

Oszustwo na BLIKA! Upewnij się, czy to faktycznie znajomy prosi o pożyczkę

Data publikacji: 14.01.2025 15:00

Coraz częściej spotykamy się z przypadkami oszustw dokonywanych za pomocą systemu BLIK. Przestępcy, przejmując konta na portalach społecznościowych, podszywają się pod naszych znajomych i wyłudniają pieniądze. Przykładowa wiadomość może brzmieć tak: „Hej, mam sprawę, jesteś? Opłacisz mi coś BLIKIEM? Ja Ci odeślę, bo mi coś nie działa”. Czy w takiej sytuacji wiesz, jak się zachować?



Przykładowa próba wyłudzenia. Fot: KPP w Cieszynie

Jak działają oszuści?

Schemat oszustwa jest zazwyczaj bardzo podobny. Przestępcy włamują się na konto na portalu społecznościowym i przejmują je. Następnie wysyłają do znajomych ofiary wiadomości z prośbą o udostępnienie kodu BLIK. Podszywając się pod właściciela konta, prowadzą luźne rozmowy, aby nie wzbudzać podejrzeń. Zwykle proszą o kwoty rzędu kilkuset złotych i obiecują szybki zwrot pieniędzy.

Osoby, które sądzą, że pomagają znajomemu, podają kod BLIK i zatwierdzają transakcję w aplikacji mobilnej. Po otrzymaniu kodu oszuści wypłacają gotówkę z bankomatu lub płacą za zakupy w Internecie. Co gorsza, transakcji dokonanych za pomocą BLIKA nie można cofnąć.

Jak się zabezpieczyć?

Aby uniknąć oszustwa, warto przestrzegać kilku podstawowych zasad przekazuje policja:

- Należy przede wszystkim dobrze zabezpieczyć dostęp do konta na portalu społecznościowym, wykorzystując w tym celu dwuskładnikowe uwierzytelnienie logowania. Pamiętajmy również o wylogowaniu się z konta po zakończeniu użytkowania!
- Nie należy podawać wygenerowanego kodu Blik bez potwierdzenia, czy to faktycznie nasz znajomy prosi o pożyczkę. Wystarczy zadzwonić do znajomego, aby upewnić się, czy faktycznie on znalazł się w potrzebie.
- Zawsze należy dokładnie sprawdzić dane transakcji przed jej zatwierdzeniem w aplikacji bankowości mobilnej, np., gdzie nasze pieniądze będą wypłacone.

red./KPP w Cieszynie