Oszustwa na BLIK – nie daj się okraść !!!

BLIK jest szybką i bezpieczną metodą płatności w Internecie oraz w sklepach stacjonarnych. Kod BLIK służy do zainicjowania transakcji, a po akceptacji w aplikacji mobilnej Banku, dochodzi do realizacji transakcji i pobrania pieniędzy z konta.

Należy jednak pamiętać, że udostępnienie kodu BLIK osobie trzeciej może spowodować inicjację transakcji w naszym imieniu przez inną osobę – np. oszusta. Podawanie kodu BLIK nieznanym sobie osobom w Internecie może doprowadzić do kradzieży środków z rachunku i utraty oszczędności. Dlatego nigdy nie udostępniaj kodu BLIK – nawet znajomemu w mediach społecznościowych czy sprzedawcy na portalu ogłoszeniowym.

<u>Pamiętaj, żeby nie dać oszukać:</u>

- **Dbaj o kod BLIK jak o gotówkę lub kartę – nie przekazuj go nigdy nieznanym osobom**
- **W sklepie internetowym, terminalu płatniczym, bankomacie – wpisuj kod BLIK samodzielnie. Bank nigdy nie prosi o podanie kodu BLIK w innych okolicznościach**
- **Sprzedajesz coś na portalu sprzedażowym (np. OLX lub Vinted)? Nigdy nie przekazuj kodu BLIK kupującym. Pamiętaj, że za pomocą kodu BLIK nigdy nie otrzymasz pieniędzy za towar, który sprzedajesz.**
- **Twój znajomy niespodziewanie prosi Cię o kod BLIK lub przelew na telefon przez media społecznościowe? To może być oszustwo, dlatego zanim coś zrobisz, skontaktuj się ze znajomym osobiście**
- **Oszuści wysyłają SMSy z linkiem do środków, które ktoś rzekomo przekazał Ci za pomocą BLIKA. Jeśli dostaniesz taką wiadomość, nie klikaj w podany link. Ani Bank, ani operator płatności BLIK - nie wysyłają takich SMS-ów. Jeśli ktoś prześle przelew na telefon BLIK, środki automatycznie znajdą się na Twoim rachunku i nie musisz nigdzie potwierdzać, że chcesz je odebrać.**
- **zweryfikuj dane transakcji przed jej zatwierdzeniem w aplikacji mobilnej banku.**

Przykładowe scenariusze działania oszustów:

Phishing (fałszywy link, wyłudzenie kodu BLIK) – zastosowanie metod socjotechnicznych lub informatycznych mających na celu wyłudzenie danych dostępowych/kodów BLIK, które posłużą do realizacji transakcji. W ramach tego scenariusza transakcje realizowane np. za pomocą fałszywych linków, które ukierunkowane są na opłacenie transakcji dotyczących dóbr wirtualnych i ułatwiają szybką konsumpcję środków finansowych (duży odsetek zgłoszonych na rzecz zakupu kryptowalut) lub wypłaty z bankomatów.

Oszustwo transakcyjne – transakcje realizowane zgodnie z zamierzeniem użytkownika BLIK, lecz brak finalizacji transakcji w postaci dostarczenia produktu/usługi. Oszustwa transakcyjne charakteryzują się często wystawionymi w Internecie serwisami z fałszywymi sklepami/fałszywymi ogłoszeniami na portalach aukcyjnych. Po realizacji płatności kontakt ze sprzedawcą się urywa –najczęściej serwis znika po kilku dniach, a telefony kontaktowe nie odpowiadają.

Podszycie w mediach społecznościowych – scenariusz związany z wyłudzeniem danych dostępowych do kont w mediach społecznościowych (pierwsze ofiary przestępców). Przestępcy po przejęciu profili rozsyłają wiadomości do znajomych swojej ofiary z prośbą o pożyczkę w związku z nagłym zdarzeniem losowym. Środki te najczęściej są konsumowane za pomocą wypłat z bankomatów lub na giełdy kryptowalut.

Vishing (podszycie pod pracownika Banku, Urzędu) - zastosowanie socjotechniki mającej na celu wyłudzenie danych dostępowych i/lub kodów BLIK za pośrednictwem rozmowy telefonicznej i podszycia się pod pracownika instytucji publicznej lub finansowej celem realizacji transakcji. W tym scenariuszu identyfikowane są również działania przestępców, których celem jest nakłonienie ofiary przestępstwa do wypłaty środków z własnego rachunku, a następnie, za pomocą kodów BLIK, wpłata na rachunek służący do celów przestępczych.

Oszustwo na OLX / Vinted – scenariusz zakładający wyłudzenie kodu BLIK od sprzedawców na portalach ogłoszeniowych. Przestępca kontaktuje się z osobą sprzedającą i deklaruje chęć zakupu towaru. Następnie prosi o udostępnienie kodu BLIK celem dokonania wpłaty środków finansowych.