DANE, KTÓRE WYCIEKŁY Z FACEBOOKA MOGĄ WYKORZYSTAĆ CYBERPRZESTĘPCY

Dane, które wyciekły z Facebooka mogą zostać wykorzystane przez cyberprzestępców do kradzieży tożsamości lub przełamania innych zabezpieczeń - zaalarmował Rzecznik Finansowy. Jak zaleca, każdy użytkownik platformy powinien wykształcić nawyk ochrony danych osobowych.

Jak informowaliśmy na naszym portalu, wyciek danych z Facebooka, który dotyczy łącznie ponad 533 mln użytkowników, dotknął również 2,6 mln Polaków. Incydent naraża osoby korzystające z platformy na cyberataki ze strony cyberprzestepców, a koncern Marka Zuckerberga ma ograniczone pole manewru, aby ochronić je przed zagrożeniem. Udostępnione na forum hakerskim informacje ujawniają m.in. dane osobowe, adresy e-mail, lokalizacje czy numery telefonów użytkowników serwisu.

> *Tak duża baza informacji może posłużyć przestępcom do ataków z wykorzystaniem socjotechnik lub prób włamań na inne profile lub konta, w tym konta bankowe.*
>
> *Rzecznik Finansowy*

Zdaniem Rzecznika Finansowego dane te mogą służyć jako narzędzie do kradzieży tożsamości lub przełamania innych zabezpieczeń. Dlatego zaleca już teraz podjęcie odpowiednich kroków i wykształcenie nawyku ochrony danych osobowych przez każdego z nas.

Przypomina również, że telefon od nieznajomej osoby może pochodzić od oszusta i nawet jeśli dzwoniąca osoba podaje nam nasze dane celem uwiarygodnienia kontaktu, mogą one pochodzić z wycieku. „Zwracajmy także większą uwagę na otrzymywane od nieznajomych wiadomości e-mail i SMS, które także mogą zawierać złośliwe oprogramowanie służące do oszustw lub kradzieży” - radzi Rzecznik.

Zaznaczył, że wyciek adresów e-mail może pozwolić oszustom na podszycie się pod prawdziwe organizacje, w tym banki, w których znajdują się nasze rachunki. Zwrócił też uwagę na istotne niebezpieczeństwo kradzieży środków finansowych z rachunku bankowego. „Dążąc do minimalizacji wystąpienia tego ryzyka, warto sprawdzić, czy korzystamy w banku z silnego uwierzytelniania dla wszelkich możliwych rodzajów czynności” - napisał.

Rzecznik podkreślił, że jedną z częstszych form ataku jest wiadomość do zaktualizowania swoich poufnych danych. Inna forma oszustwa to tzw. oszustwo „na dopłatę”, polegające na podszyciu się pod kurierów, firmy energetyczne, komorników lub urzędy celem nakłonienia do dokonania opłaty

przez kliknięcie w link prowadzący do fałszywej bramki płatności. „Zachowajmy czujność w przypadku otrzymania takiego linka. Znacznie bezpieczniej będzie samodzielnie wprowadzić w przeglądarce adres strony banku lub skorzystać z utworzonej wcześnie samodzielnie zakładki” - przestrzegł.

Rzecznik Finansowy przypomniał, że w przypadku wystąpienia nieautoryzowanej transakcji płatniczej należy ten fakt niezwłocznie zgłosić bankowi wraz z wnioskiem o zwrot środków, a także równolegle złożyć zawiadomienie o możliwości popełnienia przestępstwa najbliższej jednostce policji.

„Zgodnie z aktualnym stanem prawnym bank powinien zwrócić kwotę nieautoryzowanej transakcji na konto klienta nie później niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji lub po dniu otrzymania zgłoszenia od klienta”. Podkreślił też, że w dobie coraz powszechniejszych oszustw z wykorzystaniem kradzieży tożsamości, warto z rozwagą przedstawiać swoje dane w sieci.

SZP/PAP

Czytaj też: Wyciek danych z Facebooka. Incydent dotknął milionów Polaków