Uważaj na telefonicznych oszustów!

Ostrzegamy przed telefonami od osób, które podają się za pracowników banku, powołują się na względy bezpieczeństwa i nakłaniają Cię do podania poufnych danych do bankowości oraz zainstalowania na Twoim urządzeniu aplikacji do zdalnej weryfikacji.

Wiesz jak łatwo stracić swoje oszczędności i udostępnić dane przestępcom?

W ostatnich miesiącach bardzo zwiększyli aktywność. Otrzymujemy coraz więcej sygnałów o oszustwach-**telefonach z fałszywych infolinii.**

NIE DAJ SIĘ OKRAŚĆ. ZACHOWAJ CZUJNOŚĆ.

Pracownik Banku dzwoniąc do Ciebie **nigdy nie prosi** o:

- instalację dodatkowych aplikacji, które miałyby potwierdzić Twoją tożsamość, zatwierdzić płatność lub podnieść poziom bezpieczeństwa,
- podanie haseł dostępu do żadnego z serwisów (internetowego, mobilnego, telefonicznego).
- kodów do autoryzacji transakcji.

Jak działają przestępcy:

- maskują numer telefonu i podszywają się np. pod numer Banku lub innego banku czy instytucji (np. Biuro Informacji Kredytowej, Związek Banków Polskich),
- przedstawiają się jako pracownicy infolinii lub jednostek związanych z bezpieczeństwem,
- nakłaniają do podania danych do logowania w bankowości elektronicznej, kodów autoryzacyjnych czy danych z kart płatniczych, powołując się na przykład na konieczność potwierdzenia tożsamości, względy bezpieczeństwa, incydenty naruszenia danych,
- nakłaniają do uruchomienie aplikacji umożliwiających kontrolowanie Twojego komputera lub telefonu np. AnyDesk, TeamViewer, QuickSupport.

Przypominamy:

Nikomu nie dawaj dostępu do swoich urządzeń, za pomocą których korzystasz z bankowości elektronicznej!

Jeżeli nie jesteś pewien czy rozmawiasz z pracownikiem Banku rozłącz się.