

Myślisz, że to bank albo policja. Dzwonią, znają Twoje dane, mówią spokojnie, ale stanowczo: „Twoje pieniądze są zagrożone”.

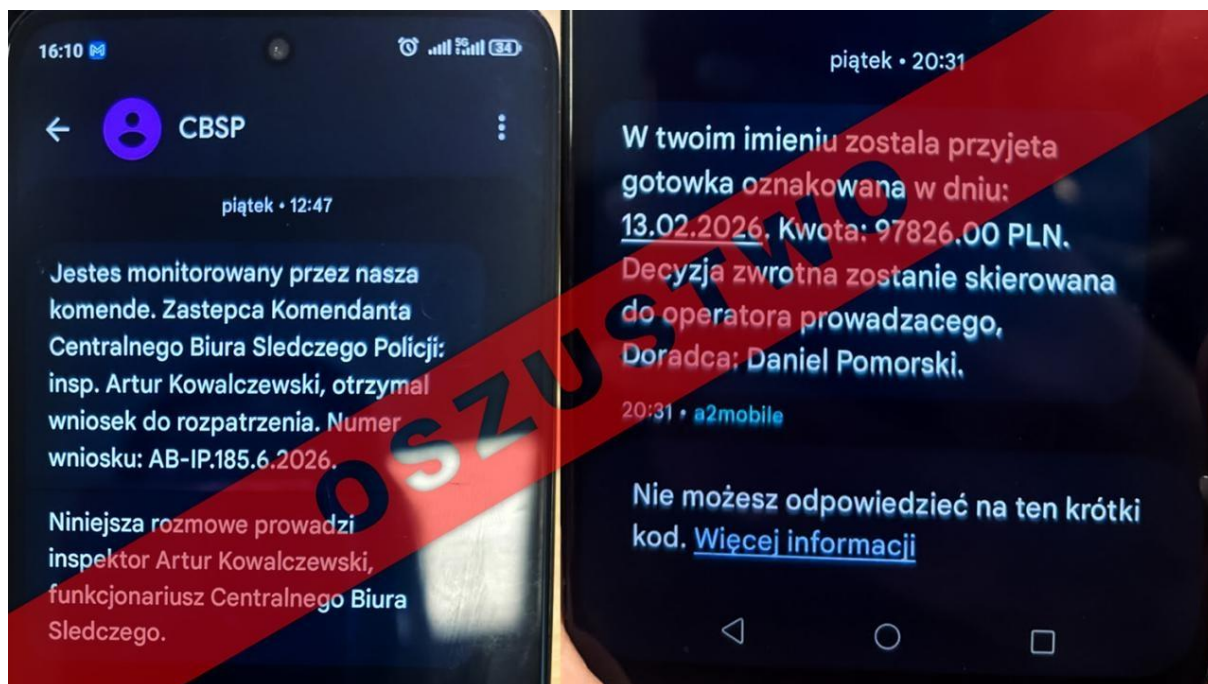
Ostrzegamy przed przestępcami, którzy podszywają się pod pracowników banku, policji lub innych instytucji, próbując wzbudzić zaufanie i nakłonić Cię do działań, które mogą prowadzić do utraty pieniędzy lub przejęcia kontroli nad Twoim urządzeniem.

Jak działają oszuści?

1. Dzwonią, podając się za pracownika banku, policjanta lub inną osobę zaufania publicznego.
2. Twierdzą, że:
 - a. złożono w Twoim imieniu **wniosek kredytowy**,
 - b. wykryto **podejrzaną transakcję**,
 - c. Twoje konto jest **zagrożone**,
 - d. trwa **tajna akcja policyjna** i musisz **zabezpieczyć środki** na tzw. „konto techniczne”,
 - e. nastąpiło inne nietypowe i wymagające Twojego działania zdarzenie.
3. **Wywierają presję czasową**, mówiąc, że musisz działać natychmiast, bo inaczej stracisz pieniądze lub poniesiesz konsekwencje prawne.
4. **Chcą być cały czas na linii** – również wtedy, gdy jesteś w oddziale banku.
5. **Mówią Ci, co masz powiedzieć pracownikowi banku**, by nie wzbudzić podejrzeń, sugerując, że pracownik banku jest zamieszany w to oszustwo.
6. **Zabraniają kontaktu z rodziną, przyjaciółmi, pracownikami banku czy organami ścigania**, twierdząc, że są oni „powiązani” lub że „to tajna operacja”.
7. **Mogą wysyłać SMS-y z kodami**, które rzekomo mają potwierdzać tożsamość pracownika banku podczas rozmowy – to ma stworzyć fałszywe wrażenie, że rozmawiasz z prawdziwym konsultantem.

Mogą nakłonić Cię do zainstalowania aplikacji z nieznanej strony internetowej lub z linku przesłanego w wiadomości SMS, e-mailu bądź przez komunikator, tłumacząc to potrzebą zabezpieczenia Twoich środków.

Oszuści rozsyłają fałszywe SMS-y podszywające się pod CBŚP, dlatego policja apeluje, by nie reagować na takie wiadomości ani na ewentualne późniejsze próby kontaktu. Funkcjonariusze podkreślają, że to próba oszustwa i przypominają, by nie udostępniać nieznajomym danych, ani nie klikać podejrzanych linków.



Jaki jest cel oszustów?

1. **Wyłudzenie pieniędzy**, np. poprzez przelewy, kody BLIK, wypłaty gotówki i dane karty.
2. **Pozyskanie danych logowania** do bankowości (hasła i kody).
3. **Przejęcie kontroli nad urządzeniem**.

Pracownik banku nigdy nie poprosi Cię o:

1. Hasła do bankowości,
2. Kody BLIK,
3. Kody SMS dotyczące logowania lub autoryzacji transakcji,
4. Wykonania transakcji na jakikolwiek rachunek bankowy,
5. Zainstalowanie dodatkowego oprogramowania lub aplikacji w celu zabezpieczenia konta czy pieniędzy,
6. Użycie karty płatniczej w celu „zabezpieczenia środków” – nie prosimy o przyłożenie karty do telefonu (NFC), by rzekomo ochronić Twoje pieniądze.

Żaden pracownik banku nie zabroni Ci rozmowy z bliskimi, ani z organami ścigania w sprawie bezpieczeństwa Twoich środków. **To nie są tajne akcje** – to manipulacja.

Bank nigdy nie dzwoni z numerów 800 88 88 88 / 61 647 28 46 – są to numery Infolinii SGB. Na te numery Ty możesz zadzwonić do nas.

Co zrobić, jeśli masz wątpliwości:

1. **Zakończ rozmowę** natychmiast.
2. **Skontaktuj się bezpośrednio** z placówką banku lub z Infolinią SGB:
 - a. 800 88 88 88 (bezpłatnie)
 - b. 61 647 28 46 (z zagranicy; opłata zgodna z taryfą operatora)