

# Stracili łącznie kilkadziesiąt tysięcy złotych...

Data publikacji: 14.07.2020 12:56

Policjanci przypominają o oszustwach internetowych i apelują o zachowanie szczególnej ostrożności przy transakcjach związanych z płatnościami oraz podawaniem swoich danych w sieci Internet!.



Fot: Pixabay.com

Ostatnio informowaliśmy o tym, jak mieszkaniec Cieszyna w porę zareagował na próbę ataku oszustów na jego konto bankowe. Tego niestety nie udało się zrobić w ostatnim czasie mieszkańcom naszego powiatu, którzy stracili łącznie kilkadziesiąt tysięcy złotych...

Sposób oszustwa szczegółowo opisuje asp. Krzysztof Pawlik, rzecznik prasowy cieszyńskiej policji - ***Mieszkańcy naszego powiatu, otrzymali wiadomości o treści „Twoja przesyłka została wstrzymana z powodu nadwagi. Ureguluj należność 1.50 zł aby uniknąć zwrotu przesyłki do nadawcy”. Pokrzywdzeni, korzystali z licznych zakupów za pomocą sieci Internet, dlatego też otworzyli otrzymany link. Następna wiadomość brzmiała „Twoja przesyłka została wstrzymana z powodu nadwagi. Ureguluj należność 1.50 zł, aby uniknąć zwrotu przesyłki do nadawcy”. Do każdej informacji załączony był link kierujący na fałszywą stronę banku. Kolejna informacja dotyczyła domniemanych problemów z logowaniem do banku i brzmiała : „Przepraszamy za możliwe problemy przy płatności banku”. Po otwarciu strony za pomocą przesłanego linku pojawiła się strona ładząco podobna do strony związanej z transakcjami płatniczymi, gdzie był wybór banku. Pokrzywdzeni wybrali ikonę banku i zostali przekierowani na jego stronę, z tą różnicą, że była to strona fałszywa. Wszystko było ładząco podobne do logowania na prawdziwej stronie bankowości internetowej, ( np. podczas wpisywania hasła strona żądała jedynie kilka znaków hasła jak standardowo przy logowaniu), jednakże po zalogowaniu ukazał się komunikat, aby wpisać cały nr PESEL- gdzie bank nigdy nie żąda takich danych przy przelewie. W dalszej kolejności ukazał się komunikat o wysłaniu SMS z kodem dostępu. Pokrzywdzeni otrzymali SMS z banku o treści „Bank. Aktywujesz urządzenie mobilne. Kod autoryzacji. Pokrzywdzona podała otrzymany kod i zatwierdziła. Następnego dnia pokrzywdzona nie mogła się zalogować swojej bankowości elektronicznej posługując się swoim loginem oraz hasłem. W kontakcie z bankiem pokrzywdzona otrzymała nowe dane logowania po zresetowaniu starych.***

Jak się okazało nieustalona osoba dokonała nieautoryzowanych operacji na rachunku pokrzywdzonych m.in. przez wypłaty BLIK-iem czy też zaciągnięcie szybkiego kredytu. Wskazany link zamiast zlecenia płatniczego w bankowości elektronicznej zawierał zlecenie zmiany autoryzowanego urządzenia z dostępem do bankowości elektronicznej. W ten sposób pokrzywdzeni przekazali dostęp do swojego konta nieustalanej osobie.

Red./ma.tpras,