

Aplikacje na smartfony kradną tożsamość

OCHRONA DANYCH | Kiedy instalujemy w telefonie niewinną grę, często zgadzamy się na przetwarzanie informacji o nas.

EDYTA HOŁDYŃSKA

Tysiące stron internetowych i aplikacji na smartfony ułatwiają życie, ale bywają także bardzo niebezpieczne.

Spiesząc się i akceptując wszystkie pytania, które producent aplikacji zadaje przed jej zainstalowaniem, możemy się narażać na kradzież danych osobowych.

Wojciech Wiewiórowski, generalny inspektor ochrony danych osobowych (GIODO), alarmuje, że nie każdy twórca aplikacji przestrzega polityki prywatności zgodnej z ustawą o ochronie danych osobowych.

W sieci z dowodem na czole

Problem jest o tyle poważny, że podczas rejestracji w serwisach internetowych aż 42 proc. osób automatycznie stosuje się do instrukcji logowania i nie sprawdza poziomu zabezpieczeń ani posiadanej przez serwis polityki prywatności. Wykazała to socjolog Anna Wilk w badaniach przeprowadzonych na zlecenie firmy Fellowes.

Dodatkowo 25 proc. badanych udostępniło swoje prywatne dane osobowe bez żadnych ograniczeń w Internecie. Aż 18 proc. osób jest gotowych podać swój PESEL, adres zamieszkania czy nazwisko panienskie matki, jeśli takie są wymagania aplikacji. 33 proc. ankietowanych doświadczyło problemu kradzieży tożsamości, lub takie niebezpieczeństwo spotkało ich bliskich.

Badania pokazały także, że problem dotyczy głównie ludzi młodych, którzy najsłabiej zabezpieczają się przed kradzieżą danych – mówi Anna Wilk. – Spośród ponad 1,5 tys. respondentów aż 48

proc. stanowiły osoby w wieku 26–44 lata. Celem badań było sprawdzenie stanu wiedzy społeczeństwa o kradzieży tożsamości.

Uważaj, na co się godzisz

Na bezprawne posiadanie i wykorzystanie naszych danych możemy być narażeni już w momencie zakupu nowego smartfona. W jego systemie są już zainstalowane aplikacje, które, by poprawnie działać, mają dostęp do informacji o nas. Aplikacje portali społecznościowych, obecnie niemal w każdym modelu, mają wiedzę nie tylko o imieniu i nazwisku użytkownika, adresie e-mail i numerze telefonu. By poprawnie działać, zjadają także dostęp do informacji o naszej lokalizacji. A jeśli sami zdecydujemy się dodać np. zdjęcia

– Żaden producent nie oferuje nam swojej usługi za darmo – przestrzega Wojciech Wiewiórowski. – Cena, jaką płacimy za nierozważne instalowanie aplikacji na telefon, jest dostęp do informacji o nas. Instalując je, zwróćmy uwagę na to, jakie zapisy regulaminu musimy zaakceptować. Niejednokrotnie bowiem zgadzamy się na wykorzystywanie naszych danych pod przykrywką polityki prywatności. Przed instalacją aplikacji należy się poważnie zastanowić nad tym, czy producentowi faktycznie potrzebne jest przetwarzanie naszych danych. I czy wobec tego chcemy taką aplikację mieć w swoim telefonie.

Producenci jak widmo

O tym, że problem jest poważny, przestrzega także Katarzyna Szymielewicz z Fundacji Panoptikon.

Istnieją na rynku aplikacje pisane specjalnie po to, by wyciągać dane osobowe od użytkowników – mówi. – Najczęściej służą do zabawy, to np. gry rozpowszechniane na serwisach społecznościowych. Ich twórcy doskonale wiedzą, że przeciętny użytkownik, zwłaszcza dziecko, zorientowany na zabawę i relaks, nawet nie przeczyta regulaminu i bezrefleksyjnie zaakceptuje wszystkie warunki. Niektóre z nich można by uznać za niezgodne z polskim prawem, jednak mało która firma oferująca takie „darmowe” aplikacje ma siedzibę w Polsce – tłumaczy Szymielewicz. Jeśli dojdzie do kradzieży danych osobowych za pomocą smartfonów, bardzo trudno ustalić winnego. Nasz telefon z zapisanymi hasłami i numerami kont może się znaleźć w niepowołanych rękach, a złodziej może np. zdecydować się na zakup drogiego przedmiotu i zażądać przesyłki pod swój adres.



– Tak jak po zgubieniu dowodu osobistego, na który złodziej może wziąć kredyt, tak i w tym przypadku bardzo trudno będzie udowodnić przed sądem, że nie znajdowaliśmy się w tym samym miejscu co nasz telefon i że wcześniej go zgubiliśmy – uświadamia Wiewiórowski.

Usługodawcy telefonii komórkowej, którzy sprzedają smartfony, nie biorą na siebie odpowiedzialności za aplikacje i działania, bo ich nie produkują. Do twórców bardzo trudno dotrzeć, ponieważ najczęściej są to producenci zagraniczni.

Za udostępnienie danych lub umożliwienie dostępu do danych osobom nieupoważnionym grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat dwóch, ale trudno złapać sprawcę.

Kogo ukarać

Jacek Mrozek z Uniwersytetu Warmińsko-Mazurskiego w Olsztynie przypomina, że odpowiedzialności karnej podlega zawsze osoba, a nie firma czy instytucja.

– Jeśli chodzi o zagranicznego sprawcę przestępstwa naruszenia danych osobowych obywatela polskiego, to stosuje się polskie przepisy karne, przy czym warunkiem jego odpowiedzialności jest uznanie takiego czynu za przestępstwo obowiązującą w państwie, w którym czyn popełnił, czyli nierzadko siedzibie firmy. Jeśli

zagraniczny sprawca przestępstwa przetwarza dane przy wykorzystaniu środków technicznych (np. serwera) znajdujących się poza terytorium Polski, to wobec niego nie ma zastosowania polska ustawa o ochronie danych osobowych. GIODO nie może zatem wobec niego wszcząć postępowania administracyjnego – tłumaczy Mrozek.

Jest szansa, że Unia Europejska przyjmie nowe prawo, lepiej chroniące nasze dane. W ciągu dwóch lat ma powstać rozporządzenie, które będzie obowiązywało wszystkie firmy działające na europejskim rynku, bez względu na to, gdzie formalnie mają siedzibę. Dopiero wtedy będzie możliwość ścigania twórców niebezpiecznych aplikacji z całego świata.

Prawdziwym ciosem w bezpieczeństwo danych osobowych, jak przestrzega GIODO, byłaby jednak planowana jeszcze w maju 2013 r. nowelizacja ustawy o kredytach konsumenckich, która umożliwiałaby łatwe pobieranie kredytów online.

– Poważnie zaniepokoiłoby się już podczas posiedzenia komisji sejmowej, która zajmowała się nadzorem nad rynkiem finansowym, a przy okazji pracowała nad zmianą ustawy o kredytach konsumenckich – dodaje Wiewiórowski.

Kredyt online

Pojawiły się bowiem propozycje, by rozluźnić przepisy, które wymagają pisemnego

poświadczenia przy zawieraniu umów o kredyt. Konieczność złożenia podpisu poważnie przeszkadza systemom kredytowania online, dlatego są naciski, aby z niego zrezygnować.

– Takie rozluźnienia prawne byłyby bardzo nierozsądnym posunięciem – tłumaczy Wiewiórowski. – Zawieranie umowy o kredyt przez Internet jest bardzo niebezpieczne. Złodziejami tożsamości, którzy skorzystają z tego, że akurat nie ma nas przy komputerze. Bank nie zażąda dodatkowego podpisu, więc umowa zostanie zawarta. A ofiara obciążona kredytem.

Posłowie zgodzili się z GIODO, że do czasu stworzenia rządowego projektu zmian i przeprowadzenia badań nad zagrożeniami, jakie niesie tego rodzaju rozwiązanie, nie będą nad nim dyskutować.

GIODO radzi, że aby ustrzec się przed konsekwencjami kradzieży tożsamości, oprócz roztępnego korzystania z nowinek technologicznych i podwójnego zabezpieczania wszystkich swoich transakcji bankowych online, np. poprzez potwierdzanie przelewów hasłem i dodatkowo kodem otrzymanym z banku przez e-sesamów, warto także zainstalować programy antywirusowe i antyspamowe. Zarówno w swoich komputerach, jak i smartfonach, za których pośrednictwem coraz częściej sprawdzamy stan naszego konta, a nawet płacimy rachunki. ■