

Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich ostrzega klientów banków korzystających z bankowości elektronicznej przed przestępcami, którzy podszywając się pod znajomych z Facebooka wyłudniają 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 kilku 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.

The image shows a screenshot of a Facebook chat interface. At the top, there is a search bar, a profile picture placeholder, and the text 'Strona główna'. Below this is a navigation bar with a '+ Nowa wiadomość' button and icons for chat, settings, and search. The chat messages are as follows:

G
siemka 😊 mam prosbe ;p potrzebuje zrobic przelew nie mam nic na koncie ;p dasz rade mi to zrobic? odeśle Ci z napiwkkiem haha 😊

S
Hej 😊 jasne nie ma sprawy 😊 podaj nr konta i juz robię 😊

G
sie tam płaci przez przelewy24 😊
co miesiac tam place bo kupuje tam kody na kanały tv a teraz mi braklo na koncie xD 😊 wybiera sie tylko bank i sie loguje i przeważnie sie kilka minut czeka na kod sms z banku potwierdzający i tyle 😊
ok to jest tam na liście 😊
to daje link do mojej płatności :))\

pay-przelewy24.ugu.pl/payment

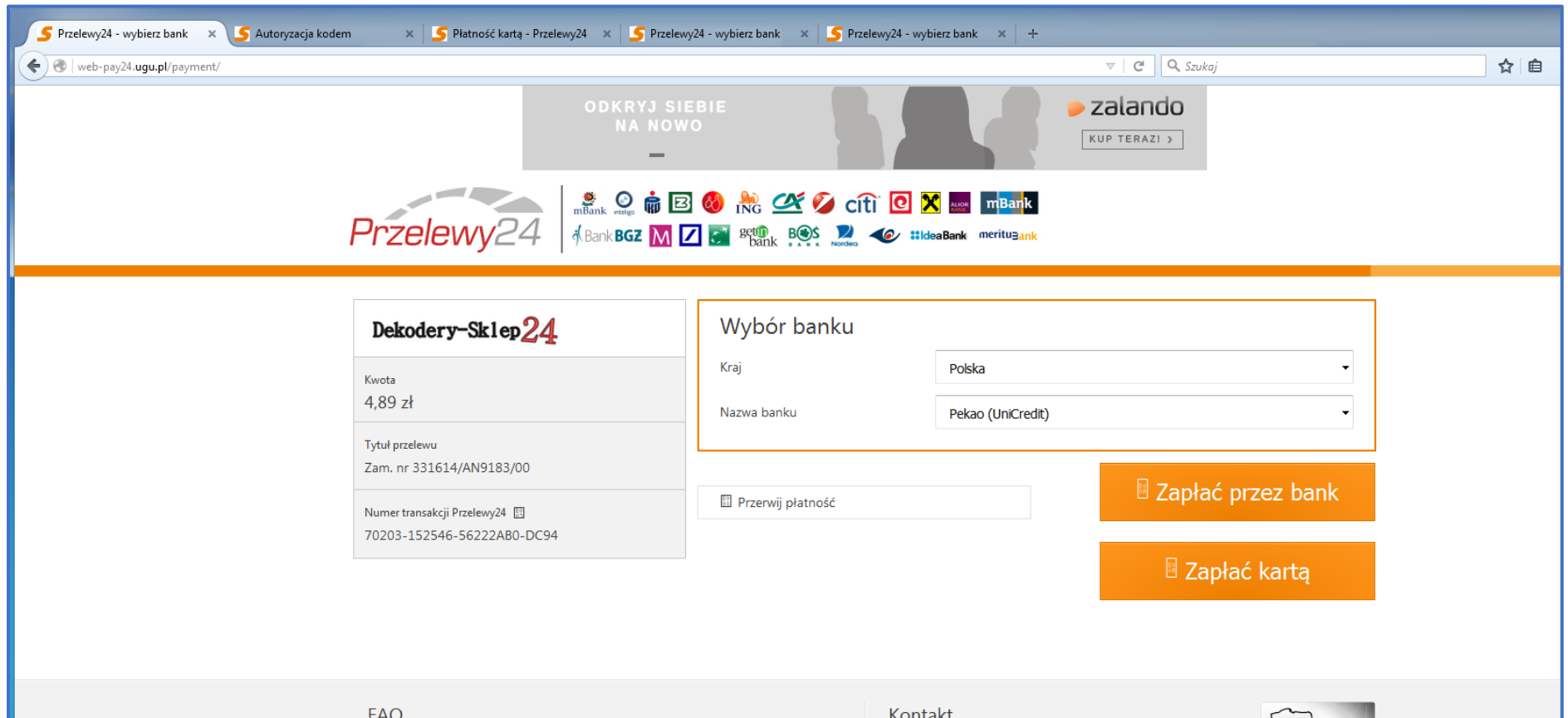
jak bedziesz na stronie KOD SMS to musisz poczekać pare min i dopiero przyjdzie a jak przyjdzie to wpisz od razu zeby kod nie wygasł

Three grey callout boxes provide additional information:

- Left callout:** Uważaj na prośby przełania jakiegokolwiek sumy - nawet jeśli wydaje Ci się, że rozmawiasz ze swoim znajomym.
- Bottom-left callout:** Zwróć dokładną uwagę na przesyłane linki do dokonania płatności. Mogą kierować do fałszywych stron.
- Right callout:** Przeczytaj uważnie wiadomość. Cyberprzestępcy często piszą o problemach z logowaniem lub blokowaniem konta. Chcą na Tobie wymusić szybką reakcję. Dlatego zastanów się spokojnie nad sprawą, a gdy masz wątpliwości, zadzwoń do banku.

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.

The screenshot displays the Przelewy24 website interface. At the top, there is a navigation bar with the Przelewy24 logo and a row of logos for various banks including mBank, Inteligo, ING, Citi, and others. Below this, the main content area is divided into sections. On the left, there is a box for 'Dekodery-Sklep24' containing transaction details: Kwota 4,89 zł, Tytuł przelewu Zam. nr 331614/AN9183/00, and Numer transakcji Przelewy24 70203-152546-56222AB0-DC94. The central part of the page is titled 'Wybór banku' and features a dropdown menu for 'Kraj' set to 'Polska' and another dropdown for 'Nazwa banku'. The bank selection dropdown is open, showing a list of banks under the heading 'Często używane banki', with 'Alior Bank' selected. Below this, there is a section for 'Inne banki' listing various other banks. A 'Przerwij płatność' button is visible below the bank selection area. At the bottom of the page, there is a footer with 'FAQ' links, a 'Konta' section, and two TÜV Saarland certification logos.

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

The screenshot shows a mobile application interface for logging into a bank. At the top, there is a horizontal bar containing logos of various Polish banks: mBank, inteligo, BZ WBK, ING, AXA, Citi, X, ALIOR BANK, mBank, Bank BGZ, M, Z, getbank, BOS BANK, Nordea, IdeaBank, and merituBank. Below this bar, the main content area is titled "Zaloguj się do banku". It features three input fields: "Identyfikator", "Hasło", and "Token (opcjonalnie jeżeli wymagany)". To the left of these fields is a vertical sidebar with three grey rectangular buttons. At the bottom right, there is a large orange button labeled "Dalej" with a mobile phone icon. The number "94" is visible on the left side of the screen.


94

Zaloguj się do banku

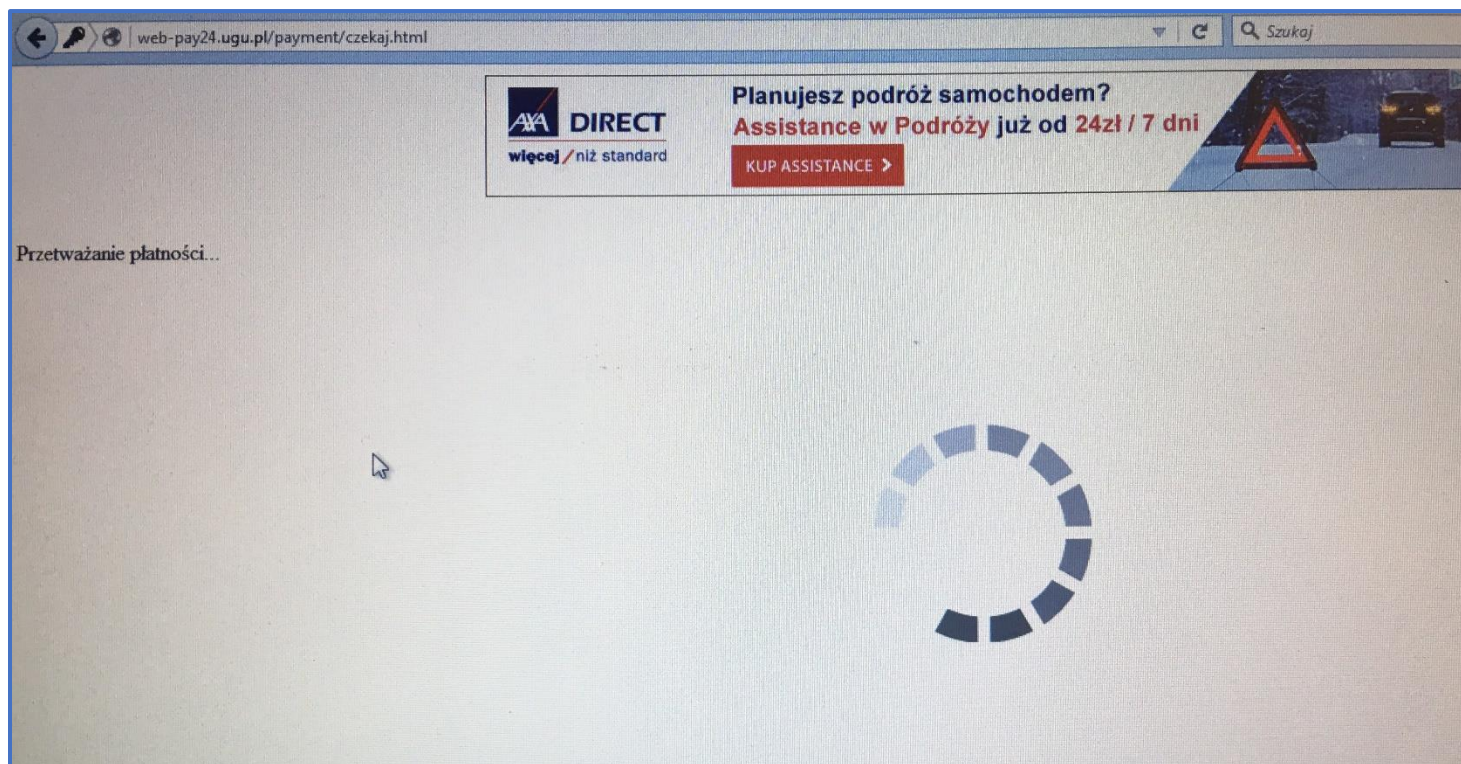
Identyfikator

Hasło

Token *(opcjonalnie jeżeli wymagany)*

 Dalej

- W przypadku, kiedy ofiara poda powyższą informację, przestępcy na ich podstawie logują się równoległe 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.

The screenshot shows a mobile banking application interface. At the top, there is a horizontal bar containing logos of various banks: ING, Citi, mBank, GZ, M, getbank, BOŚ BANK, Nordea, IdeaBank, and meritusank. Below this bar, the main content area is white with an orange border. The text "Wpisz kod SMS" (Enter SMS code) is displayed in a large font. Below the text is a long, empty rectangular input field. To the left of the input field, there is a button with a red "X" icon and the text "Przerwij płatność" (Cancel payment). To the right of the input field, there is a large orange button with a white "EO OR" icon and the text "Potwierdź przelew" (Confirm transfer). At the bottom of the screen, there is a grey bar with the text "Kontakt" (Contact) on the left and a small logo on the right.

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

The screenshot shows a web browser window with several tabs open, including 'Przelewy24 - wybierz bank', 'Autoryzacja kodem', 'Płatność kartą - Przelewy24', and 'Logowanie do banku - Prz...'. The address bar shows 'web-pay24.ugu.pl/payment/card.html'. A promotional banner at the top reads: 'Na dobry początek, na realizację marzeń! Pożyczka na raty do 3 000 zł. Idź do ferratum.pl/bank-ferratum'. Below the banner is the Przelewy24 logo and a row of logos for various banks: mBank, inteligo, B, ING, AXA, citi, X, ALIOR, mBank, Bank BGZ, M, Z, getbank, BOS, NORDIA, IdeaBank, and merituBank.

The main content area is divided into two columns. The left column contains transaction details:

- Logos for VISA, VISA Electron, V PAY, MasterCard, Maestro, and Maestro.
- Kwota: 4,89 zł
- Tytuł przelewu: Zam. nr 331614/AN9183/00
- Numer transakcji Przelewy24: 70203-152546-56222AB0-DC94

The right column is titled 'Płatność kartą' and contains the following input fields:

- Numer Karty:
- Miesiąc:
- Rok:
- CVV/CVC2:
- Imię:
- Nazwisko:

At the bottom of the page, there is a button labeled 'Przerwij płatność' and a large orange button labeled 'Zapłać'.

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.