Getin Noble Bank S.A.
ul. Przyokopowa 33
01-208 Warszawa
Infolinia +48 (22) 203 03 01
Internet www.noblebank.pl

Bezpieczne płatności

1. Nie należy podawać informacji o karcie na stronach, które nie są zaufane. Adres strony przez którą dokonuje się płatności powinien zaczynać się od HTTPS i mieć symbol kłódki, co oznacza, że połączenie jest szyfrowane. Warto uważnie czytać pojawiające się w przeglądarce komunikaty o zagrożeniach. Nie wolno ignorować ostrzeżeń o błędnym lub nieważnym certyfikacie i koniecznie powinno sięzachować ostrożność. Dwukrotne kliknięcie na symbol kłódki umożliwia wyświetlenie informacji o certyfikacie (np. data ważności i dla kogo został wystawiony).

2. Należy zachować ostrożność przy przekazywaniu numeru karty telefonicznie. Nie należy udostępniać numeru karty nikomu, kto dzwoni prosząc przez telefon o numer karty płatniczej. Jeżeli połączenie inicjujemy samodzielnie, również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

3. Nie należy odpowiadać na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie. Nigdy nie należy odpowiadać na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywany „phishingiem".

4. Nie wolno zapisywać kodu PIN na karcie, ani przechowywać go razem z kartą.

5. Numer karty i inne poufne kody umożliwiające dokonane transakcji należy chronić. Przestępcy mogą próbować wejść w posiadanie numeru PIN, numeru CVV2 lub CVC2 (ostatnie trzy cyfry numeru umieszczonego na pasku do podpisu na odwrocie karty), rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznych, kamerą video lub w inny sposób.

6. Zawsze trzeba dokładnie sprawdzać, czy informacje zawarte w SMSie autoryzacyjnym są zgodne z danymi transakcji. Szczególnie zwróć uwagę czy zgadza się numer rachunku oraz kwota transakcji. Jeżeli urządzenie zostało zainfekowane wirusem może on spowodować, że dane transakcji zostaną podmienione na inne. Szczególnej weryfikacji wymaga skopiowany do formatki przelewu numer rachunku, ponieważ może on zostać podmieniony na inny.

7. W przypadku, gdy dane zawarte w SMSie autoryzacyjnym nie zgadzają się z tymi wprowadzonymi samodzielnie lub gdy otrzymamy kod autoryzacyjny mimo, że braku zlecenia operacji, należy niezwłocznie skontaktować się z Centrum Obsługi Klienta Private Banking lub Oddziałem. Warto pamiętać, że nigdy nie prosimy o zatwierdzenie kodem SMS operacji, które nie zostały zlecone samodzielnie.

8. Trzeba regularnie sprawdzać historię dokonywanych transakcji. Jeśli zostaną zauważone nieprawidłowości, niezwłocznie trzeba zgłosić ten fakt przez Centrum Obsługi Klienta Private Banking lub w Oddziale.