BANK SPÓŁDZIELCZY W ZALESZANACH
Grupa BPS

„Ważna informacja o blokadzie kart w związku z incydentem bezpieczeństwa u operatora”

Szanowny Kliencie,

w związku z incydentem bezpieczeństwa, o którym poinformowały organizacje płatnicze Visa i Mastercard, do którego doszło w systemach informatycznych jednego z operatorów płatniczych, przekazujemy informacje o możliwym ryzyku oraz działaniach podjętych w celu ochrony naszych klientów.

Operator płatniczy, będący odrębnym od Banku Spółdzielczego w Zaleszanach administratorem danych, zablokował nieuprawniony dostęp do swoich systemów oraz wdrożył dodatkowe zabezpieczenia.

Jakie dane mogły zostać ujawnione?

- *adresy zamieszkania i adresy e-mail,*
- *numery telefonów,*
- *adresy IP,*
- *informacje dotyczące kart płatniczych.*

Co zrobiliśmy, aby chronić Twoje środki?

W trosce o bezpieczeństwo Twoich środków zablokowaliśmy kartę płatniczą, której mógł dotyczyć incydent. Blokada dotyczy wyłącznie karty, a nie Twojego rachunku bankowego. Nadal masz dostęp do pieniędzy na swoim koncie.

Co zrobić po otrzymaniu nowej karty plastikowej?

- *aktywuj kartę;*
- *dodaj ją ponownie do portfela cyfrowego w telefonie lub zegarku (tokenizacja);*
- *zaktualizuj dane karty w serwisach, w których opłacasz subskrypcje, np. Netflix lub Spotify;*
- *sprawdź, czy płatności cykliczne są realizowane prawidłowo.*

Pamiętaj, że zablokowanie karty nie oznacza automatycznego anulowania subskrypcji.

Po otrzymaniu i aktywacji nowej karty plastikowej możesz dalej dokonywać płatności.

Czy Twoje pieniądze są bezpieczne?

Samo ujawnienie danych nie oznacza utraty pieniędzy. Istnieje jednak ryzyko wykorzystania tych informacji przez oszustów, np. podczas prób wyłudzenia danych przez telefon, SMS lub e-mail.

Dlatego zachowaj szczególną ostrożność i nie udostępniaj nikomu haseł, kodów PIN ani kodów autoryzacyjnych.

Jak możesz dodatkowo zadbać o bezpieczeństwo?

<u>Zalecamy:</u>

- *zastrzeżenie numeru PESEL i włączenie powiadomień o jego wykorzystaniu;*
- *zmianę haseł do poczty elektronicznej i innych serwisów, w których używasz tych samych danych logowania;*
- *zachowanie ostrożności wobec podejrzanych telefonów, wiadomości SMS i e-maili;*
- *niezwłoczny kontakt z Bankiem w przypadku zauważenia podejrzanej transakcji.*

Jeżeli skontaktuje się z Tobą nieznana osoba, powołując się na incydent, zakończ rozmowę i samodzielnie skontaktuj się z Bankiem, korzystając z oficjalnego numeru telefonu.”