

GIODO: jak bezpiecznie korzystać ze smartfonów

publikacja: 20.08.2016 aktualizacja: 20.08.2016, 17:16



Foto: AFP

Generalny inspektor ochrony danych osobowych radzi, jak bezpiecznie korzystać ze smartfonów i chronić swoje dane osobowe w wirtualnej rzeczywistości.

W związku z coraz większą popularnością aplikacji mobilnych wykorzystujących technologię geolokalizacji oraz wirtualnej rzeczywistości (jak np. Pokemon Go, HERE City Lens Corinth Micro Anatomy Augmented, dostępnych także w Polsce na urządzenia mobilne), generalny inspektor ochrony danych osobowych zachęca do ostrożnego i bezpiecznego użytkowania urządzeń przenośnych.

Prywatność

W pierwszej kolejności GODO zaleca zapoznanie się z polityką prywatności poszczególnych aplikacji oraz wszelkimi udostępnianymi komunikatami, z których dowiedzieć się można do jakich danych będzie miała dostęp konkretna aplikacja i w jakim celu będzie je wykorzystywać.

- W tym zakresie szczególną uwagę należy zwrócić na postanowienia regulaminów dotyczące przekazywania za pośrednictwem aplikacji danych osobowych do państw - zaznacza.

Dane osobowe

Według GODO, należy rozważnie korzystać z nieznanymi sieci bezprzewodowych Wi-Fi oraz pamiętać, że niektóre z aplikacji mobilnych (ale także stron internetowych oraz sieci Wi-Fi) mogą podczas korzystania z nich gromadzić informacje o lokalizacji użytkowników.

- Sprawdzajmy zatem jakie dane globalizacyjne są przesyłane przez aplikacje - ostrzega inspektor ochrony danych osobowych.

Istotne jest także, jakie dane udostępniają zainstalowane aplikacje oraz sprawdzić w urządzeniu mobilnym zakładkę "Prywatność", aby wiedzieć się jakie informacje o sobie udostępniamy.

- Z uwagi na szeroki zakres informacji gromadzonych na urządzeniu, jaki bardzo często wiąże się z użytkowaniem aplikacji, upewnijmy się, czy na pewno chcemy by dana aplikacja miała uprawnienia np. do SMS, fotografii, filmów, email, kontaktów, czatów itp. - radzi GODO.

Tryb

W przeglądaniu stron w celu minimalizacji gromadzonych na urządzeniu mobilnym informacji np. o lokalizacji, o odwiedzanych stronach itp. powinniśmy stosować tryb prywatny.

- Nie klikajmy zatem podejrzanych linków i nie przeglądajmy podejrzanych stron - zaleca GODO.

Jeśli jest to możliwe, to należy stosować wbudowane w urządzeniu oprogramowanie umożliwiające uruchomienie trybu prywatnego w celu oddzielenia danych prywatnych od służbowych lub innych informacji.

Wizerunek

Gry i aplikacje oparte na modelu tzw. rozszerzonej rzeczywistości mogą rejestrować m.in. wizerunki innych osób poprzez użycie kamery aparatu. Zatem o ile to możliwe, należy unikać fotografowania osób trzecich w trakcie korzystania z aplikacji.

Zabezpieczenia

Zdaniem GODO powinniśmy szczególnie chronić swoje dane do logowania oraz regularnie zmieniać trudne do odgadnięcia hasła.

Oprogramowanie

Bezpieczeństwo może także zapewnić korzystanie z oprogramowania z legalnego źródła.

- Nie wykonujemy Jailbreaking z zainfekowanym oprogramowaniem systemowym. Stosujemy oprogramowanie chroniące nasze urządzenie (antywirus, Firewall, anty spam, itp.) - przypomina inspektor ochrony danych osobowych.

Według GIODO każdy powinien również znać przysługujące mu prawa tak, by był w stanie skutecznie reagować na wszelkie naruszenia jego prywatności w tym przypadku przetwarzania jego danych osobowych bez podstawy prawnej.

Źródło: GIODO

[© Licencja na publikację](#) [© © Wszystkie prawa zastrzeżone](#)