Aplikacje mobilne – uważaj na zagrożenie

W związku z coraz większą popularnością aplikacji mobilnych wykorzystujących technologię wirtualnej rzeczywistości (przykładów nie trzeba daleko szukać– weźmy np. ostatni hit czyli aplikacja FaceApp), Prezes Urzędu Ochrony Danych Osobowych zachęca do ostrożnego i bezpiecznego użytkowania urządzeń przenośnych. Często nie zdajemy sobie sprawy jak wiele danych na swój temat przekazujemy koncernom technologicznych – bo niewiele osób podczas instalacji aplikacji wczytuje się w kolejne komunikaty, jakie musimy zatwierdzić zanim system rozpocznie pobieranie. Jeśli do tej pory tego nie robiliście, po lekturze tego tekstu zmienicie podejście.

Oto kilka wskazówek z serwisu UODO dotyczących bezpiecznego korzystania ze smartfonów:

- **Czytaj regulaminy i polityki prywatności.** W pierwszej kolejności zalecamy wszystkim użytkownikom zapoznanie się z polityką prywatności takich 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 zwracamy na postanowienia regulaminów dotyczące przekazywania za pośrednictwem aplikacji danych osobowych do państw trzecich.
- **Rozważnie korzystaj z nieznanych sieci bezprzewodowych Wi-fi.** Należy także pamiętać, że niektóre z aplikacji mobilnych (ale także stron internetowych oraz sieci Wi-Fi) mogą podczas korzystania z nich gromadzić informacje o lokalizacji użytkowników. Sprawdź, jakie dane geolokalizacyjne są przesyłane przez aplikacje.
- **Ustal, jakie dane osobowe udostępniają zainstalowane aplikacje**. Sprawdź w urządzeniu mobilnym zakładkę Prywatność i dowiedź się, jakie informacje o sobie udostępniasz. Z uwagi na szeroki zakres informacji gromadzonych na urządzeniu, jaki bardzo często wiąże się z użytkowaniem aplikacji, zachęcamy do refleksji, czy na pewno chcemy, by dana aplikacja miała uprawnieninia np. do SMS, fotografii, filmów, email, kontaktów, czatów itp.
- **Nie klikaj podejrzanych linków, nie przeglądaj podejrzanych stron**. Stosuj tryb prywatny (incognito) w przeglądaniu stron w celu minimalizacji gromadzonych na urządzeniu mobilnym informacji np. o lokalizacji, o odwiedzanych stronach itp.
- Jeśli to możliwe, **stosuj wbudowane w urządzeniu oprogramowanie umożliwiające uruchomienie trybu prywatnego** w celu oddzielenia danych prywatnych od służbowych lub innych informacji.
- Gry i aplikacje oparte na modelu tzw. rozszerzonej rzeczywistości mogą także rejestrować m.in. **wizerunki innych osób** poprzez użycie kamery aparatu. Jeśli to możliwe, należy unikać fotografowania osób trzecich w trakcie korzystania z aplikacji.
- **Chroń swoje dane do logowania** oraz wykonuj regularną zmianę trudnego do odgadnięcia hasła.
- **Aktualizuj oprogramowanie.** Korzystaj tylko z oprogramowania z legalnego źródła. Stosuj oprogramowanie chroniące twoje urządzenie (antywirus, Firewall, anty spam itp.).
- **Każdy powinien również znać przysługujące mu prawa** tak, by był w stanie skutecznie reagować na wszelkie naruszenia jego prywatności, w tym przypadki przetwarzania jego danych osobowych bez podstawy prawnej.

I na koniec mała rada od redakcji serwisu powiat.hajnowka.pl – z każdej aplikacji korzystaj z głową! Nie ulegaj chwilowej modzie – choć Instagrama, Facebooka oraz Twittera zalewają dziesiątki tysięcy powiadomień, nie musisz udostępniać tysiąc pierwszej. Poza tym miej świadomość, że odinstalowanie aplikacji nie sprawi, że dane, które do tej pory udostępniłeś, automatycznie znikną z serwera. Nie wiesz również w jaki sposób i gdzie przetwarzane są Twoje dane ani co stanie się z nimi stanie, gdy firma – właściciel pobranej aplikacji, zakończy działalność. Chroń swoją prywatność - bo ma kluczowe znaczenie dla Twojego bezpieczeństwa!

za: uodo.gov.pl

oprac. Katarzyna Miszczuk