Prawidłowe korzystanie z systemów bankowości internetowej chroni należycie Państwa środki na rachunkach bankowych.

Mając na uwadze należytą ochronę środków zgromadzonych na rachunkach zwracamy się z uprzejmą prośbą o zachowanie szczególnej staranności i ostrożności podczas korzystania z bankowości internetowej zwłaszcza w szczególnych przypadkach:

- nie należy wchodzić na stronę logowania do systemu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do banku;
- nie należy odpowiadać na żadne e-maile dotyczące weryfikacji Twoich danych (np. identyfikatora, hasła) lub innych ważnych informacji - bank nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej;
- zawsze przed logowaniem należy sprawdzić, czy adres strony banku rozpoczyna się od https://;
- należy zawsze przed logowaniem zweryfikować Certyfikat Bezpieczeństwa Banku (dla kogo został wystawiony oraz odcisk certyfikatu), którego szczegóły są dostępne poprzez kliknięcie na symbol kłódki w oknie przeglądarki;
- przed potwierdzeniem operacji SMS należy uważnie przeczytać SMS z kodem, aby upewnić się, że dotyczy on właściwego przelewu oraz czy numer rachunku na który wysyłane są środki jest zgodny ze zleceniem klienta;
- należy unikać przeklejania numerów rachunków (to jest używania funkcji: kopiuj / wklej, ctrl+c / ctrl+v, ctrl+insert / shift+insert), zalecane jest ich ręczne wpisywanie do zleceń w systemie bankowości internetowej albo o uważną kontrolę wklejanego numeru rachunku i porównanie tego numeru z oryginalnym, kopiowanym numerem rachunku;
- nie należy przesyłać mailem żadnych danych osobistych typu hasła, numery kart kredytowych, itp.;
- nie należy przechowywać nazwy użytkownika i haseł w tym samym miejscu oraz nie należy udostępniać ich innym osobom;
- należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach, u znajomych);
- należy na bieżąco aktualizować system operacyjny (Windows) oraz szczególnie narażone na ataki hakerskie oprogramowania, takie jak: przeglądarki internetowe, java, flash player oraz oprogramowanie do obsługi plików pdf;
- należy zawsze stosować oprogramowanie antywirusowe oraz zapory (firewall) i dbać o ich bieżącą aktualizację;
- instalując jakiekolwiek oprogramowanie na komputerze należy zachować szczególną ostrożność, a w szczególności nie należy instalować albo uruchamiać oprogramowania pochodzącego z niepewnych źródeł oraz stron internetowych;
- należy zawsze kończyć pracę korzystając z polecenia – Wyloguj;

W przypadku wątpliwości co do prawidłowego działania bankowości internetowej, należy niezwłocznie skontaktować się z Bankiem. Bank na Państwa wniosek dokona zmiany loginów do bankowości internetowej wszystkim osobom uprawnionym do rachunku oraz przekaże klientowi zalecenia, jakie powinien zrealizować. W celu niedopuszczenia do dalszych nieuprawnionych działań na rachunku należy:

- odłączyć od sieci i zabezpieczyć w niezmienionym stanie komputer z którego został wykonany nieuprawniony przelew, gdyż komputer ten stanowi zagrożenie dla pozostałych użytkowników sieci (jeśli tacy są), ponieważ istnieje prawdopodobieństwo, że jest na nim zainstalowane wrogie oprogramowanie umożliwiające przestępcom dostęp przez internet do tego komputera;
- wykonać kompleksowe sprawdzenie swojej sieci i pozostałych komputerów podłączonych do tej sieci pod kątem szkodliwego oprogramowania;
- zarządzić, aby wszyscy użytkownicy posiadający dostęp do bankowości internetowej zmienili hasło do logowania;
- zarządzić, aby wszyscy użytkownicy zmienili hasła do swoich lokalnych zasobów (systemy, maile, komputery, itd);
- złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa na policję i upoważnić Bank do przekazywania organom ścigania dokumentacji i informacji stanowiących tajemnicę bankową, które są niezbędne do wyjaśnienia okoliczności transakcji zrealizowanej z rachunku klienta, poprzez system bankowości elektronicznej.

W ostatnim czasie wiele publikuje się na temat stwierdzonych ataków hakerskich na rachunki klientów banków. Media informują, że wykryto liczne przypadki ataków hakerskich na rachunki klientów banków, korzystających z systemów bankowości internetowej. Polegają one na:

1) wyłudzeniu danych potrzebnych do przeprowadzenia transakcji w systemie bankowości internetowej poprzez przekierowanie do spreparowanej strony www kontrolowanej przez przestępcę, przypominającej graficznie stronę;
2) zainstalowaniu złośliwego oprogramowania, które po użyciu przez klienta funkcji kopiuj/wklej podmienia numer rachunku ze schowka na numerem rachunku należący do przestępców /wirus VBKlip/;
3) zainstalowaniu złośliwego oprogramowania, a następnie znalezieniu ciągu liczb, który odpowiada numerowi rachunku bankowego i zamianie go na numer rachunku podstawiony przez przestępców – dzieje się to w chwili, gdy klient stara się wykonać operację przelewu środków z poziomu systemu bankowości internetowej /wirus Banatrix/.

W ten sposób właśnie może dochodzić do skutecznych kradzieży środków z rachunków klientów.

Przypominamy, że przestrzeganie zasad korzystania z systemów bankowości internetowej chroni należycie Państwa środki na rachunkach bankowych