

## Uważaj na oszustwa na BLIK! Bądź ostrożny!

Chodź płatności BLIK są bezpieczne bardzo często zachęca oszustów do korzystania z niego w celu wyłudzenia pieniędzy. Poniżej przykładowe scenariusze oszustw i zasady co robić by nie dać się okraść.

Oszustwo na BLIK polega na wyłudzeniu kodu do płatności. Oszuści najczęściej żerują na naszych emocjach i pośpiechu, próbując wyłudzić pieniądze.

Przykładowe działania oszustów.

- Wiadomość od znajomego lub członka rodziny: Przesłany wiadomości w mediach społecznościowych, takich jak Facebook czy Messenger. Następnie, podszywając się pod Twoich bliskich, proszą o pilną pożyczkę zazwyczaj na niewielką kwotę i podanie kodu BLIK. Swoją prośbę tłumaczą zazwyczaj nagłą sytuacją, na przykład brakiem gotówki z powodu zgubieniem bądź kradzieżą portfela. Pożyczkę obiecują zwrócić w krótkim czasie. Ofiara oszustwa nie widzi potrzeby dodatkowej weryfikacji ponieważ oszust korzysta z tożsamości członka rodziny bądź znajomego;
- Pomyłkowy przelew: Niespodziewanie otrzymujesz na swój telefon prawdziwe środki, a chwilę później kontaktuje się z Tobą oszust (dzwoniąc lub wysyłając SMS-a) i prosi o ich zwrot na inny numer bądź rachunek. Zachowaj ostrożność, ponieważ te pieniądze mogą pochodzić z przestępstwa! Zwracając je na własną rękę, nieświadomie bierzesz udział w praniu brudnych pieniędzy, stając się tak zwanym słupem (Komunikat Rzecznika Finansowego pod linkiem: <https://rf.gov.pl/oszustwo-na-blika-nie-kazda-rada-jest-wlasciwa/>) ;
- Fałszywe zakupy w internecie: Przesłany wiadomości na popularnych portalach sprzedażowych, takich jak OLX czy Vinted. Ofiara dostaje w aplikacji WhatsApp wiadomość od potencjalnego klienta, który jest zainteresowany produktem przez InPost. Oszust wysyła smsa od InPost z linkiem. Po kliknięciu w link ofiara musi tylko wpisać dane karty bankowej na którą wpłyną środki. W kolejnej zakładce pojawia się już tylko prośba o wpisanie kodu BLIK i potwierdzenie wpłaty.
- Pracownik banku – z ofiarą kontaktuje się rzekomy Pracownik Banku i informuje o próbie zaciągnięcia zobowiązania na rachunku bankowym i żeby potwierdzić tożsamość. Prosi o podanie informacji o ilości środków zgromadzonych na rachunku bankowym. Ofiara udziela niezbędne informacji, a następnie oszust prosi o wygenerowanie kodu BLIK, który ma pomóc w zdemaskowaniu oszusta. Po otrzymaniu kodu przestępcy wykorzystują go natychmiast do pobrania pieniędzy w bankomacie.

Jak skutecznie się chronić?

- Zawsze dzwoń do znajomych do członka rodziny: Jeśli ktoś prosi Cię o kod BLIK za pośrednictwem komunikatora internetowego, bezwzględnie zadzwoń do tej osoby i upewnij się, że to z nim rozmawiasz. Upewnij się, czy to faktycznie ona potrzebuje Twojej pomocy;

- Nie odsyłaj samodzielnie omyłkowych przelewów: Gdy otrzymasz pieniądze od obcej osoby, powiadom o tym Bank, który zajmie się bezpieczną procedurą zwrotu środków;
- Nie podawaj szczegółowych danych przez telefon rzekomym pracownikom Banku: pracownik Banku i tak ma te dane w systemie i nigdy nie poprosi o takie informacje;
- Przed potwierdzenie transakcji dokładnie upewnij się czego dotyczy ta płatność, jaka jest kwota i do kogo trafi: nie działaj pochopnie;
- Nie klikaj w linki przychodzące we wiadomościach z nieznanymi numerami telefonów: zapewne przeniosą Cię natychmiast do stron wyłudających dane lub pieniądze;
- Przed zalogowaniem się na konto w Banku sprawdź czy adres strony jest właściwy;
- Stosuj dwuskładnikowe uwierzytelnienie kont społecznościowych: przy próbie logowania każda osoba będzie musiała potwierdzić specjalnym kodem wysyłanym na autoryzowany numer telefonu komórkowego

## **PAMIĘTAJ!!!**

Płatności BLIKIEM są bezpieczne. Samo zagrożenie nie wynika ze sposobu płatności. Zarówno BLIK jak i aplikacja mobilna ma szereg zabezpieczeń gwarantujących bezpieczną transakcję. Samo zagrożenie wynika z niebezpieczeństwa fałszywego znajomego, członka rodziny bądź osoby trzeciej. Jeśli sam nie podasz oszustowi swoich danych, nie klikniesz w link, nie udostępnisz hasła ani kodów i właściwie zabezpieczasz swoje konto oraz smartfon to prawdopodobieństwo oszustwa jest znikome.