Bezpieczeństwo korzystania z Bankowości Internetowej i Bankowości Mobilnej.

Przypominamy, że Bank nigdy:

- nie prosi o podawanie haseł jednorazowych podczas logowania do serwisu transakcyjnego;
- nie wysyła wiadomości lub komunikatów z prośbą o podanie TelePIN, danych kart płatniczych i kredytowych;
- nie prosi o podawanie informacji dotyczących Twojego telefonu (numer, marka i model) w czasie logowania, sprawdzania stanu konta i przeglądania historii operacji;
- nie prosi o przesyłanie lub potwierdzanie haseł dostępu, numerów NIK ani kodów PIN;
- nie wysyła na telefon żadnych aplikacji do zainstalowania;
- nie wysyła do klientów wiadomości e-mail zawierających link do serwisu bankowości internetowej (czyli kierujących na stronę logowania do serwisu Banku).

Jeśli otworzyłeś wiadomość od przestępców i kliknąłeś w link i/lub wpisałeś dane karty, jak najszybciej skontaktuj się z nami wysyłając mail na adres: kontakt@nestbank.pl
lub zadzwoń na **801 800 188** lub **22 438 41 41**, zmień hasła dostępu oraz zastrzeż kartę, której dane podałeś (zastrzec kartę możesz dzwoniąc na numer **22 438 41 41**) !
Jeżeli wprowadziłeś kody SMS na fałszywej stronie, sprawdź jakich operacji dotyczyły hasła i anuluj je.

Chroń swoje dane:

• Dane otrzymane od banku (w szczególności NIK, kody SMS) a także hasła i kody dostępu ustanawiane samodzielnie, umożliwiające zalogowanie się w systemie oraz przeprowadzenie transakcji powinny być chronione. Nie udostępniaj tego rodzaju danych innym osobom.
• Nigdy nie zapisuj hasła do logowania w Bankowości Internetowej ani Kodu Dostępu do Bankowości Mobilnej w miejscu dostępnym dla osób nieupoważnionych ani też w pamięci telefonu bądź komputera.
• Pamiętaj – Numer Identyfikacyjny Klienta (NIK) jest numerem nadawanym przez Bank i nie można go zmienić. Nigdy nie podawaj go osobom postronnym.
• Pamiętaj o regularnej zamianie hasła do logowania – zalecana jest zmiana nie rzadziej niż co 2 miesiące lub każdorazowo, gdy masz podejrzenie, że dostęp do hasła miały osoby nieupoważnione.
• Pamiętaj o odpowiednim stopniu skomplikowania hasła, co utrudnia jego odgadnięcie. Zalecane jest, aby w haśle używać: wielkich i małych liter, cyfr oraz znaków specjalnych. Hasło nie powinno zawierać elementów łatwych do odgadnięcia przez osoby nieupoważnione (np. imienia, nazwiska, daty urodzenia, adresu zamieszkania).

Ignoruj wiadomości e-mail, których nadawca prosi o podanie chronionych danych:

• Nest Bank nigdy nie wysyła do swoich klientów zapytania o hasło, NIK, Kody Dostępu lub inne poufne informacje, jak również nie przesyła linków do stron transakcyjnych.
• Wiadomość zawierająca pytanie o chronione dane i zawierająca link na stronę internetową (łudząco przypominającą stronę banku) należy potraktować jako próbę wyłudzenia poufnych informacji.
• O każdej tego rodzaju wiadomości powiadom bank i w żadnym wypadku nie odpowiadaj na taką wiadomość.

Podczas każdego logowania stosuj się do zasad bezpieczeństwa, a każdą zauważoną nieprawidłowość niezwłocznie zgłaszaj do banku:

• Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.
• Jeśli podczas logowania pojawią się niestandardowe komunikaty, zapytania o dane osobowe lub dodatkowe formatki z pytaniem o hasło, zignoruj je i natychmiast poinformuj o tym bank.
• Nie używaj wyszukiwarek internetowych do znalezienia strony logowania.
• Nigdy nie ignoruj różnic w wyglądzie strony lub w wymaganych przez system danych – do logowania służy wyłącznie identyfikator i hasło.
• Przed zalogowaniem sprawdź czy połączenie jest szyfrowane – adres strony powinien zaczynać się do https://, a nie http://, zaś na dole okna przeglądarki powinien pojawić się symbol kłódki (brak kłódki lub kłódka otwarta oznacza brak szyfrowania).
• Dobrze jest sprawdzić dane certyfikatu bezpieczeństwa serwisu, klikając na ikonę żółtej kłódki.
• Sprawdź też datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

Korzystaj tylko ze sprawdzonych i pewnych komputerów:

Nie należy korzystać z Bankowości Internetowej używając komputerów znajdujących się w miejscach dostępnych dla szerokiego grona użytkowników, np. w kawiarence internetowej, hotelu, bibliotece - komputery w takich miejscach mogą nie być odpowiednio zabezpieczone.

Twój komputer powinien być wyposażony w odpowiednie oprogramowanie zabezpieczające.

Zadbaj o:

• Uruchomienie firewalla, który chroni przed niepowołanym dostępem do komputera z sieci internetowej (np. w systemie Windows będzie to polegało na aktywowaniu „zapory systemu Windows") i jego konfigurację uniemożliwiającą nieautoryzowany dostęp do komputera.
• Zainstalowanie i regularną aktualizację programu antywirusowego, co pozwala zminimalizować ryzyko związane z rozsyłaniem niechcianej korespondencji, przejęciem danych lub przejęciem komputera.
• Aktualizację systemu operacyjnego i ważnych dla jego funkcjonowania aplikacji (np. przeglądarki internetowe) – instalowanie „łat" do systemu tworzonych przez producenta oprogramowania.

• Instalowanie tylko legalnego oprogramowania – programy niewiadomego pochodzenia mogą zawierać wirusy lub inne szkodliwe oprogramowanie.
• Nieotwieranie załączników z wiadomości niewiadomego pochodzenia – takie wiadomości mogą zawierać wirusy i inne programy pozwalające na szpiegowanie aktywności użytkownika.

Korzystaj wyłącznie z oficjalnych aplikacji Nest Banku:

Korzystaj wyłącznie z wersji aplikacji mobilnej publikowanej przez Bank w sklepach aplikacji właściwych dla systemu operacyjnego Twojego telefonu. Dbaj o aktualność aplikacji na Twoim telefonie.

W przypadku wszelkich wątpliwości, niejasności lub zaobserwowanych nieprawidłowości skorzystaj ze wsparcia Infolinii Banku dostępnej w następujących dniach i godzinach :

801-800-188

Dla telefonów komórkowych:

22 438-41-41

7.00-24.00 poniedziałek-sobota

8.00-20.00 niedziela

Dane kontaktowe Banku:

Nest Bank SA

ul. Wołoska 24

02-675 Warszawa

Kapitał zakładowy: 316 387 000 zł