Cyberdefence 24

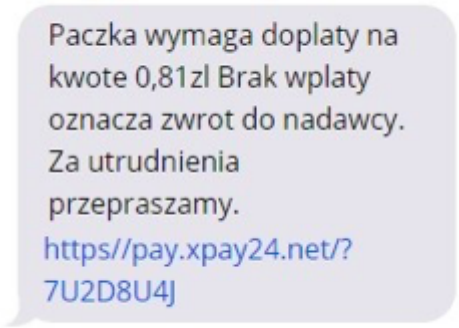
aut. Sylwia Gliwa 16.11.2020

UWAGA WYŁUDZENIE! ATAK NA KONTO BANKOWE W 3 KROKACH

3 proste kroki wystarczą, aby zdobyć dostęp do naszego konta. Uważasz, że jesteś ostrożny? Pamiętaj, że cyberprzestępcy są coraz sprytniejsi. Choć sposób „na dopłatę do paczki" wydaje się być już przestarzały, banki wciąż ostrzegają przed tego typu chwytami – jak widać, wciąż są osoby, które nieopatrznie dają się nabrać.

„Cyberprzestępcy są coraz bardziej aktywni w sieci – mogą Państwo otrzymać sms lub e-mail z fałszywym linkiem" – informuje swoich klientów Santander Bank Polska przesyłając jednocześnie scenariusz ataku, którego mogą stać się ofiarą. Jak wygląda typowy scenariusz przed którym ostrzega bank?

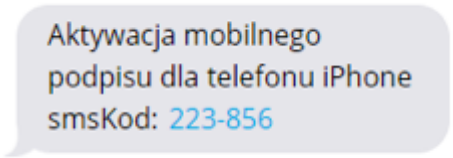
Krok 1 – czyli przygotowanie fałszywego e-maila lub wiadomości sms, który następnie przesyła do potencjalnych ofiar. Zazwyczaj jest to prośba o przesłanie niewielkiej kwoty za wykonanie usługi (np. dezynfekcję paczki czy dopłatę za jej dostarczenie) a w wiadomości „dla Waszej wygody" dodają link do bezpośredniej płatności.



Komunikat Santander Bank Polska

Krok 2 - jak nie trudno się domyśleć kliknięcie w taki link albo bezpośrednio infekuje urządzenie albo kieruje do podrobionej strony banku lub szybkich płatności. Bank radzi, aby zawsze sprawdzać adres strony logowania do banku z tym poprawnym.

Krok 3 – teraz już zaczyna się proces wyłudzania danych. Przestępca będzie starał wyciągnąć jak najwięcej informacji odnoszących się do konta ofiary tj. NIK (Numer Identyfikacyjny Klienta), hasło, kody autoryzujące różnych dyspozycji. „Cyberprzestępca chce dotrzeć do momentu, gdzie doda nowe urządzenie zaufane, na którym aktywuje mobilny podpis, tak aby móc wykonywać przelewy bez udziału właściciela rachunku" – przypomina bank.



Komunikat Santander Bank Polska

Santander przypomina o konieczności sprawdzania sms z autoryzacją – czego dotyczy dyspozycja i potwierdzenia wszystkich zawartych w nim danych. A co jeśli coś nam się nie zgadza? Przerwij transakcję i skontaktuj się z bankiem – przypomina Santander.

Wcześniej swoich klientów ostrzegał m.in. Bank Millennium. W krótkim oświadczeniu rozesłanym do klientów poinformowano o wykrytym nowym sposobie działań cyberprzestępców, którzy przejmowali środki finansowe poprzez pozyskanie od klientów informacji niezbędnych do aktywacji aplikacji mobilnej. O tym sposobie na wyłudzenia pisaliśmy tutaj.

Jeszcze we wrześniu, również Bank Millennium, otrzymał sygnały o jeszcze innym sposobie wyłudzeń - klienci odbierali połączenia od przestępców podszywających się pod pracowników banku, którzy dzwonili w sprawie rzekomych podejrzanych transakcji na koncie/karcie i prosili o podanie danych oraz zainstalowanie aplikacji QuickSupport, która umożliwiała zdalne sterowanie urządzeniem użytkownika.