Trusteer Rapport.

Szanowni Państwo, w ostatnim czasie pojawiły się doniesienia z innych banków o złośliwym oprogramowaniu infekującym telefony komórkowe użytkowników bankowości internetowej, które podszywa się pod oryginalny program zabezpieczający IBM®Security Trusteer Rapport™.(**bezpłatnie oprogramowanie IBM Security Trusteer Rapport. Rozwiązanie to chroni przed atakami złośliwego oprogramowania oraz wyłudzaniem poufnych danych – phishingiem.)**

Wirusem zostaje zainfekowany komputer**,** z którego przestępcy mogą przejąć wpisywane podczas procesu logowania zarówno identyfikator klienta jak i hasło. Po zalogowaniu, prezentowany jest fałszywy komunikat informujący o konieczności zainstalowania w telefonie komórkowym oprogramowania o nazwie **Trusteer Rapport**, rzekomo podnoszącego poziom bezpieczeństwa podczas korzystania z bankowości elektronicznej

Użytkownik w pierwszym kroku proszony jest o wskazanie systemu operacyjnego urządzenia: Dalej następuje prośba o wprowadzenie numeru telefonu, z jakiego klient korzysta akceptując transakcje w banku i na ten numer wysyłana jest wiadomość SMS zawierająca link do instalacji wspomnianego wyżej oprogramowania. Po zakończeniu instalacji (faktycznej infekcji urządzenia mobilnego), przestępcy mają możliwość przejęcia pełnej kontroli, a co za tym idzie również haseł SMS-owych niezbędnych do autoryzacji transakcji.

W przypadku zainstalowania w telefonie złośliwej aplikacji, zalecamy przywrócenie ustawień fabrycznych telefonu.

Prosimy nie pobierać i nie instalować oprogramowania z nieznanych źródeł! Zalecamy również wyłączenie w ustawieniach systemowych telefonu opcji dotyczącej możliwości instalacji oprogramowania z niezaufanych źródeł.

Przypominamy, że SK bank nigdy nie wymaga instalacji na urządzeniach mobilnych żadnego dodatkowego oprogramowania, zwłaszcza takiego, które miałoby podnosić poziom bezpieczeństwa wykonywanych operacji lub dostępu do serwisu transakcyjnego.