

Robisz zakupy przez internet? Zachowaj czujność!

1. **Korzystaj tylko z zaufanych sklepów internetowych.** Sprawdzaj opinie o sklepie, w którym chcesz zrobić zakupy.
2. **Nie loguj się do banku z linków, które podsyłają Ci kupujący lub sprzedający:**
 - w mailach,
 - w SMS-ach,
 - przez komunikatory internetowe.

Kupuj lub sprzedawaj tylko za pośrednictwem płatności udostępnionych przez sklep, w którym robisz zakupy.

Pamiętaj! Nie klikaj w podejrzane linki i nie podawaj swoich danych do logowania czy danych swojej karty.



Mechanizm działania:

- Oszust (może być osobą sprzedającą lub kupującą) podaje Ci link do fałszywej strony, której celem jest wyłudzenie Twoich danych.
- Link przekierowuje Cię do strony, która wymusza podanie danych karty. Kiedy podasz dane, otrzymasz informację, że oszust zapłacił za przedmiot, a płatność się powiodła. Zobaczysz też informację o nadaniu paczki na równie podejrzany adres.
- Na Twój numer telefonu przychodzi wiadomości z potwierdzeniem odebrania płatności, ale wyłącznie po wejściu w link z SMS-a.
- Nawet jeśli nie sprzedajesz lub nie kupujesz na portalach sprzedażowych, na Twoją skrzynkę mailową mogą przychodzić fałszywe wiadomości podszywające się pod różne serwisy. Najczęściej, gdy klikniesz w link, zostaniesz przekierowana/y na fałszywą stronę banku. Tam masz podać swoje dane do logowania lub dane swojej karty płatniczej, aby rzekomo odebrać pieniądze.

3. Wpadła Ci w oko oferta produktu w zadziwiająco niskiej cenie?

Jeśli coś wydaje się podejrzane, to prawdopodobnie takie jest. Pamiętaj, że bardzo okazjna cena drogiego produktu w sklepach internetowych to popularne oszustwo.

4. Wygrałeś/ęś w loterii, w której nie brałeś/ęś udziału? Znalazłeś/ęś niesamowitą promocję?

Upewnij się czy to prawdziwa oferta. W tym przypadku zostaniesz poproszona/y o uiszczenie symbolicznej kwoty. Jednorazowa opłata wstępna najczęściej kończy się cyklicznym obciążaniem Twojego rachunku na pokaźne sumy pieniędzy.

Intercity Polska
Sponsorowane
Identyfikator biblioteki: 1006876563686389

PKP Intercity oferuje program socjalny dla wszystkich mieszkańców Polski - certyfikat na 1 rok bezpłatnych przejazdów pociągami PKP Intercity za jedyne 9 zł!

Aby wziąć udział, kliknij przycisk „Przesli wniosek teraz” na dole postu i otrzymaj kartę z darmową dostawą 📄



**1 ROK DARMOWYCH PRZEJAZDÓW
PKP INTERCITY ZA JEDYNE 9zł!**

Intercity Polska Prześlij wnio...

Intercity Polska
Sponsorowane
Identyfikator biblioteki: 979874389750445

PKP Intercity świętuje swoje 20-lecie! Z tej okazji dajemy każdemu wyjątkową okazję - otrzymanie certyfikatu PKP Intercity na 1 rok bezpłatnych przejazdów za jedyne 9 zł!

Aby wziąć udział, kliknij przycisk „Przesli wniosek teraz” na dole postu i otrzymaj kartę z darmową dostawą 📄



**1 ROK DARMOWYCH PRZEJAZDÓW
PKP INTERCITY ZA 9 ZŁ!**

Intercity Polska Prześlij wnio...

👉 **Reklama na portalu Facebook fałszywej oferty promocyjnej przewoźnika kolejowego.** Źródło: CSIRT KNF/ Raport zagrożeń fraudowych.



Mechanizm działania:

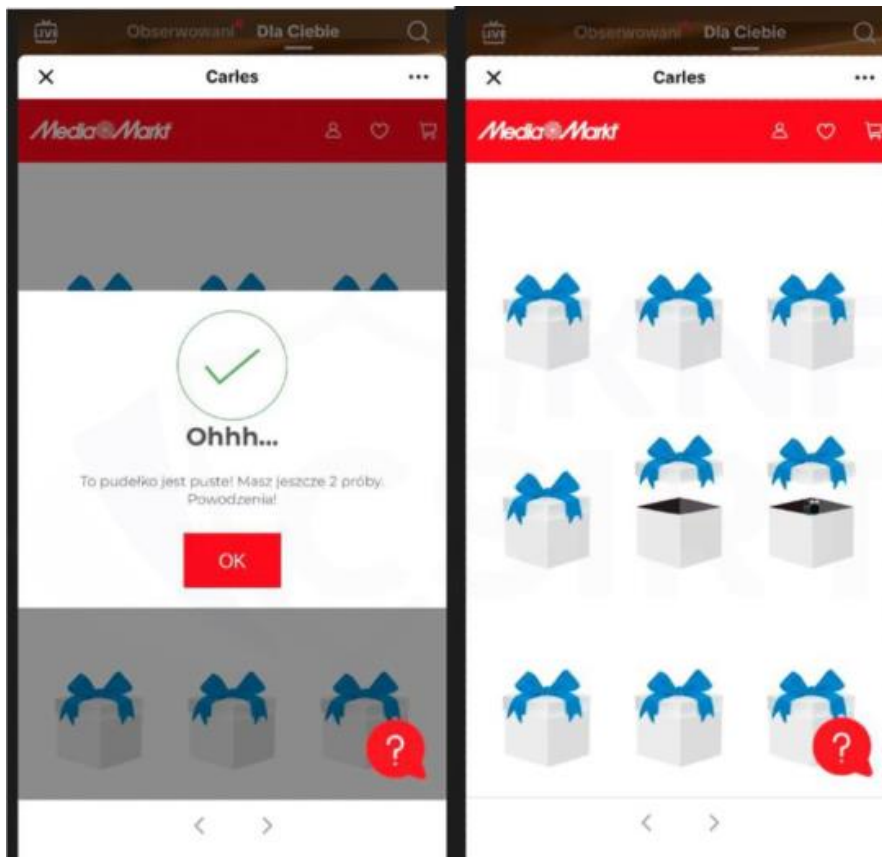
- Wpadła Ci w oko reklama na portalu społecznościowym z zaskakująco korzystną ofertą (często wręcz nierealną)?
- Klikasz w nią i otwiera się strona z rzekomą promocją.
- Gdy przejdziesz kilka kroków, musisz podać dane swojej karty, aby skorzystać z „atrakcyjnej” oferty.
- Dostajesz SMS-a z kodem, dzięki któremu możesz dodać karty do cyfrowego portfela. Kod podany w wiadomości musisz podać na stronie, aby skorzystać z oferty.
- Pierwsza kwota przedstawiona w „reklamie” pobierana jest od razu. Po kilku dniach lub miesiącach możesz zauważyć kolejne nieuprawnione transakcje. Opłaty będą pobierane cyklicznie. Z biegiem czasu mogą być coraz wyższe. „Regulamin” pobierania opłat jest często ukryty, pisany małymi literami.



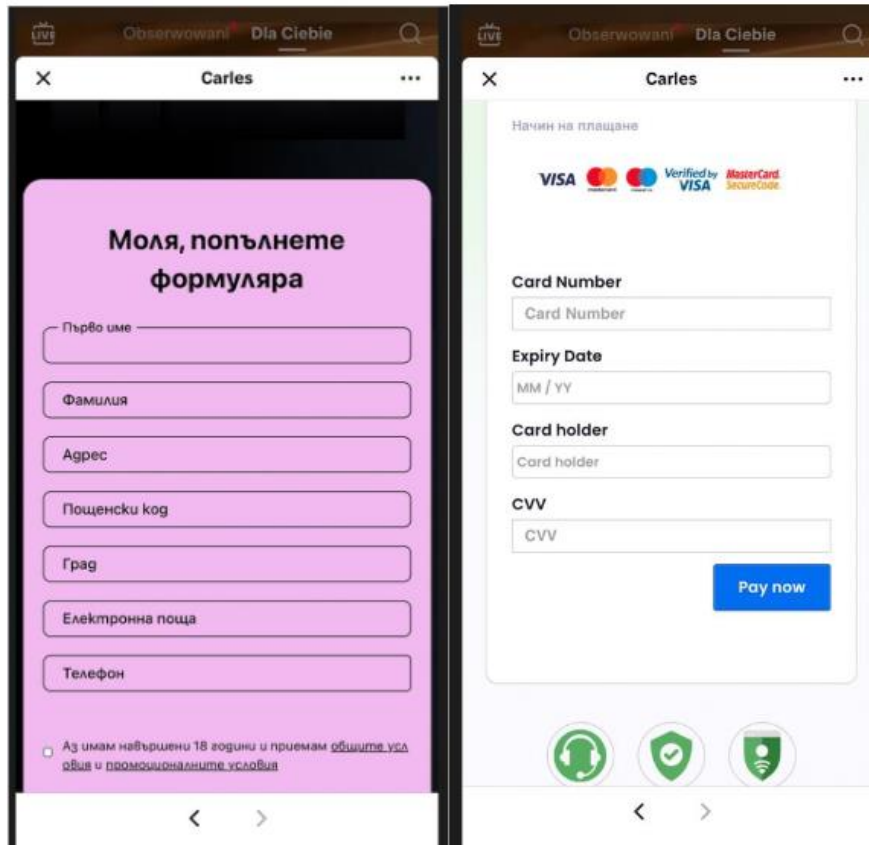
👉 Reklama na portalu Facebook fałszywej sprzedaży. Źródło: SCIRT KNF/ Raport zagrożeń fraudowych.



👉 Reklama na portalu społecznościowym oferująca rzekomą możliwość otrzymania telefonu wartego kilka tysięcy za 9 złotych. Źródło: SCIRT KNF/Zarabianie przez oglądanie.



👉 Losowanie fałszywej nagrody. Źródło: SCIRT KNF/Zarabianie przez oglądanie.



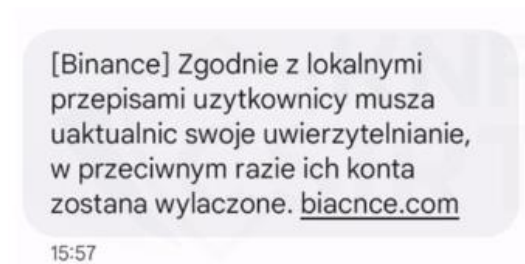
👉 Ekran wyludzania danych osobowych oraz informacji o kartach płatniczych. Źródło: SCIRT KNF/Zarabianie przez oglądanie


5. Czytaj dokładnie treści SMS-ów oraz maili. Zwracaj uwagę na to, co autoryzujesz.

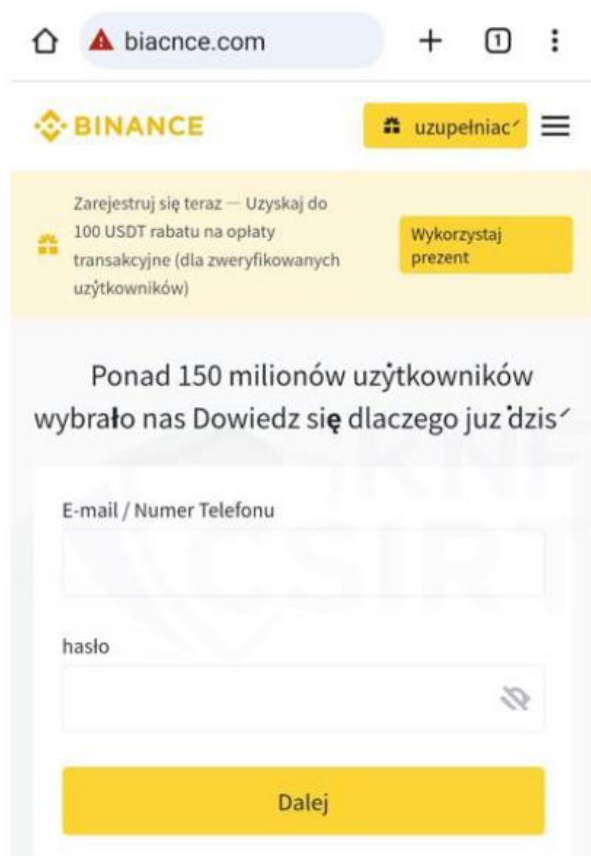
Gdy dodasz swoją kartę płatniczą do wirtualnego portfela, otrzymasz powiadomienie autoryzacyjne z banku. Dokładnie czytaj oraz weryfikuj każde powiadomienie dot. transakcji.


6. Uważaj na fałszywe SMS-y.

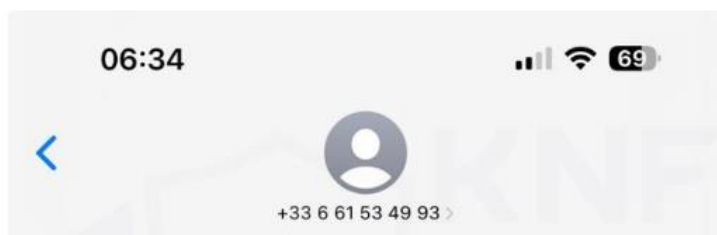
Pamiętaj, że oszuści mogą podszywać się pod popularne firmy. Gdy klikniesz w link zostaniesz przekierowana/y na stronę phishingową. Na stronie będziesz proszona/y o przekazanie swoich danych osobowych, danych karty płatniczej czy danych logowania do Twojego banku. Te dane trafią do oszustów.



 **Wiadomość SMS podszywająca się pod giełdę kryptowalut.** Strona phishingowa zawiera błędy, nazwa odbiega od tej, która została podana w nawiasie. Źródło: SCIRT KNF/Raport zagrożeń fraudowych.



 **Wygląd strony phishingowej podszywającej się pod giełdę kryptowalut.** Oryginalna strona jest tłumaczona na język polski, czasowniki są odmienione oraz uwzględnione są polskie znaki. Źródło: SCIRT KNF/ Raport zagrożeń fraudowych.



Wiadomość
Dzisiaj, 00:47

UPS: Twoja paczka oczekuje na przetworzenie: <https://parcell-ups.com>

 Wiadomość SMS podszywająca się pod firmę kurierską z linkiem do strony phishingowej. Źródło: SCIRT KNF/ Raport zagrożeń fraudowych.



 Wygląd po kliknięciu w link strony phishingowej podszywającej się pod firmę kurierską. Źródło: SCIRT KNF/ Raport zagrożeń fraudowych.

The screenshot shows a web browser at the URL `parcel-ups.com/main/card.p`. The page features the UPS logo and navigation icons. The main heading is "Płatność za opłaty celne" (Payment for customs fees), with a sub-heading "Krok 2 z 2" (Step 2 of 2). Below this, there are logos for VISA, Mastercard, DISCOVER, and AMERICAN EXPRESS. A security notice states: "Bezpieczna płatność w wysokości 1.99 €" (Secure payment of 1.99 €). The payment form consists of three input fields: "Numer karty" (Card number), "Data ważności (MM/RR)" (Expiration date), and "CVV". A large yellow "Zapłać" (Pay) button is at the bottom.

👉 **Wyludzenie numeru karty, daty ważności oraz kodu CVV pod pretekstem płatności za opłaty celne.** Źródło: SCIRT KNF/ Raport zagrożeń fraudowych.

7. Pamiętaj o usłudze 3D-Secure.

To dodatkowe, darmowe zabezpieczenie płatności kartą w internecie. Zakupy kartą w sklepie, który obsługuje 3D Secure potwierdzisz na dwa sposoby:

- w aplikacji mobilnej
- poprzez udzielenie odpowiedzi na pytanie weryfikacyjne oraz podanie hasła 3D Secure (jednorazowego kodu SMS), które otrzymasz na numer telefonu komórkowego podany przez Ciebie do kontaktu w Twoim Banku.

Więcej o usłudze 3D Secure dowiesz się na stronie: <https://bs.bialystok.pl/klienci-indywidualni/karty/usluga-3d-secure/>.



Dbaj o bezpieczeństwo i:

- kupuj tylko w zaufanych sklepach – sprawdź opinie innych klientów
- nie podawaj danych swojej karty płatniczej na stronach, do których link otrzymałaś/eś w SMS-ie lub mailu
- dane karty płatniczej wpisuj wyłącznie na stronie, która wyświetli się po zatwierdzeniu Twoich zakupów
- zawsze sprawdzaj szczegóły płatności przesłane przez Twój bank w SMS-ie lub pushu zanim potwierdzisz płatność
- nigdy nie przesyłaj zdjęć lub skanu karty. Nie publikuj ich w mediach społecznościowych
- nie podawaj osobom nieupoważnionym danych karty, czy haseł potrzebnych do potwierdzenia płatności
- aktualizuj antywirusa na urządzeniach, z których korzystasz
- jeśli zgubisz kartę, skontaktuj się placówką banku obsługującą Twój rachunek
- ustaw limity transakcji internetowych i limity transakcji MOTO w takiej wysokości, jaka jest Ci potrzebna. Dbaj o to, żeby nie były za wysokie
- ustaw metodę weryfikacji transakcji internetowych w usłudze 3D Secure
- używaj nieoczywistych haseł, trudnych do odgadnięcia przez inne osoby,

aby nie dać się oszustom!

Jeśli zauważysz podejrzaną transakcję, które nie były przez Ciebie autoryzowane, natychmiast zastrzeż swoją kartę wybierając jeden z następujących sposobów:



- w aplikacji mobilnej Nasz Bank (zakładka „Karty”)
- w serwisie Internet Banking (zakładka „Karty”)
- zadzwoń do placówki obsługującej Twój rachunek
- zadzwoń na Infolinię czynną 24/7:
 - 800 88 88 88 (bezpłatne połączenie)
 - 61 647 28 46 (z zagranicy; opłata zgodna z taryfą operatora)