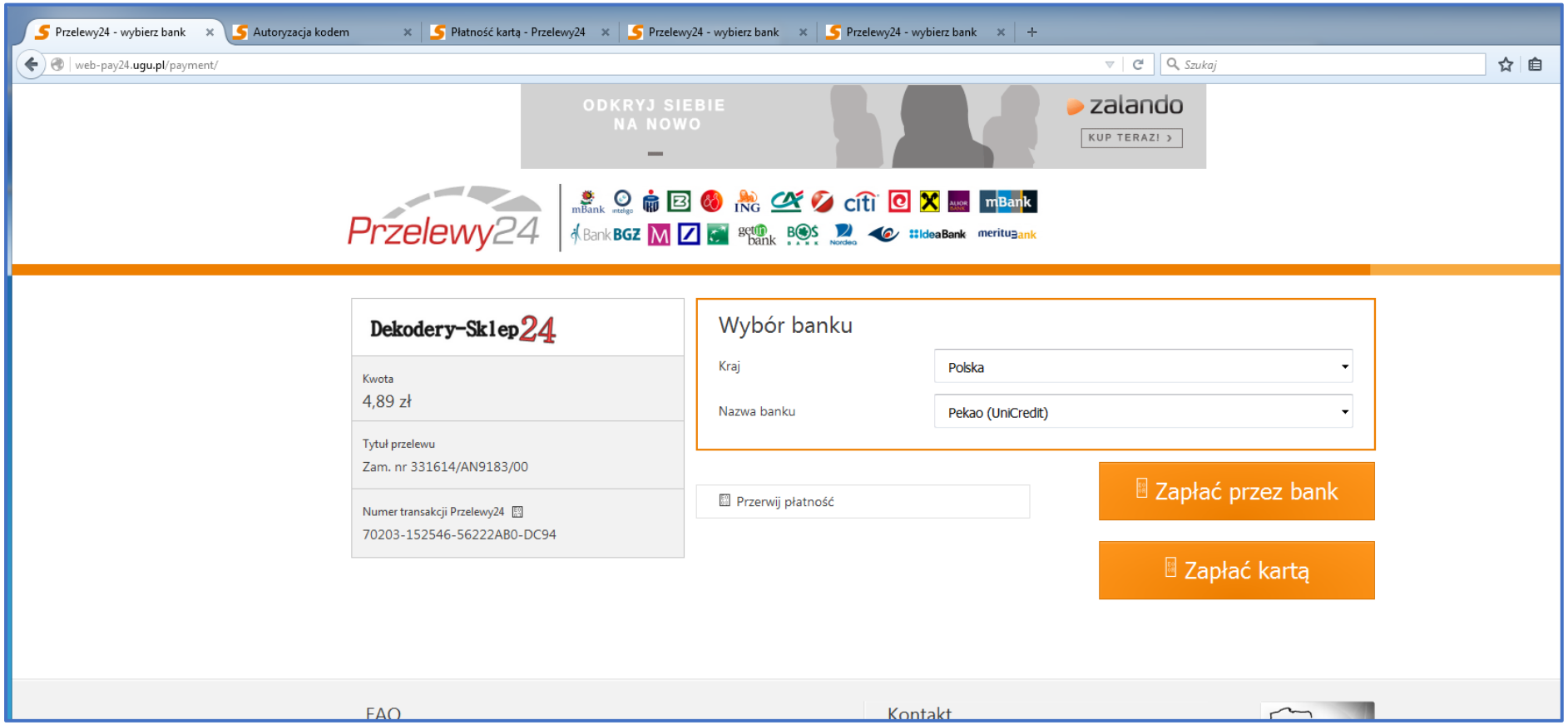
Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich ostrzega klientów banków korzystających z bankowości elektronicznej przed przestępcami, którzy podszywając się pod znajomych z Facebooka wyłudzają dane do bankowości elektronicznej. Dane te służą następnie do kradzieży środków z rachunków klientów.

Mechanizm jest następujący:

- Przestępca podszywający się pod znajomego ofiary z Facebooka prosi o wykonanie przelewu kliku złotych, ponieważ musi pilnie za coś zapłacić.
- Jako metoda płatności sugerowana jest jedna z usług szybkich płatności.
- Ofiara otrzymuje w trakcie korespondencji link do fałszywej strony, przy pomocy której ma dokonać płatność.
- Jednocześnie jest wstępnie informowana o tym, iż kod SMS na potrzeby potwierdzenia płatności może przyjść z kilkuminutowym opóźnieniem.

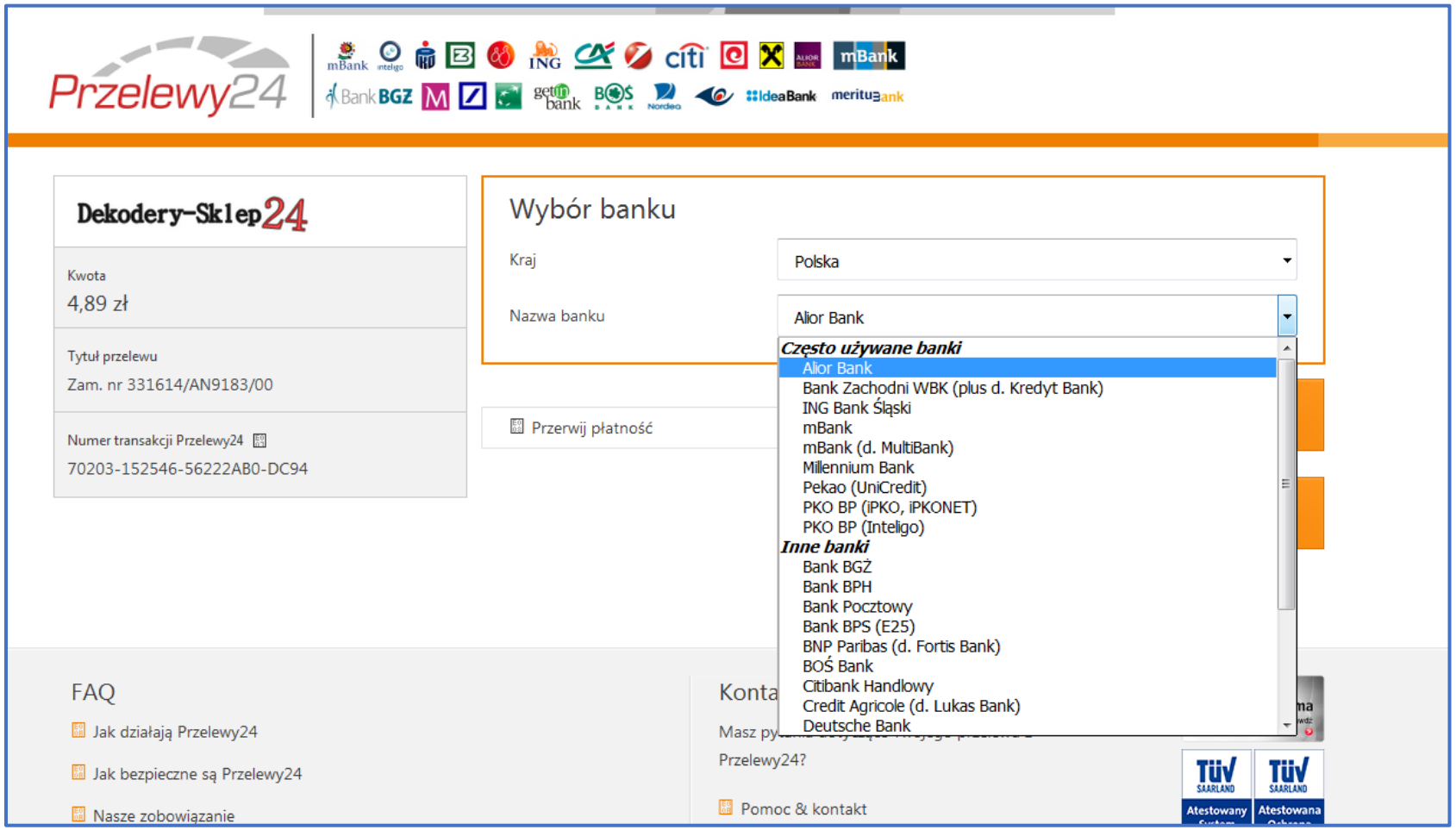
Przykładowa korespondencja na Facebooku. Źródło : www.mbank.pl/uwazniwsieci/page/chron-dane/przyklady.html

- Osoba, która kliknie na link zostaje przekierowana na fałszywą stronę przypominającą z wyglądu usługę szybkiej płatności ze spreparowanymi danymi do płatności na kwotę 4,89 zł.

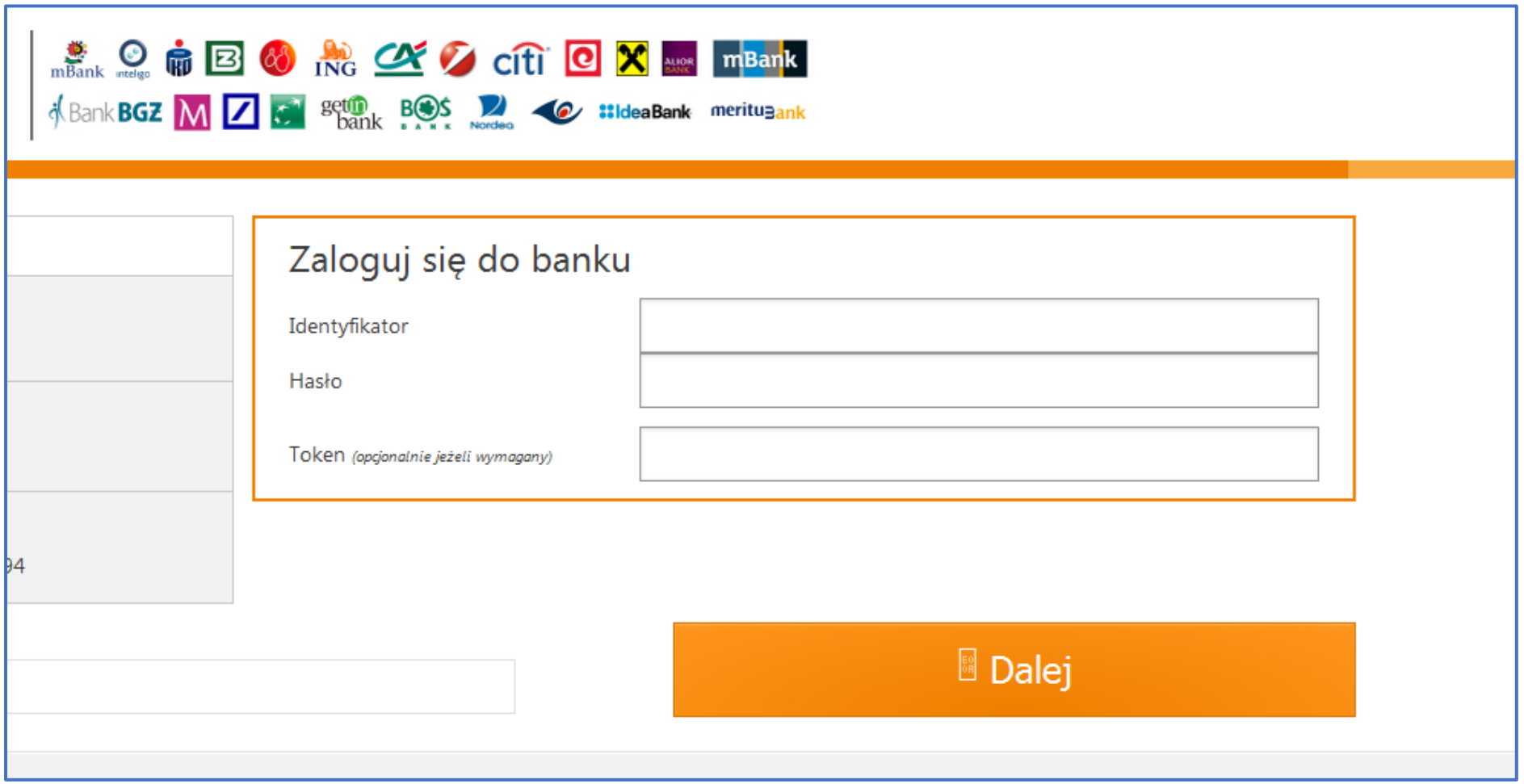


- do wyboru jest „Zapłać przez Bank” lub „Zapłać kartą”.

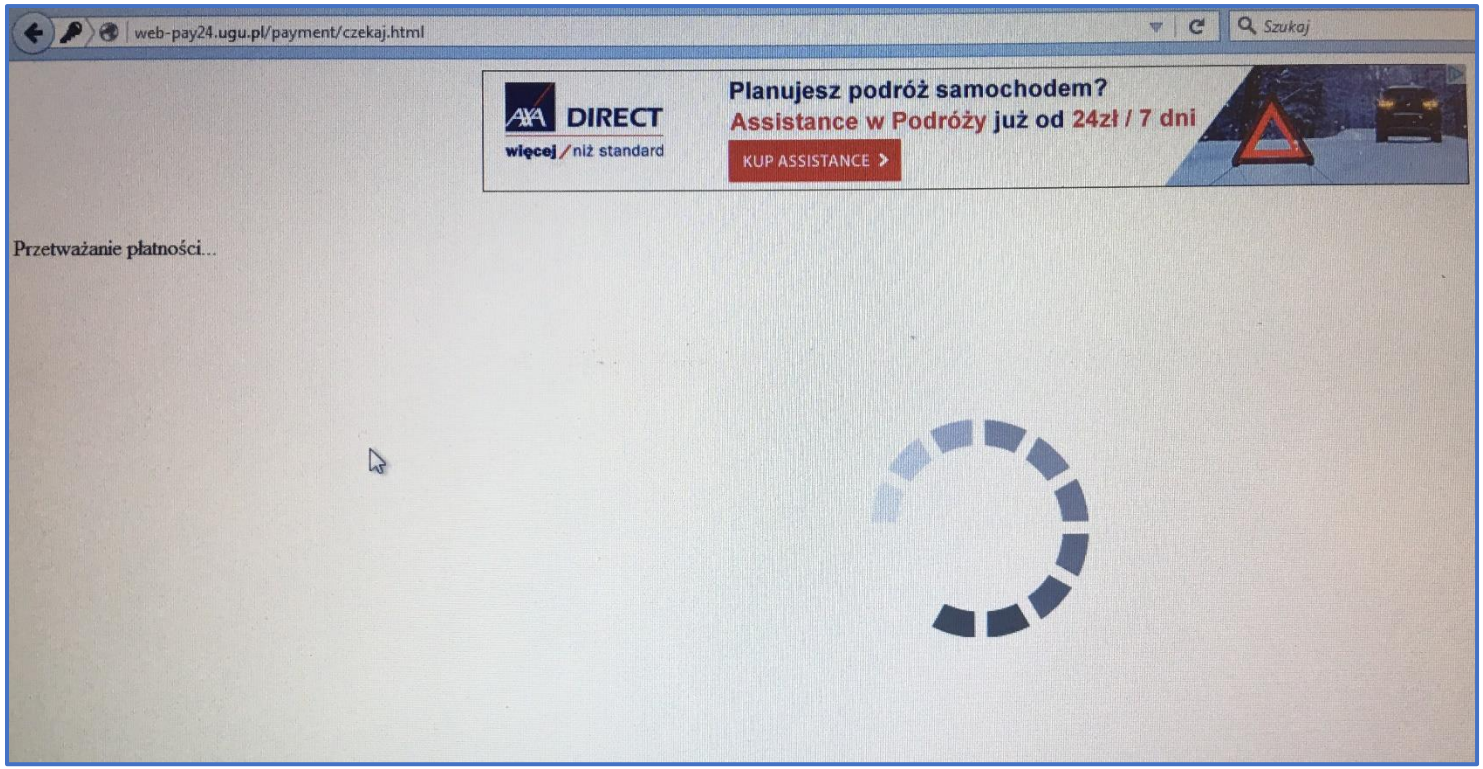
- W przypadku wyboru „Zapłać przez Bank” nieświadoma osoba ma do wyboru bank, którego jest klientem. Do wyboru jest większość banków w Polsce.



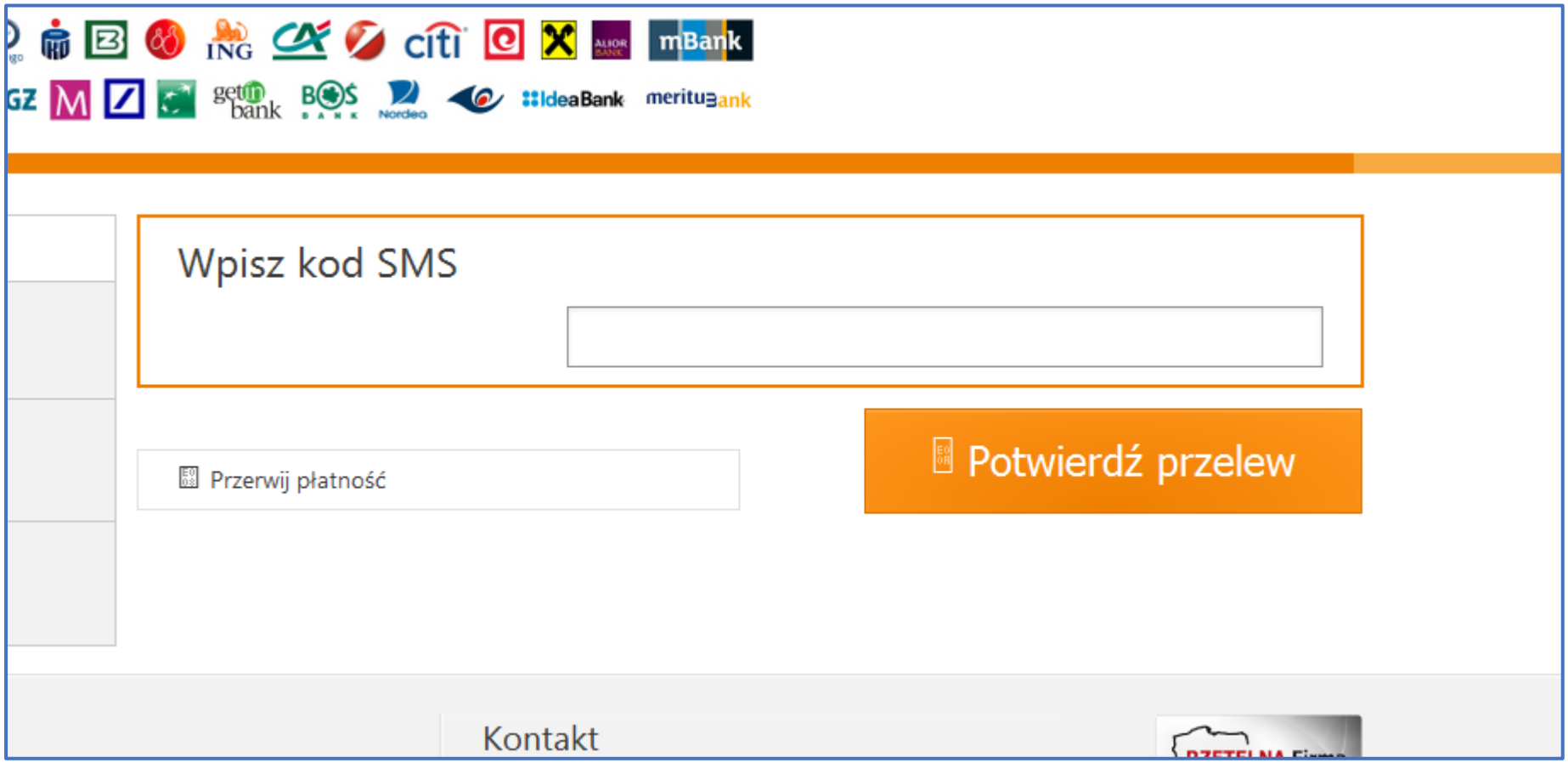
- Po wybraniu banku, w następnym kroku ofiara proszona jest o podanie danych do logowania.



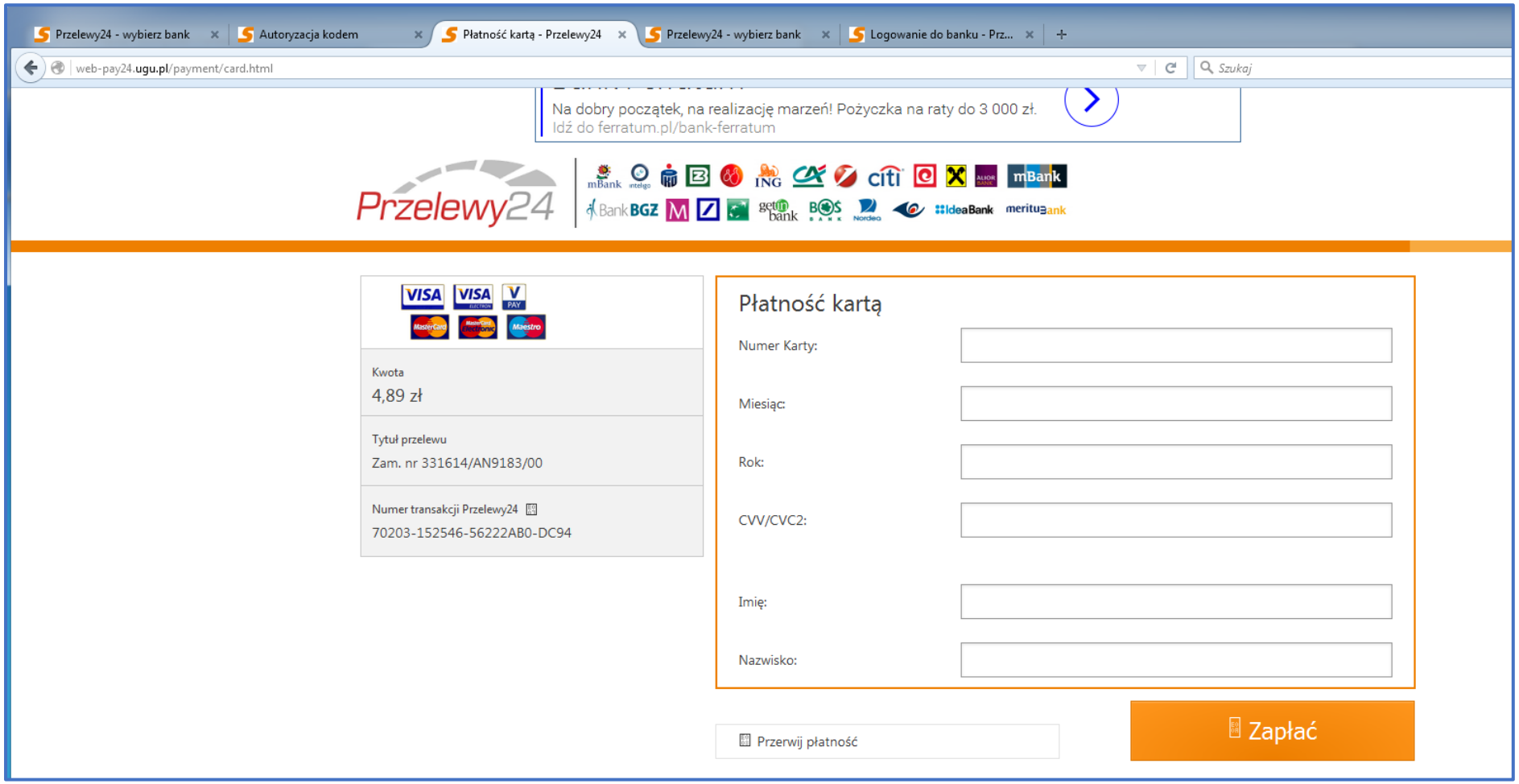
- W przypadku, kiedy ofiara poda powyższą informację, przestępcy na ich podstawie logują się równolegle do bankowości internetowej danej osoby i przygotowują przelew z rachunku klienta na maksymalną kwotę z dostępnych środków.
  W tym czasie widzi on na fałszywej stronie komunikat o przetwarzaniu płatności.



- Po kilku minutach na ekranie pojawia się prośba o podanie hasła SMS. Po jego wpisaniu przez ofiarę przestępcy autoryzują przelew z jego rachunku.



- W przypadku wybrania na pierwszej stronie opcji „Zapłać kartą” otwiera się strona, która wyłudza wrażliwe dane karty, mogące służyć do dokonywania płatności przez Internet.



Bankowe Centrum Cyberbezpieczeństwa przypomina, żeby nie otwierać podejrzanych linków, adresy do serwisów bankowych wpisywać ręcznie, podawać dane logowania i kody autoryzujące jedynie na stronach bankowości elektronicznej swojego banku, oraz uważnie czytać treść SMS-ów otrzymywanych z banku dotyczących czynności, które autoryzujemy.

W przypadku identyfikacji takiego lub podobnego zdarzenia należy poinformować swój bank oraz zgłosić incydent na skrzynkę cert@cert.pl.