

AV-Comparatives



Mobile Security Review

Language: English

August 2013

Last revision: 20th August 2013

www.av-comparatives.org

Contents

Introduction	3
Overview.....	6
Tested products.....	8
Battery usage.....	9
Detection of Android malware	11
AVC UnDroid Analyser.....	11
AhnLab V3 Mobile	13
avast! Mobile Security	16
Bitdefender Mobile Security Premium	20
ESET Mobile Security.....	23
F-Secure Mobile Security.....	26
IKARUS mobile.security	29
Kaspersky Mobile Security.....	32
Lookout PREMIUM	35
Quick Heal Total Security	38
Sophos Security and Antivirus	41
Trend Micro Mobile Security	45
Webroot SecureAnywhere.....	48
Conclusion	51
Appendix – Featurelist.....	52
Copyright and Disclaimer	53

Introduction

Smartphones represent the future of mobile telephony. In April 2013 they exceeded 55% of the mobile phone market¹, and will surely replace conventional mobile phones sooner or later. For many people, such devices are much more than just telephones. They can be used for Internet banking, Facebook, taking and storing photos, organising one's entire life. This brings some risks; the same features that benefit the user make the devices attractive to criminals. Smartphones can be infected with malicious software, and sensitive data can be stolen. Phishing attacks work just as effectively with smartphones as with any other device.

Using a desktop or laptop PC without security software has become unthinkable. With mobile phones, this sense of responsibility has not yet reached the majority of users, even though important personal data, personal photos and even company data may be stored on smartphones. Due to automatic synchronisation of emails and even files via cloud storage services, more may be stored on the phone than the user really wants.

Mobile phones are small but expensive, making them a target for thieves. Security software must make it difficult for thieves to access the data on them, reducing the attractiveness of stealing them. Without protection, criminals have an easy job. After stealing a phone, the thief swaps the SIM card, and the phone is no longer reachable by its owner. Alternatively, they may leave the original SIM card in and make calls at the owner's expense, or use it for further criminal activities. To counteract such scenarios, modern security products for mobile phones are equipped with a range of different features.

Theft protection

Almost all the products in the test provide a theft-protection feature. One of the most important functions is the lock, which protects the smartphone with a password and thus prevents unauthorised access. Remote deletion of data also belongs to the standard features of a security program for smartphones. The locate function allows the phone to be found if it has been lost; we note that in the case of theft, some manufacturers warn against using this feature to hunt the thief down.

Manufacturers provide two different methods of controlling theft-protection features. The first is text messages. Commands are sent from another phone and cause the relevant action to be carried out. The second is a web interface. Both variants have their advantages and disadvantages. Text-messages almost always work, even if the sender is in a different country from the recipient phone. On the other hand, web interfaces are very intuitive to use and often allow multiple devices to be administered from one account. The disadvantage of text-message commands is that the user has to note them, and requires a second mobile phone from which to send them. If the web interface is to be used, the mobile phone must be connected to the Internet. In some circumstances, e.g. if the phone is lost when abroad, the Internet connection may effectively have been disabled.

The location function is very useful, but can be misused to track people. It is possible to install security software on someone else's phone, or to give them a phone with the software pre-installed,

¹ http://www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/The_Mobile_Shift

in order to follow their movements. This is of course perfectly acceptable in the case of parents keeping an eye on their children, but may be entirely inappropriate in other circumstances.

Malware protection

With the help of malware protection functions, smartphones can be scanned for malicious software, which can then be quarantined or deleted. For this function to be effective, malware signatures must be kept up to date. When travelling abroad, users need to take care not to fall into the roaming-costs trap.

Due to its high and rapidly growing market share (currently 74.4%)², we have once again used Google's Android operating system to test mobile security software. The report contains details of products from leading manufacturers who chose to have their products tested and reviewed. The tests were conducted in July 2013 using Samsung Galaxy S3 Mini smartphones running Android 4.1.2.

Battery usage

Late in the afternoon, a smartphone user might wish they had a portable power station with them. The multiple functions of modern phones mean that even power-saving processors are not able to reduce the battery usage greatly. GPS, email, Internet, and especially the large displays found in most smartphones mean that power usage is high. It can easily happen that heavy use of the smartphone means that the battery is empty by the afternoon. There are three ways to prevent this. The user can make limited use of the phone, carry a solar-powered battery charger around, or take measures to reduce the power consumption during use as much as possible.

- **Display settings:** The display is the greatest user of power in the phone. It makes sense to let the display adjust itself automatically to the ambient light, or to reduce it manually, in order to save power. Some smartphones automatically reduce screen brightness when the battery is low.
- **Locating:** Switch GPS off. Navigating and locating the phone (e.g. for photos with geo-location) require a high degree of calculation by the processor, as the location must constantly be recalculated. Only switch GPS on when you really need it. Likewise, WiFi and Bluetooth should only be switched on when necessary. This applies to all functions of the mobile phone; switch off what you do not need, and the battery will last noticeably longer.
- **Multi-tasking:** Under Android, apps may run in the background, in some cases for a long time, without being used at all. Using the Task Manager to close unused apps saves battery life, as they would otherwise be using up power. In Android, the Task Manager can be opened simply pressing and holding the Home button.

Exchange, Gmail: Not only email and contact synchronisation, but also Facebook and other social networks such as LinkedIn update their data from the Internet. Some unknown background services run which can be switched off or changed to a less frequent synchronisation schedule. Battery life can be extended by a third if email synchronisation is changed from instant to every quarter of an

² <http://www.gartner.com/newsroom/id/2482816>

hour. This is also true for status updates from Facebook etc. Every new Facebook update switches the display on and plays an audio notification, both of which use up the battery.

Security Software: Many users are still convinced that security software on an Android smartphone is power-hungry. However, our tests show that this is no longer the case. The effect of security software on battery life can be more or less ignored. Backups, updates and malware scans, on the other hand, clearly do increase battery usage significantly. There is an advantage to products that can be configured so that they only carry out such operations when the device is on charge.

Overview

The perfect mobile security product does not exist. However, this report enables you to compare the advantages and disadvantages of each of the products and narrow down the choice. Installing the test version of potentially suitable products makes it easier to decide on the best solution. New versions of products, with improvements and new features, are released especially frequently in the field of Android security products.

By participating in this test, the manufacturers have shown their dedication to producing high-quality mobile security software for their customers. The report shows that we have found errors or imperfectly functioning features; the manufacturers have taken these problems very seriously and are already working on solutions. In many cases the errors have already been fixed. As the core functionality of the tested products has already reached a very good standard, we are pleased to be able to give our Approved Award to all the participating products.



AhnLab V3 Mobile makes a very mature impression. It offers innovative functions such as file encryption and a well-designed network monitor.

avast! Mobile Security is a very comprehensive security product and is even available free. The suite, which already had a great range of features last year, now boasts a web interface too.

New to the market is **Baidu Mobile Manager**, which is available free, in Chinese only. As well as security features, it contains a number of check-up functions to improve the phone's performance.

Bitdefender Mobile Security is a clearly designed security product. The well-designed web interface, which can be used to manage multiple devices, stands out.

In terms of optical design, **ESET Mobile Security** has been greatly revised in the new version. This has had a very positive effect on the usability of the product, which is outstanding. The app offers good functionality too.

F-Secure Mobile Security and **Trend Micro's Mobile Security** offer optimal security for families. As well as classic features such as theft protection, both suites provide comprehensive parental controls, which protect children when surfing the Internet.

IKARUS mobile.security provides the user with a clearly designed security product containing all the important features. Additionally, more exotic but valuable functions such as a URL blocker and USSD protection are included.

Kaspersky Mobile Security allows users to protect their private sphere by hiding text messages, call logs and contacts. The biggest change in this year's version is the inclusion of a web interface.

Kingsoft Mobile Security is available free, in Chinese only. The security product is very simple to use, and offers useful features such as a secure QR-code scanner and ad blocker.

The integrated backup feature of **Lookout PREMIUM** prevents data being lost by saving it to the cloud. The other features of the suite also impressed in our test.

Qihoo 360 MobileSafe is a free security product, currently available only in Chinese³. The product has a wide range of functions, including theft protection, various optimisation tools, app manager, network manager, and spam blocker.

Taking part in our review for the first time is **Quick Heal Total Security**. The product surprised us pleasantly with its extensive functionality. Practical components such as the backup feature and network monitor round the suite off.

Relative to last year, **Sophos Security and Antivirus** has made a quantum leap. The mini-app has developed into a comprehensive security suite, which impressed us in terms of both optical design and functionality.

Tencent Mobile Manager is a free security product in Chinese language. The well-designed app provides theft-protection, privacy protection, and other innovative functions.

Users who want to be able to control theft-protection features using both text messages and a web interface should take a look at **Webroot SecureAnywhere Mobile**. Its various app inspectors can also find resource-hungry apps.

³ An English version will be soon available.

Tested products

The products listed below were tested for this report. The manufacturers either provided us with the newest versions of their respective products, or confirmed that the latest version was available from the Google Play store (as at July 2013). After the test, the manufacturers were given the opportunity to rectify any errors we found in their products. We have noted in the report any problems that have subsequently been fixed.

- AhnLab V3 Mobile 2.1.0.3.178
- Avast! Mobile Security 2.0.4993
- Baidu Mobile Manager 2.0
- Bitdefender Mobile Security Premium 1.2.365
- ESET Mobile Security 2.0.766.0-0
- F-Secure Mobile Security 8.1.12262
- IKARUS mobile.security 1.7.13
- Kaspersky Mobile Security 10.4.47
- Kingsoft Mobile Security 2.3.2.775
- Lookout Premium 8.17-8a39d3f
- Sophos Security and Antivirus 3.0.1154(7)
- Tencent Mobile Manager 4.1.1.986
- Trend Micro Mobile Security 3.1.0.1095
- Qihoo 360 MobileSafe 4.0.1
- Quick Heal Total Security 1.01.063
- Webroot SecureAnywhere Mobile 3.3.0.5566



The mobile products of **Baidu**, **Kingsoft**, **Qihoo 360** and **Tencent** are currently only available in Chinese. The full reports on these products are thus only included in the Chinese version of the review, available on our Website⁴.

A comprehensive list of all the mobile security products available on the market can be found under <http://www.av-comparatives.org/list-mobile/>

⁴ <http://www.av-comparatives.org/mobile-security/>

Battery usage

Measuring the battery usage of a device would at first glance appear to be very easy. When one takes a closer look, however, it becomes apparent that there are difficulties. In particular, the way individual users use their mobile phones can vary greatly. Some make use of the phone's multimedia capabilities; others use the phone to read documents, while some still just use it as a phone. We need to distinguish between power users, who take full advantage of the phone's technical capabilities and functions, and "traditional" users who just use it for phone calls.

In order to find the right balance of telephone usage for this test, we conducted a survey in April 2012. Over a thousand smartphone users from all over the world were asked to respond anonymously to our questions about how they used their phones. It became clear that most users take full advantage of the capabilities of their phones. 95% surf and mail with their phones, over 66% listen to music over the Internet or watch online videos. It is noteworthy that 70% of users never switch their phones off.

Smartphones are becoming more and more important, and very few users leave any function of their phones unused. The smartphone is becoming the omnipresent means of communication, an extension and even replacement of the computer. Telephony is becoming more of a background function, with over 41% of users spending 10 minutes or less actually talking on their phones. 29% of the users spend more than an hour a day on the Internet.

The answers from our mobile security survey (April 2012) were used as the basis for our usage statistics. This data was used to form the typical daily usage patterns for the battery-life test.

Environmental conditions

To measure the battery usage (battery drain) precisely, we worked with x.test and Agilent to use an ISO-calibrated measuring device for our tests. This high-precision instrument can measure battery drain exactly. An automated standard test run, emulating real users in accordance with the survey data, was carried out multiple times.

External Influences

In order to exclude environmental and technical influences, we took pains to ensure that each device was tested under exactly the same conditions, compatible with influences ECMA-383⁵.

The 3G and WiFi connections are susceptible to variations caused by e.g. the weather conditions. In order to minimise/remove such fluctuations, we put a WiFi base station and our own UMTS base station in our testing lab. We could thus determine that the energy required establishing a wireless connection was the same for each product.

Battery usage is naturally dependent on the type of mobile phone. Various factors influence battery drain, an important one being the nature of the display. A larger screen will of course take more battery power than a smaller one. The type of display (LCD, OLED, AMOLED, etc.) is also relevant. Using the same phone for all test candidates allowed us to rule out any such differences influencing our test.

⁵ <http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-383.pdf>

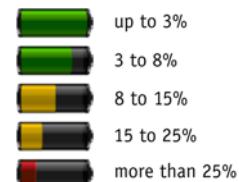
We measured the power consumption while performing the following task based on average usage (according to our mobile phone usage survey) as follows:

- **Making phone calls** (30 minutes a day)
- **Viewing pictures** (82 minutes a day)
- **Browsing websites** (stored on a local server to avoid the influence of Internet connection speed fluctuations; 45 minutes a day)
- **Watching YouTube** videos online with the integrated YouTube app (17 minutes a day)
- **Watching locally stored videos** on the device (13 minutes a day)
- **Receiving and sending mails** using the integrated Google Mail client (2 minutes a day)
- **Opening documents** stored on the device, like PDFs and Word documents (1 minute a day)



In our test, we found that most mobile security products only have a minor impact on battery life.

Manufacturer	Battery usage	Manufacturer	Battery usage
AhnLab		Kingsoft	
avast!		Lookout	
Baidu		Sophos	
Bitdefender		Tencent	
ESET		Trend Micro	
F-Secure		Qihoo	
IKARUS		Quick Heal	
Kaspersky		Webroot	



Overall, we can give the manufacturers of mobile security suites good marks when it comes to battery usage. In this year's Battery-Drain Test, there were however two products that did not reach the top level:

- **Qihoo** has very fancy animations, e.g. when connecting a phone call. This looks pretty, but takes processor usage, which ultimately places a strain on the battery.
- In the case of **Webroot**, we were able to trace the increased battery usage to the "*Execution Shield*", a real-time protection component that checks every app on execution for malware and sends its hash to the cloud. When this feature was deactivated, the battery usage sank to below 3%. After the test, Webroot released a newer version (3.4.0.5650). At their request, we re-ran the test using this version. A small improvement was noted, but the score remained above 3%.

Detection of Android malware

Methods of attacking mobile phones are getting more and more sophisticated. Fraudulent applications attempt to steal smartphone users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from Google Play or reputable app makers' own stores. Avoid third-party stores and Sideload⁶. Another indication of untrustworthy apps is irrelevant access rights. For example, an app that measures the speed at which you are travelling has no need to access your phone book or call log. Of course, even if an app does this, it is not a clear-cut indication that it is malicious, but it makes sense to consider whether it is genuine and should be used. A look at the reviews in the app store is also a guide; avoid apps with bad or dubious reviews. If you Root your smartphone, you will have more functionality on the phone, but equally the opportunity for malicious apps to take control will also increase. Another point to consider is the warranty. It is not legally clear cut whether the warranty is still valid if the phone is rooted. In many cases, the warranty will be considered null and void.

How great is the risk of infection with an Android smartphone?

This question is difficult to answer, as it depends on many different factors. In western countries, if using only official stores such as Google Play, the risk is lower than in many Asian countries, especially China. There are many rooted phones and unofficial app stores, which increase the chance of installing a dangerous app. In many Asian countries the smartphone is used as a replacement for the PC, and is frequently used for online banking. Banking apps are also becoming more popular in Europe and the USA. There is a high risk involved in receiving the mTan code on the same phone that is used to carry out a money transfer. In western countries, assuming you stick to official app stores and don't root your phone, the risk is currently relatively low, in our opinion. However, we must point out that "low risk" is not the same as "no risk". Also, the threat situation can change quickly and dramatically. It is better to be ready for this, and to install security software on your smartphone. Currently, we would say that protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

AVC UnDroid Analyser

At this point we would like to introduce AVC UnDroid, our new malware analysis tool, which is available free to users. It is a static analysis system for detecting suspected Android malware and adware and providing statistics about it. Users can upload .apk files and see the results in various analysis mechanisms.

We invite readers to try it out: <http://www.av-comparatives.org/avc-analyzer/>



⁶ <http://en.wikipedia.org/wiki/Sideload>

Test Set

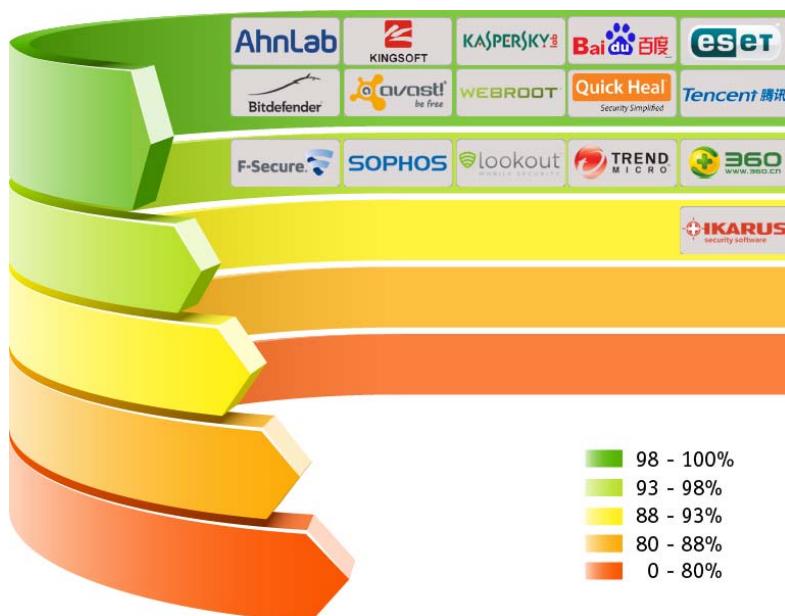
The malware used in the test was collected by us in the four weeks prior to the start of the test. 2,947 malicious applications were used to form a representative test set. So-called "potentially unwanted apps" were not included. The security products were updated and tested on the 23rd of July 2013.

The test was carried out on genuine Android smartphones (no emulators were used). The test set consisted exclusively of .apk files. Each individual app was manually installed; this was done to test which technologies were employed by each security product to protect against malicious apps.

We also carried out a false-positive test. The top 100 apps from Google Play that are not supported by advertising were used for this. None of the security products tested produced any false alarms with these 100 clean apps.

Detection rate results

1. AhnLab , Kingsoft	99.9%
2. Kaspersky	99.7%
3. Baidu, ESET	99.6%
4. Bitdefender	99.4%
5. avast!	99.0%
6. Webroot	98.9%
7. Quick Heal	98.6%
8. Tencent	98.1%
9. F-Secure	97.1%
10. Sophos	96.3%
11. Lookout	96.0%
12. Trend Micro	95.6%
13. Qihoo	93.6%
14. Ikarus	91.0%



AhnLab V3 Mobile

AhnLab V3 Mobile is a security product for Android, with the most important security features, such as a malware scanner, theft protection and anti-spam.



Installation

AhnLab V3 Mobile was provided for us by AhnLab as an APK file. Installation was a simple process. After the licence agreement had been accepted, we had to register the device, which took only a few seconds and did not require the entry of any further user information. We were then taken to the start screen.

Starting the program

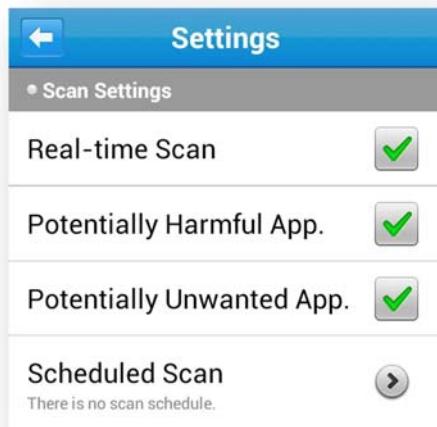
There is no introduction to AhnLab V3 Mobile, the user simply has to explore the product to discover its features. There is no initial update. The real-time protection, which is activated by default, can be switched on or off directly from the home screen. All the other components can be activated from the same place. The details of the last update and last scan are shown in the bottom right-hand

corner of the screen; immediately after installation, both are shown as "N/A".

Scan

The Scan module allows the user to run two different scan types: *Smart Scan*, which checks all installed apps for malicious behaviour, and *Intense Scan*, which additionally checks all files on the device. Details of the last *Scheduled Scan* are also shown, as is the time of the next one. The settings for this can be changed in the global configuration menu. The interval (daily or weekly) can be set, as can the time of day.

The settings also include options for the sensitivity of the scan.



Anti-Theft Protection

To use this component, a password of between 4 and 10 characters must be created. The app also has to be registered as a device administrator. Overall, we found the setup very simple. Text-messages are used to control the theft-protection component; there is no web interface. The commands are listed in an overview and can be tested.

Lock

Text-message command:

"#lock <Password> <Message>"

This command locks the smartphone, preventing it being accessed by unauthorised persons. The previously defined password is

needed here. We liked the fact that it is possible to send a personal message to be displayed on the lock screen. Another plus point is that after 10 incorrect password entries, a text message with the position of the phone will be automatically sent to the sender of the lock command.

A minus point is that the lock screen does not allow emergency calls to be made. It is also not very secure. Pressing the Home button shows the Home screen; it is possible to navigate through this and view installed apps. It is also possible to start programs, even if the lock screen then appears after a few seconds. The lock screen is thus not really up to the task.

Remote Data Delete

Text-message command: "#remove <Password>"

This command deletes personal data from the phone. The phone is not returned to factory settings, which means that the anti-theft software remains installed and working. Although the text-message log was not deleted, we found that this component very largely worked well. All the contacts, files, calendar entries, browser history and bookmarks were wiped. It was however possible to recover data from the SD card with common freeware tools.

Remote Wipe Reset

Text-message command: "#kill <Password>"
This command deletes personal data and resets the device to factory settings.

In contrast to the Remote Data Delete, the result of this was not satisfactory. Neither the contacts on the SIM card nor the files on the SD card were deleted. We would recommend sending the Remote Data Delete command before using Remote Wipe Reset.

Remote Location Tracking

Text-message command: "#locate <Password>"

When the command has been sent, the sender promptly receives a reply with a link to the phone's location in Google Maps, complete with co-ordinates. Whilst the term "tracking" suggests a continuous trail is recorded, rather than one-off points, we found the locate function worked very well.

SIM card swap

If the SIM card is changed, an SMS containing details of the phone's location will be sent to the trusted phone number.

Anti-Spam

AhnLab's anti-spam component enables calls and texts to be blocked using a blacklist. There are a few possible ways of adding numbers: from the call and text-message logs, from the address book, or manually. For each number, it is possible to block just calls, just texts, or both.

Additionally, texts can be blocked based on their content. Keywords with a length of between two and ten words can be defined. We don't know why there is an upper word-length limit. We also note that the filter function is case-sensitive, which again seems to be a questionable restriction.

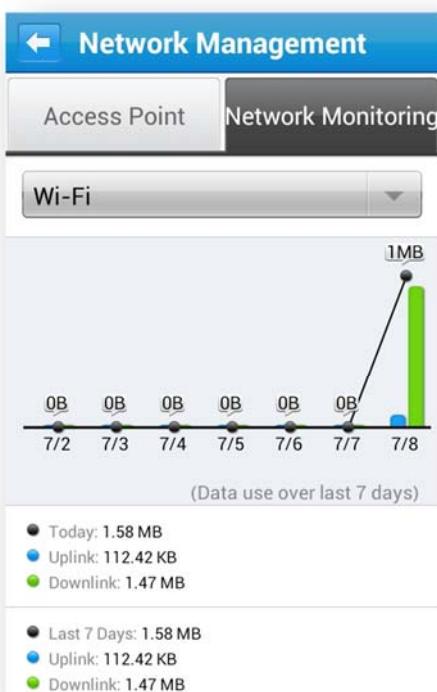
All blocked calls and texts can be displayed in a sub-menu. We found the functionality of the anti-spam function to be satisfactory overall. The component is not activated by default;

this was not initially clear to us, and in our test we assumed it was not working. Showing the status of the feature within its menus would be an improvement.

Network Management

The Network Management menu gathers together network-related functions.

When the device connects to a WiFi hotspot, a pop-up appears that allows the user to deactivate WiFi, or permanently allow or deny access to this hotspot. A list of known access points allows these to be managed.



The use of mobile networks can be limited; if mobile network usage reaches a pre-defined limit, the user will be alerted. *Network Monitoring* provides the user with data usage statistics. These can be sorted according to mobile and WLAN traffic. The amounts of data uploaded and downloaded within various time periods can be displayed separately.

File Encryption

File Encryption allows individual files to be encrypted. Via a file browser, multiple files can be selected and encrypted using a password of four to ten characters. The result

is a file with the ending *.aed, which cannot be opened. Decryption also uses the AhnLab software. There is no restriction on the type of files that can be encrypted, so pictures, videos, PDF files etc. can all be protected this way.

Updates

Updates are carried out automatically. The user can decide whether this happens only over WiFi or using the mobile network as well. As with scheduled scans, the timing of automatic updates can be configured.

Help

AhnLab's help function has been very clearly organised. We liked the step-by-step instructions for particular tasks. However, we were rather annoyed to find that pressing the Back button when using help returns the user to the Start screen or main Help page.

Deinstallation

There is no deinstallation wizard, but a step-by-step guide is provided in the Help function. The app has to be removed from the device administrators, and can then be uninstalled using the Android App Manager.

We were not required to enter a password to remove the program. This represents a security risk, as a thief can easily uninstall the theft protection.

Summary

AhnLab V3 Mobile provides the most important security features for Android Smartphones. As well as the classic functions, the program provides innovative features such as file encryption and network management.

avast! Mobile Security

avast! Mobile Security is a comprehensive security product for mobile telephones and tablets, provided free of charge. Its main functions include antivirus, browser protection and theft protection.



Installation

We installed avast! Mobile Security via the Google Play Store. The installation process was very simple, requiring only the acceptance of the licence agreement. The user can decide whether to send anonymous usage data to the manufacturer.

Starting the program

When the program is first started, the home screen is displayed; this indicates the wide scope of the product. The obvious status display in the top right-hand corner of the screen initially indicates "Outdated", but once the automatic update has been carried out, this changes to "Secured".

Navigating the menu system is very largely intuitive. Only the activity logs, which are displayed by swiping to the right, might remain undiscovered by some users.

Virus Scanner

The Virus Scanner checks all installed apps for malware. The user can optionally select to activate file scanning as well. Pressing and holding this checkbox produces a menu, from which a specific folder can be selected for scanning. Along the bottom of the screen are buttons for configuring an automatic scan. Day and time can be selected.

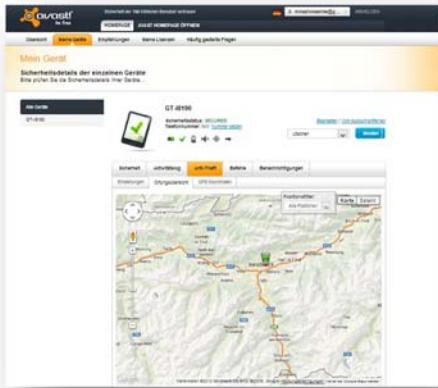
Anti-Theft

The Anti-Theft component is a stand-alone application that has to be installed separately. This has the advantage that the Anti-Theft app can be hidden; it is seamlessly integrated with the rest of the suite, and the user would otherwise not notice that it is an independent program.

The installation requires an easy but relatively comprehensive setup procedure. A name, the telephone number of a friend/family member, and a 4-6 digit PIN have to be entered. The avast! account then has to be registered, and the user has to log on, if the web interface is to be used.

Activating the Anti-Theft component automatically puts it into Stealth Mode, meaning it is hidden from view. It can be unhidden by calling the number used as the PIN.

A very loud yellow symbol makes very clear that configuration has not been completed, and it is pointed out that avast! must be assigned administrator privileges.

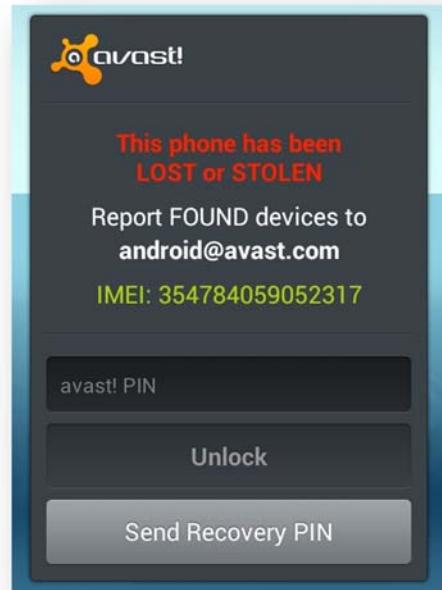


The Anti-Theft component can be controlled either via a web interface, or by using a multitude of text-message commands. As well as the standard lock, locate and wipe commands, avast! offers functions such as the forwarding of SMS messages, calls and call logs. A complete list of the available functions can be seen by going to <http://www.avast.com/en-gb/free-mobile-security#tab3> and clicking on "Control via SMS".

Lock

Text-message command: "<PIN> LOCK"

When the command has been received, the device is locked and the lock screen displayed. Honest finders are asked to notify avast! that the device has been found (the lock-screen text can be customised). This involves sending the the IMEI (International Mobile Equipment Identity, unique identifying number) to android@avast.com. The IMEI is displayed on the lock screen. Additionally, the phone plays the audio message "This phone has been lost or stolen" (only available in English). The device can be unlocked by entering the correct PIN.



The Lock function is not without its problems in practice. When the phone is locked, it is still possible to open the Android Notification Bar, and thus change settings, by swiping the screen downwards. Holding the Home button displays the list of recently used apps, whereby personal information could be visible. avast! inform us that this will be rectified in the next release.

Additionally, it is not possible to make an emergency phone call, which could prove dangerous, and may be illegal in some countries.

Siren

Text-message command: "<PIN> SIREN ON"

This command plays the same sound as when the phone is locked, but without locking the phone. It is thus useful for locating the phone when it has been mislaid.

Locate

Text-message command: "<PIN> LOCATE <INTERVALL>"

This command is used to find the location of the phone. The sender of the text command receives a reply with a link to an online map with location co-ordinates, mobile phone service provider and mast. The optional

parameter *Interval* indicates how often, in minutes, the process is repeated. Frequent sending of location data allows continual tracking of the phone's location to be carried out. This web interface is obviously ideal for this, as the movements of the phone can be clearly displayed on a map.

Wipe

Text-message command: „<PIN> WIPE“

avast! Mobile Security provides two variants of the Wipe function. There is a standard delete function, or thorough delete can be found in the advanced settings of Anti-Theft. Both deletion types reset our test device to factory settings, whereby all our personal data and all files on the internal storage were deleted.

The thorough delete variant wrote 1,000 junk files of 1 MB each onto the internal storage, as a means of making it impossible to recover any of the original data.

In our test, with both forms of deletion, only media files such as .mp3 or .jpg were deleted. All other file types (in our test we had .exe, .dll and .txt files) remained unaltered on the card.

Even in the case of thorough deletion, we found that those files that were deleted from the SD card could be restored with a free program.

Hard Reset Protection

For users with rooted devices avast! offers a hard reset protection. By enabling this function the security product survives a factory reset and will not be removed.

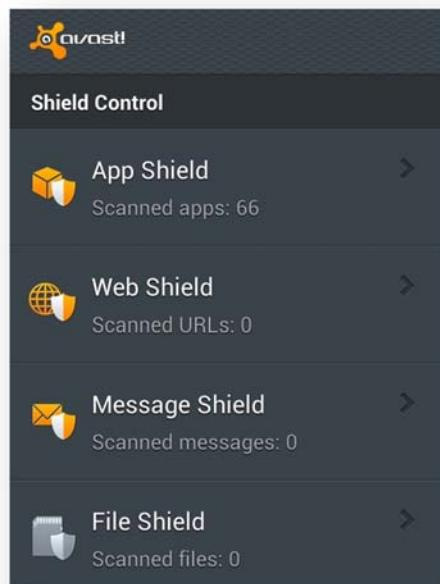
Privacy Advisor

The Privacy Advisor categorises apps that require special privileges such as *Access Messages*. This provides users with an overview of potential data protection issues on their devices. Tapping any of the six categories shows the apps listed within. If the

user then taps a specific app, detailed information is displayed, along with a button that stops the program immediately.

Application Manager

The Application Manager analyses running and installed apps' use of CPU, RAM, storage and other resources, and allows users to stop apps they consider too greedy.



Shield Control

Various real-time protection functions can be found under *Shield Control*. These are as follows:

App Shield

App Shield scans apps for malicious functions, either during installation or on execution, according to configuration.

Web Shield

This component protects the user from phishing sites and web pages with malicious code. Both the standard browser and Google Chrome are supported.

Avast also provides a spelling checker, which is supposed to recognise and correct wrongly typed URLs (to prevent typo-squatting). However, in our test, we were unable to find a case where this feature was activated.

Message Shield

This scans all incoming messages for phishing links and dangerous URLs. This worked reliably in our test. The feature can also be used to block messages from unknown senders.

File Shield

This scans files on read/write for malicious behaviour. This also worked perfectly in our test.

SMS and Call Filter

In order to prevent unwanted calls and texts, avast! provides the *SMS and Call Filter*. This allows groups to be created, for which calls and texts can be blocked, either at particular times or altogether.

The members of a group can be contacts from the address book, phone numbers, or fields such as all anonymous callers or senders. avast! use the blacklisting principle here.

Firewall

The firewall can only be activated if the device has been rooted. This is a normal restriction of the operating system for non-rooted devices.

Network Meter

This component lists the volume of data used by all installed apps. This can be itemised by WiFi, 3G, Roaming or All. Tapping one of the apps allows its data use to be shown by date (today, month, year).

Update

avast! Mobile Security is automatically updated by default. The user can decide whether this should occur via WiFi, 3G or roaming connections.

Help

Apart from the Anti-Theft feature, avast! do not provide any local help on the smartphone. Users requiring assistance have to visit the manufacturer's website; a comprehensive FAQ

section is provided, which should cover most questions and problems.

Deinstallation

A deinstallation wizard is provided for the user to remove the theft protection. This requires the PIN to be entered. This also has to be entered if the app is uninstalled using the Android App Manager, meaning that the theft protection cannot be uninstalled by unauthorised users.

Future prospects

avast! have announced a future commercial version, which is to include additional functions such as backup of apps and photos, extended anti-theft, application locking, and an advanced privacy scanner.

Licence

avast! Mobile Security is available free to everyone without any restriction of functionality.

Summary

avast! Mobile Security provides a wide range of functionality and is available free. We particularly liked the various configuration options and remote commands, which allow extensive remote control functions.

Bitdefender Mobile Security Premium

Bitdefender Mobile Security Premium is available as a 14-day trial version. When the trial period has expired, the user has to purchase a licence. The software combines a cloud-based malware scanner with surfing protection and theft protection. The latter can be operated by web or text-message interface.



Installation

Bitdefender was easy to install from the Google Play store. After the licence agreement has been accepted, the user has to assign the device a name for use with the web interface, and then log in to a Bitdefender account or specify a Google account. This is also for use with the web interface. A brief overview of the features is displayed; installation is then complete, and the home screen of the program is displayed.

Starting the program

After successful completion of the installation, the user sees a very prominent notification (in yellow) that a scan should be run, along with a reminder (where applicable) that a 14-day test version is being used.



After a malware scan there are 3 scenarios: the user sees a green status, meaning the device is safe, or an orange or red status, if there are issues that require the user's attention. There is no mention of update status; this is because virus definitions are not stored locally, but in the cloud.

Malware Scanner

This enables the user to check installed apps and the memory of the mobile phone for malware. Only one configuration option is available to the user, namely whether to start a scan automatically when the mobile phone is connected to another device.

The malware scanner only works if there is an Internet connection, due to the use of the cloud for detection.

Application Audit

The Application Audit feature lists all apps that have special permissions, such as Internet access, access to private data or chargeable services. The apps can be filtered by category, in order to provide an overview. Clicking on one of the listed apps takes the user to the relevant Android App Info page.

Web Security

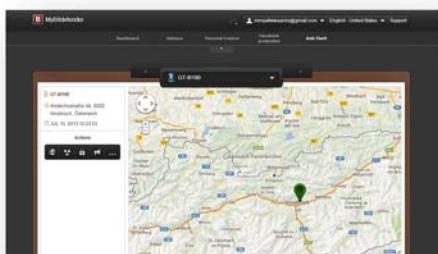
Web Security protects the user against phishing attacks, untrustworthy websites and malware. It works with the standard Android browser and Google Chrome.

Anti-Theft

The theft protection module is deactivated by default. It can be operated using a stylish web interface⁷, which allows the

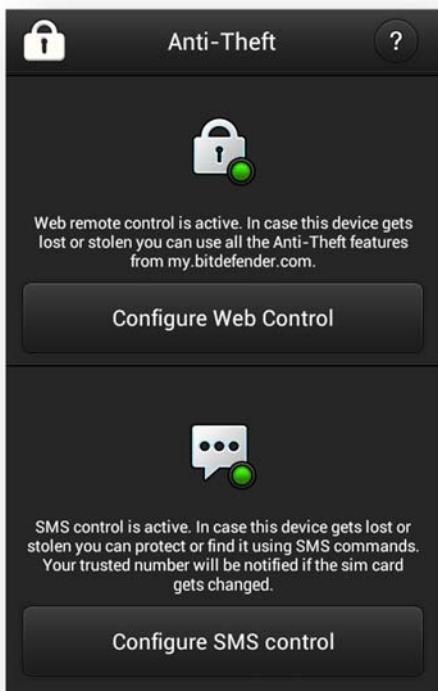
⁷ <http://my.bitdefender.com>

administration of multiple devices, or text-message commands.



Starting the Anti-Theft component displays a brief overview, then asks the user to provide the app with administrator rights. A PIN of between four and eight digits must be defined, and a trusted telephone number entered. The latter is used to send notifications to in the event of a SIM-card change. It is also the only number that can be used to send a Wipe command.

There is a range of options for both methods of operation (web and text). For example, it is possible to disable some elements of the web interface functionality, or text messaging in its entirety. The PIN has to be entered to make any configuration changes.



Locate

Text-message command: “bd-<PIN> locate”

This command locates the device in the event of loss or theft. When the command has been sent, the sender receives by return a message with a link to Google Maps, showing the location and the time this was determined. If the web interface is used, this similarly shows the position on a map. There is no means of tracking the device by means of continuous location determination.

Lock

Text-message command: “bd-<PIN> lock”

This command locks the device and so protects against unauthorised access. Bitdefender uses the standard lock screen integrated into Android. This does not allow any logos or messages to be displayed, but is entirely secure; it is not possible to get around it, and it is always possible to make an emergency call.

Wipe

Text-message command: “bd-<PIN> wipe”

This function deletes all personal data from the user's smartphone, making it inaccessible to third parties. Once the command has been received, the device is immediately reset to factory settings.

Unfortunately we note that none of the files on the external SD card were deleted.

Call me

Text-message command: “bd-<PIN> callme”

This function can only be operated by text message. It causes the device to call the sender's number, and activates the loudspeaker. It allows contact to be made with an honest finder.

Answer

Text-message command: “bd-<PIN> answer”

This function is similar to Call Me. In this case, the text message is sent, and then the user can call the device, which will automatically answer.

In our test, this feature did not work. The call was not answered, and we did not receive any text messages in reply. Bitdefender inform us that the feature does not work with Android 4.1 or above.

Help

There is no specific help function for the software. However, each function has its own brief but useful information text.

Deinstallation

There is no uninstaller provided to remove the software. The user thus has to know that administrator rights have to be removed. This requires entering the PIN, to prevent a thief from disabling the software.

Licence

Bitdefender Mobile Security can be tested free for 14 days. A licence is then required, which costs €8.99 if purchased In-App.

Summary

Bitdefender Mobile Security provides the user with an easy-to-use security product for the smartphone. It has a comprehensive range of anti-theft functions.

A plus point is the intuitively designed web interface, which allows the user to manage multiple smartphones from one account.

When it comes to the malware scanner, we feel that Bitdefender should not rely on the cloud alone, as malware recognition is not possible without an Internet connection.

ESET Mobile Security

ESET Mobile Security is a security app that includes the components Antivirus und Anti-Theft. The Premium version additionally provides SMS and Call Filters, Anti-Phishing and System Audit components and advances Anti-Theft features; in particular a remote wipe and a SIM Guard.



Installation

We installed ESET Mobile Security from the Google Play Store. When the program is first started, an end-user licence agreement has to be accepted. The user can also agree to send anonymous usage data to ESET by means of a checkbox, an option that is disabled by default. In the next configuration step, *ESET Live Grid* can be deactivated (it is active by default); this is an early-warning system, which uses data recently gathered from participating users. Finally the licence is checked, and a notification informs the user that an initial scan is going to start.

Starting the program

After the initial configuration, the user is taken to a clear home screen (see screenshot above). This provides to all the individual components of the suite. Active components

are marked with a green tick, inactive ones with a grey on/off switch, and components requiring attention with an orange triangle. Additionally, Premium Components (only available in the Premium version) display a blue banner. The Premium suite can be tested free for 30 days; an email address has to be provided.

Antivirus

The Antivirus feature allows the system to be scanned for malware. The depth of scanning can be configured, and the quarantine list, scan logs and update details can be seen. The advanced settings allow the user to change items configured during the installation, and to set the default reaction when malware is discovered.

Anti-Theft

The Anti-Theft component has to be configured on the first start. This involves entering a security password, with an optional reminder phrase. Although there is no minimum password length, ESET warns users that short passwords are not secure. To prevent unauthorised deinstallation of the program, it is suggested that the program should be made a device administrator. Next, there is information about text-message commands, and the possibility to use a different password for these. After this, the current SIM card is registered as trusted, and a trusted phone number is entered. We liked the fact that it is possible to edit the text displayed when the device is locked. To use text-message commands for this feature, a password is required. A unique Anti-Theft password is recommended, although the standard security password can be used.

SIM Guard

This feature is intended to prevent unauthorised changes of the SIM card. If an unregistered SIM card is inserted, the device is locked. The function worked perfectly in our tests; we had the choice of entering the security password to unlock the phone, or calling emergency numbers. We note that

after an unregistered SIM card has been inserted, a password confirmation is required, even after the original card has been re-inserted. There is a slight security risk here, in that there is no limit to the number of attempts to enter the password, but we otherwise found the function sensible and well executed.

Lock

Text-message command: “eset lock <Password>”

When the command has been received, the device is locked and the lock screen is displayed. The message sender will also receive a confirmation text message with IMEI and IMSI (device identification data). The same highly resistant lock screen is deployed as for the SIM Guard. If the user has forgotten the password, they can either send a reset command from another phone, or send a reset email directly from the lock screen of their own phone.

Siren

Text-message command: “eset siren <Password>”

This command provides the same functionality as Lock, except that additionally a very loud alarm sound is played for a minute.

Find

Text-message command: “eset find <Password>”

This component allows a stolen or lost smartphone to be located. After sending the text message, the message sender receives a reply containing a link to Google Maps with the relevant co-ordinates for the phone's location.

Wipe

Text-message command: “eset wipe <Password>”

This feature deletes all personal data from the user's smartphone, to prevent this being read by third parties. The phone is NOT reset to factory settings, in order that the software remains installed and its anti-theft functions

retained. However, calendar entries, browser history, Favorites and SMS log are not deleted. ESET inform us that they have plans to rectify this in the next product update. On the other hand, the memory cards were wiped clean, and it was impossible to recover data from the external SD card using a commonly used free program.

SMS & Call Filter (Premium)

This function enables the user to create comprehensive rules for blacklisting and whitelisting calls and messages. Rules can be set up to determine what sort of contact is allowed for particular people at particular times.



Anti-Phishing (Premium)

Anti-Phishing protects the user against phishing sites when browsing the Internet. ESET checks the installed browsers for compatibility. Although ESET Mobile Security claims that it “integrates with most common browsers”, in practice this only means the Android browser and Google Chrome. Firefox, Opera and Dolphin are not supported.

 Chrome Supported	✓
 Internet Supported	✓
 Opera Mini Not supported	✗
 Firefox Not supported	✗
 Dolphin Browser Not supported	✗

In our test, the phishing protection worked perfectly for the two supported browsers. A warning page from ESET was displayed, recommending that the user leave the site immediately.

Security Audit (Premium)

The Security Audit feature provides information about system settings and program privileges that might represent a security risk. In our test, we were informed that, amongst other things, the USB Debug Mode and Installation From Unknown Sources settings were active. The Device Monitoring feature includes notifications such as roaming calls and data, insecure WiFi connections, and memory usage.

Help

ESET provides the user with a help file that covers all the available components. Tapping the question-mark symbol in a component takes the user to the appropriate section of the help text.

Deinstallation

The program can be uninstalled from its own settings menu, or from the Android App Manager. If the Anti-Theft component is activated, the security password has to be entered, regardless of which deinstallation method is used. Removing the app via the internal menu asks for the reason for

uninstalling, and then proceeds with a single click.

Licence

The majority of the functions are included in the free version of the software. A licence for the Premium features such as automatic scans, automatic updates, phishing protection, SIM Lock, Wipe and Security Audit can be obtained for \$14.95 a year from www.eset.com. These features can be tested free for 30 days.

Summary

ESET offers a slick security suite for Android smartphones, which impressed us with its intuitive interface. The functionality of ESET Mobile Security is equally well thought-out.

Aside from the wipe function missing some data (which ESET have promised to rectify), we have one suggestion for improvement: the product would be completed by the inclusion of a web interface.

F-Secure Mobile Security

F-Secure Mobile Security is a security product that provides all the important functions of a mobile suite. As well as anti-theft and antivirus protection, the Premium version of the software also includes parental controls, browser protection and a call/text blocking function.



Installation

We downloaded and installed F-Secure's suite from the Google Play store. When the app is first started, the user is required to accept the licence agreement, which requires an Internet connection. A 30-day trial licence can then be activated. Setting up the theft protection requires that a security password be created; this must be at least 5 characters long and is checked for complexity. We were not allowed to use "qqqqq" as a password, although no information was supplied as to what would be acceptable. We then tried "qqqq1" and this was accepted. After creating the password, the user has to enter a trusted phone number, which will be used to receive messages about SIM-card changes. Finally, F-Secure offers to run an initial scan.

Starting the program

The program's start screen displays the message that the device is protected, along with the number of days of the trial period remaining. Navigating through the app is done by means of swipe gestures or tapping the buttons displayed along the bottom of the screen.

Anti-Virus

This component protects the system against malware. The respective dates of the last update and last scan are shown. A full device scan can be started, or a scheduled scan configured; the frequency can be set to daily, weekly or monthly. Additionally, the Cloud Protection feature can be either deactivated completely, or set to run only when no roaming costs would be incurred. There is also an option to switch off the real-time protection.

Anti-Theft

The Anti-Theft component is controlled by sending text-message commands to the phone, in combination with the password. There is no web interface. The functions available are as follows:

Lock

Text-message command: "#lock#<Password>"

This command locks the phone's screen using the Android lock screen. This is very robust, and prevents any unauthorised access to the device. Once the command has been sent, the PIN-requirement for the lock screen is permanently switched on.

Locate

Text-message command: "#locate#<Password>"

This function enables a lost or stolen phone to be found. When the command has been sent, the sender receives a message by return with the co-ordinates of the phone, and a link to Google Maps.

Alarm

Text-message command:

"#alarm#<Password>#<Count>"

This command functions in the same way as the Lock command, but additionally sounds an alarm.

The parameter *Count* determines the number of times the alarm will be set off; if this is not stated, the alarm sounds continuously. Setting the parameter to "0" switches the alarm off.

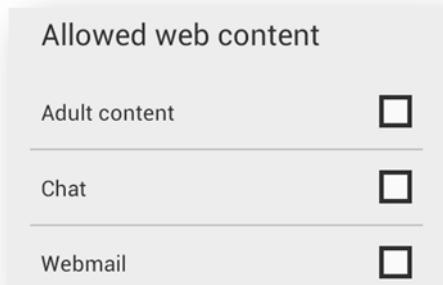
Wipe

Text-message command: "#wipe#<Password>"

The Wipe command serves to delete all personal data stored on the smartphone. First of all, the external SD card is wiped, then the device is reset to factory settings. In our test, all data was successfully deleted except for Contacts on the SIM card; the deletion process was completed in just a few moments. We were unable to restore any of the deleted data using our free tool.

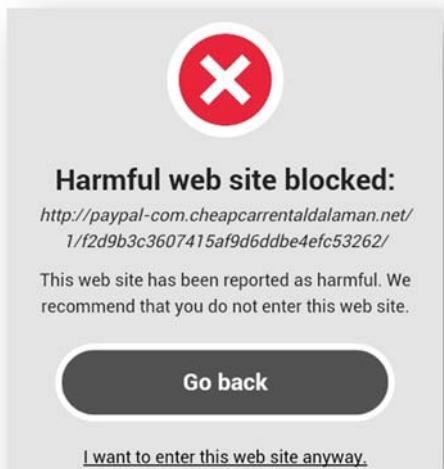
Parental Control

This feature makes inappropriate Internet content/installed apps inaccessible to children. The user can choose between the profiles *Child*, *Teen* and *Adult*, each of which has a different preconfigured filter. Each level can be individually adapted. Examples of content areas that can be blocked are weapons, gambling and illegal downloads.



Safe Browser

F-Secure's Safe Browser feature provides a separate browser app that protects against phishing sites. It is possible to block other browsers and allow only the Safe Browser to be used. If a page is blocked, a warning message is shown with the options of going back or continuing:



If Parental Control is enabled, F-Secure's Safe Browser is always used to view websites.

Whilst we approve of Safe Browser in principle, we feel that global phishing protection, where the user has the choice of which browser to use, would be more practical.

Safe Contacts

This feature enables the blocking of calls and text messages from particular numbers, which can be entered manually or imported from the Contacts list. A simple blacklist is used. If a number is added to the list, all incoming and outgoing calls and all incoming text messages are blocked. It is not possible to block just calls or just texts.

Help

F-Secure provides an online FAQ. Additionally, each component has its own short but informative help text.

Deinstallation

Deinstallation is password protected. Under the menu More | About is a deinstallation wizard. Once the password has been entered, the program is removed immediately. The software can also be uninstalled from the Android App Manager; it first has to be removed from the list of device administrators, which also requires the password to be entered.

Licence

F-Secure allows the user to test all features of the program free for 30 days. Using it after the trial period requires a licence to be purchased; this costs €7.45 and is valid for 6 months.

Summary

F-Secure performed well in our test. The Parental Control feature and simple navigation made a good impression. The Safe Browser is also good, even if support for other browsers would be an improvement.

IKARUS mobile.security

IKARUS mobile.security is a neatly designed security app for Android smartphones. It includes important security functions such as a virus scanner, theft protection and URL filter.

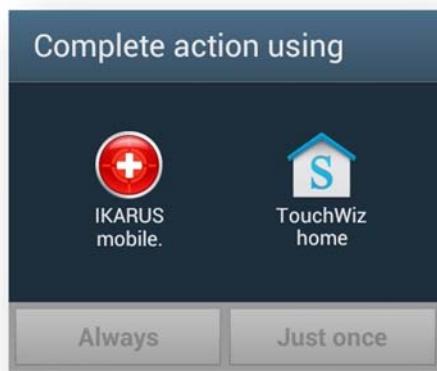


Installation

We downloaded and installed IKARUS mobile.security from the Google Play store. The installation process is relatively long, as it includes configuration of the various components.

The first step is to accept the licence agreement. IKARUS then runs an update, and licensing follows. The user can activate the product using a previously purchased key (which can be scanned as a QR code), by making an in-app purchase using Google Play, or opting for the 30-day test version. Alternatively, the free version can be selected, which has restricted functionality.

The protection features then need to be configured. The USSD protection comes first.



For this, IKARUS has to be defined as the standard app for telephone calls. Next comes the configuration of the anti-theft component, which the user can switch on or off. If the feature is to be used, the app has to be made a device administrator and lock screen administrator. The user has to define a password, which must contain at least six characters, with at least one letter and at least one number. After this, the user is taken through a brief introduction to the text-message commands for the theft-protection component. The blacklisting function and URL filter, which protects the user when surfing the Internet, are configured during the setup process.

When installation is complete, IKARUS recommends running an initial malware scan.

Starting the program

When the program is run, the home screen is shown. The current protection status is displayed at the top of the screen, the text reading "Your system is protected" if all is well. The time of the last malware scan is also displayed.

AntiVirus

IKARUS' AntiVirus component allows the user to scan all installed apps, or the complete system. A scheduled scan can be configured, with frequency options being twice daily, daily, every second day or every week. Details of any infections already discovered can be displayed.

As with the scans, updates can be carried out automatically, with the same configuration options. It is also possible to restrict updates to times when the device is connected to the Internet by WiFi (in order to save data charges), or allow them with any Internet connection.

At the bottom of the screen is a checkbox, activated by default, which allows anonymous malware recognition data to be sent to IKARUS' labs.

Monitoring

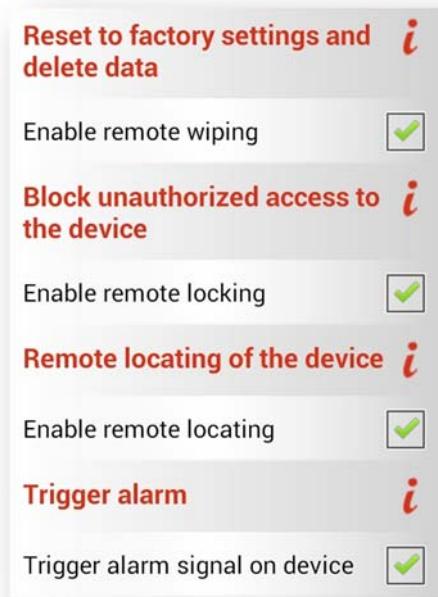
Monitoring is IKARUS' term for real-time protection, which covers new apps, changes to files and USSD code protection. Each of these sub-functions can be switched on and off independently.

URL Filter

The URL filter protects the user against dangerous websites when surfing the Internet. IKARUS do not state which browsers are supported; in our test, the protection worked with both the standard Android browser and Google Chrome.

The phishing test page provided at amtso.org was not recognised.

Theft Protection



IKARUS lists all the available theft-protection functions and allows each to be deactivated. The features are controlled by text message, a web interface is not available.

If a component is to be disabled, the password has to be entered. Whilst this is in principle a good thing, we feel it would be more practical to protect the entire dialog box with the password, rather than demanding it for every checkbox that is unticked.

Wipe

Text-message command: „*wipe: <Password>*“
This command deletes all personal data from the device, in order to prevent it being accessed by third parties if the phone is lost or stolen. This is done by resetting the phone to factory settings. Unfortunately, the process did not delete the data on the external SD card, which IKARUS should definitely rectify.

Lock

Text-message command: „*lock: <Password>*“
As soon as the command is received, the device is locked with a lock screen, and the sender receives a confirmation text in reply. The lock screen is secure and cannot be bypassed, but emergency calls can still be

made, which is optimal. A text message is also sent when the phone is unlocked.

Locate

Text-message command: “*locate: <Password>*”

When the phone has been successfully located, the sender receives a text message in reply, with a link to the appropriate coordinates on Google Maps.

Alarm

Text-message command: “*alarm: <Password>*”

This command works just like Lock, but plays a loud siren-like sound too. This works even if the phone ring settings have been set to vibrate.

SIM Card Protection

If the mobile phone is stolen and a different SIM card inserted, the device will be locked and the thief will be unable to access the data. The phone can be unlocked by entering the correct password.

Message Blacklisting

Message Blacklisting prevents the receipt of messages from unwanted senders. The user interface is very simple, and allows merely the addition or deletion of numbers. Numbers can be entered directly, or imported from the address book or the “Recent Messages” list.

We liked the automatic answer feature, which sends a customisable message to the sender when a message is blocked.

Info

This provides version information for the product. There are also email addresses and telephone numbers with which the user can contact IKARUS, and a feature which can send the system log to support staff.

Restart Setup

This feature requires the password to be re-entered. The settings made in the initial setup are reset, and the user is taken through

the same configuration steps as during the installation.

Help & Support

IKARUS assists the user when configuring the device with short but informative information boxes. Although the IKARUS website contains manuals for many other products, we could not find one for mobile.security. There is an FAQ with about 20 questions, although these are rather superficial.

Deinstallation

IKARUS mobile.security provides a deinstallation wizard to remove the product. The password has to be entered to use this. A succinct dialog box is displayed, and then the program is removed without further ado.

The program can be removed without having to enter the password, if the Android App Manager is used. We see this as a serious security risk, as a thief could easily use this to completely deactivate the theft protection.

Licence

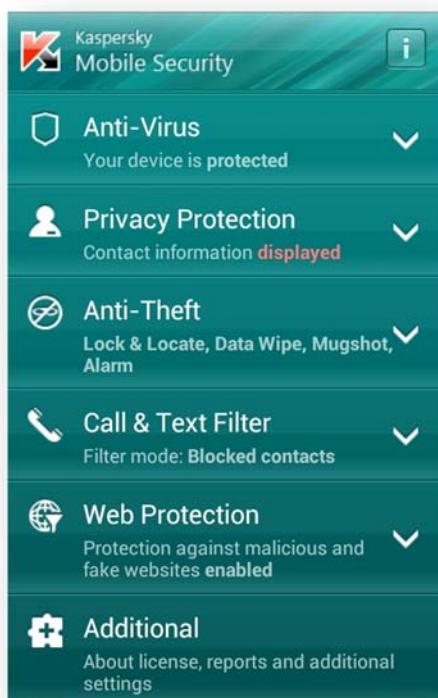
IKARUS allows users to test mobile.security free for 30 days. To continue using the program after this time, the user can buy a perpetual use licence for €19.95 from the Google Play store, or a 1-year licence for .00 from the IKARUS website.

Summary

IKARUS mobile.security has all the important features of a mobile security suite. USSD protection and a URL filter are included. The user interface is very clean and easy to use. However, the Wipe function and deinstallation protection need to be improved.

Kaspersky Mobile Security

Kaspersky Mobile Security is a very comprehensive security app. In addition to a virus scanner, real-time antivirus protection, anti-theft and call/text filter, it includes phishing and privacy protection.



Installation

Kaspersky provided us with the APK file and a licence for the full version. Running the installer launches a configuration wizard. First of all, the user has to enter their country of residence and accept the licence agreement. The app is then made a system administrator, in order to enable the anti-theft component. After this, a Kaspersky account has to be created; this requires just an email address and a password, which must be at least 8 characters long and contain uppercase and lowercase letters and numbers. Finally, the wizard recommends running a scan. The user is then taken to the app's start screen, which provides access to the individual components.

Starting the program

When the program is started, a well-designed home screen is shown, which displays all the components in drop-down menus. A red

warning message catches the eye, which informs us that none of our contacts has been hidden. We find the alert inappropriate, as many users will have no need to hide any of their contacts, and this does not represent a direct security risk. However, the alert can be hidden in the upcoming version of the program, according to Kaspersky.

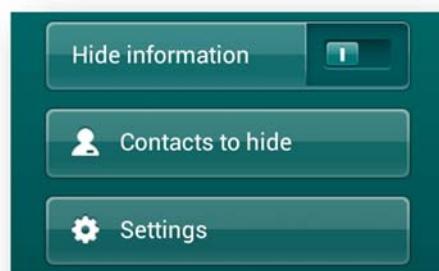
Anti-Virus

The Anti-Virus component can scan the device for malicious software. The user can start a scan manually, or set the time and frequency of automatic scans. Additionally, Kaspersky monitors the installation of new apps and, if desired, file operations.



Manual scans can be set to scan the entire device, just apps, or just a selected folder. The user can decide whether to scan apps on installation using the *Kaspersky Security Network* (cloud-based malware detection).

Privacy Protection



Privacy Protection enables communication with selected contacts to be hidden. These can be entered manually or imported from the address book. Items that can be hidden are the contact details, text-message log, received text messages, and call logs.

Anti-Theft

The Anti-Theft component prevents unauthorised access to the mobile phone if it is lost or stolen, and assists in finding it again. The feature can be controlled using the web interface or text messages (Kaspersky say this is in case the user's device does not have an Internet connection). We note that commands sent via the web interface are not carried out immediately, but only via synchronisation, which takes place every 30 minutes:



We feel this is an unacceptable delay in carrying out the theft-protection commands. Kaspersky inform us that they hope to rectify this very soon.

Sub-components of the feature are as described below.

Lock & Locate

Text-message command: "find: <Password>"
This command locks the device, and then determines its position. The user first receives confirmation that the device has been successfully locked, and then an SMS with the current position, in the form of longitude and latitude co-ordinates. In our opinion, this form of location information is not very useful, as these values have to be entered manually in an online map. A link directly to the position on such a map would be better.

We were pleased to see that the message displayed on the lock screen can be edited. The lock screen itself was very secure and could not be bypassed. It was always possible to make an emergency call.

Alarm

Text-message command: „alarm: <Password>“

This command locks the phone and sounds an alarm. As the screen is simultaneously locked, the alarm cannot be deactivated, which might prove very off-putting to a thief.

Mugshot

This command can only be initiated from the web interface. The function locks a stolen device and takes photos of the potential thief using the front camera; these can be viewed in the web interface.

Hide

Text-message command: „hide: <Password>“

Sending this command activates the Privacy Protection component and thus hides all contacts in the address book.

Wipe

Text-message command: wipe: <Password>

This deletes all personal data from the mobile phone, but without resetting the device to factory defaults. This has the advantage that the theft-protection software remains installed and active. In our test, the browser history, bookmarks and text-message log were not deleted. The data on the external SD card was deleted, but could be restored with a free data recovery program. Kaspersky have promised improvement in the next version.

Full Reset

Text-message command: fullreset: <Password>

This command deletes data on the external SD card, and then resets the device to factory settings. Although this completed successfully, it was still possible to recover the data from the external SD card.

Call & Text Filter

This component allows blacklists and whitelists to be created, although only one of these can be active at a time. It is possible to except individual contacts in the address book from any blocking features. There is also a

feature for blocking text-message senders whose telephone numbers include non-numerical characters. We found the Call & Text Filter to be logically designed.

Web Protection

This feature only works with the default Android browser, not with any alternatives. There is a text anti-phishing component, which blocks text messages with links to phishing sites. In our test, this particular feature did not work, in that text messages with phishing links were not blocked. However, as soon as the links were clicked, they were recognised and blocked by Kaspersky Web Protection.



such, but Kaspersky also offer Kaspersky Mobile Security Lite, which is available for free from the Google Play store; its components "function with some restrictions", according to the Kaspersky website. It can be upgraded to the full version at any time. However, changes to the license model are expected soon.

Summary

Kaspersky's Mobile Security provides many sensible and well thought-out functions. The manufacturer has also considered the ergonomics of the program and created an intuitive user interface.

The product is not without its problems, however. It was possible to restore data from the external SD card after it had been wiped, and there is a delay of up to 30 minutes after sending theft-protection commands from the web interface.

Help

Kaspersky provides its users with a comprehensive local help service. Tapping the info-symbol within any dialog of the app takes the user to the relevant help page. After installation, tips are shown in every menu, which we found to be very useful.

Deinstallation

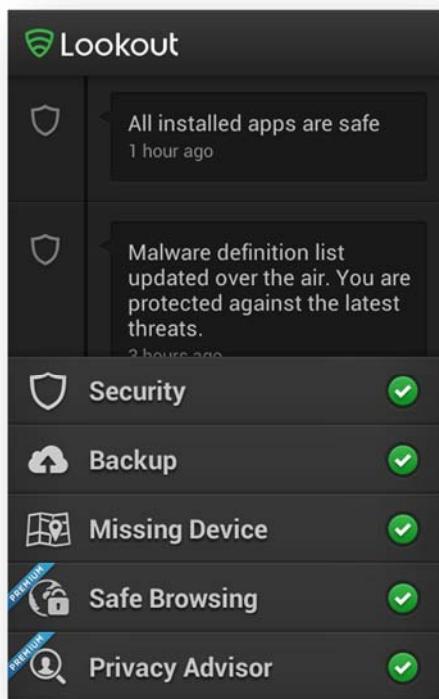
The app can be uninstalled using a wizard. This requires the password to be entered. If an attempt is made to uninstall the app manually, the screen is locked when the user tries to remove the administrator rights; this makes it impossible for a thief to disable the theft protection.

Licence

Kaspersky Mobile Security requires a commercial licence, which costs €10.95 and is valid for a year. There is no test version as

Lookout PREMIUM

Lookout PREMIUM provides the user with modern security features such as antivirus, anti-spam, surfing and theft-protection. A backup function completes the suite.



Installation

We downloaded and installed Lookout PREMIUM from the Google Play store. After installation, the user can test the PREMIUM features free for two weeks. After this, a licence can be purchased, or the program will automatically downgrade to the free version.

There is a brief guide to the scope of the program, after which the user has to create a Lookout account (or log in with an existing one). The product is then configured. The user can decide whether to activate the Privacy Advisor, Backup and Safe Browsing features, whereby the program recommends activating all of them. After this step, setup is complete.

Starting the program

When the program is started, the clearly designed home screen is shown. The upper half of this shows activity logs, the lower half

provides access to the program's functions. A malware scan is started immediately; for all other functions, a green tick (checkmark) is shown, indicating that all is well.

Security

The Security component of Lookout protects the user against malware. Under this menu there is a button to start a scan with, and a log of previous activity. A message in the top part of the screen indicates that real-time protection is active.

Automatic scans can be configured in the settings. Possible intervals are daily or weekly, and a preferred time can be set. The on-demand scan only covers installed apps, not all files. Lookout tell us that their real-time protection monitors all changes to files on the device, and so scanning is limited to installed apps, in order to save battery life.

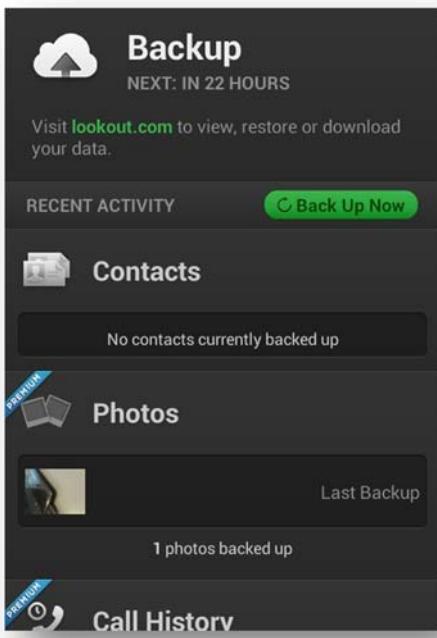
Backup

The Backup function saves contacts, pictures and call logs to a Lookout server, whereby pictures and call logs are only saved by the Premium version. After the first backup, the data can be viewed and downloaded in the web interface.⁸

The backup can be run automatically on a daily or weekly basis. Although we see the feature as being essentially good and sensible, we do see a problem with it: it is not possible to choose which type of Internet connection to use for the backup (e.g. WiFi). Somebody who takes a lot of photos will create a lot of data traffic, which could be very expensive, especially if the user is travelling abroad.

We liked the fact that the Backup can be run from the web interface. If the user's phone is lost or stolen, they can at least save their data.

⁸ <http://lookout.com>



It should be noted that only contacts saved on the phone itself are backed up. Contacts in the Google account or saved on the SIM card are not backed up. Lookout does not make the user aware of this.

Missing Device

Missing Device is the theft-protection component of Lookout. It is controlled by web interface; there are no text-message commands. The menu of the same name displays a map with the current position of the device. The user can thus easily test the location function.



Underneath this, there is a button entitled "Enable Better Protection". Tapping this allows the user to make Lookout a device administrator. The change can be undone in the settings menu.

The theft protection functions are listed and briefly described at the bottom of the screen.

Scream

This function can be tested directly from the menu, though of course it would normally be run from the web interface. It causes a loud siren to be played on the phone, and the display to flash red and blue. The phone is not locked, as it is not a security feature, but is intended to help find a mislaid phone.

Locate

This component serves to find the phone if it has been lost or stolen. The user merely has to log on to the web interface, the position will be found very quickly and displayed on Google Maps.

Signal Flare

Signal Flare is a clever feature that locates the phone before the battery has run down. The position can be found in the web interface.

Lockcam

Lockcam is used when the device is locked. If the wrong password is used three times, Lookout takes a photo of the thief with the front camera, and sends it by mail to the owner.

Lock

This function allows the user to lock their lost or stolen phone remotely and so prevent unauthorised access. This is only available in the Premium version. To lock the device, the user logs on to the web interface and clicks "Lock"; the PIN to unlock the phone can be defined here. It is possible to display a message, and even contact details, for potential honest finders.

The lock screen cannot be bypassed, but an emergency call can be made.

Wipe

This function is also reserved for users of the Premium suite. If the Wipe command is sent, the device will be reset to factory settings.

Lookout (like all Android apps) can only wipe the external SD card if the program has device administrator rights. We note that the program does not prompt the user to assign administrator rights either during installation or when the program is started.

In our test, Lookout deleted all the data on the SD card, although we were able to recover this using a common free tool.

Safe Browsing

The Premium feature Safe Browsing protects the user when surfing the Internet with the default Android browser and Google Chrome. It can be deactivated in the settings. It is also possible to see statistics regarding the number of scanned sites.

Privacy Advisor

Privacy Advisor, also a Premium feature, finds apps that might represent a threat to the user's privacy. All installed apps are listed according to their access rights. Categories include location services, access to contacts or messages. Tapping a group shows all the apps with the relevant permission. Tapping one of the apps shows all other permissions and detailed information.

Help

Lookout provides a comprehensive FAQ service online; an active Internet connection is of course necessary to use this.

Deinstallation

There is no deinstallation wizard provided. If the app has been made a device administrator, Lookout advises that this has to be deactivated before removing the product. No password is needed to uninstall the app, enabling a thief to bypass the protection easily.

Licence

Lookout offers a free version with reduced functionality. The Premium version can be purchased for €2.26 a month or €22.66 a year, and includes the features Safe Browsing,

Privacy Advisor, Wipe, Lock, restoring data onto a new device, plus backup of call logs and photos.

Summary

Lookout offers a well thought-out security product, which stands out due to features like the Lockcam and comprehensive backup function. The other protection features also impressed in our test. There is some room for improvement, however, such as offering users on-demand scans of the entire SD card or adding deinstallation protection.

Quick Heal Total Security

Quick Heal Total Security is a suite with an extensive range of features. As well as the classic functions such as theft protection, the software also offers components such as a network monitor and backup feature, which impressed us in our test.



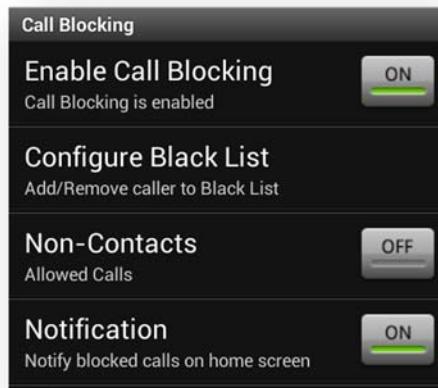
Installation

We downloaded the installation file from the manufacturer's website. After accepting the licence agreement, the user has to activate the product. This can be done by entering an existing key, or purchasing a new one; alternatively, the software can be tested free for a limited time.

The theft-protection components are then configured. A password of between 6 and 20 characters has to be entered. The answers to two questions have to be registered, in case the password needs to be reset; users should of course select questions to which only they know the answer. A trusted contact is then entered, to be informed in the event of a SIM card swap. We were pleased to see that deinstallation protection can be activated.

Call Block

This prevents the user being disturbed by unwanted calls. The feature is based on a blacklist. Any numbers entered in the list will be blocked. The user can also choose to block all numbers not in the address book.



The user can choose whether or not to be notified in the event that a call is blocked. Overall, we found that the feature was very simple and easy to configure, and it worked perfectly in our test.

SMS Block

The SMS Block stops unwanted text messages, in a similar way to the call blocker. However, it has more comprehensive configuration options. We were actually confused by the first option; an "SMS Scan" can be activated, but there is no further information as to what this means. We can only imagine that it scans SMS messages for malicious links. However, we were unable to provoke such a reaction in our test.

Quick Heal offers a second protection mechanism, in the form of a text-spam blocker. This allows texts from the groups contacts, non-contacts and senders with non-numerical addresses to be blocked. Additionally, blacklists and whitelists can be created, and individual senders added. There is also a list of blacklisted keywords – messages containing any of them will be blocked. Overall, we felt that the feature does

its job, but lacks the very simple configuration method of the Call Blocker.

Anti-Theft

To configure this feature, the password entered during installation has to be entered. The user then has access to a wide range of configuration options. The theft protection functions, listed below, are all controlled by text-message command; there is no web interface.

Locate

Text-message command: “**TRACE <Password>**”

When the command has been received, a reply is sent to the sender with link to a page on Quick Heal’s website, which has a Google Maps map embedded in it. This shows the location of the device.

Block

Text-message command: “**BLOCK <Password>**”

On receipt of the command, the phone is locked using a nicely designed lock screen. This displays a message, which can be freely edited in advance by the user. The lock screen is very secure and cannot be bypassed, but allows emergency calls to be made, and also enables the trusted number (entered during setup) to be called.

SIM Lock

This locks the device in the event that the SIM card is changed. It can be switched on or off. The user can decide whether to send a message to the trusted number in the event of a card change. We were pleased to see that multiple SIM cards can be registered as trusted, so that users with more than one SIM can change them over without further ado.

Wipe

Text-message command: “**WIPE <Password>**”

This function deletes personal data from the smartphone, in order to prevent unauthorised access. The device is not reset to factory settings, which has the advantage that the

theft-protection software remains installed and active. Quick Heal did not delete the browser history or bookmarks in our test. We were also able to restore the data on the external SD card using a free tool. The manufacturers tell us that the newest version of the product includes a secure deletion method, which prevents any data being recovered.

Virus Protection

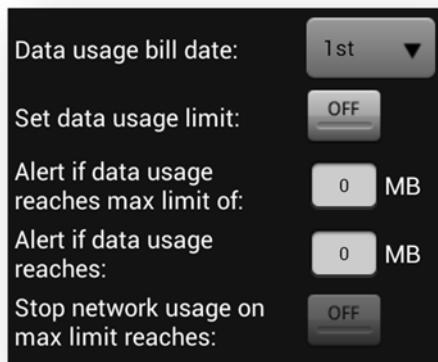
The Virus Protection feature allows the device to be checked for malware. It is possible to configure a standard action to be taken when malware is detected; the options are repair, delete or skip. This also applies to the real-time protection. In the event of a false positive, the user can define individual apps or files as safe.

Performance Monitor

The Performance Monitor shows the current use of resources, such as remaining battery life, CPU usage and memory usage. A list of installed apps and their memory usage can also be shown. Rather annoyingly, this list can only be ordered alphabetically; to find a resource-hungry app, the user must scroll through the whole list.

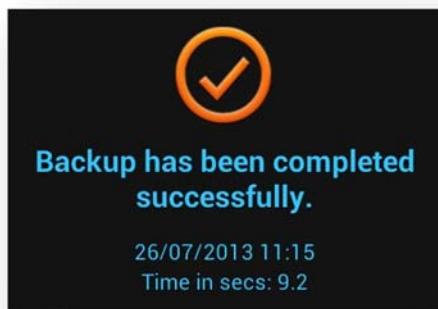
Network Monitor

The Network Monitor measures data traffic for 2G, 3G and WiFi connections. The user can set monthly limits and, optionally, cut the Internet connection if these are exceeded. Another limit can be set, reaching which notifies the user. A separate view displays all the apps that have created Internet traffic, along with the relevant data usage.



Backup

The backup component creates backup copies of contacts, calendar entries and text messages. These are saved on a Quick Heal server. If the user loses any data from the phone, it can be restored simply by tapping the Restore button. It is also possible to set an automatic backup, which runs at definable intervals (between daily and monthly).



Backed-up data can be restored to a different device. In the event that a device is lost, all the data can be transferred to a new one.

Web Security

The Web Security component protects the user against phishing sites and sites pushing malware. Quick Heal also provides parental controls, which allow parents to block certain categories of website. We note that this only works with the standard Android browser, not with Google Chrome. Trusted sites can be added to a whitelist, meaning they will never be blocked. Changing the settings of the parental control feature did not by default

require a password to be entered (although password protection can be enabled).

Help

A help file is provided to assist users with questions. This is clearly laid out and easy to understand. There is also an FAQ, although this is rather limited, having only about 20 questions.

Deinstallation

Via the context menu > Help > Deactivation it is possible to deactivate the licence, after which the product is automatically uninstalled. The password has to be entered to allow this, also if the Android App Manager is used. There is thus no opportunity for a thief to bypass the theft protection by uninstalling the app.

Licence

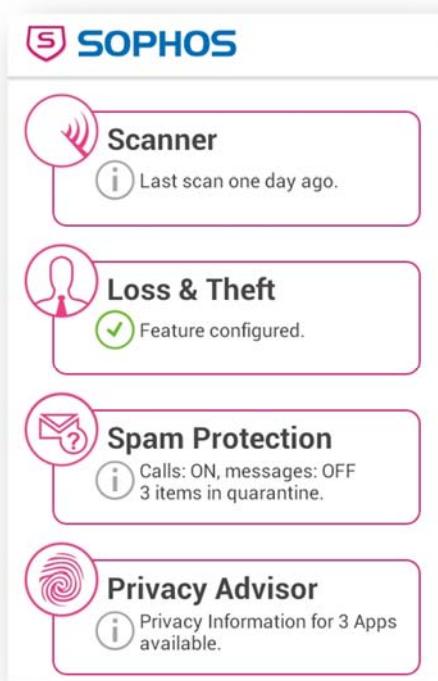
Quick Heal Total Security can be purchased from the Google Play store for €10.76, the licence being valid for a year. It is possible to test most features of the product free for 30 days.

Summary

Quick Heal Total Security gives the impression of being a very mature product with all the functionality a user could wish for. We did find the interface rather unintuitive in places, however, which is perhaps something Quick Heal could improve.

Sophos Security and Antivirus

Sophos Security and Antivirus is a security suite with all the important components of a modern security product, and is available free.



Installation

We downloaded and installed Sophos Security and Antivirus from the Google Play store. After the installation, the user merely has to accept the licence agreement, after which the start page of the app is displayed. An initial malware scan is run.

Scanner

The scanner searches the mobile phone for malicious software. In the settings, the user can decide whether to use cloud features when scanning; these can be deactivated when roaming, or set only to be used when there is a WiFi connection. When malware is found, the user has the choice of ignoring it, deleting it, or displaying more information about it. It is also possible to activate or deactivate the recognition of potentially unwanted apps. Additionally, scheduled scans can be set, with the interval being between six hours and three days. Sophos also provides

real-time protection, which checks newly installed apps and changes to files.

Web Protection

Somewhat hidden in the settings is the Web Protection function. This protects the user against malicious websites when surfing the net. The warning levels are Standard, Maximum and Never. The feature worked very well in our test.

Loss & Theft

In the event that the mobile phone is lost, this feature can play an alarm, lock the device, locate it, or delete the data from it. The functions are controlled by text message only, there is no web interface. The text messages can only be sent by trusted phone numbers, which are defined in advance. The sender has to include the password in the message. Commands sent from other phones are ignored, even if the correct password is included.

We liked the theft-protection's overview screen, which shows which components are active, and which still need to be configured.

- | | |
|--------------------------------------|-----------------------|
| ✓ | Feature selection |
| ! | Device administrator |
| ! | Lock screen |
| ✓ | Location services |
| ✓ | Secure wipe |
| ! | Phone numbers |
| ! | Text message password |

Lock

Text-message command: Lock <Password>

This command locks the mobile phone using the current Android settings. An icon with a lock message is also displayed. The lock screen is very secure and cannot be bypassed. When the lock command has been successfully carried out, a reply is sent to the sender.

Alarm

Text-message command: Alarm <Password>

This command locks the screen, just like the Lock command. Additionally, an alarm sound is played, which could be very off-putting for a thief.

Locate

Text-message command: Locate <Password>

When the command has been received, the device will attempt to locate its position using GPS and WiFi. When this has been achieved, the sender will receive a reply with the approximate co-ordinates and a link to the location on Google Maps; this is followed later by another message with more precise co-ordinates.

Locate at Low Battery

If this function is activated, the phone will be located whenever the battery runs low; the details will be sent to the trusted phone numbers.

Unlock

Text-message command: Unlock <Password>

This command defines a new, randomly chosen password for the device. The sender receives a text message containing the new password.

Wipe

Text-message command: Wipe <Password>

Sophos has gone to a lot of trouble with the wipe command. The user can define the type of wipe to be used for individual file types. In addition to simple deletion, files can be overwritten with junk (secure wipe). This means that the process will take longer. In our test, the secure wipe functioned as

expected; the files on the SD card could not be restored using our usual means.

	Fast	Secure
Audio files	<input type="radio"/>	<input checked="" type="radio"/>
Secure wipe		
Pictures	<input type="radio"/>	<input checked="" type="radio"/>
Secure wipe		
Movies	<input type="radio"/>	<input checked="" type="radio"/>
Secure wipe		
Downloads	<input type="radio"/>	<input checked="" type="radio"/>
Secure wipe		
Other files	<input type="radio"/>	<input checked="" type="radio"/>
Secure wipe		

SIM Change

If the SIM card is swapped, a message with the IMEI and IMSI will be sent to all the trusted phone numbers. The device will also be locked using the Android lock screen.

Spam Protection

Spam Protection prevents the user being bothered by unwanted calls or texts. It is possible to switch either sub-component on or off completely, i.e. to use just call blocking or just text blocking. However, it is not possible to separate them for a particular contact; i.e. either both calls and texts are blocked, or neither. An intuitive menu allows numbers to be added to the blacklist and whitelist. If a number should accidentally be added to both lists, the whitelist has priority.

There are also options for blocking anonymous calls and texts, and any number not in the address book.

If the text-blocking function is active, Sophos can protect against malicious URLs in text messages. This worked well in our test, although we noticed that texts with malicious URLs were also blocked when the text-blocking function was deactivated, although Sophos inform us that this has been rectified in the latest version.

The blocked text messages can be found in Quarantine, where they can be viewed, restored, or deleted.

Privacy Advisor

The Privacy Advisor lists apps that may present a risk to the user's privacy. Sophos categorises the apps according to threat level (high, medium and low), and marks them red, yellow or white in the list. The user can filter them according to the following categories: apps that incur costs, have access to personal information, or can access the Internet.

Security Advisor

The Security Advisor makes the user aware of any settings on the mobile phone that may represent a risk to security. Sophos checks six different settings, such as whether a screen lock or device encryption is active. Clicking on one of the entries displays information, and a button that leads directly to the relevant Android settings page.



App Protection

This component makes it possible to password-protect apps with a four-character password. When this has been set, a warning appears that the App Protection can be bypassed by using the Task Manager. However, Sophos provide a solution in the form of another app, Sophos Security and

Antivirus Guard, which ensures that the security suite cannot be terminated.

The configurable parameter *Grace Period* defines how long the app can be used before being locked again. Two minutes is the default.

As self-protection, Sophos protects itself and the Android settings with a password; this cannot be deactivated. Additional apps can be protected with the same password.

Help

Sophos provides the user with comprehensive help in the form of info-boxes for every component. We find this entirely adequate, but would like to see more assistance for the deinstallation process.

Deinstallation

There is no uninstall wizard. Security Advisor has a message stating that the program must be removed from the device administrators before it can be uninstalled. Once this has been done, the app can be uninstalled using the Android App Manager.

Neither the removal of device administrator privileges nor the subsequent removal of the program required the password to be entered. A thief could thus easily deactivate the theft protection. We understand that if the App Protection feature is activated, AND the separate *Sophos Security and Antivirus Guard* app has been installed, that deinstallation without password entry is then prevented. We feel this is a complicated procedure for protecting against unauthorised deinstallation.

Licence

Sophos Security and Antivirus is free and without restriction for private use.

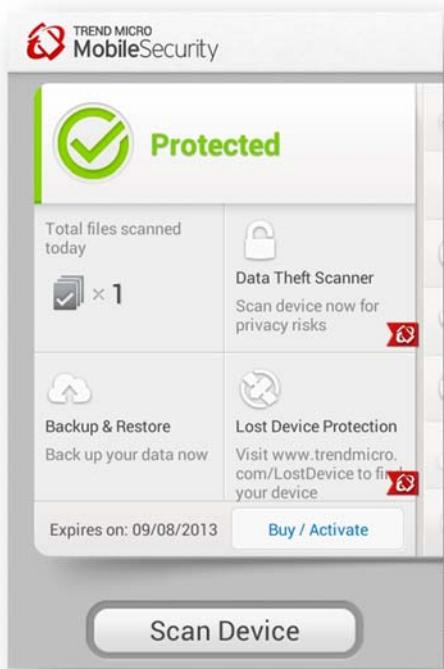
Summary

Sophos Security & Antivirus offers all the functions of a modern security suite and is free. The app gives the impression of being

mature and well balanced. We note there has been an obvious extension of the functionality compared to the version in last year's report.

Trend Micro Mobile Security

Mobile Security by Trend Micro provides important protection functions such as theft protection and antivirus, along with safe surfing and parental control.



Installation

We downloaded and installed Trend Micro Mobile Security from the Google Play store. The start screen is shown as soon as the licence agreement has been accepted.

Starting the program

The user is shown a short introduction to the program and its interface, e.g. swiping to the right to open the controls for extended functions. A message box indicates that the user should create a Trend Micro account, or log on with an existing one.

On the start screen are buttons for the Malware Scanner, Data Theft Scanner, Backup and Anti-Theft. The static "Scan Device" button is very striking, as it remains permanently visible in the Home Screen view.

Virus Scanner

Clicking the Virus Scanner button takes the user to the appropriate page. This also has a

button for scanning the device immediately, plus a variety of configuration options, such as whether to use cloud scanning or scan the SD card. Updates can be carried out immediately and/or automated. In the latter case, the interval can be daily, weekly or monthly. It is also possible to set the app to only update when the device is connected to the Internet by WiFi. As an option, a scan can be run after every update. Scanning and update events are listed in a log.

Data Theft Scanner

The Data Theft Scanner checks the apps installed on the device for possible threats relating to the theft of private data. Trend Micro also provides a real-time scan for this component, which checks newly installed apps for such risks.

The Data Theft Scanner is not very aggressive in its operation. Apps such as Facebook, which due to their privileges have great potential to steal personal information, are not listed as a risk.

Safe Surfing and Parental Control

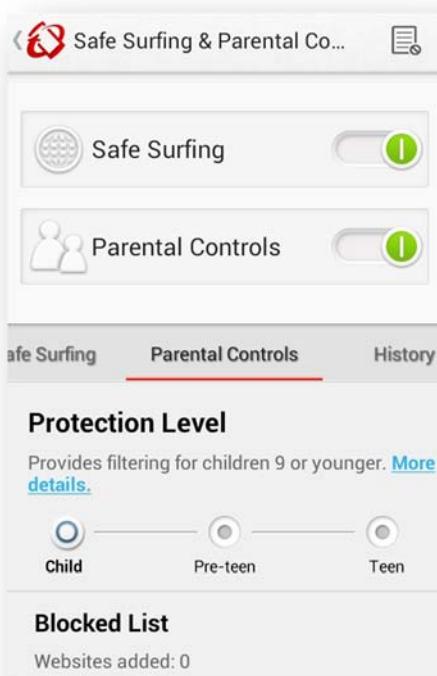
This feature combines two Internet-related protection functions. Safe Surfing protects the user whilst surfing the Internet, whereby the security levels High, Medium or Low can be selected. The High level blocks websites with the slightest possible risk, whilst Low is less strict and ignores minor threats.

For Parental Control, a password of at least 8 characters has to be defined. Suitable protection for internet-surfing children can then be defined. This can be varied according to the age of the child, and specific websites can be blocked or allowed using a blacklist or whitelist respectively.

The Uninstall Protection prevents a child or adolescent from simply uninstalling the app. We feel that this should not be limited to child protection, and that a global

deinstallation protection would make more sense.

The deinstallation protection did not function adequately in our test. Whilst the phone was blocked after the device administrator function had been removed, when the device was rebooted, it was fully accessible for about 60 seconds. The app can easily be uninstalled without entering a password during this time. However, Trend Micro tell us that this will be improved in the next release.



There is a log within the Safe Surfing and Parental Control feature that shows all websites that have been blocked; this includes both websites defined as threats, and websites unsuitable for children.

Call & Text Blocking

Trend Micro provides the ability to block unwanted calls and text messages. Calls and texts can be blocked and configured separately. For each communication type, the use of a blacklist or a whitelist can be set, along with the action to be taken when an item is blocked. For example, in the case of

text messages, an automatic reply can be defined.

For text messages, it is possible to create a list of keywords; any messages containing one of these words will be blocked.

The Call & Text Blocking feature also creates logs, which enable the user to see which calls and texts have been stopped.

Lost Device Protection

Lost Device Protection is Trend Micro's theft-protection feature. The protection functions, such as locating, locking and wiping are provided. The feature is controlled by a web interface; there are no text-message commands.

In our test, before we were able to send any command (such as Lock), there was sometimes a significant delay while the system attempted to locate the phone.

It is quite possible for the phone to be in a location where it can connect to a mobile network, but location is slow or impossible. In such cases, it makes no sense to us that e.g. a Lock command can only be sent when the phone's location has been fixed.

Changing any of the settings in Lost Device Protection requires the password to be entered, so that a thief cannot simply deactivate the theft protection.

Locate

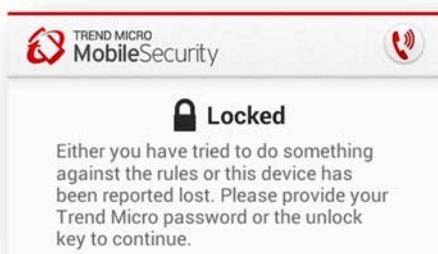
The Locate function shows the position of a lost or stolen phone in Google Maps. The action is carried out automatically when the web interface is opened.

SIM Card Lock

This locks the device when the SIM card is removed or swapped. The SIM Lock feature took a long time to work in our test. Once the device had been restarted, we were able to use it normally for about 60 seconds before the lock was applied.

Lock

This function locks the device, thus making it unusable for third parties. It can only be unlocked by entering the correct password. When the phone is locked, emergency calls can still be made, and a new password (to be sent by email) can be requested.



However, it is also possible to open the Android Notification Bar, change settings and look at messages. Also, pressing and holding the Home button displays the list of recent apps, which could be a privacy threat. However, Trend Micro inform us that these problems will be rectified in the next release.

Siren

This command plays a loud alarm sound; the device is not locked, so it serves only to find the phone if it has been mislaid.

Wipe

Trend Micro offers two variants of Wipe. Partial Remote Wipe removes personal data from the device, while Full Remote Wipe additionally resets the device to factory settings.

In our test, Wipe largely functioned well, although we were able to restore the data on the SD card using popular free data-recovery tools.

Backup & Restore, Scan Facebook

Whilst both of these functions can be found in Trend Micro Mobile Security's menus, they are in fact both independent apps. Clicking either item takes the user to the Google Play store, from where they can be installed.

Help

The user is provided with a comprehensive help function, with a great deal of useful information. Additionally, information boxes can be shown for each component, to help the user with the item's configuration.

Deinstallation

It is possible to remove the app from the list of device administrators, although the device will be locked immediately afterwards. If the phone is restarted, the lock is not reactivated for some time, allowing a thief to uninstall the theft protection/parental control features.

Licence

The basic version of Trend Micro Mobile Security is free. For the Premium version with Safe Surfing, Parental Control, Locate, Lock, Wipe, SIM Lock and deinstallation protection, a licence has to be purchased. This costs €19.95 and is valid for one year. The Premium functions can be tested free for 30 days.

Summary

Trend Micro provides a security solution for Android with a wide range of functions. The Parental Control feature, amongst others, impressed us in our test. The theft protection includes all the functions to be expected of a modern security program, but still has definite room for improvement.

Webroot SecureAnywhere

Webroot's SecureAnywhere is a balanced security product that is available free. For users with more extensive requirements, the Premium version can be purchased; this provides an even more comprehensive set of features.



Installation

We downloaded and installed SecureAnywhere from the Google Play store. After accepting the licence agreement, the user must either create a new Webroot account, or log in to an existing one. The password must have at least six characters. Setup is completed by registering the app as a device administrator.

Starting the Program

When the program was first started, a yellow warning message appeared, indicating that we had not activated the Android lock screen. When we had rectified this, the display turned green, indicating that the device was protected. A virus scan was run automatically.

Anti-Virus

The Anti-Virus component of SecureAnywhere protects the user against malicious software.

The Shields setting allows four different real-time protection functions to be activated: installation, file system, app execution, and diallers:



There is additionally an automatic malware scan, which can be run hourly, daily or weekly. The same intervals can be applied to automatic updates, which can also be run manually. We note that the product does not recognise the EICAR test file as malware.

In our battery usage test, we noticed an increase of 6% when SecureAnywhere is installed, largely attributable to the Execution Shield. We would suggest that the developers should try to improve this.

Secure Web Browsing

Secure Web Browsing protects the user while surfing the Internet. If a website is blocked by the software, users have the option of classifying it as safe if they feel it has been wrongly classified. The site will then be allowed in future. In our test, phishing sites were only blocked when using the standard Android browser; the manufacturers say that the upcoming version 3.4 will also support Chrome.

Lost Device Protection

The theft-protection component can be controlled using text messages or a web interface. The latter is well designed and intuitive to use, and allows multiple devices

to be administered. For each device, protection status and logs of e.g. malware can be seen.

If the user locates a device through this interface, no further commands can be carried out until the location has been successfully completed.



Scream

Text-message command: “*scream <Password>*”

This function causes a shrill alarm to sound, without locking the device. It thus serves to locate a mislaid device at home, rather than being a security feature. Once started, the sound cannot be stopped; the user has to wait two minutes until the feature switches itself off.

Lock

Text-message command: “*lock <Password>*”

This function locks the device, to prevent it being accessed by third parties. The Android lock screen, which is very secure and cannot be bypassed, is used in the background. However, Webroot’s own lock screen is used as an overlay. This displays a message (which can be customised in the web interface) for potential honest finders.

Wipe

Text-message command: “*Wipe <Password>*”

This function is only available in the Premium version. When the command has been received, the device is locked, personal data

is wiped, and the device is then reset to factory settings. In our test, files on the external SD card were not deleted. Webroot say that they are considering introducing an SD-card wipe feature in a future release.

Locate

Text-message command: “*Locate <Password>*”

This function allows a lost or stolen phone to be found. If the command is sent from the web interface, the position of the phone will be shown in a Google Maps map. While the position is being determined, no other commands can be given, which is rather problematic if the location process takes some time. Webroot inform us that they may enable command queuing in a later release.

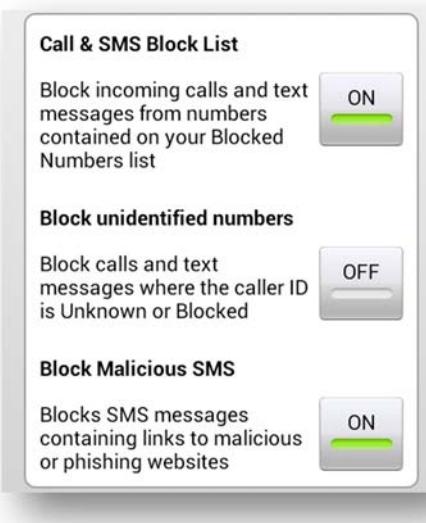
If the command is sent by text message, a message will be received in reply which contains a link to the relevant location in Google Maps.

SIM Lock

This feature is also only available in the Premium version. If the trusted SIM card is removed, the device will be locked. A thief thus cannot use the device with their own SIM card.

Call & SMS Blocking

This component prevents unwanted calls and texts being received, using the blacklisting principle. The user can add known troublemakers to the list, meaning they will be unable to make contact by calling or texting the phone. It is also possible to block anonymous calls, i.e. calls from callers who do not display their own number. Webroot additionally provides protection against text messages with links to malicious sites; this worked perfectly in our tests.



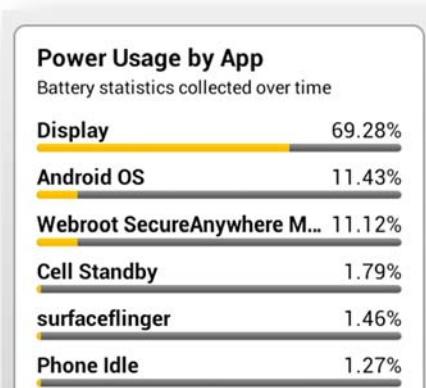
Texts and calls that have been blocked are clearly displayed in a list. This shows not only the date, but also the content of text messages, and the reason the text/call was blocked.

App Inspector

The App Inspector checks installed apps for privacy risks. An example would be apps that can access messaging or location functions. Apps with high battery usage are also listed.

Battery Monitor

The Battery Monitor provides detailed information about the battery. Charge status and temperature are shown, along with battery-hungry apps. This is displayed visually in the form of a bar chart (please note that the relatively high battery consumption by Webroot itself might be due to our testing its features):



Network Monitor

The Network Monitor shows apps that use the network. The protocol used, local and remote IP addresses and ports, and the status are all shown. Tapping an entry carries out a who-is query for the remote IP address, and shows details such as ISP and approximate location.

Help

Webroot provides users with a comprehensive online help feature, which of course requires an active Internet connection. We found the scope and detail of the help service to be adequate. Within the app itself are mini information-texts for each menu entry, which we found very useful.

Deinstallation

Deinstallation can be carried out with a single click using the uninstall wizard provided. In the free version, no password is needed, making it easy for a thief to deactivate the theft protection. However, in the Premium version, a deinstallation mechanism requires the password to be entered before the program can be uninstalled.

Licence

Webroot SecureAnywhere can be used free and without restriction in its reduced-functionality version. A licence for the Premium version, which includes deinstallation protection, SIM lock and various App Inspectors, can be purchased for €15.75 and is valid for a year.

Summary

Webroot's SecureAnywhere performed well in our test. Even the free version provides reliable theft protection and various filters. The deinstallation protection, SIM lock and app inspectors make the Premium version attractive. However, some areas of the theft protection could be improved, and an extension of the phishing protection would be desirable.

Conclusion

For some people, smartphones have already become a replacement for a PC. Others save personal and professional information, which may be of great interest for thieves. Phishing is a potential form of attack that affects users of any device with access to the Internet. Saving credit card details in various shopping apps, especially the Google Play store, can lead to high costs being incurred, either through malware or through unauthorised access. The same applies to the mobile phone contract.

The potential for attacks is great, especially in the case of an open operating system such as Android, which gives the developers of harmless apps a wide range of opportunities. Unfortunately, the programmers of malicious software have exactly the same opportunities, which they abuse.

Mobile security software protects the user against the great majority of such threats, and should not, in our opinion, be regarded as merely optional. Nonetheless, many users do not employ such protection, and are at risk. We find this hard to understand, as there is a wide range of software, including free products, that provide a high level of security. The argument that security products affect the performance or battery life of smartphones has very largely been disproved in our test.

Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives e.V. (August 2013)