WYDZIAŁ PREWENCJI KWP W ŁODZI

https://lodzka.policja.gov.pl/el2/aktualnoc/52199,MAM-PILNA-PROSBE-PODSTEPNE-OSZUSTWA-NA-BLIK-a.html
2020-11-23, 18:18

MAM PILNĄ PROŚBĘ! PODSTĘPNE OSZUSTWA NA BLIK-A

Oszuści coraz częściej podszywają się pod znajomych na portalach społecznościowych i zwracają się z pilną prośbą o pożyczkę. Za pomocą otrzymanego kodu do płatności mobilnej okradają konto osoby oszukanej. Przypominamy, by zachować czujność, aby nie paść ofiarą przestępstwa i nie stracić swoich oszczędności.

Oszustwo **„na BLIKA”** polega na wyłudzeniu kodu do płatności przez telefon i w ten sposób okradzenia konta osoby oszukanej. Proceder robi się coraz bardziej popularny i odbywa się w całym kraju.

Jak działa ta metoda?

Oszuści podszywają się pod osobę znajomą, którą mamy w swoich kontaktach w komunikatorze, bądź kogoś z rodziny, prosząc o szybką pożyczkę i podanie kodu BLIK. Najczęściej tłumaczą się pilną potrzebą zrealizowania przelewu albo uiszczenia jakiejś opłaty i chwilowym brakiem dostępu do środków zgromadzonych na własnym koncie (blokada środków, prace techniczne na stronach banku, oczekiwanie na przelew wynagrodzenia za pracę, itp.). Oszust nigdy nie o dużą sumę pieniędzy.

Wystarczy tylko, że zalogujemy się do swojego banku i w aplikacji wygenerujemy kod do płatności telefonem, a następnie przekażemy go „znajomemu”. To zajmuje kilka minut. Oszuści mając kod BLIK mogą bez problemu wypłacić naszą gotówkę. Właściciel konta musi potwierdzić transakcję, jednak przekonany, że pomaga bliskim lub znajomym w potrzebie – niejednokrotnie robi to bez namysłu. Oszuści bardzo sprytnie formułują wiadomości, co powoduje, że nasza czujność zostaje uśpiona.

Co powinniśmy zrobić?

Zanim udzielimy „pożyczki” najlepiej po prostu zadzwonić do rzekomego bliskiego i sprawdzić czy osoba, która do nas napisała rzeczywiście potrzebuje naszej pomocy. Jeśli osoba, która odebrała połączenie, nie ma pojęcia o całym zdarzeniu lub nie jest naszym znajomym, to wiemy, że ktoś próbuje wyłudzić od nas pieniądze.

Zasady ostrożności:

- najlepiej stosować dwuskładnikowe uwierzytelnianie swoich kont społecznościowych (zalogowanie się wymaga potwierdzenia SMS);
- zawsze warto zadzwonić do osoby, która pisze do nas przez komunikator internetowy, potwierdzając tożsamość „znajomego”;
- zawsze trzeba sprawdzić dane transakcji przed jej zatwierdzeniem w aplikacji bankowości mobilnej przestępca nie skorzysta z kodu, dopóki nie potwierdzimy transakcji na naszym telefonie;
- należy chronić swój telefon oraz dane do logowania na nasze konta bankowe

NIE PRZEKAZUJEMY PIENIĘDZY OBCYM OSOBOM

NIE PRZESYŁAMY PIENIĘDZY NA PODANE PRZEZ OBCE OSOBY NUMERY KONT