

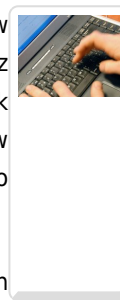
# KOMENDA POWIATOWA POLICJI W CIESZYNIE

<http://www.cieszyn.slaska.policja.gov.pl/ka6/informacje/wiadomosci/252625,Uwaga-na-wlamania-i-oszustwa.html>  
2019-06-19, 19:46

## UWAGA NA WŁAMANIA I OSZUSTWA!

**Często chcemy pomagać i dlatego oszuści niestety to wykorzystują. W ostatnim czasie coraz częściej zdarza się, że złodzieje przejmują konta na Facebooku i wysyłają wiadomości do znajomych z listy. Podszywając się pod kogoś innego proszą o pożyczkę i przekazanie kodu BLIK. Jeśli więc ktoś poprosi Was o pieniądze, zanim mu je przekazacie, zweryfikujcie wiadomość.**

Schemat wyłudzenia pieniędzy jest w tym wypadku podobny. Złodziej najpierw włamuje się na profil pokrzywdzonego. Rozsyła do wszystkich znajomych wiadomość z prośbą o pilną pożyczkę. Przystępcy rozmowę rozpoczynają w różny sposób, jak choćby w ten dramatyczny sposób: „Hej, mam do Ciebie ogromną prośbę, jestem w pilnej potrzebie- zostałem okradziony...”, więc od razu przechodzili do sedna. Prosi o przekazanie numeru BLIK.



Wiadomość tę rozsyłają za pomocą aplikacji messenger do wszystkich znajomych danej osoby, której włamali się na konto społecznościowe. Tak więc pokrzywdzeni odczytują wiadomość, jako otrzymaną od znajomego czy znajomej. Oszuści nie proszą jednak ofiary o przelew, a o uruchomienie aplikacji banku i podanie sześciocyfrowego kodu BLIK, a następnie potwierdzenie wypłaty pieniędzy z bankomatu.

Złodzieje proszą o różne kwoty. Jeżeli ktoś odmówi nie rezygnują- proszą o niższe „pożyczki”. Niestety, już kilka osób uwierzyło oszustom i straciła swoje pieniądze.

### Jak nie dać się oszukać?

Przede wszystkim właściwie zabezpieczmy własne konta- czy to bankowe, czy społecznościowe. Zalecane jest:

- ustawienie trudnego do złamania hasła i uruchomienie ( duże i małe litery oraz cyfry, a także znaki specjalne jak np. \* # \$ itp. )
- dwuskładnikowego uwierzytelnienia podczas logowania na Facebooku ( aby to zrobić, należy wejść w ustawienia, a następnie w zakładkę bezpieczeństwo i logowanie)

Jeśli ktoś korzysta z BLIK-a, to w żadnym wypadku nie powinien nikomu podawać kodu BLIK, a tym bardziej zatwierdzać transakcji na swoim smartfonie, jeśli sam jej nie wykonuje. **Zawsze też tego rodzaju prośbę możemy zweryfikować dzwoniąc do znajomego upewniając się, że to naprawdę on potrzebuje tej gotówki!** Często bowiem osoba, której przejęto konto, nie jest tego świadoma i orientuje się dopiero po telefonie od prawdziwego znajomego.

Niestety przestępcy wykorzystują naszą naiwność i pośpiech, w którym żyjemy. Właśnie dlatego tak ważne są ostrożność i czujność oraz przede wszystkim odpowiednie zabezpieczenie swojego konta.

Zachęcamy do zapoznania się z [DOBRYMI PRAKTYKAMI](#) w Internecie na stronie [www.stojpomyslpolacz.pl/stp/dobre-praktyki](http://www.stojpomyslpolacz.pl/stp/dobre-praktyki) - znajdziecie tam Państwo wiele cennych i przydatnych informacji , nie tylko na temat właściwego zabezpieczenia konta.

Ocena: 0/5 (0)

[Tweetnij](#)