OSZUSTWO „NA ZNAJOMEGO” Z MEDIÓW SPOŁECZNOŚCIOWYCH

Ostrzegamy przed wyłudzaniem pieniędzy przez osoby podszywające się pod znajomych w mediach społecznościowych. Kiedy ktoś pisze przez internetowy komunikator, że potrzebuje szybkiej pomocy finansowej i prosi o podanie kodu do płatności mobilnych (BLIK) – należy zachować szczególną ostrożność.

Przestępcy przejmują konta w serwisach społecznościowych i próbują przekonać ofiary do przekazania im pieniędzy. Zwykle jest to uzasadniane nagłą sytuacją. Często proszą o wypłacenie pieniędzy za pomocą polskiego systemu płatności mobilnych BLIK. Ofiara musi podać specjalny kod, a następnie potwierdzić transakcję w swojej aplikacji bankowości mobilnej. W ten sposób sama daje przestępcy pieniądze.

Wiele osób, sądząc, że koresponduje ze swoim znajomym podaje kod BLIK, a następnie w aplikacji mobilnej banku potwierdza PIN-em realizację transakcji, nie sprawdzając jej szczegółów. Godząc się na realizację transakcji użytkownicy tracą pieniądze na rzecz osoby podszywającej się pod znajomych z sieci społecznościowych.

Takiego wyłudzenia bardzo łatwo uniknąć:

1. **NALEŻY STOSOWAĆ DWUSKŁADNIOWE UWIERZYTELNIENIE SWOICH KONT SPOŁECZNOŚCIOWYCH (WÓWCZAS O WIELE TRUDNIEJ PRZEJĄĆ NASZE KONTO – ZALOGOWANIE SIĘ WYMAGA POTWIERDZENIA SMS)**
2. **ZAWSZE WARTO POTWIERDZAĆ TOŻSAMOŚĆ „ZNAJOMYCH”, KTÓRZY PISZĄ DO NAS PRZEZ INTERNETOWE KOMUNIKATORY – NAJLEPIEJ ZADZWONIĆ DO TAKIEJ OSOBY.**
3. **ZAWSZE TRZEBA SPRAWDZAĆ DANE TRANSAKCJI PRZED JEJ ZATWIERDZENIEM W APLIKACJI BANKOWOŚCI MOBILNEJ (PRZESTĘPCA NIE SKORZYSTA Z KODU, DOPÓKI NIE POTWIERDZIMY TRANSAKCJI NA NASZYM TELEFONIE).**
4. **TRZEBA CHRONIĆ SWÓJ TELEFON ORAZ SZCZEGÓLNIE PIN DO APLIKACJI MOBILNEJ BANKU.**