIEREN

Wenn Sie Theft Aware das erste Mal installieren, installieren Sie eine Testversion des Produkts. Diese Testversion verfügt über volle Funktionalität aber deaktiviert sich nach einer gewissen Zeitperiode selbst. Um Theft Aware nach Ablauf der Test-Periode weiter benutzen zu können müssen Sie eine Theft Aware Voll-Lizenz kaufen.

Sie haben dazu folgende Möglichkeiten:

- Besuchen Sie unsere Website unter <http://www.theftaware.com> und klicken Sie auf **KAUFEN**
- Wählen Sie im Hauptmenü den Punkt *Lizenzen / Gutscheine* um die Lizenz zu erwerben:

Auf Webseite kaufen

Diese Option leitet Sie auf unsere Website zum Lizenzkauf weiter. Sie können Ihre Lizenz per PayPal oder Banküberweisung bezahlen.

Wenn Sie den Kaufprozess abgeschlossen haben können Sie mit der Option *Lizenz aktivieren* aus dem gleichen Menü fortfahren (siehe unten).

Android Market Kauf

Ab Build 1715: Mittels dieser Option können Sie eine Lizenz über das neue *Android In-App Bezahlssystem* kaufen. Dabei wird *Google Checkout* als Zahlungsmethode verwendet. Diese Option erscheint nur wenn Sie ein Handy mit einer **Android Version von mindestens 1.6** besitzen und Sie die **Android Market Applikation Version 2.3.4** oder höher auf Ihrem Gerät installiert haben.

Bei Abschluss des Kaufs über diese Methode wird Ihre Lizenz sofort aktiviert, es ist keine separate Lizenz-Aktivierung mehr vonnöten.

Lizenz aktivieren

Wenn Sie diese Option anwählen wird Theft Aware mit unseren Servern Kontakt aufnehmen um Ihre gekaufte Lizenz abzufragen. Nach erfolgreichem Abschluss wird die Theft Aware Testversion automatisch in eine Vollversion umgewandelt. Sie können diese Option auch benutzen wenn Sie Ihr Telefon neu aufsetzen mussten und Sie eine bereits gekaufte Theft Aware Lizenz erneut aktivieren wollen.

Dieser Vorgang benötigt Internetzugang am Telefon. Wenn Sie am Telefon KEINEN Internetzugang haben, kontaktieren Sie uns bitte unter support@theftaware.com und wir werden Ihnen helfen, die Lizenz ohne Internetzugang zu aktivieren.

Gutschein einlösen

Wenn Sie einen Lizenz-Gutschein für Theft Aware erworben oder erhalten haben, müssen Sie die Lizenz nicht wie oben beschrieben kaufen und dann aktivieren. Sie können statt dessen die *Gutschein einlösen* Option verwenden. Wählen Sie die Option und geben Sie Ihren Gutscheincode und Ihre Email ein. Nach dem Einlösen ist alles erledigt und Theft Aware wird automatisch in eine Vollversion umgewandelt.

BENUTZEROBERFLÄCHE IM UNSICHTBAREN MODUS ÖFFNEN

Im unsichtbaren Modus können Sie Theft Aware nicht wie üblich vom Anwendungs-Menü aus starten da Theft Aware unsichtbar ist. Deshalb hier die nächste Innovation: Theft Aware kann gestartet werden indem der *ZUGRIFFSCODE ANGERUFEN WIRD*. Wenn Sie den Zugriffscode beispielsweise auf **2222** gesetzt haben, *RUFEN* Sie einfach **2222** an. Dieser Anruf wird sofort und ohne Kosten zu verursachen unterbrochen und die Theft Aware Benutzeroberfläche erscheint in wenigen Sekunden.



Bild 6:
2222 eingeben



Bild 7: Theft Aware
öffnet sich

Theft Aware kümmert sich ausserdem darum dass keine Spur des gewählten Zugangscodes in der Anrufliste aufscheint indem es diese Einträge sofort nach dem Wählvorgang entfernt.

VERTRAUENSWÜRDIGE SIM KARTE HINZUFÜGEN

Üblicherweise sendet Theft Aware eine Benachrichtigungs-SMS sobald die „vertrauenswürdige“ SIM Karte aus dem Telefon entfernt und durch eine andere ersetzt wird. Von Version 2.0 an können Sie mehrere „vertrauenswürdige“ SIM-Karten verwalten. Die momentan eingesetzte SIM Karte wird akzeptiert sobald Sie die Theft Aware Konfiguration einmal starten.

Führen Sie folgende Schritte durch damit Theft Aware der neuen SIM Karte vertraut:

- schalten Sie die Theft Aware Telefonsperre aus wenn sie aktiviert ist
- schalten Sie das Telefon aus
- entfernen Sie die alte SIM Karte
- legen Sie die neue SIM Karte ein
- schalten Sie das Telefon wieder ein
- starten Sie die Theft Aware Benutzeroberfläche

In diesem Moment fügt Theft Aware die eingelegte SIM Karte der Liste der vertrauenswürdigen SIM Karten hinzu. Eine Benachrichtigung informiert Sie darüber.

Die Liste der vertrauenswürdigen SIM Karten kann ab Build 1755 auch gelöscht werden. Drücken Sie die Menü-Taste, öffnen Sie das Menü *Erweitert* und wählen Sie dann *SIM-Liste löschen* aus.

THEFT AWARE 2.00 SMS-FERNSTEUER-KOMMANDOS

Theft Aware kann mittels einfacher SMS-Fernsteuer-Kommandos ferngesteuert werden. Dazu müssen die *System* und *SMS Befehle Erlauben* Einstellungen auf der Einstellungs-Seite aktiviert sein. Bitte lesen Sie dazu im Kapitel *Einstellungs-Seite* nach.

Wenn die Einstellung *SMS Befehle erlauben* auf *Von Benachrichtigungsnummern* gesetzt ist, werden Befehle nur von Absenderrufnummern erlaubt die mit einer der eingestellten Benachrichtigungsnummern übereinstimmen. Alle SMS-Fernsteuer-Kommandos die von anderen Rufnummern gesendet wurden werden ignoriert.

Ein *authorisiertes* SMS-Fernsteuer-Kommando bewirkt am Zieltelefon keine Signaltöne, Klingeltöne, Lichtsignale oder andere SMS Empfangs-Benachrichtigungen. Die SMS wird auch nicht in der Nachrichtenbox des Zieltelefons angezeigt. Dies gilt auch für alle Antworten des Zieltelefons an Sie.

Autorisierung der SMS-Fernsteuer-Kommandos

Alle SMS-Fernsteuer-Kommandos müssen mit dem Theft Aware Zugangscode beginnen. Ist der Zugangscode beispielsweise auf **2222** gesetzt ist, sollte ein Sperr-Kommando so aussehen:

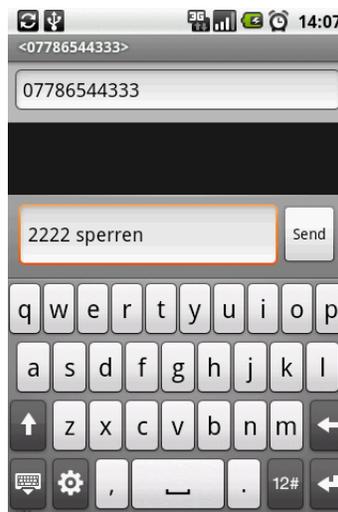


Bild 8: Alle SMS beginnen mit dem Zugangscode

Wenn der Zugangscode nicht übereinstimmt, wird sie ignoriert und als normale SMS weitergeleitet, was in der Auslösung *sämtlicher Empfangs-Benachrichtigungen am Zieltelefon resultiert*.

Neu ab Build 1654: SMS Kommandos können nun durch Angabe von **##** beendet werden. Es kommt teilweise vor dass, wenn Sie SMS über zB. eine SMS Webseite abschicken, Werbetext an den SMS Text gehängt wird. Damit kann Theft Aware das Kommando nicht mehr richtig interpretieren. Wenn Sie nun das Kommando mit **##** beenden, ignoriert Theft Aware den ganzen Text der danach kommt und Ihr Kommando funktioniert perfekt.

Beispiel: 2222 SPERREN ## sms.at dies ist ein Werbetext... → Theft Aware sieht nur 2222 SPERREN

Das Mobiltelefon als Gestohlen markieren (Neu ab Build 1732)

SMS Kommando: **VERLOREN**
Beispiel: **2222 VERLOREN**

Markiert das Telefon als VERLOREN. Das Kommando löst die gleichen Aktionen wie ein SIM-Kartenwechsel aus (Abhängig von den Einstellungen: Ortung, Sperre, Sirene, Deaktivierung des USB Debugging etc.).

Das Mobiltelefon als Gefunden markieren (Neu ab Build 1732)

SMS Kommando: **GEFUNDEN**
Beispiel: **2222 GEFUNDEN**

Markiert das Telefon als GEFUNDEN. Das Kommando deaktiviert die Telefonsperre sowie den Sirenenton.

Das Mobiltelefon sperren

Dieses Kommando *sperrt das Mobiltelefon*. Es ist danach nicht mehr möglich das Telefon zu benutzen. Dies wird jedoch die Aufmerksamkeit eines Diebes auf sich ziehen. Das Telefon kann folgendermaßen entsperrt werden:

- a) senden Sie das *ENTSPERREN* Kommando oder
- b) geben Sie am Zieltelefon den gültigen Zugangscode ein

SMS Kommando: **SPERREN**
Beispiel: **2222 SPERREN**

Das Mobiltelefon entsperren

Dieses Kommando *entsperrt* das Zieltelefon wieder.

SMS Kommando: **ENTSPERREN**
Beispiel: **2222 ENTSPERREN**

Die Sirene aktivieren

Dieses Kommando *aktiviert die Sirene*. Dies wird jedoch die Aufmerksamkeit eines Diebes auf sich ziehen.

SMS Kommando: **SIRENE EIN**
Beispiel: **2222 SIRENE EIN**

Sie können die Sirene durch Senden des **SIRENE AUS** Befehls stoppen. Die Sirene kann **IMMER** durch Ausschalten des Theft Aware Systems gestoppt werden.

Die Sirene deaktivieren

Dieses Kommando *deaktiviert die Sirene*.

SMS Kommando: **SIRENE AUS**

Beispiel: **2222 SIRENE AUS**

Aktualisierung der Telefoninformation (einmalig)

Durch dieses Kommando wird Theft Aware der Absender-Nummer des Kommandos eine aktuelle Benachrichtigungs-SMS zusenden. Diese enthält aktuelle Daten über das Mobiltelefon (zB. GPS Daten).

SMS Kommando: **AKTUALISIEREN**

Beispiel: **2222 AKTUALISIEREN**

Aktualisierung der Telefoninformation (in Zeitintervallen)

Eine spezielle Version des AKTUALISIEREN Kommandos lässt Ihnen die Benachrichtigungs-Daten in bestimmten Zeitabständen zukommen.

SMS Kommando: **AKTUALISIEREN <Zeitabstand in Minuten>**

Beispiel: **2222 AKTUALISIEREN 60**

Beschreibung: Sendet die Benachrichtigungs-Daten alle <Zeitabstand> Minuten

Sie können die Benachrichtigungen durch Senden des **AKTUALISIEREN STOP** Befehls stoppen. Die Benachrichtigungen können IMMER durch Ausschalten des Theft Aware Systems gestoppt werden.

Anruf veranlassen

Durch dieses Kommando wird Theft Aware einen Anruf veranlassen. So können Sie dann hören was auf der anderen Seite der Verbindung passiert. Der Anruf wird bestmöglichst versteckt.

SMS Kommando: **RUF AN [Telefonnummer]**

Beispiel: **2222 RUF AN, 2222 RUF AN +43660122249282**

Wird *[Telefonnummer]* nicht angegeben, ruft das Zieltelefon die Absendernummer der Fernsteuer SMS zurück. Wird *[Telefonnummer]* angegeben, ruft das Zieltelefon die angegebene Telefonnummer an.

Das Mobiltelefon löschen

Dieses Kommando verursacht eine Löschung von vertraulichen Daten am Zieltelefon. Entfernen Sie Kontakte, Anrufliste, Sms/MMS, Mediendateien, Kalendareinträge und Browser-Verlauf vom Telefon. Löschen Sie die Dateien auf der Speicherkarte um Ihre Daten zu schützen. **Vorsicht: die Daten können NICHT wiederhergestellt werden.**

SMS Kommando: **LÖSCHEN**

Beispiele: **2222 LÖSCHEN**

SMS-Weiterleitung

(Neu ab Build 1710)

Wenn Sie dieses Kommando senden, beginnt Theft Aware, am Zieltelefon eingehende SMS Nachrichten unsichtbar an ein anderes Telefon weiterzuleiten. Keine Sorge: Die Theft Aware SMS Befehle werden auch bei eingeschalteter SMS-Weiterleitung ausgeführt.

SMS Kommando: **WEITERLEITUNG SMS [Telefonnummer]**

Sample: **2222 WEITERLEITUNG SMS, 2222 WEITERLEITUNG SMS +4355003938833**

Wird keine Rufnummer angegeben werden eingehende SMS unsichtbar an die Absenderrufnummer des SMS Kommandos weitergeleitet. Wenn eine Rufnummer angegeben ist, werden eingehende SMS an die angegebene Rufnummer weitergeleitet. Dieses Kommando überschreibt alle vorherigen Weiterleitungs- und CC-Einstellungen.

Die Weiterleitung kann mit **WEITERLEITUNG SMS STOP** oder durch Starten der Theft Aware Oberfläche aufgehoben werden.

SMS Carbon Copy

(Neu ab Build 1710)

SMS Kommando: **CC SMS [Telefonnummer]**

Sample: **2222 CC SMS, 2222 CC SMS +4355003938833**

Dieses Kommando funktioniert wie die SMS Weiterleitung, nur werden die SMS am Zieltelefon nach Weiterleitung nicht gelöscht sondern zugestellt (CC ist die Abkürzung für Carbon Copy). Dieses Kommando überschreibt alle vorherigen Weiterleitungs- und CC-Einstellungen.

Die Weiterleitung kann mit **CC SMS STOP** oder durch Starten der Theft Aware Oberfläche aufgehoben werden.

Anruf Carbon Copy

(Neu ab Build 1710)

SMS Kommando: **CC ANRUF [Telefonnummer]**

Sample: **2222 CC ANRUF, 2222 CC ANRUF +4355003938833**

Mit diesem Kommando können Sie sich über eingehende Anrufe am Telefon per Nachricht informieren lassen. Die Nachricht wird an die Absenderrufnummer des Kommandos geschickt wenn keine andere Rufnummer angegeben wird. Dieses Kommando überschreibt alle vorherigen Anrufweiterleitungseinstellungen.

Notiz: Wir haben auf eine direkte Weiterleitung von Anrufen verzichtet da diese je nach Netz unterschiedlich konfiguriert werden müssen. Weiters können Weiterleitungseinstellungen nicht unsichtbar für den Dieb installiert werden.

Die Weiterleitung kann mit **CC ANRUF STOP** oder durch Starten der Theft Aware Oberfläche aufgehoben werden.

Anruf und SMS Carbon Copy (Neu ab Build 1710)

SMS Kommando: **CC ALLE [Telefonnummer]**
Sample: **2222 CC ALLE, 2222 CC ALLE +4355003938833**

Das Kommando bündelt den CC SMS und den CC ANRUFBE Befehl. Dieses Kommando überschreibt alle vorherigen SMS- und Anrufweiterleitungs-Einstellungen.

Die Weiterleitung kann mit **CC ALLE STOP** oder durch Starten der Theft Aware Oberfläche aufgehoben werden.

Wichtige SMS sichern

Durch dieses Kommando können Sie sich SMS Nachrichten vom Zieltelefon zuschicken lassen. So können Sie wichtige SMS retten, auch wenn das Telefon verloren oder gestohlen wurde.

SMS Kommando: **ABFRAGE <Abfrage-Limit> SMS**

Beispiel: **2222 ABFRAGE 5 SMS**

Beschreibung: Leitet die neuesten gespeicherten SMS weiter (Eingang und Gesendete). Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

SMS Kommando: **ABFRAGE <Abfrage-Limit> EMPFANGENE SMS**

Beispiel: **2222 ABFRAGE 5 EMPFANGENE SMS**

Beschreibung: Leitet die neuesten im Eingang gespeicherten SMS weiter. Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

SMS Kommando: **ABFRAGE <Abfrage-Limit> GESENDETE SMS**

Beispiel: **2222 ABFRAGE 5 GESENDETE SMS**

Beschreibung: Leitet die neuesten im Ausgang gespeicherten SMS weiter. Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

SMS Kommando: **ABFRAGE <Abfrage-Limit> SMS FÜR xxxxxxxxxxxx**

Beispiel: **2222 ABFRAGE 5 SMS FÜR 436502111555**

Beschreibung: Leitet die neuesten gespeicherten SMS weiter die zur angegebenen Telefonnummer passen (Eingang und Gesendete). Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

SMS Kommando: **ABFRAGE <Abfrage-Limit> EMPFANGENE SMS FÜR xxxxxxxxxxxx**

Beispiel: **2222 ABFRAGE 5 EMPFANGENE SMS FÜR 436502111555**

Beschreibung: Leitet die neuesten im Eingang gespeicherten SMS weiter die zur angegebenen Telefonnummer passen. Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

SMS Kommando: **ABFRAGE <Abfrage-Limit> GESENDETE SMS FÜR xxxxxxxxxxxx**

Beispiel: **2222 ABFRAGE 5 GESENDETE SMS FÜR 436502111555**

Beschreibung: Leitet die neuesten im Ausgang gespeicherten SMS weiter die zur angegebenen Telefonnummer passen. Das Abfrage-Limit muss angegeben werden. Es werden maximal <Abfrage-Limit> SMS übertragen.

Kontakte sichern

Mit diesem Kommando können Sie sich *alle primären Telefonnummern und Email-Adressen Ihrer Telefonbuch-Kontakte* zuschicken lassen. Ein Kontakt wird durch genau eine SMS übertragen.

SMS Kommando: **ABFRAGE KONTAKTE**

Beispiel: **2222 ABFRAGE KONTAKTE**

Beschreibung: Leitet alle Telefonbuch-Kontakte weiter

Kürzliche Protokoll-Einträge abrufen

Dieses Kommando erlaubt Ihnen, die kürzlich geschehenen Anrufs- und SMS-Ereignisse abzurufen die auf Ihrem Telefon durchgeführt wurden.

SMS Kommando: **ABFRAGE PROTOKOLL <Abfrage-Limit>**

Beispiel: **2222 ABFRAGE PROTOKOLL 10**

Beschreibung: Leitet die letzten <Abfrage-Limit> Anrufs- und SMS-Ereignisse weiter. Das Abfrage-Limit muss angegeben werden.

Jedes Anrufs- oder SMS-Ereignis wird als seine separate SMS weitergeleitet. Anrufs-Ereignisse enthalten die Telefonnummer und die Anruf-Dauer in Sekunden. SMS-Ereignisse enthalten die Telefonnummer und eine Kurzversion des SMS-Textes.

Theft Aware Einstellungen ändern

Diese Kommandogruppe ermöglicht es, die Theft Aware Einstellungen über SMS zu ändern.

SMS Kommando: **SETZE BESITZER <Name des Besitzers>**

Beispiel: **2222 SETZE BESITZER Charles Chaplin**

Beschreibung: Ändert den Theft Aware Besitzer-Eintrag auf <Name des Besitzers>

SMS Kommando: **SETZE CODE <Zugangscod>**

Beispiel: **2222 SETZE CODE 3333**

Beschreibung: Ändert den Theft Aware Zugangscod auf <Zugangscod>. Sie müssen 4-6 Ziffern angeben.

SMS Kommando: **SETZE BENACHRICHTIGUNG 1 <Benachrichtigung 1>**

Beispiel: **2222 SETZE BENACHRICHTIGUNG 1 +4366012220192**

Beschreibung: Setzt die erste Benachrichtigungs-Nummer auf <Benachrichtigung 1>. Sie müssen eine gültige Mobil-Telefonnummer angeben. Es dürfen nicht beide Benachrichtigungs-Nummern zur selben Zeit leer sein.

SMS Kommando: **SETZE BENACHRICHTIGUNG 2 < Benachrichtigung 2>**

Beispiel: **2222 SETZE BENACHRICHTIGUNG 2 +43660122220192**

Beschreibung: Setzt die zweite Benachrichtigungs-Nummer auf *<Benachrichtigung 2>*. Sie müssen eine gültige Mobil-Telefonnummer angeben. Es dürfen nicht beide Benachrichtigungs-Nummern zur selben Zeit leer sein.

SMS Kommando: **SETZE APPSPERRE <App-Sperrmodus>**

Beispiel: **2222 SETZE APPSPERRE 1**

Beschreibung: Konfiguriert ob Theft Aware den Zugriff auf Telefoneinstellungen und/oder den Telefon-Programm-Manager verhindert. Wenn Sie den *<App-Sperrmodus>* auf 0 setzen, wird der Zugriff zu allen Einstellungen gewährt. Wenn Sie den *<App-Sperrmodus>* auf 1 setzen, wird der Zugriff auf den Programm-Manager verhindert. Wenn Sie den *<App-Sperrmodus>* auf 2 setzen, wird der Zugriff auf ALLE Telefoneinstellungen verhindert.

SMS Kommando: **SETZE SPERRMODUS <Sperrmodus>**

Beispiel: **2222 SETZE SPERRMODUS 1**

Beschreibung: Setzt den Theft Aware Sperrmodus. Ist der *<Sperrmodus>* 0, kann das Telefon nur durch ein SMS Kommando gesperrt werden. Ist der *<Sperrmodus>* 1, wird das Telefon automatisch durch SIM Karten-Wechsel gesperrt, weiters kann eine SMS-Kommando-Sperre aktiviert werden.

SMS Kommando: **SETZE TEXT <Sperrtext>**

Beispiel: **2222 SETZE TEXT Bitte rufen Sie mich unter +4313283483 an**

Beschreibung: Dieses Kommando ändert den Sperrtext der von Theft Aware während einer Telefonsperre angezeigt wird.

SMS Kommando: **SETZE SMS <SMS Einstellung>**

Beispiel: **2222 SETZE SMS 1**

Warnung: Eine Veränderung dieser Einstellung kann die SMS Fernsteuerungs-Funktionalität von Theft Aware ausschalten. In diesem kann das Telefon nicht mehr via SMS gesteuert werden!

Beschreibung: Setzt die Theft Aware SMS Konfiguration. Setzen Sie *<SMS Einstellung>* auf 0, um nur SMS Befehle von den Benachrichtigungsnummern zu erlauben. Setzen Sie *<SMS Einstellung>* auf 1, um SMS Befehle von allen Rufnummern zu erlauben. Setzen Sie *<SMS Einstellung>* auf 2 um keine SMS Befehle mehr zu erlauben.

SMS Kommando: **SETZE SIRENE <Sirenenmodus>**

Beispiel: **2222 SETZE SIRENE 1**

Beschreibung: Setzt den Theft Aware Sirenenmodus. Ist der *<Sirenenmodus>* 0, wird bei einer Sperre keine Sirene ausgelöst. Ist der *<Sirenenmodus>* 1, wird bei einer Telefonsperre automatisch die Sirene aktiviert.

SMS Kommando: **SETZE AUTOGPS <Modus>**

Beispiel: **2222 SETZE AUTOGPS 1**

Beschreibung: Hier können Sie einstellen ob Theft Aware versuchen soll, bei einer GPS-Abfrage das GPS auf nicht-gerooteten Handies einzuschalten wenn dieses in den Einstellungen ausgeschaltet ist. Dies funktioniert nur auf Handies ab Android 1.6 und **kann je nach Modell unerwünschte Dialoge** verursachen. Wenn Sie für *<Modus>* 0 angeben wird die Einstellung deaktiviert, wenn Sie für *<Modus>* 1 angeben wird die Einstellung aktiviert.

SMS Kommando: **SETZE KARTENTYP <Kartentyp>**

Beispiel: **2222 SETZE KARTENTYP 2**

Beschreibung: Setzt den Theft Aware Kartentyp. Ist der *<Kartentyp>* 0, werden Karten-Links auf unsere Webseite generiert wo Sie erweiterte Kartenfunktionalität nutzen können. Ist der *<Kartentyp>* 1, werden Karten-Links im Google Maps kompatiblen Format versendet. Ist der *<Kartentyp>* 2, werden Karten-Links im Yahoo! Maps kompatiblen Format versendet. Ist der *<Kartentyp>* 3, werden Karten-Links im Microsoft Bing Maps kompatiblen Format versendet.

SMS Kommando: **SETZE AKKU <Akku Modus>**

Beispiel: **2222 SETZE AKKU 1**

Beschreibung: Setzt die Theft Aware Akku-Modus Einstellung. Ist der *<Akku Modus>* 0, wird keine SMS im Falle eines niedrigen Akku-Stands versendet. Wenn der *<Akku Modus>* 1 ist, versendet Theft Aware IMMER eine Benachrichtigung im Falle eines niedrigen Akku-Stands. Bei *<Akku Modus>* 2 wird die Nachricht nur versendet, wenn eine fremde SIM im Telefon eingesetzt ist.

SMS Kommando: **SETZE LÖSCHMODUS <gründliches Löschen Modus>**

Beispiel: **2222 SETZE LÖSCHMODUS 1**

Beschreibung: Ändert die Einstellung für gründliches Löschen (0 für AUS, 1 für EIN).

SMS Kommando: **SETZE GPS LIMIT <GPS Zeitabfrage Limit>**

Beispiel: **2222 SETZE GPS LIMIT 1**

Beschreibung: Setzt das Theft Aware GPS Zeitabfrage Limit. Ist das *<GPS Zeitabfrage Limit>* 1, wird ein Zeitlimit von einer Minute eingestellt. Ist das *<GPS Zeitabfrage Limit>* 2, wird ein Zeitlimit von zwei Minuten eingestellt. Ist das *<GPS Zeitabfrage Limit>* 5, wird ein Zeitlimit von fünf Minuten eingestellt. Ist das *<GPS Zeitabfrage Limit>* 10, wird ein Zeitlimit von zehn Minuten eingestellt.

SMS Kommando: **SETZE DEBUGSPERRE <Sperrmodus>**

Beispiel: **2222 SETZE DEBUGSPERRE 1**

Neu seit Build 1732, nur für gerootete Geräte. Beschreibung: Setzt die USB-Debugging Sperre. Ist der *<Sperrmodus>* 1 wird die USB-Debugging-Sperre bei SIM-Wechsel und Verlust aktiviert, ist der *<Sperrmodus>* 0, wird die USB-Debugging-Sperre bei SIM-Wechsel und Verlust deaktiviert.

SMS Kommando: **SETZE DATENVERBINDUNG <Modus>**

Beispiel: **2222 SETZE DATENVERBINDUNG 1**

Neu seit Build 1795, nur für gerootete Geräte. Beschreibung: Setzt die *Datenverbindung erzwingen* Einstellung. Ist der *<Modus>* 1 wird die Einstellung aktiviert, ist der *<Modus>* 0, wird die Einstellung deaktiviert.

SMS Kommando: **SETZE ORTUNG <Zeit Intervall>**

Beispiel: **2222 SETZE ORTUNG 1**

Diese Option wurde mit Build 1652 entfernt, da durch Android-Bedingte Umstände eine vertrauenswürdige SIM Karte als nicht vertrauenswürdig erkannt werden kann und damit eventuell eine größere Menge an ungewollten SMS versandt wird. Wir bitten um Ihr Verständnis.

SMS Kommando: **SETZE SYSTEM <System Modus>**

Beispiel: **2222 SETZE SYSTEM 0**

Warnung: Dieser Befehl schaltet den Theft Aware Schutz aus. Danach ist Theft Aware nicht mehr erreichbar!

Beschreibung: Ändert den System-Status von Theft Aware. Setzen Sie den System Modus auf 0 um Theft Aware auszuschalten und in den sichtbaren Modus zurückzukehren.

Starten und Beenden der Theft Aware Oberfläche

SMS Kommando: **STARTEN** oder **BEENDEN**

Beispiel: **2222 STARTEN**

Beschreibung: Startet oder beendet die Theft Aware Konfigurationsoberfläche am Zieltelefon.

Neustart des Telefons

(Nur für gerootete Geräte, neu seit Build 1732)

SMS Kommando: **NEUSTART**

Beispiel: **2222 NEUSTART**

Beschreibung: Startet das Telefon neu.

Fernsteuer-Entwicklungs-Schnittstelle

Theft Aware kann mittels SMS Kommando beliebige am Telefon installierte Programme starten und dabei Daten an das Programm übergeben. Die Schnittstelle ist ab Build 526 gültig (Sie können die Build Nummer im Copyright Bildschirm Ihrer Theft Aware Installation finden).

SMS Kommando: **<VOLL QUALIFIZIERTER ACTIVITY ODER SERVICE NAME> <ARGUMENTE>**

Beispiele:

2222 at.domain.package.Activity Test → dies startet die Aktivität oder den Service *at.domain.package.Activity* und übergibt *Test* als Parameter.

2222 at.domain.package.Activity This is my command line → dies startet die Aktivität oder den Service *at.domain.package.Activity* and übergibt *This is my command line* als Parameter.

Die Activity oder der Service müssen sich in der Package-Wurzel befinden (Unterpakete sind momentan nicht unterstützt).

Der Datentransfer erfolgt über Intents:

```
Intent i = new Intent();
i.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
i.putExtra("number", origNumber);
i.putExtra("cmd", data);
i.setComponent(cName);
```

Das heisst dass Sie in der Activity oder im Service die Absender Nummer über das String Extra "number" und die Befehlszeile über das String Extra "cmd" auslesen können. Theft Aware versucht immer zuerst eine Activity zu starten, wenn diese nicht gefunden wird, wird ein Service gesucht und gestartet, wird keiner gefunden wird eine Fehler SMS zurückgesendet.

Viel Spass beim Entwickeln von eigenen Kommandos. Wenn Sie Verbesserungsvorschläge zur Schnittstelle haben senden Sie diese bitte an support@theftaware.com!

ERWEITERTE OPTIONEN

Sie können die erweiterten Optionen von Theft Aware benutzen, indem Sie die Menü-Taste drücken und das Menü *Erweitert* öffnen.

Test SMS senden

Hier können Sie überprüfen ob Theft Aware erfolgreich SMS senden kann. Es wird versucht, unsichtbare Test SMS an alle angegebenen Benachrichtigungs-Nummern zu verschicken.

Diebstahl simulieren

Dies simuliert ein Diebstahls-Ereignis. Wenn alles richtig funktioniert, sendet Theft Aware Benachrichtigungs-SMS an alle angegebenen Benachrichtigungs-Nummern. Dies kann einige Zeit dauern, da in diesem Schritt auch GPS Daten ermittelt werden.

Sperre simulieren

Dies simuliert ein SPERREN SMS-Fernsteuer-Kommando. **Im Erfolgsfall blockiert dies Ihr Telefon für 10 Sekunden.**

SIM-Liste löschen

(neu seit Build 1755)

Diese Option löscht die Liste der vertrauenswürdigen SIM-Karten. Die momentan eingelegte SIM Karte wird dann als einzig vertrauenswürdige SIM Karte in der Liste belassen.

Anhang A – Unterstützte Geräte

Die Android Version von Theft Aware unterstützt Android-basierte Mobiltelefone die mit einer **Android-Version 1.5 oder höher** ausgestattet sind.

Weiters ist Theft Aware auch noch für Nokia Symbian Mobiltelefone verfügbar. Bitte besuchen Sie <http://www.theftaware.com> für weitere Details dazu.

Anhang B - Sprachen

Die Symbian Version von Theft Aware wird in folgenden Sprachen ausgeliefert:

- English
- German

Anhang C - Kundendienst

Unser Kundendienst ist von 09:00 – 18:00 CET (GMT + 1) via Email erreichbar: support@theftaware.com
Wir versuchen Ihr Anliegen innerhalb eines Werktags zu bearbeiten und Ihnen eine Rückmeldung zu geben.

Anhang D - Partnerprogramm

Wollen Sie Partner von AVAST Software werden und mit dem Verkauf unserer Software Geld verdienen?
Dann besuchen Sie bitte <http://partners.theftaware.com>.