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

Co można zrobić, aby unikać zagrożeń:

1. Do logowania się do Bankowości należy używać tylko zaufanego sprzętu. Nie powinno się logować się z niezaufanych komputerów (np. w kafejkach internetowych) oraz z publicznych sieci WiFi.
2. Adres strony logowania należy wprowadzać do przeglądarki internetowej wyłącznie ręcznie.
3. Poprawność adresu strony logowania zawsze powinna być weryfikowana.
4. Połączenie t musi być szyfrowane, zatem należy sprawdzić czy w pasku znajduje się ikona kłódki oraz czy adres składa się z ciągu znaków https://
5. Należy weryfikować poprawność certyfikatu bezpieczeństwa strony.
6. Nie powinno się udostępniać, ani zapisywać na swoim komputerze i telefonie loginu oraz hasła do Bankowości Internetowej i Mobilnej.
7. Wymagana jest regularna zmiana swoje hasło do logowania. Ta opcja dostępna jest po zalogowaniu do Bankowości Internetowej w zakładce Ustawienia, Zmiana hasła.
8. Aby się wylogować z Bankowości Internetowej należy użyć przycisku „Wyloguj" widocznego w prawym górnym rogu ekranu.
9. Powinno się korzystać z systemu operacyjnego, przeglądarek internetowych i programów antywirusowych wspieranych przez producentów.
10. Regularna aktualizacja systemu operacyjnego, przeglądarki internetowej i programów antywirusowów jest wymagana.
11. Warto pobierać aktualne bazy wirusów programów antywirusowych i systematycznie wykonywać skanowanie urządzeń.
12. Powinno się korzystać z najbardziej aktualnych przeglądarek internetowych.
13. Nie zaleca się instalować oprogramowania z niezaufanych źródeł. Programy na telefon należy pobierać i instalować wyłącznie z oficjalnych sklepów Google Play, Apple App Store lub Windows.
14. Zachęcamy do bieżącego aktualizowania aplikacji bankowości Getin Mobile i Noble Mobile do najnowszych dostępnych wersji.
15. Nie należy odpowiadać na wiadomości od podejrzanych nadawców, ani otwierać załączniki w tych wiadomościach oraz korzystać z zawartych w nich linków.
16. Nie wolno udostępniać osobom trzecim danych logowania do Twojej Bankowości ani kodów autoryzacyjnych.
17. Wymagane jest ustalenie bezpiecznego hasło logowania do Bankowości, którego nie wykorzystuje się w innych serwisach, szczególnie społecznościowych.
18. Dodatkowym zabezpieczeniem podczas logowania jest włączenie maskowania hasła do Bankowości Internetowej. Polega ono na tym, że zamiast pełnego hasła podaje się tylko kilka wybranych znaków, np. trzeci, piąty i dziewiąty znak hasła. System losuje inne znaki do wypełnienia i na tej podstawie identyfikuje klienta.
19. Regularne sprawdzanie historii operacji jest zalecane.
20. Warto dopasować limity transakcji dla Bankowości Internetowej i Mobilnej tak, aby odpowiadały indywidualnym potrzebom.
21. Dzięki włączeniu usługi SMS Info można otrzymywać powiadomienia o operacjach na swoim rachunku.
22. Informacje dotyczące logowań do Bankowości Internetowej można sprawdzać w sekcji Ustawienia, Kanały Dostępu, Bankowość Internetowa – Próby logowania.
23. Zaleca się regularne czytanie aktualności dostępnych na stronie internetowej getinbank.pl oraz na stronie logowania do Bankowości Internetowej.
24. W razie wątpliwości i podejrzeń dotyczących bezpieczeństwa należy niezwłocznie poinformować o tym Bank kontaktując się z Centrum Obsługi Klienta Private Banking (pod numerem +48 22 203 03 01) lub dowolnym oddziałem.

Centrum Obsługi Klienta Noble Private Banking tel. +48 22 203 03 01