STOP

OSZUSTOM W SIECI

CHROŃ SWOJE PŁATNOŚCI!

rzeszów stolica innowacji

blik

POLICJA

UWAGA! Oszuści atakują w sieci

Podają się za Twoich znajomych

1. Przestępcy włamują się na konta w serwisach społecznościowych.
2. Podszywają się pod Twoich znajomych i rozsyłają prośby o pieniądze.
3. Zwykle jest to uzasadnione nagłą sytuacją, np. „Muszę pilnie coś zapłacić i nie wziąłem ze sobą karty".
4. Proszą o podanie kodu BLIK.
5. Podajemy kod i akceptujemy płatność w aplikacji naszego banku, bez jej weryfikacji.

! JEŻELI TAK ZROBISZ, STRACISZ PIENIĄDZE!

Podają się za pracowników banków lub portali inwestycyjnych

1. Ukrywają numer telefonu i podają się np. za pracownika banku czy portalu.
2. Dzwonią do Ciebie pod pozorem ochrony zgromadzonych na koncie środków lub okazji inwestycyjnej.
3. Proszą o zainstalowanie aplikacji lub oprogramowania typu AnyDesk, TeamViewer, QuickSupport.
4. Dzięki takim programom sprawcy widzą zawartość Twojego urządzenia i mogą się nim zdalnie posługiwać.
5. Pomagają zainstalować takie oprogramowanie, po czym uzyskują dostęp do Twoich danych bankowych.

! JEŻELI TAK ZROBISZ, STRACISZ PIENIĄDZE!

Oszuści, podszywając się pod Ciebie, wypłacają pieniądze, zaciągają pożyczki, dokonują swobodnie płatności, obciążając Twoje konto.

JAK NIE DAĆ SIĘ OSZUKAĆ W SIECI

Łatwo możesz uchronić się przed oszustwami – pamiętaj:

1. **ZAWSZE SPRAWDZAJ,** komu i jakie dane przekazujesz.
2. **ZANIM PRZEKAŻESZ** kod BLIK, dane do logowania, dane z kart płatniczych, sprawdź tożsamość odbiorcy – **ZADZWOŃ, UPEWNIJ SIĘ,** że to Twój znajomy.
3. **ZANIM POTWIERDZISZ** transakcję, sprawdź jej szczegóły (kwotę i odbiorcę).
4. **NIE KORZYSTAJ** z podejrzanych formularzy logowania, czy podsyłanych linków. Loguj się tylko przez oficjalne strony banków i ich aplikacje.
5. **PAMIĘTAJ** – pracownik banku dzwoniąc do Ciebie nigdy nie prosi o instalację dodatkowych aplikacji, podanie pełnego hasła, kodu PIN czy kodów do autoryzacji transakcji.