

Komórka wszystko powie. Twojemu bankowi

2013-04-08 (12:36)

Aplikacje mobilne banków zbierają dane o naszych połączeniach telefonicznych, mogą zajrzeć do naszych kontaktów w komórce, a nawet zrobić nam zdjęcie. Niektóre żądają dostępu do ustawień wibracji czy lampy błyskowej. Po co? By nas sprzedać!

Bankowość mobilna staje się coraz popularniejsza. Według nieoficjalnych danych może z niej korzystać już milion Polaków. Jednocześnie mało kto zdaje sobie sprawę, co oznacza zainstalowanie aplikacji mobilnej banku na swoim telefonie.

Programy tego typu żądają od nas dostępu do numerów telefonów naszych znajomych z książki adresowej, informacji z kim, kiedy i jak długo rozmawialiśmy. Inne mogą sprawdzić, z jakich aplikacji zainstalowanych na telefonie korzystamy i w jaki sposób. Część aplikacji umożliwia nawet wykonanie połączenia przez telefon bez naszej wiedzy czy odczyt danych zapisanych w pamięci telefonu. Zgodę na dostęp do tego typu poufnych informacji wyrażamy w momencie zainstalowania aplikacji.

Takie działania nie podobają się Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO). Zdaniem Wojciecha Wiewiórowskiego banki nie mają prawa żądać od nas tego typu informacji.

- Jeśli podpisaliśmy umowę na prowadzenie konta wraz z darmowym dostępem do rachunku przez bankowość mobilną, to nie oznacza, że wyraziliśmy zgodę na zbieranie o nas informacji - mówi Wirtualnej Polsce szef GIODO.

Choć za ściągnięcie aplikacji często nie musimy zapłacić ani złotówki, to nie oznacza to, że są one bezpłatne. Walutą są dane o nas, wykorzystywane w celach reklamowych.

- Polacy muszą sobie zdawać sprawę, że dając dostęp do tego typu informacji o sobie, w rzeczywistości handlują z bankiem. Kiedyś mówiło się, że nie ma darmowych lunchy. Dziś możemy stwierdzić, że nie ma darmowych aplikacji. Za nie się płaci, tylko na różne sposoby. Zazwyczaj informacją o nas - i co gorsze - często o naszych znajomych - tłumaczy Wojciech Wiewiórowski.

A banki mają coraz to większe pragnienie zajrzenia do naszej prywatności. W lutym wiceprezes Alior Banku Michał Hucal mówił w jednym z wywiadów, że w zbieraniu danych o klientach są lepsi od KGB. Dlaczego? Bo jego bank na tym zarabia. Trudno stwierdzić, czy żartował, czy się tym chwalił.

Banki, które spytaliśmy o to, po co im informacje ściągane z naszych telefonów, twierdzą jednak, że nie wykorzystują w żaden sposób poufnych danych. Muszą natomiast prosić o dostęp, bo tego wymaga program, w którym aplikacja jest tworzona.

- Wszystkie te rzeczy wynikają z wymagań frameworku (to podstawowy program, na bazie którego tworzony jest program - przyp. red.), który został wykorzystany w budowie naszej aplikacji. Bank nie przetrzymuje, ani nie wykorzystuje informacji - mówi Miłosz Gromski z biura prasowego ING Banku Śląskiego. Aplikacja tego banku żąda dostępu do danych pamięci i informacji o połączeniach. <br

Także mBank, którego aplikacja przy instalowaniu prosi o zgodę na możliwość czytania kontaktów, możliwość automatycznego wybierania numerów czy odczytywanie statystyk rozmów, twierdzi, że z nich nie korzysta.

- Tego typu dane nie są przez bank przechowywane. Aplikacja ich nie archiwizuje, nie przechwytuje i nie wykorzystuje w żaden inny sposób niż wskazany w regulaminie (ma służyć do usprawnienia wysłania potwierdzeń). Nigdzie ich też nie przesyła. Bank nikomu tych danych nie udostępnia ani nie wykorzystuje - mówi Krzysztof Olszewski, rzecznik mBanku.

Jak dodaje, przy ściąganiu apki każdy klient łatwo może dowiedzieć się, na udostępnienie jakich danych wyraża zgodę.

- Klienci korzystający z bankowości za pośrednictwem swojego telefonu mogą nie tylko pobrać specjalną aplikację banku, ale również korzystać z lekkiego serwisu transakcyjnego bezpośrednio w swojej mobilnej przeglądarce internetowej - dodaje rzecznik mBanku.

I choć banki zaprzeczają, że z wiedzy ściąganej z naszych telefonów korzystają, to nie ulega wątpliwości, że taką wiedzę posiadają. I wcześniej czy później chętnie z niej skorzystają. Już dziś niemal każdy bank wie, gdzie znajdują się jego klienci. Prawie wszystkie programy żądają dostępu do lokalizowania klientów przy pomocy GPS z dokładnością 2-3 m lub po stacjach bazowych (z dokładnością od 10 do 2000 m).

Oczywiście banki proszą o udostępnienie nam naszej lokalizacji, abyśmy mogli dowiedzieć się, gdzie jest najbliższy bankomat czy oddział. W środowisku bankowym coraz więcej mówi się jednak o reklamowym wykorzystaniu geolokalizacji. Przechodząc obok sklepu konkretnej sieci możemy z banku dostać informację SMS-em o zniżce, jeśli zapłacimy kartą.

- Najtrudniejsza rzecz to rozróżnienie, co jest informacją niezbędną do świadczenia usługi, a co nie. Trudno mi jednak znaleźć wyjaśnienie, po co bankowi dostęp do lampy błyskowej w telefonie - mówi Wojciech Wiewiórowski z GODO.

A lokalizacja chodzących po mieście numerów kont bankowych to świetny biznes. Po nałożeniu trasy kilkudziesięciu tysięcy klientów zarabiających powyżej 5 tys. łatwo będzie można taką mapę sprzedać firmom oferującym kampanie billboardowe.

- Osoby, które zachłysnęły się ideą big data, muszą zdawać sobie sprawę, że nie odkryli Ameryki. To są rzeczy znane od lat. Trzeba pamiętać, że ochrona prywatności jest wpisana do konstytucji. Oczywiście w 1997 roku, gdy pisano konstytucję przepisy miał chronić obywatela przed państwem, ale to prawo w identyczny sposób odnosi się do działań banków czy innych firmy prywatnych - ostrzega Generalny Inspektor Ochrony Danych Osobowych.

Dane, jakie o klientach aplikacji mobilnych dostają ich producenci, to problem nie tylko w Polsce. Sprawie przygląda się m.in. grupa techniczna Artykuł 29, która skupia europejskich rzeczników ochrony prywatności. Ostatnio w tej sprawie wydali alarmujący raport ostrzegający przed zbyt dużą ingerencją apek w prywatność użytkowników smartfonów.

We wrześniu tego roku w Polsce ma się też odbyć światowy zjazd rzeczników ochrony danych osobowych. Głównym tematem spotkania mają być właśnie aplikacje mobilne.

Sebastian Ogórek </br

(Wirtualna Polska)

Copyright © 1995-2013