Podszywają się pod bank

Data publikacji: 11.03.2016 15:20

To kolejna taka próba wyłudzenia danych dostępu do kont bankowych. Tym razem oszuści wzięli na cel mBank. Wysyłają maile z informacją o blokadzie konta i fałszywym linkiem do strony logowania.

Kolejne maile o tytule „Blokada konta mBank", „Blokada rachunku mBank", „Weryfikacja w systemie mBank" lub „Nowa wiadomość mBank" pojawiły się na setkach skrzynek pocztowych w Polsce.

Przestępcy, pod pozorem zablokowania rachunku, zachęcają do odwiedzenia strony internetowej przypominającej stronę mBanku (zdjęcie główne artykułu, przykładowy mail oszustów poniżej artykułu). Kiedy przejdziemy na stronę podaną w mailu warto zwrócić uwagę, że połączenie z tą stroną nie jest szyfrowane, brakuje również poprawnego certyfikatu.

Pracownicy banku apelują, o ignorowanie takich wiadomości, nie wchodzenie na podane linki i nie wpisywanie na otwartej z takiego maila stronie żadnych danych. Jeśli już daliśmy się podejść oszustom, skontaktujmy się natychmiast z bankiem: ***- Jeśli otworzyłeś wiadomość od przestępców i kliknąłeś w link i/lub wpisałeś dane karty, jak najszybciej skontaktuj się z nami wysyłając mail na adres: alert@mbank.pl lub zadzwoń na mLinię 801 300 800, zmień hasła dostępu oraz zastrzeż kartę której dane podałeś! Jeżeli wprowadziłeś kody sms na fałszywej stronie sprawdź jakich operacji dotyczyły hasła i anuluj je.***

Kartę możesz również zastrzec samodzielnie w serwisie internetowym mBanku w zakładce „Moje Finanse" -> „Karty" -> „Zastrzeż kartę" wybierając z listy rozwijanej „Karta skradziona" i potwierdzając operację.

PRZYPOMINAMY!
mBank nigdy nie prosi o podawanie żadnych danych poufnych, w szczególności:
- nie żąda podawania haseł jednorazowych podczas logowania do serwisu transakcyjnego;
- nie prosi o podanie telekodu, danych kart płatniczych i kredytowych;
- danych dotyczących Twojego telefonu (takich jak numer, marka i model) w czasie logowania, sprawdzania stanu konta i przeglądania historii operacji;
- nie prosi o podanie kodu PIN do karty, aplikacji etc.;
- nie wysyła na telefon komórkowy żadnych certyfikatów bezpieczeństwa lub innych aplikacji do zainstalowania;
- nie wysyła do klientów wiadomości e-mail zawierających link do serwisu bankowości internetowej (czyli kierujących na stronę logowania do serwisu mBanku).

red.