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

Bezpieczne urządzenia

Aby bezpiecznie korzystać z Bankowości należy zadbać o bezpieczeństwo urządzeń, na których używamy systemów bankowych, czyli o własne komputery, telefony i tablety.

BEZPIECZNY KOMPUTER

1. Komputer wykorzystywany do łączenia z bankowością powinien mieć zainstalowany system operacyjny dla którego producent zapewnia aktualizacje i są one instalowane.
2. Należy korzystać tylko z zaufanych urządzeń i starać się używać komputera osobistego, unikać komputerów dostępnych w kawiarenkach internetowych czy innych ogólnodostępnych miejscach.
3. Urządzenie powinno mieć zainstalowany program antywirusowy z aktualną bazą wirusów. Dzięki temu jest zabezpieczone przed większością złośliwego oprogramowania, które jest już znane. Warto regularnie wykonywać skanowanie systemu, aby wykryć potencjalne zagrożenia i nie wyłączać programu antywirusowego podczas korzystania z Internetu.
4. Powinno sięaktualizować oprogramowanie, system operacyjny i przeglądarki internetowe zgodnie z zaleceniami i rekomendacjami dostawców. Aktualny system i oprogramowanie gwarantuje większe bezpieczeństwo, ponieważ wiele aktualizacji naprawia luki w zabezpieczeniach, które przestępcy mogą wykorzystać.
5. Należy używać zapory sieciowej (firewall), która pomaga chronić komputer przed atakami z sieci.
6. Systematyczna aktualizacja przeglądarek internetowych zapewnia większy poziom bezpieczeństwa. Bankowość Internetowa dostępna jest dla: Google Chrome od wersji 51, Mozilla Firefox od wersji 34, Microsoft Edge od wersji 13, Internet Explorer w wersji 11, Opera od wersji 20, Safari od wersji 7.
7. Dobrą praktyką jest zabezpieczanie urządzenia dodatkowym hasłem. Chroni to nasz komputer przed dostępem osób niepowołanych np. w sytuacji gdy zgubimy urządzenie, na którym korzystamy z systemu bankowego.
8. Oprogramowanie należy instalować na komputerze jedynie z oficjalnych źródeł. Pirackie wersje programów nie są wspierane przez producentów w kwestiach bezpieczeństwa. Drastycznie rośnie też ryzyko, że pobierzemy nieświadomie złośliwe oprogramowanie.
9. Bank nigdy nie prosi o zainstalowanie dodatkowych zabezpieczeń np. certyfikatów, aplikacji antywirusowych lub innego dodatkowego oprogramowania.
10. Powinno się zachować ostrożność i nie otwierać żadnych wiadomości i plików, które wydają się podejrzane, a ich pochodzenie nie jest potwierdzone. Trzeba je niezwłocznie usunąć z dysku. Szczególnie warto zwrócić uwagę na e-maile proszące o podanie danych logowania do Bankowości, danych osobowych, teleadresowych czy kodów autoryzacyjnych. Nie wolno odpowiadać na tego typu wiadomości, ani otwierać zamieszczonych w nich załączników i korzystać z zawartych w nich linków.

BEZPIECZNY TELEFON I TABLET

1. Warto upewnić, że telefon, z którego korzystamy na co dzień posiada aktualny system operacyjny dostarczony przez producenta. Trzeba go systematycznie aktualizować.
2. Aplikacje Getin Mobile i Noble Mobile oraz inne programy powinny być instalowane wyłącznie z oficjalnych sklepów z aplikacjami (Google Play, Apple App Store, Sklep Windows).
3. Zalecamy nieuruchamianie aplikacji Getin Mobile i Noble Mobile na urządzeniach posiadających odblokowane konto super użytkownika.
4. Warto na bieżąco aktualizować aplikacje Getin Mobile i Noble Mobile do najnowszych wersji.
5. Dostęp do prywatnego urządzenia powinien być zabezpieczony trudnym do odgadnięcia kodem lub hasłem.
6. Nie powinno się odczytywać kodów QR nieznanego pochodzenia.
7. W przypadku zgubienia lub kradzieży urządzenia na którym zainstalowana jest aplikacja Getin Mobile lub Noble Mobile lub na który wysyłane są kody autoryzacyjne niezwłocznie trzeba zgłosić ten fakt w Centrum Obsługi Klienta Noble Private Banking lub w Oddziale. Aktywne urządzenia mobilne na których zainstalowane są aplikacje Getin Mobile i Noble Mobile można usunąć po zalogowaniu się do Bankowości Internetowej w sekcji Bankowość Mobilna.