

# KOMENDA POWIATOWA POLICJI W KOŁOBRZEGU

<https://kolobrzeg.policja.gov.pl/zkl/aktualnosci/aktualnosci/50400,Przypominamy-ze-oszusczy-wykorzystuja-OLX-WhatsApp-czy-Vinted.html>

2022-12-06, 12:54

## PRZYPOMINAMY, ŻE OSZUŚCI WYKORZYSTUJĄ OLX, WHATSAPP CZY VINTED!

Od pewnego czasu oszuści w celu wyłudzenia danych z naszej karty posługują się platformą OLX, VINTED oraz komunikatorem WhatsApp. W związku z tym cały czas przypominamy użytkownikom o metodach jakimi posługują się przestępcy, by wyłudzić nasze dane, a w konsekwencji wyczyścić konto bankowe. Wskazujemy jak uniknąć oszustwa oraz co zrobić, gdy zostaniemy oszukani. Apelujemy do użytkowników o rozwagę i ostrożność!



### JAK UNIKNĄĆ OSZUSTWA?

- Czytaj SMS-y od Banków. Zwróć uwagę na to, co autoryzujesz.
- Poznaj zasady bezpieczeństwa swojego banku i stosuj się do nich gdy korzystasz z portali aukcyjnych
- Miej ograniczone zaufanie do potencjalnych kontrahentów.
- Rozliczaj się bezpośrednio przez dany portal. Unikaj bezpośrednich transakcji. Uważaj na próby nawiązania kontaktu poza portalem, np. przez WhatsApp czy Messenger. Zobacz instrukcje płatności z OLX
- Oszuści mogą podrobić stronę portalu aukcyjnego – tak samo jak i każdą inną stronę, również naszą. Dlatego zwracaj uwagę na adres widoczny w przeglądarce. Zobacz poradnik OLX
- Zwróć uwagę na poprawność językową strony, na której przekazujesz dane karty. Fałszywe strony często zawierają błędy, są napisane niegrammatycznie.

### CO ROBIĆ, GDY ZOSTANIESZ OSZUKANY?

- Koniecznie skontaktuj się ze swoim Bankiem przez infolinię.

- Możesz od ręki zastrzec swoją kartę w bankowości lub aplikacji swojego banku. Karta w ten sposób przestanie działać również w Google Pay i Apple Pay.
- Poinformuj Policję.
- Na oficjalnym blogu OLX możemy przeczytać „Pamiętaj, że OLX nie generuje linków do opłacenia zakupu, czy do podania danych do otrzymania płatności za oferowany przez Ciebie przedmiot. Jedyną stroną, do której przekierujemy Cię podczas finalizacji Płatności OLX, jest Dotpay – za jej pośrednictwem realizowana jest wpłata.”
- Pamiętaj! Weryfikuj kto i co do Ciebie pisze. Nie wpisuj nigdzie numeru swojej karty. Nie klikaj w nieznajome linki do stron.
- Policja apeluje o zachowanie szczególnej ostrożności. Nie korzystajcie nigdy z linków, które przychodzą w wiadomościach. Najbezpieczniej jest wpisać samodzielnie adres internetowy strony danego serwisu ogłoszeniowego lub banku. Sprawdzajmy zawsze, czy witryna jest bezpieczna. Jeśli korzystamy z kodów autoryzacyjnych przesłanych SMS-em przez bank lub inne instytucje sprawdzajmy zawsze, czy zawiera polskie znaki.
- Trzeba też pamiętać, by przy podawaniu danych karty bankowej zachować szczególną ostrożność. Należy upewnić się, czy oszuści nie zastawili na nas pułapki.
- Przed potwierdzeniem operacji zawsze sprawdźmy też, czy zgadza się numer konta odbiorcy oraz kwota, jaką chcemy przelać. To może nas uratować przed utratą pieniędzy.