BLIK, choć jest bezpiecznym środkiem płatności, bardzo często zachęca oszustów do korzystania z niego w celu wyłudzania pieniędzy. Zapoznaj się z metodami oszustwa na BLIK i zasadami jakie stosować, aby nie dać się okraść.

Na czym polega oszustwo na BLIK?

Oszustwo na BLIK polega na **wyłudzeniu kodu do płatności**, najczęściej z wykorzystaniem komunikatorów, bądź kont w serwisach społecznościowych. Z potencjalną ofiarą kontaktuje się cyberprzestępca i podszywając się pod członka rodziny lub znajomego prosi o pilną pożyczkę. Aby zrealizować swój cel namawia

do wygenerowania kodu płatności telefonem, a następnie przesłania go „znajomemu".

Oto przykładowe scenariusze działania oszustów:

• **Pilna pożyczka** – przestępca włamuje się na konto w mediach społecznościowych rodziny ofiary. Pisze o potrzebnie pilnej pożyczki na niewielką kwotę i wygenerowanie kodu BLIK. Pożyczkę obiecuje zwrócić za kilka dni. Ponieważ korzysta z tożsamości bliskiej osoby nieświadoma ofiara nie widzi konieczności dodatkowej weryfikacji.

• **Zgubienie lub kradzież portfela** – przestępca kontaktuje się z ofiarą i przekonuje, że zgubił portfel lub został mu on skradziony a potrzebuje gotówki. Przekonuje, że sprawa jest pilna, bo musi za coś zapłacić. W takich okolicznościach, gdy w grę wchodzą emocje i trzeba szybko działać, ofiara nie weryfikuje okoliczności ani tożsamości osoby kontaktującej się z nią.

• **Pracownik banku** – z ofiarą kontaktuje się rzekomy pracownik banku. W rozmowie telefonicznej oszust informuje, że wykryto próbę zaciągnięcia zobowiązania na rachunek tej osoby. Aby potwierdzić tożsamość klienta, prosi o podanie informacji dotyczących stanu rachunku, wysokości zgromadzonych środków itd. Nieświadoma ofiara udziela wszystkich informacji. Następnie przestępca prosi o wygenerowanie kodu BLIK, który pomoże w zdemaskowaniu oszusta. Kod ten posłuży oczywiście do pobrania pieniędzy z bankomatu.

• **Zakup na OLX** – ofiara wystawia na OLX produkt do sprzedaży i dostaje w aplikacji WhatsApp wiadomość od potencjalnego klienta. Pisze on, że jest zainteresowany i chciałby kupić ten produkt przez InPost. Ofiara odpisuje więc, że nie ma problemu i po chwili otrzymuje odpowiedź, że klient zaraz zapłaci. Po kilku minutach przychodzi SMS od InPost z linkiem do potwierdzenia. Ofiara kilka w odnośnik i przechodzi na stronę firmy kurierskiej. Ale aby otrzymać pieniądze, ofiara musi tylko wpisać dane karty bankowej, na którą wpłyną środki. W kolejnym oknie pojawia się już tylko prośba o wpisanie kodu BLIK i potwierdzenie wypłaty.

Żeby nie dać się oszukać, stosuj środki bezpieczeństwa:

• Nie podawaj szczegółowych danych przez telefon, nawet kiedy bank rzekomo ich wymaga

(pracownicy banku i tak mają je w systemie).

• Jeśli znajomy znienacka prosi Cię o kod BLIK w rozmowie na komunikatorze, zadzwoń do niego i upewnij się, że to z nim rozmawiasz.

• Przed potwierdzeniem transakcji BLIK sprawdź dwa razy, ile wynosi kwota i do kogo ona trafi.

• Nie klikaj w linki otrzymywane od nieznanych numerów – niemal na pewno przeniosą Cię one do stron wyłudzających dane lub pieniądze.

• Przed zalogowaniem się na konto w banku, dwa razy upewnij się, że adres strony jest właściwy.

• Nie loguj się wrażliwymi danymi w otwartych sieciach Wi-Fi, m.in. w kawiarniach.

• Stosuj dwuskładnikowe uwierzytelnienie kont społecznościowych (2FA) – dzięki niemu każda osoba próbująca zalogować się na Twoje konto będzie musiała wprowadzić specjalny kod wysyłany tylko na autoryzowany numer telefonu komórkowego.

Pamiętaj! Kiedy ktoś prosi Cię o kod BLIK:

• Nie działaj pochopnie. Najlepiej zadzwoń do tej osoby.

• Zawsze sprawdzaj, komu wysyłasz kody do płatności mobilnych.

• Nigdy nie przekazuj pieniędzy obcym osobom.

Płatności BLIKlem są bezpieczne

Pamiętaj, że zagrożenie nie wynika ze sposobu płatności, ponieważ zarówno BLIK, jak i sama aplikacja bankowa, mają szereg zabezpieczeń gwarantujących bezpieczne transakcje. Źródłem niebezpieczeństwa jest fałszywy znajomy. Pamiętaj, że jeżeli sam nie podasz nieuprawnionej osobie haseł ani kodów i właściwie zabezpieczasz swoje konto oraz smartfon, prawdopodobieństwo wyłudzenia jest znikome.