Biuletyn bezpieczeństwa bankowości internetowej

Bank DnB NORD Polska tworząc serwisy bankowości internetowych postawił przede wszystkim na zapewnienie maksimum bezpieczeństwa transakcji dokonywanych za ich pośrednictwem.
Bezpieczeństwo wynika z zastosowania nowoczesnych i sprawdzonych technologii informatycznych, które zapewniają skuteczną ochronę na wielu płaszczyznach, m.in. w komunikacji z bankiem, kontroli dostępu i autoryzacji transakcji.
Jednak bezpieczne systemy bankowe to nie wszystko, należy pamiętać również o zabezpieczeniu komputerów oraz atrybutów bezpieczeństwa wykorzystywanych w serwisie, ponieważ często okazuje się, że najsłabszym ogniwem systemu jest człowiek.
Co należy robić, aby czuć się bezpiecznie?

Pamiętaj o zabezpieczeniu swojego komputera

- Instaluj poprawki bezpieczeństwa, korzystaj z programów antywirusowych, uruchom program typu firewall.
- Na bieżąco aktualizuj bazy oprogramowania antywirusowego i bazy sygnatur oprogramowania antyszpiegowskiego. Regularnie (min. raz w tygodniu) uruchamiaj skany wykrywające wirusy i oprogramowanie szpiegujące.
- Do korzystania z systemu nie używaj komputerów publicznych (np. w kawiarenkach internetowych) - nie wiadomo, czy nie są zainfekowane.

Dbaj o atrybuty bezpieczeństwa

-Nie zapisuj i nie ujawniaj nikomu swojego identyfikatora ani hasła do systemu bankowości elektronicznej. Pamiętaj, że żaden pracownik Banku nie poprosi Cię o podanie hasła do systemu bankowości elektronicznej.
-Tworząc hasło pamiętaj, że nie może być ono zbyt łatwe. Dla łatwiejszego zapamiętywania stwórz swój osobisty algorytm układania haseł - wymyśl jakieś zdanie i ze skrótów stwórz skomplikowane hasło.

Każdorazowo sprawdzaj czy nawiązałeś bezpieczne połączenie z Bankiem

-Zawsze wprowadzaj adres systemu bankowości ręcznie. Pamiętaj, że korzystanie z odnośników zamieszczonych w treści wiadomości email lub na stronach internetowych nie należących do banku, wskazujących na serwis bankowości internetowej, wiąże się z potencjalnym ryzykiem przekierowania połączenia użytkownika do podstawionego serwisu, udającego serwis banku.
-Zawsze sprawdzaj, czy łączysz się z odpowiednią stroną.

-Sprawdzaj, czy połączenie na pewno jest realizowane w „https”.

-Po zestawieniu kanału szyfrowanego powinna pojawić się ikona zamkniętej kłódki w pasku stanu przeglądarki internetowej.

-Ostatecznym potwierdzeniem tego, że połączenie zostało nawiązane do właściwego, zaufanego serwera jest weryfikacja autentyczności i ważności certyfikatu banku (kliknij na ikonę zamkniętej kłódki). Jeśli widzisz jakikolwiek problem z certyfikatem skontaktuj się z Bankiem.

-Nie podawaj danych uwierzytelniających, dopóki nie masz pewności, że odwołujesz się do zaufanego serwisu banku.

-Po zalogowaniu do systemu bankowości internetowej należy zweryfikować datę ostatniego udanego logowania. Wszelkie wzbudzające wątpliwości przypadki niezgodności dat należy zgłaszać do Banku.

-W czasie trwania połączenia z bankiem nie wolno pozostawiać komputera bez nadzoru. Sesję należy zamknąć przez poprawne wylogowanie się i późniejsze zamknięcie okna przeglądarki internetowej.

-Nie korzystaj z odnośników zamieszczonych w treści wiadomości email lub na stronach internetowych nie należących do banku, rzekomo wskazujących na serwis bankowości internetowej.

-Jeśli łączenie z bankiem zostało nawiązane z nieznanego komputera należy przed zamknięciem okna przeglądarki wyczyścić jej bufor plików tymczasowych i cookies.