G Data Internet Security for Android

Podręcznik użytkownika

ISBN 978-83-61624-21-9

G Data Software Sp. z o.o.
ul. 28 Lutego 2, 78-400 Szczecinek
tel. 094 3729 650
faks 094 3729 659
e-mail: biuro@gdata.pl
Raiffeisen Bank Polska S.A.
78 1750 1396 0000 0000 2014 8837

Spis treści

1 G Data Internet Security for Android

G Data Internet Security for Android skutecznie chroni Twoją tożsamość oraz poufne dane przechowywane w telefonie lub tablecie przed wirusami i programami szpiegującymi. Dodatkowo zabezpiecza urządzenie przed jego zgubieniem (lokalizowanie za pomocą Google Maps™) lub kradzieżą (blokada uruchomienia urządzenia z nową kartą SIM oraz umożliwia zdalne usuwanie prywatnych danych).

Wymagania programu

Urządzenia mobilne z systemem Android 2.1 lub nowszy, 14MB wolnej pamięci

2 Instalacja i konfiguracja wstępna

Instalacja programu możliwa jest po pobraniu pliku instalacyjnego G Data Internet Security for Android ze strony producenta lub sklepu Google Play. Podczas instalacji aplikacja żąda zatwierdzenie listy niezbędnych uprawnień w systemie Android. Po zatwierdzeniu uprawnień rozpocznie się instalacja programu.

Pierwszemu uruchomieniu programu towarzyszy asystent konfiguracji ułatwiający wstępne ustawienia programu. Możesz uaktywnić testowy dostęp do aplikacji na 30 dni, lub też pełną wersję produktu. Do aktywacji pełnej wersji niezbędne są dane dostępu wygenerowane podczas rejestracji lub nabyty klucz rejestracyjny.

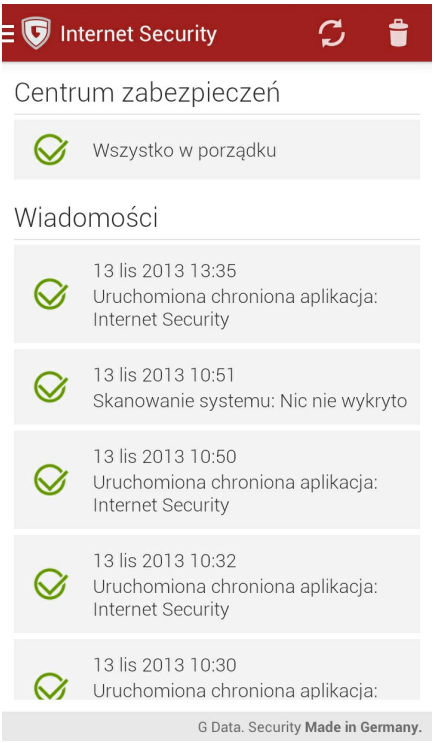
Domyślny widok programu przedstawia **Centrum zabezpieczeń**. Aby zmienić widok wystarczy dotknąć przycisk menu Internet Security.

3 Widoki menu Internet Security

Dotknij przycisk menu Internet Security aby wysunąć pasek umożliwiający przełączanie między widokami. Dotknięcie nazwy wybranego widoku spowoduje pojawienie się odpowiedniej karty ustawień.

3.1 Centrum zabezpieczeń

Sekcja **Centrum zabezpieczeń** przedstawia ogólny stan zabezpieczeń programu Internet Security.



Sekcja **Wiadomości** przedstawia chronologiczną listę zdarzeń i działań programu Internet Security for Android. Dotknij raport aby wyświetlić szczegóły. Przesuń raport w prawo lub w lewo aby usunąć wiersz.

W pasku narzędzi widoczne jest przycisk umożliwiający wymuszenie aktualizacji oraz ikona przedstawiająca kosz służąca do usuwania wszystkich raportów z sekcji wiadomości.

3.2 Skanowanie

Okno skanowania umożliwia wybór trybu skanowania.

- Zainstalowane aplikacje: Ten tryb obejmuje wszystkie zainstalowane aplikacje systemu Android. Jeśli skanowanie wykaże zagrożenie, program umożliwi bezpośrednie odinstalowanie szkodliwej aplikacji.

- System (pełne skanowanie): Skanowanie obejmuje cały system plików urządzenia włączając w to pliki na kartach SD.

Dotknij przycisk ustawień w prawym, górnym rogu okna aby zmodyfikować ustawienia dotyczące automatycznego skanowania:

- Automatyczne skanowanie: Włącza/wyłącza możliwość automatycznego skanowania tylko instalowanych aplikacji.

- Skanowanie zaplanowane: Włącza/wyłącza skanowanie według harmonogramu.

- Oszczędność energii: Powoduje, że skanowanie nie będzie odbywać się jeśli bateria będzie słaba.

- Skanuj podczas ładowania: Powoduje, że urządzenie będzie skanowane tylko podczas ładowania.

- Częstotliwość skanowania: Umożliwia ustalenie interwału harmonogramu (1, 3, 7, 14 lub 30 dni).

- Rodzaj skanowania: Przełącza między skanowaniem tylko zainstalowanych aplikacji, a skanowaniem całego systemu.

3.3 Utrata/kradzież

Konfiguracja tej funkcji umożliwia zarządzanie telefonem w przypadku jego kradzieży lub zagubienia. Możliwe jest zdalne uruchamianie określonych poleceń poprzez wysłanie wiadomości SMS.

Dotknij przycisk ustawień w pasku menu aby ustalić lub zmienić hasło dla zdalnych poleceń SMS, numeru telefonu innego urządzenia do zdalnego modyfikowania hasła poleceń SMS oraz adresu e-mail do powiadomień o

zdarzeniach związanych z działaniem modułu.

Hasło (kod PIN) będzie niezbędne do wysyłki wiadomości SMS umożliwiających zablokowanie urządzenia, usunięcie danych, uruchomienie sygnału dźwiękowego itp. Hasło będzie można zmienić zdalnie, ale tylko z telefonu o numerze skonfigurowanym w ustawieniach. Na adres mailowy są wysyłane informacje o lokalizacji GPS urządzenia, a także powiadomienia o skutku wykonania poleceń SMS. Dotknij przycisk paska menu zatwierdzający zmiany aby zapisać ustawienia. Jeśli program poprosi zatwierdź dodanie aplikacji G Data do listy administratorów urządzenia.

Polecenia SMS

Ustawienia modułu można dowolnie modyfikować. W karcie **Polecenia SMS** możesz ustalić, które polecenia SMS będą funkcjonować:

- Zlokalizuj urządzenie: Po wysłaniu na numer urządzenia SMSa o treści *password* ***locate*** urządzenie wyśle na zdefiniowany adres mailowy lokalizację GPS urządzenia.

- Usuń osobiste dane z urządzenia: Po wysłaniu na numer urządzenia SMSa o treści *password* ***wipe*** urządzenie zostanie przywrócone do stanu fabrycznego wraz z usunięciem prywatnych informacji.

- Odtwórz sygnał dźwiękowy: Po wysłaniu na numer urządzenia SMSa o treści *password* ***ring*** urządzenie włączy sygnał dźwiękowy, który może umożliwić odnalezienie zgubionego urządzenia.

- Wycisz urządzenie: Po wysłaniu na numer urządzenia SMSa o treści *password* ***mute*** spowoduje wyłączenie dźwięku w urządzeniu, dzięki czemu nie będzie na siebie zwracało uwagi.

- Zablokuj ekran: Po wysłaniu na numer urządzenia SMSa o treści *password lock* spowoduje zablokowanie ekranu urządzenia.

- Ustaw hasło blokady ekranu: Aby odzyskać dostęp do urządzenia po odzyskaniu go, może być potrzebna zdalna zmiana hasła blokady (nieużywane hasło można zapomnieć. Po wysłaniu na numer urządzenia SMSa o treści *password* ***set device password***: *devicepassword*

Indentyfikacja AntiTheft

Jeśli złodziej wymieni w urządzeniu kartę SIM, nie będzie można wysłać na nie poleceń SMS. Zabezpiecz się przed tym korzystając z opcji karty **Indentyfikacja AntiTheft**:

- Zablokuj urządzenie po zmianie karty SIM: Po wyjęciu karty SIM telefon zostanie zablokowany do chwili włożenia oryginalnej karty.

- Zlokalizuj urządzenie po zmianie karty SIM: Po wyjęciu karty SIM urządzenie wyśle na ustalony wcześniej adres e-mail lokalizację GPS urządzenia.

Aby zmienić hasło poleceń SMS, wyślij z numeru telefonu ustalonego wcześniej SMS o treści: ***remote password reset:*** *password*.

Jeśli chcesz, aby program powiadamiał Cię o niskim stanie baterii Twojego telefonu, zaznacz opcję

3.4 Ochrona przeglądarek

Moduł ochrony zapewnia ochronę przed stronami wyłudzającymi informacje. Ponieważ moduł zwiększa w niewielkim stopniu ilość pobieranych danych, istnieje możliwość skonfigurowania opcji działania ochrony przeglądarek tylko przy wykorzystywaniu połączeń WLAN w widoku Ustawienia. Opcja nie działa w trybie incognito przeglądarek mobilnych.

3.5 Uprawnienia

Widok uprawnienia wyświetla podsumowanie uprawnień nadanych zainstalowanym aplikacjom. Zwróćmy szczególne uwagę na darmowe aplikacje, które mają dostęp do książki adresowej i wysyłki wiadomości SMS. Bezpośrednio z listy aplikacji dysponującej wybranym uprawnieniem masz możliwość odinstalowania danej aplikacji.

3.6 Ochrona aplikacji

Moduł ochrony aplikacji umożliwia zablokowanie dostępu do dowolnie wybranych aplikacji. Dostęp zostanie przyznany po wpisaniu hasła (kod PIN), adresu e-mail (reset hasła) lub podaniu odpowiedzi na tajne pytanie (wyświetlenie hasła).

Skonfiguruj hasło, adres mailowy do przypomnień oraz tajne pytanie/ odpowiedź i dotknij przycisk **Zmiana danych** w pasku menu.

Pokaże się główny widok **Ochrona aplikacji** przedstawiający na razie pustą listę aplikacji objętych ochroną. Dotknij ikonę + aby dokonać wyboru aplikacji, które chcesz chronić hasłem.

3.7 Filtr przychodzących

Ten moduł umożliwia filtrowanie SMS-ów i połączeń od wybranych kontaktów:

- Biała lista: Akceptowane będą tylko numery z listy
- Czarna lista: Blokowane będą tylko numery z listy
- Kontakty: Akceptowane będą tylko numery z książki kontaktów.

Tryb **Kontakty** można łączyć z trybem białej lub czarnej listy. Program umożliwia akceptowanie połączeń anonimowych bez względu na filtry.

Po włączeniu trybu białej lub czarnej listy możesz dotknąć ikonę kłódki u góry aby edytować listę. W celu dodania numeru do listy dotknij ikonę z plusem. Możesz wyszukiwać numery w książce kontaktów lub na liście historii połączeń.

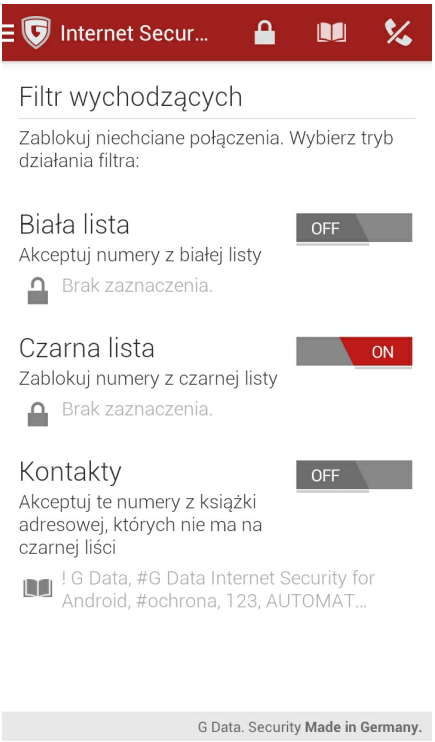
3.8 Filtr wychodzących

Ten moduł umożliwia filtrowanie SMS-ów i połączeń do wybranych kontaktów:

- **Biała lista:** Akceptowane będą tylko numery z listy
- **Czarna lista:** Blokowane będą tylko numery z listy
- **Kontakty:** Akceptowane będą tylko numery z książki kontaktów.

Wskazówka: Dozwolone jest stosowanie znaku zastępczego *, zastępującego dowolny ciąg cyfr. Składnią 0800* można w ten sposób zablokować wszystkie połączenia wychodzące do numerów **0800** itd.

Tryb **Kontakty** można łączyć z trybem białej lub czarnej listy.



Po włączeniu trybu białej lub czarnej listy możesz dotknąć ikonę kłódki u góry aby edytować listę. W celu dodania numeru do listy dotknij ikonę z plusem. Możesz wyszukiwać numery w książce kontaktów lub na liście historii połączeń.

3.9 Ukrywanie kontaktów

Ta funkcja umożliwia ukrywanie wybranych kontaktów wraz z historią połączeń i przesłanych wiadomości. W tym celu kontakty są przenoszone do zablokowanego konta G Data.

Dostęp do ukrytych kontaktów jest możliwy tylko poprzez program Internet Security for Android, po dotknięciu nazwy funkcji **Ukrywanie kontaktów**. W celu dodania kontaktu do listy dotknij ikonę z plusem. Możesz

wyszukiwać numery w książce kontaktów lub na liście historii połączeń. Aby edytować ustawienia kontaktu, dotknij jego nazwę. Możesz zablokować tylko widoczność komunikacji z kontaktem (połączenia i SMSy), a dodatkowo również widoczność kontaktu w książce adresowej. Jeśli usuniesz kontakt z listy, zostanie z powrotem przeniesiony do oficjalnej książki adresów.

3.10 Ustawienia

Ten widok pozwala na modyfikowanie globalnych ustawień aplikacji. Ustawienia pogrupowane są w następujących sekcjach.

Ogólne

Ikona powiadomienia: Umożliwia ukrycie ikonki G Data Internet Security for Android w obszarze powiadomień.

Zapisz raporty: Umożliwia lokalny zapis raportów skanowania systemu.

Aktualizacja

Automatyczna aktualizacja: Włącza automatyczne aktualizowanie sygnatur wirusów w tle.

Częstotliwość aktualizacji: Umożliwia ustawienie interwału aktualizacji (1, 3, 7, 14, lub 30 dni).

Tylko poprzez WLAN: Spowoduje, że aktualizacje będą pobierane jedynie przez sieci WiFi.

Region aktualizacji: Umożliwia wybór regionu aktualizacji (automatycznie ustawiony poprzez wersję językową).

Skanowanie

Skanowanie zaplanowane: Otwiera okno ustawień skanowania.

Ochrona przeglądarki

Tylko WLAN: Przeglądarki będą chronione tylko podczas połączeń z sieciami WiFi.