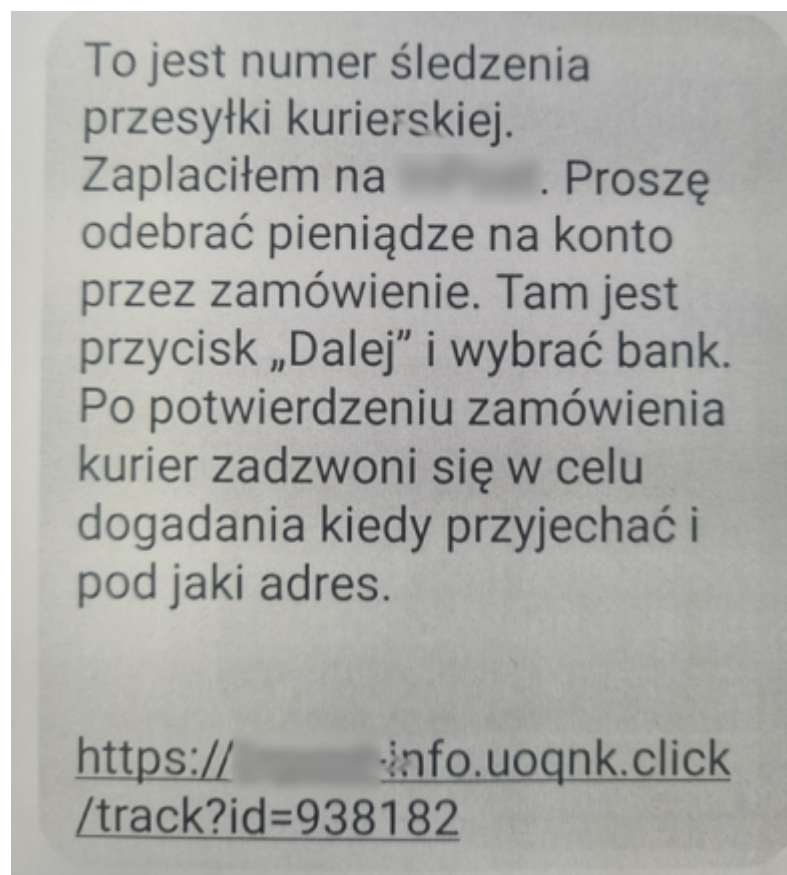




Zaufaj, a wyczyszczą Ci konto. Ona straciła 2 000 zł

data aktualizacji: 2022.11.02



Trudnią się oszukiwaniem ludzi. Śledzą portale aukcyjne i odpowiadają na ukazujące się ogłoszenia sprzedaży nawet najdrobniejszych przedmiotów. Często kontaktują się w przeciągu kilku chwil od publikacji ogłoszenia. Działają sprawnie, pewnie i mają jeden cel - dostać się do konta bankowego ofiary i ukraść, ile się da. Nieświadome ofiary oszukańczego procederu klikają w przesłane im linki, podają swoje wrażliwe dane i zamiast otrzymać należność za sprzedawane rzeczy, tracą pieniądze.

Tak właśnie stało się w miniony piątek (28 października), kiedy to nowomiejscy policjanci przyjęli zawiadomienie od mieszkanki tego powiatu o oszustwie, którego padła ofiarą.

- Kobieta wystawiła na swoim profilu na koncie społecznościowym ogłoszenie o sprzedaży ubrań dziecięcych za kwotę 50 zł. Po jakimś czasie zgłosiła się do niej kobieta, która była zainteresowana ich kupnem - podali mundurowi z nowomiejskiej KPP. - W celu finalizacji transakcji rzekoma „kupująca”

przesłała sprzedającej link do śledzenia paczki, po kliknięciu którego musiała podać trzykrotnie kody BLIK.

Jak można się domyślić, w ten sposób kupująca nie sfinalizowała transakcji, a sama straciła pieniądze z własnego konta. W tym przypadku było to 2 000 zł.

JAK DZIAŁAJĄ OSZUŚCI?

Oszustwa „na kupującego”

- Wystawiasz swoją rzecz na portalu ogłoszeniowym. Znajduje się kupiec. Odzywa się najczęściej za pośrednictwem aplikacji telefonicznej służącej do komunikacji. Twierdzi, że kupił przedmiot i za niego zapłacił, a pieniądze możesz odebrać po wejściu w link.
- Teraz oszust wysyła Ci link do witryny internetowej. Klikasz i trafiasz na stronę łudząco podobną do strony danego portalu ogłoszeniowego.
- Na stronie jest formularz z prośbą o podanie danych twojej karty i stan Twojego konta bankowego. Chcąc otrzymać pieniądze za sprzedany przedmiot, wypełniasz formularz.
- Przychodzi do Ciebie SMS z banku, z kodem do autoryzacji. Ty nie czytasz go uważnie i wpisujesz kod do formularza. W SMS-ie jest jasno napisane, że autoryzujesz dodanie Twojej karty do Google Pay lub Apple Pay. Oszust Cię okrada. Płaci twoją kartą za pomocą aplikacji płatniczej lub wypłaca nią gotówkę w bankomacie.
- Koniec. Twoje konto jest puste.

KPP NML/red. kontakt@infoilawa.pl.

Źródło: <https://www.infoilawa.pl/aktualnosci/item/69112-zaufaj-a-wyczyszcza-ci-konto-ona-stracila-2-000-zl>