

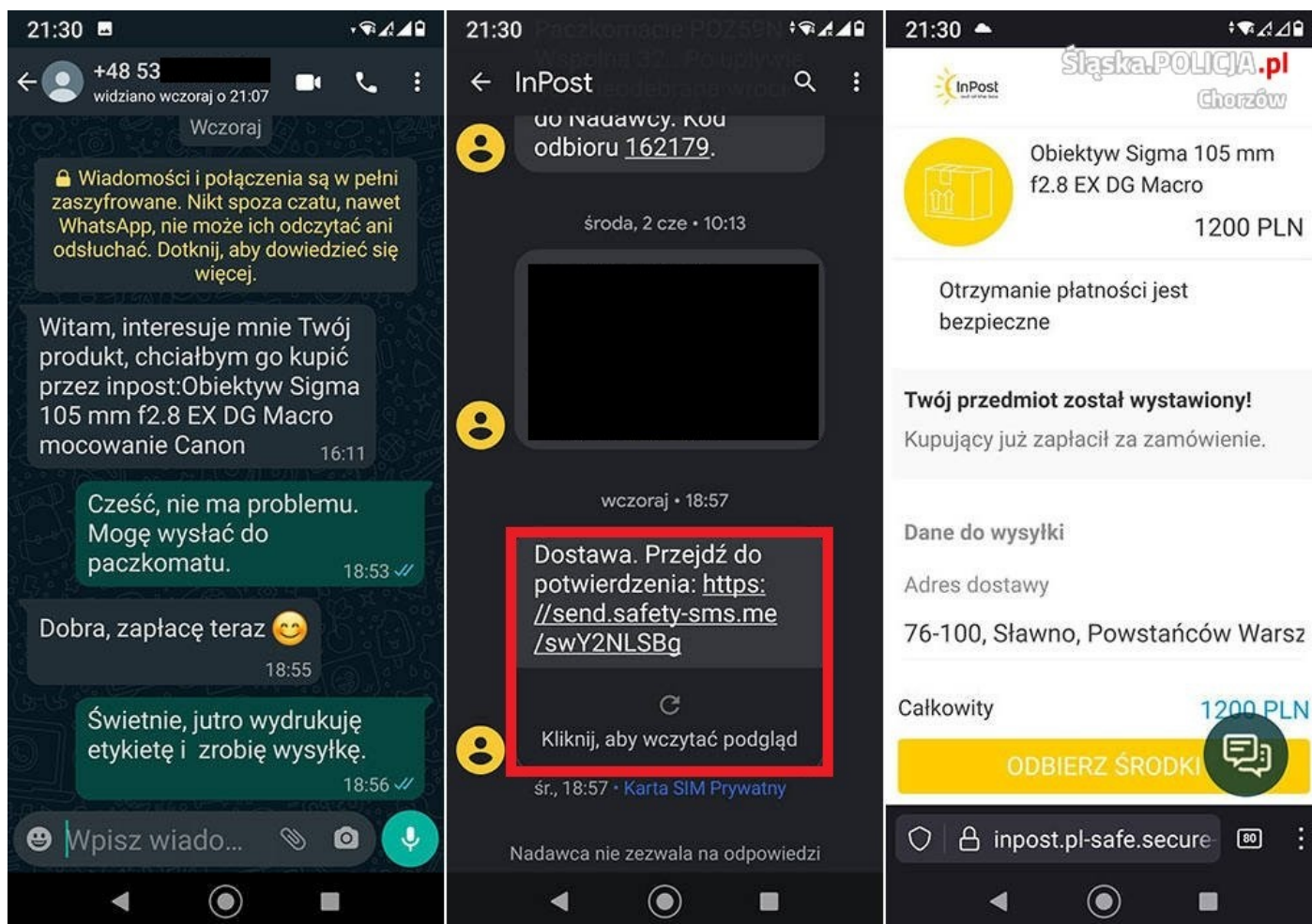
Oszustwa na OLX - na co zwracać uwagę, by nie dać się oszukać?

2022-01-20 10:49 Miejski Rzecznik Konsumentów

Fala wyłudzeń pieniędzy w Internecie stale rośnie. Jedną z metod jest **oszustwo na OLX i Whatsapp** bądź Messenger. O nowych metodach działania cyberprzestępców regularnie informuje policja, administracja i portale internetowe.

Jak przebiega oszustwo na OLX:

- Po wystawieniu produktu na portalu OLX odzywa się do ciebie osoba, która niepoprawną polszczyzną informuje, że dokonała zakupy.
- Rzekomy kupiec twierdzi, że chce zapłacić za towar poprzez usługę płatności OLX. Aby *otrzymać środki na kartę płatniczą* powinienes postępować zgodnie z instrukcjami.
- Oszust wysyła do ciebie link, który prowadzi do podrobionej strony, która udaje usługę płatności OLX. Na tej stronie znajduje się formularz, w którym musisz podać dane z karty płatniczej – numer i datę ważności karty oraz kod CVV/CVC. Niekiedy możesz zostać poproszony o podanie w formularzu przybliżonego stanu konta.
- Następnie otrzymasz SMS z banku z kodem do autoryzacji. W rzeczywistości potwierdzasz dodanie karty do Google Pay lub Apple Pay.
- Złodzieje niezwłocznie przystępują do czyszczenia konta z pieniędzy dokonując szeregu płatności kartą.



Stale apelujemy o czujność i rozwagę.

- Zwracaj uwagę na poprawność językową komunikacji z kupującym, a także strony. Większość ataków przeprowadzają obywatele państw Europy Wschodniej. Podczas rozmowy na chacie robią wiele błędów, tak jakby zdania były tłumaczone przez translator.
- Uważaj na próby kontaktu poza portalem, szczególnie z wykorzystaniem komunikatorów Whatsapp oraz Messenger.
- Nie korzystaj z rozliczeń poza portalem ogłoszeniowym. Sprawdź dokładnie instrukcję płatności na OLX.
- Dokładnie weryfikuj strony, na których się logujesz do bankowości albo podajesz dane swojej karty, bądź dane osobowe. Zwracaj uwagę na adres strony widoczny w przeglądarce.
- Sprawdzaj treść smsów z kodami autoryzującymi transakcje.

Jeśli chcesz coś sprzedać poprzez OLX, zapoznaj się z regulaminem:

<https://blog.olx.pl/2020/06/18/uwaga-na-phishing/>

Apelujemy o zachowanie szczególnej ostrożności i niekorzystanie z linków, które przychodzą w wiadomościach. Najbezpieczniej jest wpisać samodzielnie adres internetowy strony danego serwisu ogłoszeniowego lub banku.

Szczegóły: <https://www.eurolege.pl/oszustwo-na-olx/>