**Jak uchronić się przed wyciekiem danych - porady ekspertów z Kaspersky Lab**

**Ostatni przypadek wycieku danych osobistych z serwerów Facebooka jest kolejnym dowodem na to, że nawet najlepsze usługi w chmurze nie są wolne od błędów. Z tego powodu każdy użytkownik powinien mieć przygotowany plan działania na wypadek tego typu sytuacji. Eksperci z Kaspersky Lab przygotowali kilka porad, które pomogą zminimalizować ryzyko potencjalnego wycieku danych.**

Przed ubiegłym weekendem dział odpowiedzialny za bezpieczeństwo Facebooka przyznał, że z winy błędu w kodzie portalu szczegóły kontaktowe 6 milionów użytkowników stały się dostępne dla nieupoważnionych osób. Mówiąc bardziej szczegółowo, jeśli ktokolwiek pobierał archiwum danych swojego konta na Facebooku przy pomocy narzędzia Download Your Information (DYI), mógł stać się posiadaczem adresów e-mail lub numerów telefonów innych użytkowników lub ludzi, z którymi mieli oni jakiekolwiek powiązania. Aby zapobiec dalszemu wyciekowi danych, Facebook tymczasowo zablokował narzędzie DYI. Jednak to, co już raz wyciekło, na zawsze stanie się publiczne.

Jeśli dane użytkownika zostały przez kogoś pobrane, Facebook wyśle do niego wiadomość e-mail. Firma nie odpowie na pytanie “kto konkretnie pobrał moje dane”, ale poda liczbę takich osób. Zazwyczaj jest to jedna lub dwie osoby. Ponieważ wyciek miał ograniczony rozmiar, dane raczej nie zostaną użyte do kradzieży tożsamości lub innych niebezpiecznych czynności. Niemniej jednak, użytkownicy powinni pozostać czujni i zwracać uwagę na niespodziewane wiadomości lub telefony dotyczące ich adresów

e-mail/numerów telefonów, które wyciekły.

Należy pamiętać, że cyberprzestępcy często wykorzystują takie okazje do wysyłania wiadomości phishingowych, dlatego trzeba uważać podczas czytania e-maili i klikania odsyłaczy. Oficjalna wiadomość od Facebooka zawiera tylko jeden odsyłacz do specjalnej strony portalu (<https://www.facebook.com/security/notes>) i nie wymaga podawania żadnych danych.

Aby zminimalizować szkody wyrządzone przez ten i podobne wycieki, podczas zapisywania się do dowolnej usługi w chmurze warto stosować się do poniższych zasad:

Załóż specjalne konto e-mail do odbierania powiadomień z portali społecznościowych. Do komunikowania się ze swoimi znajomymi potrzebujesz oddzielnego e-maila, a do otrzymywania wiadomości z banku i innych ważnych instytucji potrzebujesz możliwie najlepiej zabezpieczonego konta.

Rozważ korzystanie z innego numeru telefonu do otrzymywania ważnych informacji.

Używaj unikatowych i skomplikowanych haseł do każdej usługi sieciowej, z której korzystasz. Do zarządzania swoimi hasłami możesz użyć menedżera haseł, takiego jak rozwiązanie wbudowane w program Kaspersky PURE.

Zawsze istnieje możliwość wystąpienia błędu. Jeśli więc oznaczyłeś niektóre posty lub zdjęcia jako “tylko dla znajomych” lub nawet jako “prywatne”, nie oznacza to wcale, że nikt ich nigdy nie zobaczy. Wychodź z założenia, że to, co publikujesz online, może kiedyś stać się publiczne - zanim opublikujesz, zastanów się dwa razy.

Jeśli przechowujesz dane w chmurze tylko do własnego użytku, pomyśl o ich zaszyfrowaniu przed przesłaniem do użytkowanego przez Ciebie serwisu online.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.