Szanowni Państwo,

Ostrzegamy przed nasilonymi atakami, oraz przypominamy, że **Bank NIGDY nie oferuje zdalnej pomocy technicznej poprzez programy/aplikacje, które można pobrać ze sklepu Google Pay lub App Store np. TeamViewer QuickSupport, Anydesk.** Są to programy zdalnego dostępu do Twojego urządzenia, poprzez które osoba trzecia może przejąć kontrolę nad Twoim urządzeniem np. telefonem czy komputerem. Przestrzegamy także przed atrakcyjnymi ofertami szybkich i dużych zysków pochodzących z nieznanych źródeł, min. inwestowanie w kryptowaluty.

Bank nigdy nie prosi przez telefon, wiadomość SMS czy e-mail o:

- Pełny login i hasło do serwisu bankowości internetowej, kod PIN do transakcji internetowych,
- Pełny numer karty płatniczej, kod karty CVV, datę ważności karty, hasło do 3D-Secure,
- Numer PESEL, Twój numer telefonu lub inne dane o które możesz zostać poproszony na fałszywych stronach, które przestępcy mogą Ci podesłać w linku.

Prosimy o zachowanie czujności i przestrzeganie poniższych zasad:

- **DO SERWISU BANKOWOŚCI INTERNETOWEJ LOGUJ SIĘ WYŁĄCZNIE POPRZEZ STRONĘ GŁÓWNĄ BANKU, NIGDY POPRZEZ PRZESYŁANE LINKI,**
- Nie podawaj żadnych kodów ze swojego narzędzia autoryzacyjnego albo aplikacji mobilnej BSGo przez telefon,
- Zawsze dokładnie czytaj treść smsów autoryzacyjnych i kodów autoryzacyjnych, jeśli nie wykonujesz przelewu, nie podawaj nikomu kodu sms do autoryzacji przelewu, jeśli nie parujesz aplikacji mobilnej nie podawaj nikomu kodu aktywacyjnego,
- Nie klikaj w żadne linki do formularzy czy serwisu transakcyjnego. Nie podawaj danych. Jedyne, o co może Cię prosić kupujący to numer konta, jeśli jesteś sprzedającym to Ty czekasz na pieniądze i nic nie musisz robić,
- Nigdy nie podawaj numeru swojej karty płatniczej, żeby otrzymać na nią pieniądze. Jeśli ktoś żąda numeru karty - chce Cię okraść i pobrać z niej pieniądze a nie przesłać na nią pieniądze,
- Zachowaj zasadę ograniczonego zaufania, zanim coś wykonasz bo rzekomo osoba dzwoniąca do Ciebie jest pracownikiem Banku, rozłącz się, a następnie zadzwoń samodzielnie do Banku, przy czym nie oddzwaniaj na numer telefonu który Ci się wyświetlił, znajdź numer kontaktowy do Banku na stronie Banku,
- Postaraj się zapamiętać imię i nazwisko osoby która do Ciebie dzwoni, jeśli nie chce Ci go podać rozłącz się, tylko wtedy dzwoniąc samodzielnie do Banku będziesz mógł zweryfikować czy taka osoba tam pracuje i czy faktycznie próbowała się z Tobą skontaktować,
- Rozliczaj się bezpośrednio przez portal, z którego korzystasz np. Allegro, OLX. Unikaj bezpośredniej komunikacji z kupującymi poprzez komunikatory typu WhattApp, Facebook, Messenger.
- Sprawdzaj w przeglądarce poprawność adresu strony, na których podajesz dane do transakcji.
- Ustaw odpowiednie limity dzienne na swojej karcie płatniczej oraz w serwisie bankowości internetowej.

Tylko własna czujność może w pełni uchronić Cię przed utratą pieniędzy czy zawirusowaniem urządzenia.