Zasady bezpiecznego korzystania z plusbank24

1. Z serwisu plusbank24 korzystaj przy użyciu zaufanych urządzeń. W szczególności unikaj korzystania z urządzeń co do których nie masz pewności, że spełniają poniższe zasady

Logując się do serwisu transakcyjnego plusbank24 zawsze wpisuj w pasku adresu przeglądarki https://plusbank24.pl lub wchodź do serwisu poprzez link umieszczony na oficjalnej stronie https://plusbank.pl.

Przed zalogowaniem upewnij się, że połączenie jest szyfrowane - adres strony logowania, powinien zaczynać się od https, a nie http. Odszukaj na stronie znaczek kłódki, aby potwierdzić, że strona posiada ważny certyfikat wystawiony dla PLUS BANK S.A. dla strony „plusbank24.pl". Certyfikat bezpieczeństwa potwierdza poprawność szyfrowanego połączenia. Zaletą rozszerzonego certyfikatu jest jednoznaczne zidentyfikowanie podmiotu certyfikatu, na rzecz którego certyfikat został wystawiony „plusbank24.pl" Przed logowaniem należy zwracać uwagę, czy pole to prezentuje właściwą nazwę.

Wszystkie operacje w plusbank24 są automatycznie zabezpieczane protokołem szyfrowania.

Podobne zasady ograniczonego zaufania stosuj w przypadku innych serwisów, które pozyskują dostęp do Twoich danych osobowych tj. poczta e-mail, portale społecznościowe, systemy płatności online.

2. Stosuj zasadę ograniczonego zaufania w przypadku wiadomości od nieznanych nadawców i/lub w przypadku otrzymania nieoczekiwanej przesyłki e-mailowej. Gdy otrzymasz e-mailem link do logowania lub jakikolwiek odnośnik nigdy nie uruchamiaj i nie wprowadzaj danych do logowania. Unikaj otwierania nieznanych plików załączonych do tego typu wiadomości.

Pamiętaj, że Bank nigdy nie prosi o przesłanie pocztą Twoich danych osobowych (np. Identyfikator, Alias, hasło, pesel, itp.) ani też żadnych innych ważnych, wrażliwych informacji. W szczególności nie odpowiadaj na e-maile dotyczące prośby o weryfikację Twoich danych. Bank nie wykorzystuje poczty elektronicznej do kontaktu w celach weryfikacji. Bank jedynie może wysłać informacje, biuletyny lub informacje o promocjach pod warunkiem, iż wyraziłeś zgodę na otrzymywanie tego typu materiałów.

3. Zawsze miej zainstalowane oprogramowanie, które zabezpiecza Twój komputer, z którego wykonujesz operacje bankowości internetowej, instaluj tylko legalne oprogramowanie, oraz regularnie instaluj wszystkie poprawki zalecane przez producenta stosowanego przez Ciebie oprogramowania. Oprogramowanie pobieraj z legalnych i oficjalnych źródeł.

4. Podczas logowania Bank nigdy nie prosi o podanie innych danych niż Identyfikator lub Alias (jeżeli go nadałeś) i hasło. Tylko w przypadku pierwszego logowania lub nowych danych dostępowych potrzebna jest jeszcze data urodzenia. Dodatkowo możesz ustawić opcję

logowania z autoryzacją kodem SMS. W takiej sytuacji system poprosi o podanie przesłanego przez Bank jednorazowego hasła SMS. Jeżeli masz ustawiony obrazek bezpieczeństwa, to powinien się on pojawić w procesie logowania.

5. Stosuj skomplikowane hasła, różne od tych jakie wykorzystujesz w innych serwisach niż do łączenia się z systemem bankowości elektronicznej.
Ze względów bezpieczeństwa zalecamy, aby hasło do kanałów Internet oraz Telefon/SMS nie było wykorzystywane do innych usług lub logowań do innych serwisów. Przy okresowej zmianie hasła, staraj się nie powielać nadanego wcześniej kodu, ale użyć zupełnie nowej kombinacji cyfr, dużych i małych liter oraz znaków specjalnych.

6. W przypadku 5-krotnego podania błędnego hasła do logowania do kanału Internet lub Telefon lub SMS hasło zostanie automatycznie zablokowane. Ponowne nadanie nowych haseł będzie możliwe dopiero po skontaktowaniu się z Bankiem.

7. Po zakończeniu pracy w plusbank24 wyloguj się z aplikacji używając przycisk *Wyloguj*. Zapewnia to bezpieczne opuszczenie sesji. W trakcie korzystania z serwisu transakcyjnego plusbank24 nie odchodź od komputera, bez wylogowania się.

8. Używając serwisu plusbank24 korzystaj tylko z jednego okna przeglądarki internetowej. Wspieramy i zalecamy korzystanie z naszego serwisu przy pomocy najnowszej wersji przeglądarki:

- Microsoft Edge ,
- Mozilla Firefox,
- Opera,
- Chrome,
- Safari.

Ze względów bezpieczeństwa podczas korzystania z bankowości internetowej plusbank24.pl należy używać najnowszej dostępnej wersji zalecanej przeglądarki. Korzystanie z innych przeglądarek lub wskazanych przeglądarek internetowych, ale w niższej wersji nie jest zalecane ze względów bezpieczeństwa oraz poprawności działania plusbank24. Zalecamy dokonywanie aktualizacji przeglądarki zgodnie z proponowanymi wewnętrznymi mechanizmami aktualizacji danej przeglądarki, które same przypominają o dostępności nowej wersji. Jednocześnie jest to najbezpieczniejsza metoda przeprowadzenia aktualizacji zmniejszająca potencjalne ryzyko uzyskania aktualizacji z nieautoryzowanego źródła.

9. W trakcie korzystania z naszego serwisu nie używaj przycisków nawigacyjnych przeglądarki takich jak dalej, wstecz, odśwież, zatrzymaj. Użycie ich może spowodować przerwanie sesji i wylogowanie z serwisu. plusbank24 jest wyposażony we wszystkie niezbędne przyciski nawigacyjne, zapewniając wygodne poruszanie się po serwisie.

10. Kluczowe czynności wykonywane w serwisie plusbank24, takie jak przelewy są zabezpieczone dodatkową autoryzacją. Zawsze weryfikuj czy dane potwierdzające autoryzację

w otrzymanym SMSie są zgodne z danymi na ekranie w plusbank24. Czas ważności kodu SMS to 10 minut. Jeżeli podczas autoryzacji czynności 5-krotnie błędnie podałeś wynikający z metody autoryzacji kod, metoda autoryzacji zostanie zablokowana. Odblokowanie metody autoryzacji będzie możliwe dopiero po skontaktowaniu się z Bankiem.

11. Nie udostępniaj swojego nr Identyfikatora, Aliasu oraz haseł osobom trzecim, nawet Pracownikom naszego Banku. W przypadku ujawnienia Identyfikatora, Aliasu lub haseł osobom trzecim, natychmiast skontaktuj się z Bankiem. Hasła do kanałów Internet, Telefon/SMS możesz samodzielnie zmienić lub zablokować w aplikacji plusbank24.

12. Stosuj zasadę ograniczonego zaufania do publicznych sieci WiFi. Tego typu połączenia mogą nie posiadać odpowiednich zabezpieczeń chroniących Twoje dane lub wręcz specjalnie gromadzić je bez Twojej wiedzy. W miarę możliwości powinno się używać własnego dostępu do Internetu tj. modem GSM/LTE.

13. Zwracaj uwagę i czytaj komunikaty prezentowane na stronach systemu plusbank24 jak również otrzymywane w trakcie realizacji transakcji smsy w tym potwierdzenia operacji. Otrzymane wiadomości powinny prezentować stan oczekiwany np. numer rachunku odbiorcy czy kwota operacji powinny się zgadzać ze zlecanym przez Ciebie. Również typ operacji powinien odpowiadać czynności aktualnie realizowanej przez Ciebie w systemie bankowości.

14. Zwracaj uwagę na nietypowe zachowanie sprzętu wykorzystywanego do pracy z systemem plusbank24 np. wyskakujące reklamy lub inne nietypowe zachowania mogące świadczyć o funkcjonowaniu oprogramowania szkodliwego na urządzeniu. W przypadku zidentyfikowania takich symptomów powinno się ograniczyć wykorzystanie takiego sprzętu do logowania do systemu plusbank24 do czasu usunięcia zagrożenia lub potwierdzenia jego braku.

15. Ograniczaj fizyczny dostęp osób postronnych do urządzeń stosowanych do korzystania z plusbank24.

16. Bezpieczne środowisko:

Pełne bezpieczeństwo wynika z bezpiecznego współdziałania zarówno Banku jak i Klienta. Oferowane mechanizmy ochrony wymagają uważnego, świadomego i konsekwentnego stosowania. Podobnie jak Bank odpowiada za programy monitorujące bezpieczną prace systemu, Klient odpowiada za stosowanie relatywnych systemów zainstalowanych w swoim komputerze. Bezpieczeństwo działania systemu zależne jest w dużej mierze od roztropności i zapobiegliwości klienta.

17. Klient Systemu Bankowości elektronicznej powinien stosować

- oryginalny, zaktualizowany system operacyjny oraz przeglądarkę,
- skuteczny program antywirusowy z aktualną bazą zagrożeń
- program typu "firewall”

Program antywirusowy - aktualizowany zgodnie z zaleceniami producenta - w trybie ciągłego monitoringu chroni komputer przed działaniem szkodliwego oprogramowania (wirusy, robaki internetowe, trojany), program "firewall" natomiast monitoruje ruch przychodzący i wychodzący pomiędzy komputerem a otoczeniem (Internet, sieć korporacyjna). Bezwzględnie powinniśmy stosować się do zaleceń producentów wybranych programów. Zalecamy regularne zabezpieczanie swojego oprogramowania, w tym systemu operacyjnego i przeglądarki. Krytyczne znaczenie ma instalacja aktualnych poprawek (ang. patch) publikowanych najczęściej na stronach producentów danego oprogramowania.

18. Plus Bank nigdy nie prosi o podawanie żadnych danych osobowych, poufnych, w szczególności:

- przesłanie wiadomością SMS/emailem kodu PIN do karty;
- potwierdzenia transakcji/wpłaty na tzw. numery Premium (numerów o podwyższonej opłacie) typu 7XX, 7XXX, 7XXXX, 9XXX, 9XXXX etc.
- nie żąda podawania haseł jednorazowych podczas logowania do serwisu transakcyjnego;
- nie prosi o podanie żadnego telekomu czy też danych do kart płatniczych i kredytowych;
- nie prosi o podanie kodu PIN do karty, aplikacji etc.;
- nie wysyła na telefon komórkowy innych aplikacji do zainstalowania czy też żadnych certyfikatów bezpieczeństwa lub linków;
- nie wysyła do klientów wiadomości e-mail zawierających link do serwisu bankowości internetowej (czyli kierujących na stronę logowania do serwisu Plus Banku) ani też do innych stron.

WAŻNE!

O każdej podejrzanej sytuacji zaobserwowanej podczas korzystania z serwisu transakcyjnego lub aplikacji mobilnej plusbank24 powiadom Bank:

- **wysyłając wiadomość** na adres bezpieczenstwo@plusbank.pl
- **kontaktując się z Centrum Obsługi Klienta** pod numerami telefonów: 801 44 55 66 lub +48 61 8 461 461. Opłata wg. stawek operatora.
  Centrum Obsługi Klienta dostępne jest od poniedziałku do soboty w godz. 8.00 - 21.00.
- **Informując pracownika Banku**.
  Lista Placówek partnerskich https://plusbank.pl/placowki-i-bankomaty