**5 powodów dla których powinieneś mieć zabezpieczenie antywirusowe w urządzeniach mobilnych**

**Marken Systemy Antywirusowe dystrybutor rozwiązań Home&amp;SOHO oraz Business firmy Bitdefender informuje - Gdybyś miał możliwość zabrania ze sobą tylko jednej rzeczy na bezludną wyspę, co by to było?**

Jakie urządzenie przechowuje i zapewnia ci dostęp do najważniejszych informacji, które posiadasz i potrzebujesz do codziennego funkcjonowania?

Jaka jest jedyna rzecz, której strasznie brakowałoby ci, gdybyś nie miał jej przy sobie przez cały dzień?

Przeważającą odpowiedzią jest: telefon komórkowy. Zazwyczaj jest też tak, że twój telefon komórkowy to bajerancki [smartfon](http://m.bitdefender.marken.com.pl/). A oto dlaczego powinieneś zadbać o jego zabezpieczenie:

1. ZAWIERA WSZYSTKIE TWOJE WAŻNE DANE

Tu jest wszystko - od wiadomości po zdjęcia, pocztę elektroniczną, historię przeglądarki (potencjalnie krępującą) , rzeczy udostępnione na [Facebook`u](https://www.facebook.com/ANTYWIRUS?ref=hl), miejsca, które odwiedzałeś, nie wspominając już o wszystkich hasłach i kontaktach (z byłym szefem i własną matką włącznie)

Wszystkie te dane są zawarte w tym jednym małym urządzeniu; kupa informacji o tobie. To sytuacja niezbyt bezpieczna.

2. URZĄDZENIA PRZENOŚNE SĄ PODATNE NA NIEBEZPIECZEŃSTWA

Wyobraź sobie jak niemiłe byłoby wysłanie jednego i tego samego smsa, do wszystkich kontaktów w twojej książce adresowej, jednego e-maila do wszystkich swoich kontaktów, jednego postu do wszystkich znajomych na [Facebook`u](https://www.facebook.com/ANTYWIRUS?ref=hl), w którym prosisz o przesłanie trochę pieniędzy, bo zostałeś obrobiony, czy coś. Matka prawdopodobnie dostałaby palpitacji serca, twoja była zmartwiłaby się, ale zapewne powstrzymałaby się przed wysyłaniem pieniędzy na podany adres, a jakaś część twoich znajomych byłaby na tyle uprzejma, aby sprawdzić czy z tobą wszystko OK.

To tylko (daleko posunięty) czarny scenariusz tego, co mogłoby nastąpić, gdyby Twoje prywatne dane zostały wykradzione z twojego smartfona. Ale nie martw się, wysłanie przez twój telefon głośnego smsa do operatora, że doładował ci konto, ma zdecydowanie większe szanse na spełnienie.

Szansa że to nastąpi istnieje, ponieważ, no cóż… urządzenia mobilne są podatne na ataki, nieważne jaki typ smartofna posiadasz. Fakt, że niektóre systemy operacyjne są odporniejsze od innych, ale...

3. ZARAZIĆ SIĘ ŁATWO

Najczęstszymi drogami na zarażenie telefonu są aplikacje ściąganie z sieci, sms, mms, e-mail i bluetooth. Każdy tego używa. Każdy klika w linki na swoich smartfonach, nie bacząc na to, gdzie ten odnośnik go zaprowadzi. Przeglądanie stron na urządzeniu mobilnym bez zabezpieczenia antywirusowego, które ostrzegłoby w porę o wejściu na zainfekowaną stronę, jest tak samo niebezpieczne jak przeglądanie stron na twoim PC. Niektórzy mają szczęście. Niektórzy nie.

Kolejnym prostym sposobem na zainfekowanie jest pobieranie z sieci bezpiecznie wyglądających wersji popularnych gier sieciowych, jak Angry Birds, szczególnie od dystrybutorów w systemie TPA (third part access). To dlatego czytanie recenzji i opisów aplikacji, które chcesz zainstalować, lub krótkie przeczytanie publikacji od producenta aplikacji, którą chcesz pobrać, może uchronić cię przed wieloma problemami. A kto ma na to wszystko czas? No cóż...

4. BRAK UWAGI MOŻE KOSZTOWAĆ SIĘ SPORO PIENIĘDZY

Jak? Najczęstszym zagrożeniem mobilnym (atakującym głównie użytkowników Androida) są spyware i trojany w sms.

Spyware zazwyczaj ściągają twoje dane (informacje GPS, informacje o kontaktach, wiadomości, historię przeglądania) i wysyłają je do kolejnych aplikacji i stron, a one korzystają z tych danych w celach reklamowych (popularny spam).

Najwyższej klasy trojany, załączone do popularnych aplikacji lub gier, są wraz z nimi instalowane i konfigurowane tak, aby wysyłać sms`y na płatne numery telefoniczne.



Tak więc wyrażanie zgody podejrzanie wyglądającym aplikacjom na sugestie typu: "wysyłaj sms lub mms w moim imieniu", lub "modyfikuj/usuń zawartość karty SD", może faktycznie wpłynąć na twój rachunek, skrzynkę odbiorczą lub całe doświadczenie sieciowe. Co gorsza, aplikacje takie jak te, mogą otworzyć "tylne drzwi", pozwalając pobrać się na twój telefon bardziej zaawansowanemu kodowi, kiedy nawet tego nie zauważysz, i pozwoli na transfer danych do złośliwej strony www, gdzie zostanie uzyskany dostęp do Twoich za pomocą pay/per/view, czy pay/per/click.

To stare powiedzenie że lepiej zapobiegać niż leczyć nigdy nie traci na aktualności, prawda?

Więc dlaczego tego nie robisz? Prawda jest taka, ze...

5. MOŻESZ WALCZYĆ SAM.

Mobilne ataki typu malware dochodzą do 155% na wszystkich platformach w ostatnim roku.

Najbardziej podatną na ataki platformą jest Android, gdzie ataki malware wzrosły o więcej niż 4500% w ciągu roku! Uważane za bardziej odporne na ataki od urządzeń bazujących na Androidzie; Iphone`y i iPad`y, również są słabo chronione przed tzw. jailbreaking`iem, czyli usuwaniem fabrycznych zabezpieczeń, tak aby otrzymywać całkowity dostęp do plików systemu. Pod względem przeglądania zawartości Internetu są tak samo słabo odporne, jak reszta urządzeń. Skoro o nich mowa, to ataki na Blackberry i Symbian również podwoiły się w ostatnim roku.

Mobilne urządzenia, smartfony są teraz na topie. Prawdopodobnie w tym momencie, gdy czytasz ten artykuł, szykuje się nowa fala spamu, scamu i virusów, które połaszą się na twoje pieniądze i dane.

Dobra wiadomość to taka, że możesz temu [zapobiec.](http://m.bitdefender.marken.com.pl/)

Oprócz biernego alarmu, czytającego jakie pozwolenie dajesz aplikacji lub odinstalowując aplikacje, zanim coś zacznie śmierdzieć, możesz przeprowadzić skan swojego telefonu pod kątem malware i [używać profesjonalnego mobilnego systemu zabezpieczającego](http://m.bitdefender.marken.com.pl/).

Wypróbuj najnowsze silniki i zabezpiecz swój telefon: [https://play.google.com/store/apps/details?id=com.bitdefender.security&hl=pl](https://play.google.com/store/apps/details?id=com.bitdefender.security&amp;amp;hl=pl) (nawet na bezludnej wyspie)