

[J.K.](#)

## GIODO zbada wyciek danych z międzynarodowej firmy pożyczkowej

publikacja: 13.04.2017    aktualizacja: 13.04.2017, 14:53



Foto: 123RF

**W związku z podejrzeniem uzyskania przez hakerów nieuprawnionego dostępu do danych klientów Wonga.com, GODO postanowił z urzędu zbadać tę sprawę.**

W ostatnim czasie media donoszą, że hakerzy przełamali zabezpieczenia jednej ze znanych międzynarodowych firm mikropożyczkowych. Istnieje podejrzenie, że uzyskali dostęp do takich danych osobowych ok. 22 tys. Polaków i 245 tys. mieszkańców Wielkiej Brytanii, będących klientami tej firmy, jak: imię, nazwisko, numer dowodu osobistego, numer PESEL, adres oraz numer telefonu.

Jakkolwiek zaatakowana firma udziela na bieżąco poszkodowanym klientom informacji dotyczących tej sprawy, a także złożyła do prokuratury zawiadomienie o podejrzeniu popełnienia przestępstwa, Generalny Inspektor Ochrony Danych Osobowych (GIODO) postanowił z urzędu podjąć działania mające na celu zbadanie i wyjaśnienie sytuacji.

Również brytyjski organ ochrony danych osobowych wszczął już procedurę wyjaśniającą. GIODO zamierza ściśle z nim współpracować, celem ustalenia, czy dane osobowych klientów

firmy były przetwarzane zgodnie z prawem w momencie dokonania ataku, a także czy jest tak również obecnie.

Niezależnie od zaleceń i wskazówek, jakie firma przekazuje osobom, których dane osobowe mogły stać się celem ataku, GIODO przypomina o działaniach, jakie warto podjąć, by zminimalizować ryzyko wykorzystania naszych danych osobowych niezgodnie z prawem, np. w celu kradzieży tożsamości i zaciągnięcia w naszym imieniu zobowiązań finansowych.

GIODO zaleca zatem, by:

- rozważyć zastrzeżenie dowodu osobistego,
- rozważyć aktywowanie tzw. alertów kredytowych, tj. powiadomień o próbie zaciągnięcia zobowiązań finansowych z wykorzystaniem naszych danych osobowych,
- zweryfikować wszystkie loginy i hasła, jakimi się posługujemy – dla bezpieczeństwa najlepiej jest bowiem, by serwisach internetowych i systemach komputerowych używać innych identyfikatorów i haseł; powinno to dotyczyć zwłaszcza ważnych usług, np. e-bankowości, e-zakupów,
- zmienić hasło wykorzystywane w kontaktach z firmą, z której dane mogły zostać wykradzione; warto zadbać, by było odpowiednio silne,
- zainstalować oprogramowanie chroniące komputer i urządzenia mobilne przed niepożądanymi działaniami złośliwego oprogramowania,
- nie odpowiadać na maile spamerów ani nieznanych osób i instytucji.

Źródło: GIODO