ZA CZYJE ZAKUPY PŁACIMY W AUTOBUSIE KARTĄ ZBLIŻENIOWĄ

. AMELIA,WWW.ADMONKEY.PL (2013-03-06 00:00:00)
admonkey.pl/za-czyje-zakupy-placimy-w-autobusie-karta-zblizeniowa/14733

Ponad 8 milionów Polaków posiada karty debetowe oraz kredytowe wyposażone w technologię NFC umożliwiającą płatności zbliżeniowe. Brak potrzeby autoryzacji wykorzystywany jest przez cyber złodziei, którzy za pomocą dwóch telefonów komórkowych płacą naszymi kartami za swoje zakupy.

amelia
Ponad 8 milionów Polaków posiada karty debetowe oraz kredytowe wyposażone w technologię NFC umożliwiającą płatności zbliżeniowe. Brak potrzeby autoryzacji wykorzystywany jest przez cyber złodziei, którzy za pomocą dwóch telefonów komórkowych płacą naszymi kartami za swoje zakupy.
Źródło: flickr-debtcovered-CC

Karty zbliżeniowe stały się standardem promowanym przez banki, które nie tylko wymieniają je na nowe, gdy upływa okres ważności naszych starych kart, ale proponują je swoim klientom w każdej chwili bez specjalnego powodu. Motyw jednak jest. Zamiana transakcji gotówkowych na elektroniczne oznacza dla banków obniżenie kosztów zabezpieczania i logistyki pieniędzy papierowych oraz zyski z opłat za korzystanie z transakcji elektronicznych. Jednak gdy nasz dostęp do pieniędzy staje się łatwiejszy, ich kradzież staje się również prostsza.

Jak dochodzi do kradzieży?

Do kradzieży dochodzi najczęściej w autobusie. Złodziejom wystarczą dwa nowoczesne telefony z systemem NFC oraz specjalne oprogramowanie, niestety dostępne w sieci. Nie ma potrzeby zakupu drogiego terminala, czy też fizycznej kradzieży karty. Złodzieje nie będą grzebać nam w torebce, ani w portfelu. Wystarczy, że stoją obok nas przez dłuższą chwilę. Jak wynika z badań i testów przeprowadzonych przez naukowców z Uniwersytetu Cambridge, sygnał przechwycony może być z odległości jednego metra. Jak dochodzi do przejęcia danych karty? Jedna z dwóch osób kradnących robi zakupy i płaci za nie zbliżeniowo. Sygnał do terminala płatniczego w kasie wysyłany jest jednak nie z karty, a z telefonu, który otrzymuje kopie sygnału karty w autobusie. Cyfrowy obraz sygnału stanowi dokładną kopię, a więc kasjer nie zauważy żadnych anomalii. Cały proces trwa zaledwie kilka chwil i nie pozostawia po sobie fizycznych śladów użytkowania karty, tzn. nikt jej nie wyciąga z naszego portfela. Jeżeli nie sprawdzimy stanu konta i nie zorientujemy się, że zapłaciliśmy za czyjeś zakupy, o sprawie nikt się nie dowie.

Brak autoryzacji transakcji zbliżeniowych jest dużym udogodnieniem zarówno dla kupujących, jak i dla sprzedawców, ponieważ efektywnie skraca i upraszcza proces płatności bezgotówkowych. Nie jest jednak bez wad. Pozwala na korzystanie z karty bez znajomości kodu PIN, a przy procederze kopiowania sygnału, również bez fizycznej kradzieży karty.

Pocieszenie może stanowić fakt, że transakcje zbliżeniowe w Polsce realizowane są wyłącznie do kwoty

50 złotych, czyli potencjalne straty z tytułu kradzieży będą niewielkie. Jednak z drugiej strony liczba tych transakcji, teoretycznie ograniczona do 5 dziennie, może spowodować wyczyszczenie naszego konta. W jaki sposób? Znany jest przypadek 78 transakcji wykonanych kartą zbliżeniową jednego dnia, ponieważ tego typu płatności wykonywane są w trybie offline i nie są rejestrowane w czasie rzeczywistym.

Banki otrzymują coraz więcej reklamacji związanych z nieprawnym użyciem kart zbliżeniowych przez osoby postronne. Z racji tego, że autoryzacja transakcji przy użyciu takiej karty odbywa się poprzez jej posiadanie w portfelu, kieszeni, nie pozostają inne ślady jej użycia, takie jak podpis, czy PIN. Ubezpieczenia kart często pokrywają straty w wyniku takich transakcji od kwoty 200 PLN, a więc jeśli straciliśmy 50, 100, lub 150 złotych, ubezpieczenie nas nie dotyczy. Warto zwrócić na to uwagę przy podpisywaniu umowy z bankiem.

Czy można bezpiecznie korzystać z kart zbliżeniowych?

Okazuje się, że najlepiej zabezpieczeni przed przechwytywaniem danych z kart płatniczych są posiadacze telefonów z możliwością płatności zbliżeniowej takich jak T-Mobile My Wallet, czy Orange Cash. Najpierw wprowadzają dane karty lub kart do telefonu, a następnie korzystają z sygnału wysyłanego z komórki podczas płatności. Uruchomienie takiej płatności wymaga autoryzacji PIN w telefonie, a więc właściciele kart są świadomi każdej transakcji. Mogą również przy pomocy kilku kliknięć wyłączyć przekazywanie danych NFC. Posiadacze kart zbliżeniowych takiej możliwości nie mają.

Testowanie nowych technologii

Nowe technologie stawiają przed projektantami, deweloperami i informatykami nowe wyzwania komunikacyjne. Nie chodzi tylko o warstwę oprogramowania i sprzęt, ale także o „user experience", czyli wrażenia użytkownika, a także jego poziom wiedzy i umiejętności do posługiwania się tą technologią. Jeżeli wrażenia są złe, a technologia trudna lub niebezpieczna w codziennym użytkowaniu, to może się nie przyjąć. Takimi prawami rządzą się finansowe aplikacje mobilne. W przypadku „płatności przez telefon" zagrożenia dla danych użytkownika mogą powstawać dopiero w momencie fizycznego kontaktu atakującego z urządzeniem, na przykład kradzieży telefonu. – Warto w procesie projektowym kłaść nacisk nie tylko na identyfikację kluczowych funkcjonalności, ale i głównych zagrożeń dla bezpieczeństwa danych – mówi Mateusz Biliński, mobility manager w Lizard Mobile. – Wspomaganie się tutaj ekspertyzą osób spoza projektu, które zadają właściwe pytania, skutecznie zwiększa szanse aplikacji na zaistnienie w świecie mobilnym – dodaje.

Warto inwestować w najnowsze technologie oraz uczyć się jak korzystać z tych, które już na co dzień nosimy w portfelu.

Jak zabezpieczyć się przed nieautoryzowanym użyciem naszej karty radzi ekspert zabezpieczeń mobilnych i internetowych Piotr Konieczny z portalu Niebezpiecznik.pl:

Kartę zbliżeniową wystarczy owinąć folią aluminiową – to sprawi, że wbudowana w nią antena nie będzie w stanie wzbudzić chipa NFC. O ile folia aluminiowa jest dość nieporęczna, to na rynku znajduje

się całkiem sporo metalizowanych etui, które spełniają tę samą rolę – zamykają kartę w klatce Faradaya.

Nie polecam nacinać karty celem przecięcia zwojów zatopionej w plastiku anteny – raz, że taka karta może zostać zatrzymana w sklepie jako "nieważna", dwa że przecięcie zwojów anteny nie wyłącza funkcji NFC (nacięta antena de facto dalej istnieje, jest tylko mniej wydajna)

Jeśli bank nie chce wymienić nam karty zbliżeniowej na wersję bez chipa NFC – to rozważmy zakodowanie karty w pamięci telefonu – płacenie telefonem z funkcją NFC ma dość znaczą przewagę nad kartami zbliżeniowymi – chip NFC nie jest aktywny do momentu, dopóki użytkownik świadomie nie aktywuje tej funkcji. Nie ma mowy o tym, że ktoś sczyta nam kartę z telefonu w autobusie – tak, jak może to zrobić ze standardową zbliżeniówką.

Badania Uniwersytetu Cambridge na temat odległości przechwytywania sygnału NFC kart zbliżeniowych: "An RFID Distance Bounding Protocol" Gerharda P. Hancke and Markusa G. Kuhn – http://www.rfidblog.org.uk/Hancke-Securecomm2005-pres.pdf

Źródło: mat. pras.