sierpień 2022

OSTRZEŻENIE PRZED ZAGROŻENIAMI
- próby wyłudzenia poufnych danych przez telefon

Ponownie ostrzegamy przed przestępcami, którzy podają się za pracowników banku lub innych zaufanych instytucji (np. policjantów).

Schemat działania oszustów:

- **podają się za pracowników banku pod pretekstem weryfikacji podejrzanego logowania czy transakcji - w toku rozmowy proszą o instalację oprogramowania, dzięki któremu mogą przejąć kontrolę nad uprzedzeniem (komputer, telefon, itp.), np. Any Desk, TeamViewer.**
- **podają się pod pracowników zaufanych instytucji (np. policjantów) informując o zagrożeniu finansów na koncie – w toku rozmowy proszą o przekazanie pieniędzy na „konto techniczne", na którym będą „bezpieczne".**

Przestępcy mogą korzystać z techniki tzw. **spoofingu** numeru telefonu, w taki sposób, by na Twoim telefonie wyświetlił się numer infolinii banku lub zaufanego pracownika banku. W rzeczywistości chcą m.in. zdobyć dane do logowania, narzędzia autoryzacyjnego lub Twoje inne, równie cenne dane.

W przypadku, gdy:

- odbierzesz podejrzany telefon lub wiadomość tekstową od osoby podającej się za pracownika banku lub instytucji zaufanej;
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych;
- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie

rozłącz się i skontaktuj się z bankiem.

Przypominamy:

- pracownicy Banku podczas rozmowy telefonicznej **NIGDY** nie proszą o podanie haseł dostępu do konta bankowego, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji,
- pracownicy Banku, **NIGDY** nie proszą o zainstalowanie żadnego dodatkowego oprogramowania na komputerach lub urządzeniach mobilnych klienta,
- **ZAWSZE** bądź ostrożny przy podawaniu danych telefonicznie i staraj się potwierdzić tożsamość rozmówcy – w przypadku jakichkolwiek wątpliwości zakończ rozmowę i skontaktuj się z Bankiem informując o zaistniałym o tym zdarzeniu,
- jeśli treść rozmowy wyda Ci się podejrzana i niestandardowa, a osoba dzwoniąca wymaga szybkiego podjęcia działań (np. podania danych, instalacji oprogramowania, podania kodów BLIK, kodów SMS, itp.) **NIEZWŁOCZNIE** zakończ rozmowę i skontaktuj się z Bankiem informując o zaistniałym zdarzeniu w celu potwierdzenia wiarygodności takiej rozmowy.
- jeśli podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie, **NIEZWŁOCZNIE** skontaktuj się z Bankiem informując o zaistniałym zdarzeniu,
- **NIGDY** nie podawaj nigdy przez telefon nadmiarowych informacji, nie zdradzaj szczegółów swoich transakcji, ani innych danych podlegających ochronie. Jeżeli masz jakiekolwiek wątpliwości – skontaktuj się osobiście z placówką Banku na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia).

sierpień 2022