Szanowni Państwo,

wiedza o bezpiecznym korzystaniu z bankowości elektronicznej jest ważnym czynnikiem ograniczającym zagrożenia występujące w tym obszarze. Świadomość użytkownika oraz rozwaga w korzystaniu ze współczesnych zdobyczy elektroniki i wymagana czujność, to poza zabezpieczeniami technicznymi stosowanymi przez Bank, nieodzowne elementy w budowaniu bezpiecznych standardów korzystania z systemów bankowości elektronicznej. Chcąc zapewnić Państwu komfort bezpieczeństwa, poprzez świadome ograniczanie najbardziej typowych zagrożeń w bankowości elektronicznej, oddajemy do Państwa dyspozycji krótki przewodnik po najważniejszych zasadach bezpieczeństwa. Zachęcamy do zapoznania się z nimi i stosowania ich w praktyce, gdyż działania zabezpieczające Banku tylko wespół z czujnością użytkownika mogą tworzyć pożądany stan bezpieczeństwa.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

1. Prawidłowy adres serwisu bankowości elektronicznej

Weryfikuj poprawność wpisywanego adresu strony www i sprawdź, czy połączenie z Bankiem jest szyfrowane (adres powinien zaczynać się od https:// oraz posiadać symbol kłódki). Nie otwieraj strony serwisu transakcyjnego Banku poprzez link z wiadomości e-mail lub wyszukiwarki internetowej. Przestępcy mogą podrabiać adresy. Korzystaj z przycisku logowania na stronie www.bs.gniezno.pl lub loguj się bezpośrednio pod adresem: https://www.bs24gniezno.pl dla systemu eBankNet oraz https://ebiznes.bs24gniezno.pl dla systemu eCorpoNet. Jeżeli korzystasz z systemu eBankNet na smartfonie lub tablecie (system moBankNet) to właściwym adresem jest: https://m.bs24gniezno.pl. Zawsze dokonuj wylogowania z systemu bankowości elektronicznej używając odpowiedniego przycisku.

2. Uważaj na podejrzane wiadomości e-mail

Nie otwieraj podejrzanych wiadomości e-mail i załączników, np.: z informacją o przesyłce kurierskiej, z informacją o fakturze, z informacją o wszczęciu procedury windykacyjnej, z załączonym zdjęciem od nieznanego nadawcy. Weryfikuj adres nadawcy i odbiorcy. Uważaj na umieszczone w wiadomościach linki. Otwarcie załącznika pochodzącego z podejrzanej wiadomości lub kliknięcie na linka, może zainfekować Twoje urządzenia wirusem komputerowym. Jest bardzo prawdopodobne, że program antywirusowy nie uchroni Państwa od takich zagrożeń.

3. Zaufane urządzenia i bezpieczna sieć

Z systemów bankowości elektronicznej korzystaj tylko na sprawdzonych urządzeniach, unikaj logowania z cudzych komputerów, tabletów i telefonów. Logując się do systemów bankowości elektronicznej, korzystaj tylko z zabezpieczonych i znanych Tobie sieci internetowych. Nie loguj się do systemów z sieci otwartych np. w kawiarniach, na dworcach. Stosuj zasadę ograniczonego zaufania.

4. Legalne i aktualne oprogramowanie, program antywirusowy

Twoje urządzenie musi mieć aktualne i legalne oprogramowanie: system operacyjny, przeglądarkę internetową oraz program antywirusowy. Przestępcy wykorzystują luki w oprogramowaniu. Aktualizacje legalnego oprogramowania często zabezpieczają przed działaniami cyberprzestępców.

5. Uważnie czytaj autoryzacyjne komunikaty SMS

Zawsze i bardzo uważnie czytaj komunikaty SMS dotyczące potwierdzenia transakcji. Podane w wiadomości informacje o czynności, numerze rachunku odbiorcy i kwocie muszą zgadzać się ze zlecanymi przez Ciebie w serwisie transakcyjnym. Zwracaj uwagę na treść komunikatu SMS z Banku, nawet jeśli wykonujesz transakcje bardzo często.

6. Chroń środki uwierzytelniające

Środki uwierzytelniające (takie jak loginy, hasła, listy haseł jednorazowych, karty zdrapki, tokeny) przechowuj w bezpiecznym miejscu, aby osoby nieupoważnione nie miały do nich dostępu. Unikaj zapisywania haseł do systemu, ustalone przez Ciebie hasło powinno być trudne i składać się z kombinacji dozwolonych znaków (małych i wielkich liter, cyfr i znaków specjalnych). Hasło do systemu bankowości elektronicznej Banku nie powinno być wykorzystywane do innych celów. Pamiętaj o częstej zmianie hasła oraz o tym, że nie wolno go udostępniać innym osobom. Nigdy nie przechowuj razem loginów, haseł oraz środków autoryzacyjnych takich jak listy haseł jednorazowych czy też karty zdrapki.

7. Wsparcie dla użytkowników

W razie jakichkolwiek pytań lub wątpliwości skontaktuj się telefonicznie z Bankiem w godz. od 7.00 do 18.00 w dniach roboczych na numer 614240821 lub za pomocą poczty elektronicznej na adres security@bs.gniezno.pl lub bezpośrednio z placówką Banku.