Komunikat bezpieczeństwa

www.bsczechowice.com.pl

Transakcje fraudowe w cyfrowym portfelu Apple Pay
11.12.2020

Szanowni Państwo,

W związku ze zwiększoną aktywnością cyberprzestępców, a tym samym zwiększoną liczbą występujących w ostatnim czasie transakcji fraudowych realizowanych w szczególności przy wykorzystaniu systemu płatności mobilnych i cyfrowego portfela Apple Pay poniżej przedstawiamy rekomendacje związane z najczęściej występującym schematem oszustw.

Klient otrzymuje fałszywy e-mail albo sms, który do złudzenia przypomina wiadomość od firmy pod którą podszywa się przestępca (firmy kurierskie, dostawcy usług). W przygotowanej przez oszusta wiadomości Klient proszony jest o dokonanie wpłaty na kwotę kilku złotych z tytułu niedopłaty w płatności za przesyłkę lub fakturę. Link do płatności, który umieszczony jest w wiadomości kieruje Klienta na fałszywą stronę, na której Klient podaje wszystkie dane nadrukowane na plastiku karty oraz kody akceptacji różnych dyspozycji również te otrzymane SMS-em na numer telefonu Klienta. Podanie danych umożliwia przestępcy **włamanie do urządzenia Klienta lub zarejestrowanie karty Klienta w cyfrowym portfelu Apple Pay na urządzeniu przestępcy**. Cyfrowy portfel Apple Pay jest najczęściej wykorzystywany przez przestępców do „fałszywej" tokenizacji kart klientów z uwagi na łatwość przeprowadzenia tego procesu. Apple pozwala na tokenizację karty w aplikacji Wallet niezależnie od użytkownika, któremu karta została wydana, należy ją potwierdzić SMSem wysłanym do użytkownika karty, który jest później przekazywany przestępcy na fałszywej stronie. Uzyskując te dane przestępca dokonuje następnie szeregu wysokokwotowych transakcji do wyczerpania środków na rachunku Klienta. Transakcje te wykonywane są najczęściej w ramach płatności mobilnych Apple Pay i jest to związane ze sposobem w jaki uwierzytelniane są transakcje kartą stokenizowaną. Po zarejestrowaniu karty i stokenizowaniu jej na urządzeniu przestępcy przy użyciu danych podanych przez Klienta na fałszywej stronie, uwierzytelnienie transakcji następuje poprzez wpisanie kodu lub znaku graficznego którym zabezpieczony jest telefon i nie są wymagane żądne inne dodatkowe zabezpieczenia co daje przestępcy nieograniczone możliwości w dostępie do środków na rachunku Klienta.

W przypadku zgłoszenia reklamacji dotyczącej takich transakcji odzyskanie środków w procesie reklamacyjnym jest w większości przypadków niestety niemożliwe, gdyż transakcje dokonywane są z silnym uwierzytelnieniem w skutek podania przez Klienta na fałszywej stronie danych oraz kodów akceptujących.