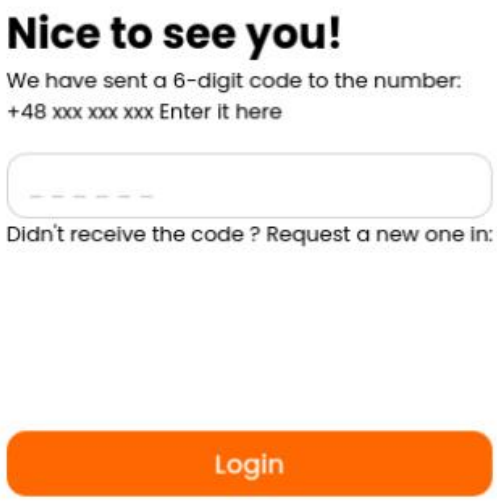


Dostaliście może ostatnio phishing SMS o rzekomej konieczności dopłaty do paczki? Nasze systemy wyłapują tego w ostatnich dniach mnóstwo, wyjątkowo dużo zgłoszeń od Was trafia też na naszą "zgłaszarkę" 508 700 900. Skąd przestępcy biorą numery do wysyłania dziesiątek tysięcy phishingowych SMSów? Z przejętych kont Orange Flex.

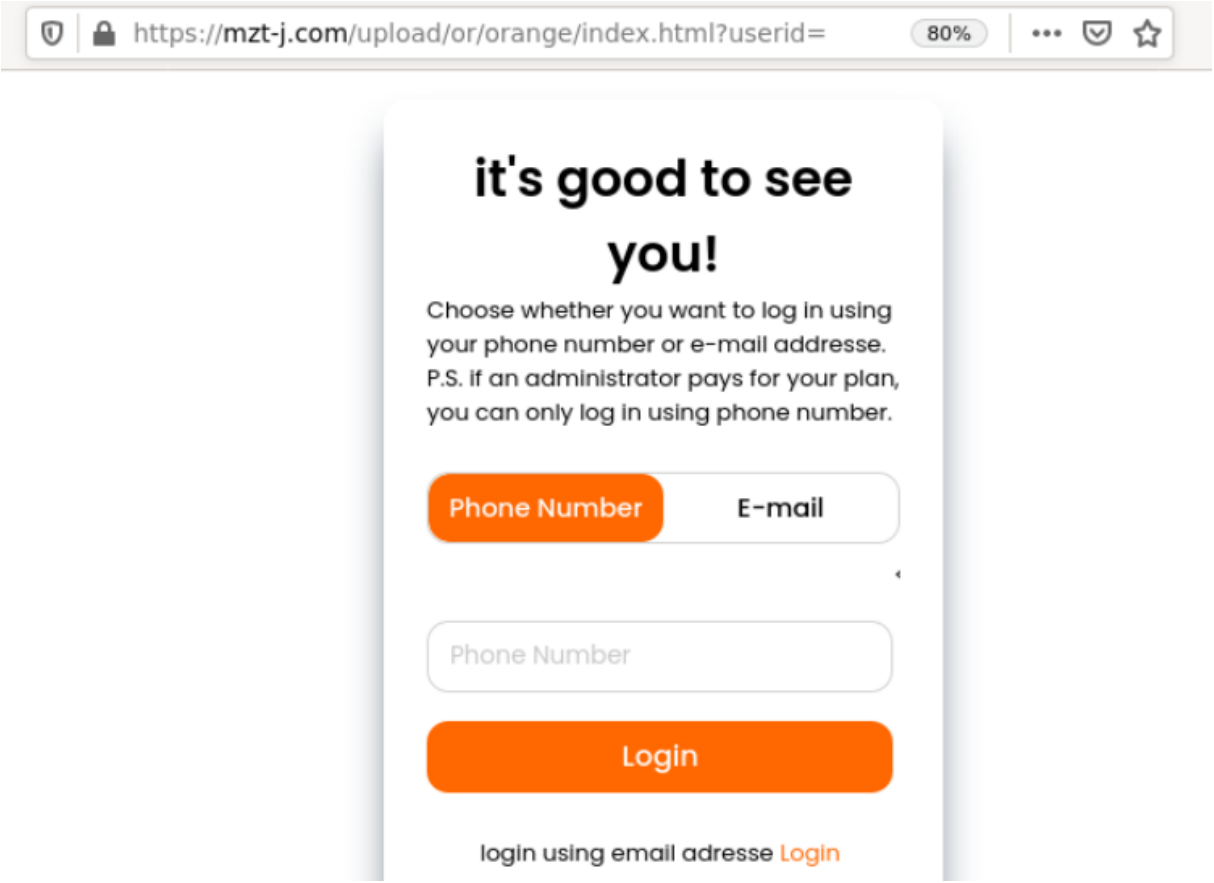
Niezły się temat trafił na urodziny Flexa, co? Phishing "na Flexa" zaobserwowaliśmy już tydzień temu, jednak wtedy - co opisywałem na stronie CERT Orange Polska - był to "próbny balon". SMS-ów nie było wiele, a gdy podczas analizy doszedłem do momentu, gdy miałem wpisać kod potwierdzający logowanie, nie doczekałem się go. Niemniej jednak strony docelowe z tego phishingu oczywiście zablokowaliśmy, dzięki czemu bardzo wiele osób uniknęło mimowolnego współudziału w rozsyłaniu phishingu (i związanych z tym kosztów).

Phishing na Flexa, ale przez stronę

Najpierw na telefon ofiary przychodził SMS. W pierwszej fali zaobserwowaliśmy kilka wariantów:

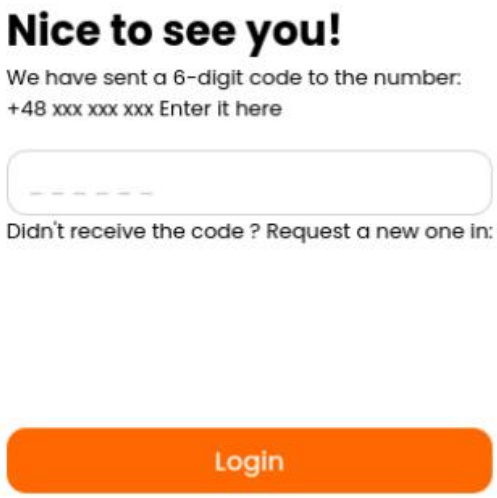
Orange Flex : Twój numer „Orange Flex" jest zablokowany, aby go ponownie aktywować, kliknij link: Drogi kliencie wygrywasz iphone 14 pro max od Orange, sprawdź szczegóły tutaj: Gratulacje wygrałeś 2000 zł od orange

We wszystkich przypadkach link wyglądał tak samo - hxxps://v[.]ht/orange-flex. Później przestępcy skupili się na pierwszej wersji. Ma to sens, biorąc pod uwagę to, co było ich celem. Myślę (mam taką nadzieję!), że konieczność zalogowania się na swoje konto Flex po to, by odebrać "wygraną" spowodowałaby u większej niż zwykle części internautów wahanie, czy aby na pewno ma to sens?



Ja akurat z Flexa nie korzystam (jaki jest najlepszy plan na świecie? służbowy oczywiście! :)), ale wiem, że na stronie mogę się zalogować co najwyżej do czatu - wszystkie aktywności związane z planem dzieją się natomiast w aplikacji.

Po wpisaniu loginu i hasła, bądź numeru telefonu, pojawiał się jeszcze monit o wpisanie kodu z SMS-a:



i koniec. Tzn. tydzień temu byłby to koniec.

Po co wysyłać samemu, skoro można "kimś"?

Okazało się bowiem, że niebawem SMS-y autoryzacyjne zaczęły przychodzić. W jednym z dwóch scenariuszy, czyli wtedy, gdy ofiara wybrała opcję z numerem telefonu. Domyślacie się o co chodzi? Przestępcy podesłali phishing "na Flexa", zalogować się jednak próbowali do serwisu Mój Orange.

Gdy im się udało, zmieniali adres e-mail na swój (lub wpisywali swój, przy logowaniu numerem telefonu). Następnie, mając pełną kontrolę nad kontem... zamawiali doń usługę eSIM! A potem, po zainstalowaniu wirtualnej "simki" rozpoczynali wolumenową wysyłkę wiadomości, które miały im już przynieść faktyczny zarobek. Trzeba przyznać, że pomysł całkiem sprytny. Tak samo - choć to akurat oczywiste - jak to, że źli ludzie zainstalowali się poza Polską, gdzie trudniej ich dopaść naszym organom ścigania. Tym razem jednak nie za wschodnią granicą, a w jednym z krajów Unii Europejskiej.

A jak to się stało, że w ogóle udało im się przejąć jakieś konta? Stawiam na korzystanie przez ofiary z WiFi "nie-Orange'owego". CyberTarcza ochroni Wasz telefon w sieci Orange, ale jeśli podepniecie go do nie-naszej sieci bezprzewodowej, tam niestety nie pomożemy :(

Co robić?

Jak zawsze - myśleć za każdym razem, gdy wpisujemy gdzieś nasze loginy i hasła. Sprawdzać adres w pasku przeglądarki, szczegółowo przeczytać treść strony i jeśli trafimy na cokolwiek podejrzanego/nielogicznego - absolutnie nie podawać naszych danych.

A jeśli macie wątpliwości, możecie też napisać do nas - mailem na cert.opl@orange.com, bądź przesłać dalej podejrzanego SMS-a na nr 508 700 900.

Źródło: blog Orange Polska https://biuroprasowe.orange.pl