ZASADY BEZPIECZNEGO KORZYSTANIA Z ELEKTRONICZNYCH KANAŁÓW DOSTĘPU

https://online.bsczluchow.pl, Aplikacja mobilna Nasz Bank, Aplikacja mobilna SGB Mobile

W trakcie korzystania z bankowości internetowej konieczne jest przestrzeganie zasad bezpieczeństwa, które zawarte są w instrukcjach użytkownika elektronicznych kanałów dostępu.

W niniejszym dokumencie opisane zostały niektóre z koniecznych warunków zachowania bezpieczeństwa podczas internetowej obsługi rachunku:

1. **Uważnie czytaj** korespondencję bankową.
2. **Zawsze loguj się do systemu bankowości elektronicznej poprzez stronę: https://online.bsczluchow.pl** – nigdy nie otwieraj strony logowania bankowości elektronicznej Twojego banku z linku otrzymanego w wiadomości poczty elektronicznej lub SMS.
3. **Sprawdzaj**, czy adres strony do logowania jest adresem bankowości elektronicznej Twojego banku, czy rozpoczyna się od https:// oraz czy połączenie z bankiem jest szyfrowane (obok paska adresowego musi być widoczny symbol zamkniętej kłódki). Sprawdzaj autentyczność certyfikatu postępując zgodnie z zasadami opisanymi w instrukcji użytkownika elektronicznego kanału dostępu.
4. **Po zalogowaniu się do usług bankowości elektronicznej nie pozostawiaj urządzenia bez nadzoru oraz pamiętaj o wylogowaniu się.**
5. Nie podawaj danych logowania do bankowości elektronicznej przez e-mail/telefon – Bank nigdy nie prosi klienta o login i hasło do konta internetowego, ani telefonicznie, ani mailowo – Bank wymaga hasła weryfikującego tożsamość klienta w kontakcie telefonicznym, nigdy hasła do konta internetowego klienta.
6. **Bank w celu skorzystania przez klienta z usług bankowości elektronicznej nie prosi o potwierdzenie hasła, numeru karty, loginu ani numeru telefonu oraz o zainstalowanie dodatkowych aplikacji bezpieczeństwa na urządzeniu klienta.**
7. **Zabezpiecz komputer i telefon** – Ostrożnie korzystaj z urządzeń, do których dostęp mają również inne osoby. Zadbaj, aby używane oprogramowanie pochodziło z legalnego i zaufanego źródła. Wszystkie urządzenia, na których logujesz się do bankowości elektronicznej powinny być odpowiednio chronione poprzez:
   1) legalne Systemy Operacyjne, które są na bieżąco aktualizowane,
   2) na bieżąco aktualizowane programy antywirusowe, które zabezpieczą sprzęt przed wirusami (jest wiele darmowych i legalnych programów antywirusowych, m.in.: Avira, Avast, AVG),

3) włączoną zaporę sieciową,
4) przeglądarki internetowe (Firefox, Google Chrome, Microsoft Edge - nie instaluj podejrzanych pluginów - wtyczek do przeglądarki),

8. Śledź doniesienia o bezpieczeństwie wykorzystywanego przez Ciebie rodzaju urządzenia oraz na bieżąco instaluj wszelkie aktualizacje oraz poprawki bezpieczeństwa systemu operacyjnego.

9. Nie zdejmuj fabrycznych zabezpieczeń systemu operacyjnego.

10. Nie otwieraj podejrzanych załączników wiadomości poczty elektronicznej i SMS oraz zamieszczonych w tych wiadomościach odnośników (hiperlinków), na urządzeniach które wykorzystujesz do usług bankowości elektronicznej.

11. Nie korzystaj na urządzeniach, na których logujesz się do bankowości elektronicznej z oprogramowani typu TeamViewer lub Anydesk, które pozwalają na pracę na zdalnym pulpicie. Bank, w celu ochrony Twoich środków może, wykrywając, że korzystasz z tego typu oprogramowania, zablokować wszystkie kanały dostępu do bankowości elektronicznej.

12. Sprawdzaj datę ostatniego logowania do bankowości elektronicznej – zwracaj uwagę na informację, która pojawia się na internetowym rachunku i sprawdź, czy wtedy naprawdę korzystałeś z konta. Jeśli nie – niezwłocznie zablokuj dostęp do systemu bankowości elektronicznej za pośrednictwem bankowości elektronicznej, aplikacji mobilnej Nasz Bank lub usługi BANKOFON (odblokowanie kanału odbywa się w ten sam sposób) lub powiadom o tym Bank i najszybciej jak to tylko możliwe –zmień hasło.

13. Jeśli otrzymasz komunikat o błędnym logowaniu i zostaniesz poproszony o podanie kodu autoryzacyjnego transakcji, zaniechaj dalszych działań i pilnie skontaktuj się z Bankiem.

14. Stwórz silne, unikalne hasło do konta – hasło do bankowości elektronicznej powinno być jedyne w swoim rodzaju: długie oraz składające się z wielkich i małych liter, cyfr i znaków specjalnych. Nie powinno być to hasło, którego używamy przy innych okazjach ani słowo, czy ciąg znaków zbyt proste do odgadnięcia.

15. Zadbaj o zachowanie poufności swojego hasła –nie udostępniaj hasła osobom trzecim oraz na żadnych stronach internetowych ani pocztą elektroniczną, czy komunikatem SMS. **Nie zapisuj hasła na komputerze i nie zgadzaj się, aby przeglądarka je pamiętała**. W razie podejrzenia, że hasło zostało ujawnione, natychmiast je zmień i zablokuj dostęp do usług bankowości elektronicznej za pośrednictwem systemu elektronicznego kanału dostępu (najszybsza forma blokady), kontaktując się z Bankiem lub za pośrednictwem BANKOFONU .

16. Pamiętaj: Zapisanie przeglądarki i urządzenia jako zaufane jest akceptacją regulaminu i umożliwi logowanie się z tego urządzenia bez stosowania metod silnego uwierzytelnienia tj. kod+SMS, autoryzacja mobilna.

17. **Cyklicznie zmieniaj hasło do logowania** w systemie bankowości elektronicznej i nie używaj tego samego hasła do wielu usług (np. poczty elektronicznej oraz bankowości elektronicznej).
18. **Weryfikuj kody SMS** – cyberprzestępcy dysponujący Twoim rachunkiem do potwierdzenia operacji potrzebują kodu z SMS (jeżeli nie korzystasz z formy uwierzytelniania w aplikacji mobilnej). Przed potwierdzeniem transakcji zawsze weryfikuj zgodność numeru konta, na które przelewasz środki pieniężne z numerem rachunku odbiorcy oraz numerem, który jest w kodzie potwierdzającym transakcję, przekazanym z wykorzystaniem SMS. Sprawdzaj zgodność kwoty złożonej przez Ciebie dyspozycji z kwotą wskazaną w potwierdzeniu przesłanym w wiadomości SMS.
19. Korzystaj z usług bankowości elektronicznej wyłącznie ze znanych i zaufanych urządzeń oraz zaufanej sieci internetowej. Korzystaj z bezpiecznych sieci WI-FI – otwarte sieci bezprzewodowe to spore ryzyko.
20. **Jeśli masz wrażenie, że wygląd strony do bankowości elektronicznej różni się od dotychczasowej – przerwij korzystanie z serwisu (wyloguj się i niezwłocznie powiadom Bank).**
21. **Włącz powiadomienia SMS** lub **zainstaluj aplikację mobilną** i włącz powiadomienia push jako metodę autoryzacji operacji– dodatkowe wiadomości SMS od Banku lub komunikaty wysyłane za pośrednictwem aplikacji mobilnej, które informują np. o zmianach na rachunku, nieudanym logowaniu (aplikacja mobilna) itp. Jeśli chcesz mieć pełną kontrolę nad kontem i tym, co się na nim dzieje włącz taką usługę – jeśli coś dziwnego zacznie dziać się na Twoim rachunku, szybko to zauważysz i będziesz mógł odpowiednio szybko zareagować. Za pośrednictwem komunikatów z aplikacji mobilnej lub powiadomień SMS otrzymujesz informacje o logowaniu się do bankowości elektronicznej (również z zagranicy), zrealizowanej transakcji, czy też wypłacie z bankomatu.
22. **Dbaj o bezpieczeństwo swojego telefonu** – korzystaj z opcji blokady ekranu oraz zaznacz w telefonie opcję pozwalająca na instalację aplikacji tylko z zaufanych źródeł.
23. **Zmień obrazek bezpieczeństwa w bankowości elektronicznej** - w prawym górnym rogu znajduje się ikona z obrazkiem. Klikając na nią w pozycji „Moje Dane" zaznaczasz –„zmień", wybierając 1 z 18 obrazków. Zapamiętaj, który z obrazków wybrałeś. W czasie kolejnych logowań sprawdź czy w prawym górnym rogu znajduje się wybrany przez Ciebie obrazek bezpieczeństwa. Jest to dodatkowa weryfikacja sprawdzająca: czy zalogowałeś się do Banku, czy na podstawioną stronę osoby niepowołanej.
24. **Sprawdzaj dane przelewu** - przed realizacją przelewu, zawsze sprawdzaj dane transakcji, ze szczególnym naciskiem na numer rachunku bankowego (NRB) odbiorcy płatności.

    Sprawdzaj poprawność w/w numeru po zaakceptowaniu płatności (przelew oczekuje na realizacje przez okres ok. 5 minut – zakładka „przelewy

oczekujące") - możesz w porę usunąć przelew jeśli stwierdzisz, że numer został podmieniony.

25. **Korzystaj z przelewów zdefiniowanych -** jeżeli wykonujesz przelewy cyklicznie (np. co miesiąc), wprowadź do systemu przelewy zdefiniowane. Utworzenie przelewu zdefiniowanego oraz jego późniejsza modyfikacja autoryzowane są PINem wywołanym przez system w chwili zatwierdzenia danych do przelewu, tj. wprowadzenia nr NRB i nazwy odbiorcy płatności (beneficjenta). Późniejsza realizacja przelewu nie będzie wymagać autoryzacji, jedynie w pierwszym tygodniu- licząc od dnia pierwszej realizacji przelewu, każdy przelew będzie musiał być potwierdzony hasłem autoryzującym. Dla potwierdzenia zmian wprowadzonych w danych odbiorcy przelewu, otrzymasz każdorazowo SMS z kodem autoryzującym wprowadzone zmiany (w przypadku wyboru takiej formy autoryzacji) lub jeżeli korzystasz z aplikacji mobilnej otrzymasz powiadomienie push. Jeżeli zmiana danych będzie wywołana bez twojej wiedzy, bardzo szybko się o tym dowiesz odczytując wiadomość SMS lub powiadomienie w aplikacji mobilnej– w takiej sytuacji powinieneś niezwłocznie zablokować dostęp do systemu bankowości elektronicznej w bankowości elektronicznej, za pośrednictwem usługi BANKOFON lub powiadomić o tym Bank i najszybciej jak to tylko możliwe - zmienić hasło. Cyklicznie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie.

26. Mając na rachunku środki pieniężne w kwocie wyższej niż aktualnie są potrzebne i nie planując w najbliższym czasie ich zadysponowania - zakładaj lokaty, , wpłacaj środki na konto oszczędnościowe – z pewnością w większym stopniu zabezpieczy to środki w sytuacji zagrożenia komputera przed działaniem ewentualnych przestępców, niż utrzymywanie ich na jednym rachunku (lokaty możesz założyć również przez Internet).

27. **Ustaw limity dla transakcji –** możesz samodzielnie określić i zmieniać maksymalny limit dla transakcji realizowanych za pośrednictwem systemu (np. 1 000,00 zł, 3 000,00 zł).Utrzymanie na stałe niższych limitów i zwiększanie ich tylko w razie potrzeby na określony czas, pozwoli zminimalizować ryzyko ewentualnych strat spowodowanych skutecznym atakiem hakerskim.

28. **Transakcje oszukańcze, podejrzane zdarzenia i nietypowe sytuacje występujące w trakcie sesji usług internetowych lub potencjalnych prób zastosowania technik manipulacji mających na celu pozyskanie informacji, należy zgłaszać do Banku pod numer telefonu:**

(59) 83 43 287 lub 83 42 472 lub 800 888 888, z zagranicy +48 61 647 28 46

PAMIĘTAJ:

Za bezpieczeństwo środowiska, na którym pracuje program, odpowiada klient (użytkownik systemu)