

POLICJA MAŁOPOLSKA

<https://malopolska.policja.gov.pl/krk/aktualnosci/14245,mam-cyberPROBLEM-Jak-nie-dac-sie-oszukac-w-Internecie-Porady-oswiecimskich-polic.html>
2022-06-26, 13:10

:(MAM... CYBERPROBLEM:) JAK NIE DAĆ SIĘ OSZUKAĆ W INTERNECIE. PORADY OŚWIĘCIMSKICH POLICJANTÓW.

Policjanci z oświęcimskiej komendy Policji z zespołu do zwalczania przestępczości gospodarczej zajmują się ściganiem cyberprzestępców. Aby przeciwdziałać zagrożeniom w sieci funkcjonariusze prezentują porady w jaki sposób można ochronić się przed cyber złodziejami i cyber oszustami. Przygotowali więc cykl artykułów pod tytułem: :(mam...cyberPROBLEM:) Dziś część 1 pt. „Jak sprzedając w Internecie nie dać się okraść”, a w niej rozmowa z panem Markiem, który sprzedając telefon ... stracił pieniądze z konta bankowego.

Masz zamiar sprzedać coś za pośrednictwem portalu ogłoszeniowego - przeczytaj uważnie poniższy dialog, aby nie stracić wszystkich pieniędzy z konta bankowego lub nie stać się kredytobiorcą mimo woli.

Marek (do kolegi policjanta): *Wyobraź sobie, że wczoraj wystawiłem na OLX telefon, odezwał się gość, że chce go kupić i od razu zaproponował, że ogarnie również kuriera. No to się zgodziłem. Podałem mu dane mojej karty i od wczoraj nie mam z nim kontaktu. A dzisiaj rano patrzę i oczom nie wierzę... z konta mi wzięto tysiaka!*

Policjant: *No to czekam na Ciebie w komendzie ...*

Marek: *Nie żartuj! Straciłem te pieniądze? Może zadzwonię do banku, żeby zablokowali ten przelew? I w ogóle aby mi podali, co się stało?*

Policjant: *Słusznie. Możesz spróbować w banku. Na pewno nie zaszkodzi. Ale na komendę i tak musisz przyjść. Tak od pewnego czasu działają oszuści, którzy udają, że chcą od Ciebie coś kupić na OLX, a tak naprawdę to zależy im tylko na danych Twojej karty płatniczej lub danych logowania do twojego konta bankowego. A jak się z Tobą skontaktował?*

Marek: *Przez WhatsApp. Mam do niego numer, ale teraz nie odbiera.*

Policjant: *I pewnie nie odbierze. Standard. To prawdopodobnie nie jest nawet numer zarejestrowany u polskiego operatora, chociaż tak wygląda. Temat ciekawy, lecz nie będę Ci nim zwracał głowy. Ale dlaczego podałeś dane swojej karty bankomatowej?*

Marek: *Bo miałem potwierdzić odbiór pieniędzy za ten telefon klikając w link, który mi przysłał ten kupujący i zalogować się do banku, a później podać dane karty łącznie z tym trzy cyfrowym kodem, co jest z tyłu.*

Policjant: *A tyle razy Ci mówiłem, że jak nie jesteś pewny na jakiej stronie internetowej jesteś, to nic tam nie podawaj. Link, który dostałeś najpewniej prowadził do fałszywej strony banku, w którym masz konto i podałeś oszustowi, jak na tacy, dane do logowania. A nie dostałeś zaraz potem SMS-a z kodem do autoryzacji z banku?*

Marek: *No jakiś tam kod przyszedł i jego też trzeba było podać na tej stronie więc wpisałem...*

Policjant: *I co było w tym SMS-ie napisane oprócz kodu?*

Marek: *Yyy...nie czytałem całego. Czekaj zaraz to sprawdzę... O kurcze, tam jest napisane, że dodaje zaufane urządzenie do obsługi konta!*

Policjant: *No właśnie. Niestety, ale to Twój kolejny błąd. Po to banki zwracają uwagę na to, co i gdzie autoryzujesz, żeby udaremnić ewentualne oszustwo. To jest ostatnia linia obrony. Czasami zamiast potwierdzenia dodania zaufanego urządzenia, kod ma autoryzować np. transakcje BLIK. Trzeba czytać te SMSy. W sumie, może jakby zamiast tekstu przesyłali obrazki, to więcej osób zwróciło by uwagę...*

Marek: *No dobra, mój błąd, teraz to łatwo Ci mówić. Skąd miałem wiedzieć, że ktoś chce mnie oszukać, a nie kupić ode mnie ten telefon?*

Policjant: *Dobre pytanie. Znam jednego policjanta, który też dał się w ten sposób oszukać, więc jak widzisz może się to przydarzyć każdemu. Oszuści cały czas wykorzystują nowe metody i wymyślają nowe historie, żebyś tylko kliknął w link i podał dane do konta. Ale podpowiem Ci na co trzeba zwrócić uwagę.*

Po pierwsze patrz na sposób w jaki pisze osoba, która chce kupić od Ciebie przedmiot. W wielu przypadkach oszustem jest osoba nieznająca dobrze języka polskiego i korzystająca z internetowego tłumacza, więc jeśli ktoś notorycznie robi błędy gramatyczne to powinno Ci się zapalić światełko ostrzegawcze.

Kolejna sprawa to linki wysyłane przez kupującego. Nie klikaj w taki link! Oszust będzie próbował Ci wmówić, że klikając musisz potwierdzić odbiór pieniędzy, które on już wpłacił. Jak już przez nieuwagę i pośpiech klikniesz w taki link, nie podawaj żadnych danych na stronie, która Ci się otworzy. Ale to naprawdę żadnych!!! Pamiętaj też, że zakupy z przesyłką przez OLX działają zupełnie inaczej.

Pamiętaj również, że symbol kłódeczki w pasku adresu strony, na której jesteś, też o niczym nie świadczy – to wcale nie jest potwierdzenie, że strona jest bezpieczna! Żeby się upewnić, czy jesteś na prawdziwej stronie Twojego banku powinieneś dokładnie sprawdzić adres w pasku przeglądarki, na który trafiłeś, czyli ten tekst w okienku na samej górze obok kłódeczki. Kiedyś postaram Ci się to dokładniej wyjaśnić.

Czasem oszust zaproponuje Ci rozmowę z konsultantem, który będzie miał Ci pomóc w potwierdzeniu odbioru pieniędzy lub prześle Ci instrukcje, gdzie masz po kolei klikać. To także są elementy oszustwa. Wiem, że teraz wszystko musi być szybkie i wygodne, ale zatrzymaj się choć na chwilę przy takiej transakcji i spójrz na wszystko „chłodnym” okiem. Jest wiele momentów, w których możesz się zorientować, że coś jest nie tak. A jeśli czegoś nie jesteś pewny, to wstrzymaj się i poproś o radę kogoś takiego jak ja. Poza tym poczytaj w wolnej chwili na stronie OLX jak można otrzymać zapłatę za ich pośrednictwem lub też zapłacić za towar, który masz zamiar kupić. Tam jest to naprawdę dobrze opisane.

Marek: *Dzięki. Teraz widzę, że faktycznie od początku coś tu śmierdziało... To widzimy się w komendzie? Mam coś ze sobą zabrać?*

Policjant: Dobrze było by, abyś miał przygotowany wydruk waszej rozmowy na Whatsapp z widocznym numerem telefonu kupującego. Poza tym koniecznie weź potwierdzenie wykonania transakcji z Twojego rachunku bankowego, żebyśmy od razu wiedzieli, gdzie oszust przelał Twoje pieniądze. O dowodzie osobistym chyba nie muszę Ci przypominać. Szczegółowe dane z banku ustalimy we własnym zakresie, więc nie musisz ich o nic dopytywać.

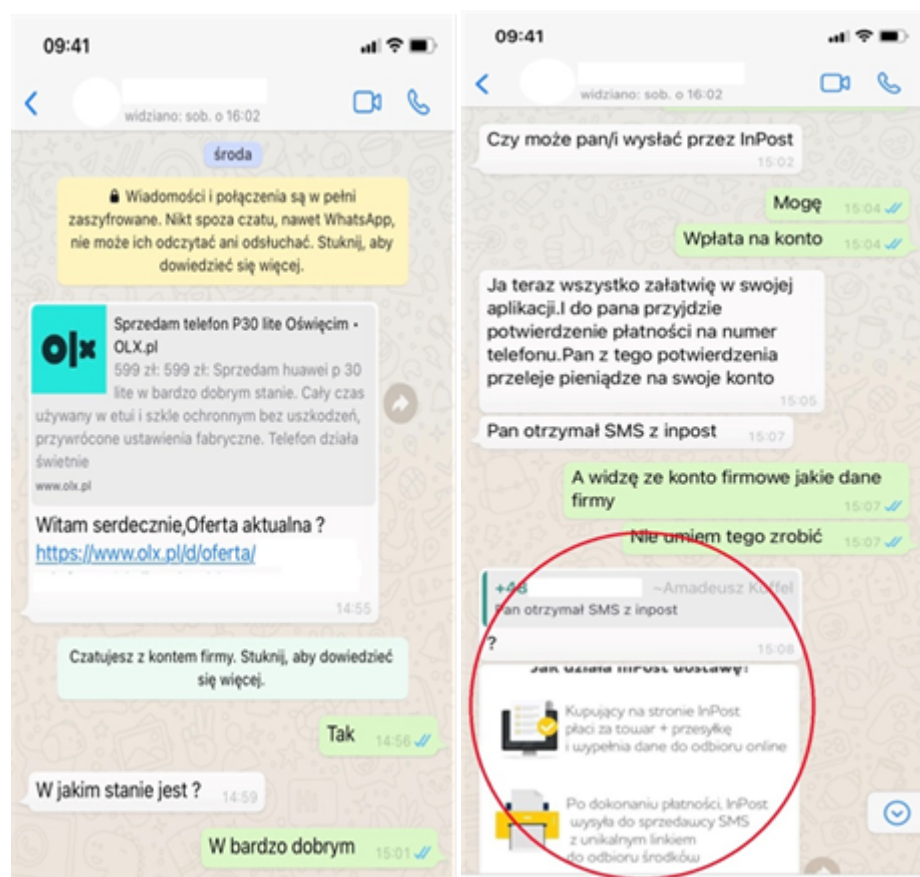
Marek: Ehh...To pewnie oprócz wizyty na komendzie czeka mnie jeszcze wymiana karty po jej zablokowaniu, wymyślenie nowych haseł do konta i rozmowa z żoną...

Policjant: Co do karty i haseł to dokładnie tak. Z żoną Ci już nie pomogę, ale tak szczerze to myślę, że im więcej osób z grona rodziny i znajomych dowie się o Twoim przypadku, to tym lepiej dla nich. Może dzięki Tobie, ktoś nie da się już w taki sposób oszukać i nawet Ci później podziękuje.

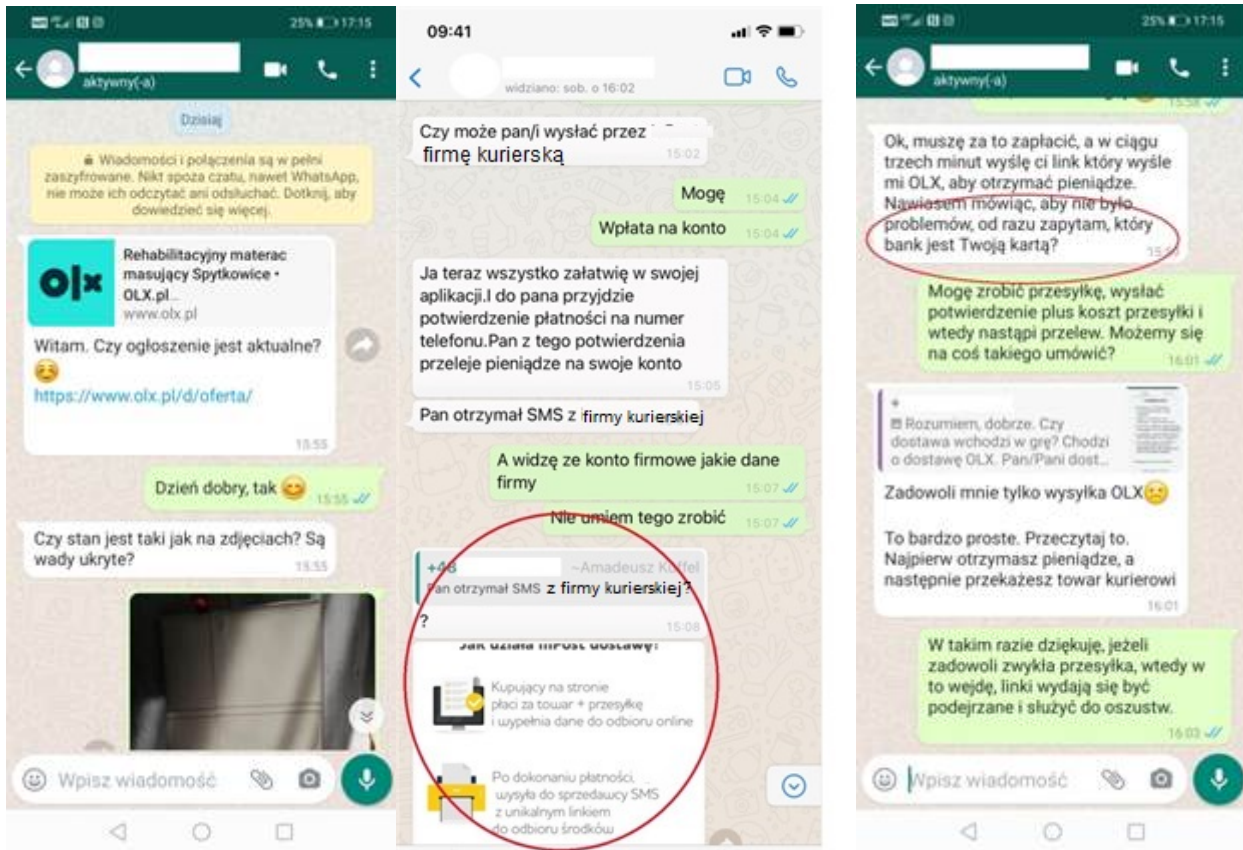
Marek: Wielkie dzięki za pomoc. A nie chcesz może kupić telefonu...?

Dla przykładu prezentujemy autentyczne rozmowy na komunikatorze, w których oszust (proszę zwrócić uwagę na jego problemy z gramatyką) próbuje wyłudzić dane od sprzedającego. Obaj sprzedający (pierwszy chciał sprzedać telefon, a drugi materac) od razu zorientowali się, że to próba wyłudzenia pomimo, że oszust spreparował nawet fałszywy komunikat firmy kurierskiej. Jeden ze sprzedających postanowił nawet trochę pożartować z oszusta ...

Sprzedaż telefonu ...



Sprzedaż materaca rehabilitacyjnego...



PLIKI DO POBRANIA



27.98 KB
Opisy do screenów 1