Cyberoszustwa inwestycyjne

Czym są fałszywe inwestycje?

To metoda oszustwa, polegająca na podszywaniu się pod maklerów giełdowych i brokerów, proponujących nowe możliwości zainwestowania środków. Nakłaniają do skorzystania z inwestycji, które wcześniej nie były dostępne na rynku dla każdego. Perfekcyjnie przedstawiona oferta staje się przekonująca, co sprawia, że ciężko rozpoznać kłamstwo.
Cyberoszuści starają się dostosować swoje ataki socjotechniczne do specyfiki rynku krajowego, obecnej sytuacji geopolitycznej, czy trendów na rynku. Ponadto, w kampaniach promujących fałszywe inwestycje bardzo często wykorzystują wizerunki znanych firm czy osób, przez co oferta i możliwość szybkiego oraz wysokiego zarobku wydają się jeszcze bardziej wiarygodne.

Przebieg oszustwa

Oszuści kontaktują się ze swoimi ofiarami telefonicznie, przy wykorzystaniu mediów społecznościowych, czy też e-mailowo, przedstawiając możliwość zainwestowania w produkt przynoszący wysokie zyski w krótkim okresie czasu. Oferty te są także publikowane na specjalnie przygotowanych do tego serwisach czy kontach w serwisach społecznościowych typu Facebook.

W tym celu oszuści wykorzystują socjotechnikę, a także brak wiedzy potencjalnych inwestorów na temat różnych form inwestycji i ryzyk z nimi związanych.

Przykładowy przebieg oszustwa fałszywej inwestycji w mediach społecznościowych

Krok 1

Oszustwo rozpoczyna się od umieszczenia reklamy fałszywej inwestycji w mediach społecznościowych, jak np. Facebook czy Instagram, wyszukiwarkach, wszelkiego rodzaju stronach internetowych.

Na tego rodzaju reklamach zazwyczaj zamieszczone są hasła mające przekonać potencjalnego inwestora o wysokich zyskach i braku ryzyka. Bardzo często używane są hasła „bezpieczna inwestycja”, „zysk bez ryzyka”, „zacznij zarabiać”. Aby dodatkowo wzbudzić zaufanie odbiorcy reklamy, cyberoszuści mogą umieścić na niej wizerunek znanej osoby – polityka, sportowca, artysty, lub logo instytucji publicznej czy spółki.

PolTime
Sponsorowane ·

✅Zapomnij o wszystkich obawach związanych z inwestowaniem!
Tysiące Polaków jest teraz częścią oficjalnego projektu ORLEN.
Zarejestruj się teraz, aby uzyskać dostęp do bezpiecznych inwestycji!.

FORMULARZ NA FACEBOOKU
Rejestracja otwarta
Zarejestruj się

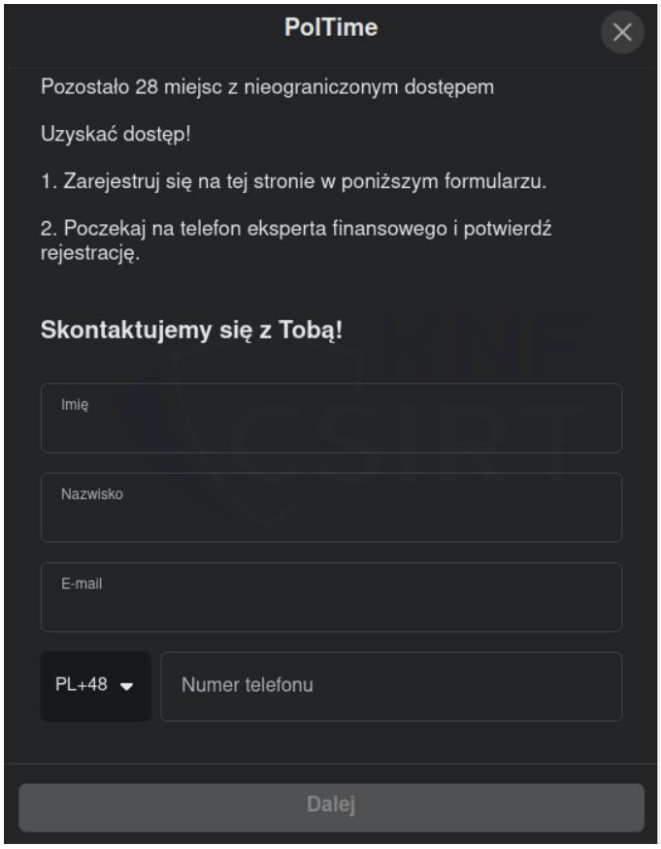
Poul Fill
Sponsorowane ·

Tylko dla Polaków

FACT.MESTOPOLAND.PRO
Mój biznes-blog
My Business Blog
Dowiedz się więcej

Krok 2

Osoba, która zdecyduje się na inwestycję, po kliknięciu w taką reklamę proszona jest o podanie swoich danych kontaktowych w celach rejestracyjnych lub instalację aplikacji do inwestowania.

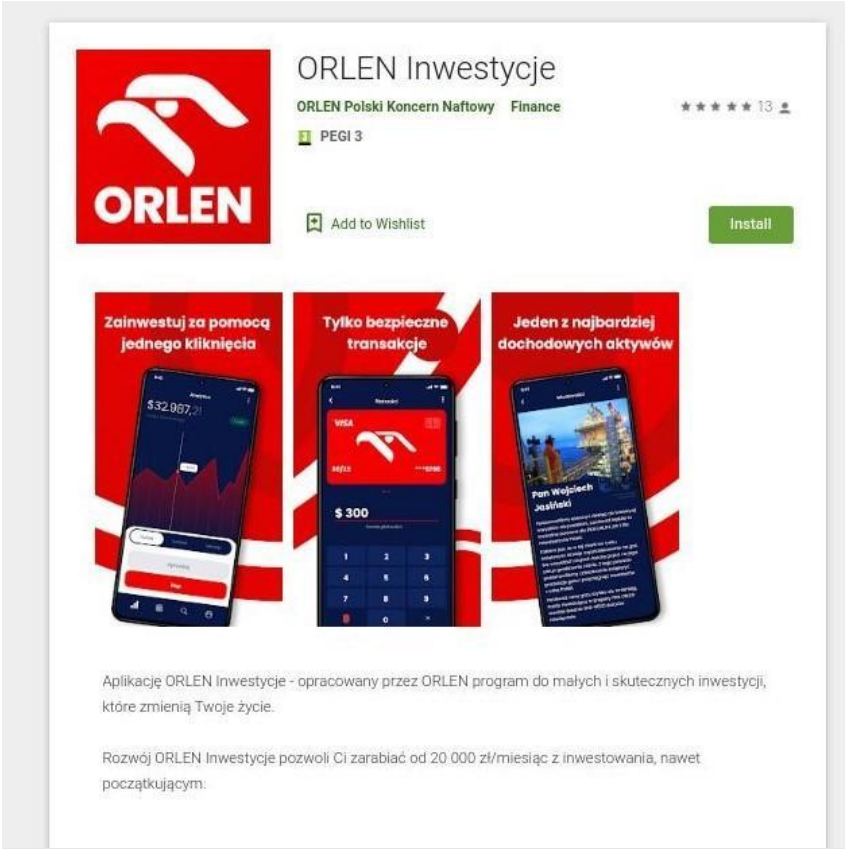


Krok 3

Po dokonaniu rejestracji z taką osobą kontaktuje się oszust, najczęściej podający się za brokera lub konsultanta inwestycyjnego. Oszust pozostając w ciągłym kontakcie telefonicznym z potencjalnym inwestorem opowiada o korzyściach wynikających z tej inwestycji. Przekonuje o bardzo wysokich zyskach, braku ryzyka. Opowiada o wynikach innych inwestorów, powołuje się na znane osoby, firmy, instytucje. W ten sposób, przy wykorzystaniu manipulacji, stara się nakłonić rozmówcę do inwestycji.

Krok 4

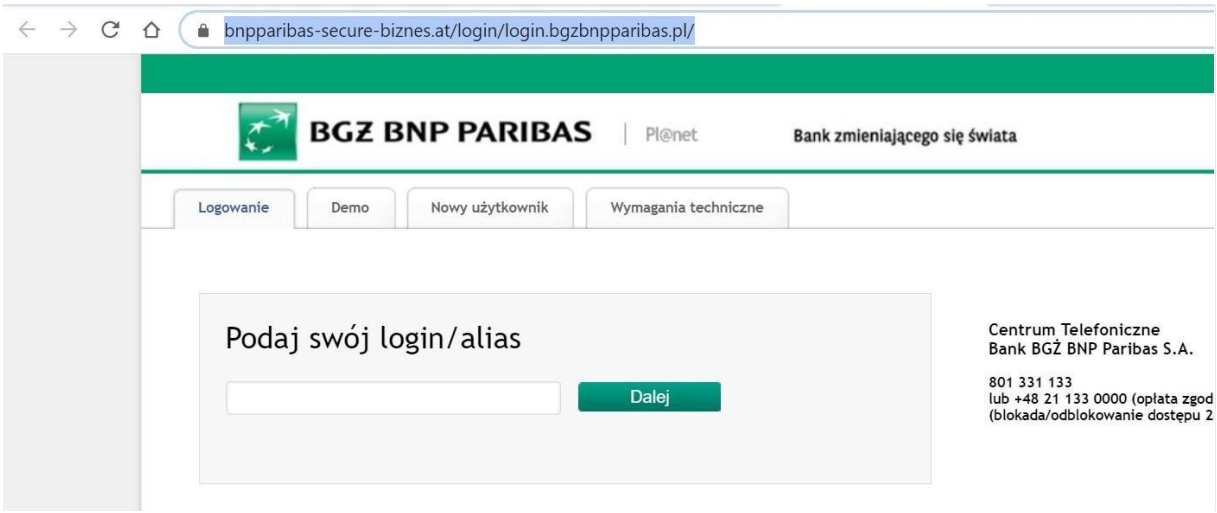
Oszust przekazuje potencjalnemu inwestorowi numer rachunku (należący najczęściej do innego inwestora) do przelewu środków na transfer inwestycyjny. Po kolejnych zrealizowanych przez inwestora przelewach, aby uśpić jego czujność i zachęcić go do dalszych inwestycji, oszuści zasilają jego rachunek drobnymi kwotami przelewanymi w rzeczywistości z rachunków innych inwestorów. Oszuści mogą również stosować perswazję wobec inwestorów przedstawiając im wyniki zysków zamieszczone na fałszywych platformach inwestycyjnych. Często przy rejestracji na fałszywej platformie inwestycyjnej oszuści udostępniają formularz, w którym należy podać dane karty płatniczej, które następnie są wykorzystywane do celów oszustów.


ORLEN Inwestycje
ORLEN Polski Koncern Naftowy
Finance
PEGI 3
13
Add to Wishlist
Install
Zainwestuj za pomocą jednego kliknięcia
Tylko bezpieczne transakcje
Jeden z najbardziej dochodowych aktywów
$ 300
Pan Wojciech Jasiński
Aplikację ORLEN Inwestycje - opracowany przez ORLEN program do małych i skutecznych inwestycji, które zmienią Twoje życie.
Rozwój ORLEN Inwestycje pozwoli Ci zarabiać od 20 000 zł/miesiąc z inwestowania, nawet początkującym.


Teraz możesz zarabiać na akcjach PKN ORLEN
Zacznij zarabiać na zasobach swojego kraju!
Nazwa
Nazwisko
E-mail
+48
Uzyskaj dostęp

Krok 5
Gdy inwestor chce wypłacić wypracowane dotychczas zyski i na tym zakończyć inwestowanie, oszuści pod pretekstem pomocy w wypłacie proszą, aby na swoim urządzeniu zainstalował legalny program do zdalnego zarządzania pulpitem, np. AnyDesk, TeamViewer, QuickSupport czy Alpemix. Po zainstalowaniu takiego programu, inwestor zostaje poproszony o zalogowanie się do swojej bankowości internetowej. Wszystkie dane wprowadzone przez inwestora są widoczne dla oszustów.

Krok 6
Oszuści stosują również dodatkowe warianty schematu informując inwestora, aby otrzymał on zwrot środków z inwestycji musi zapłacić podatek dochodowy. Gdy taki inwestor nie posiada już własnych środków na dokonanie tej opłaty, oszuści oferują mu pomoc w zaciągnięciu kredytu. Składając w imieniu inwestora internetowy wniosek o kredyt, oszuści proszą go o podanie kodów autoryzujących SMS oraz informują, że może skontaktować się z nim pracownik banku w celu potwierdzenia zobowiązań.



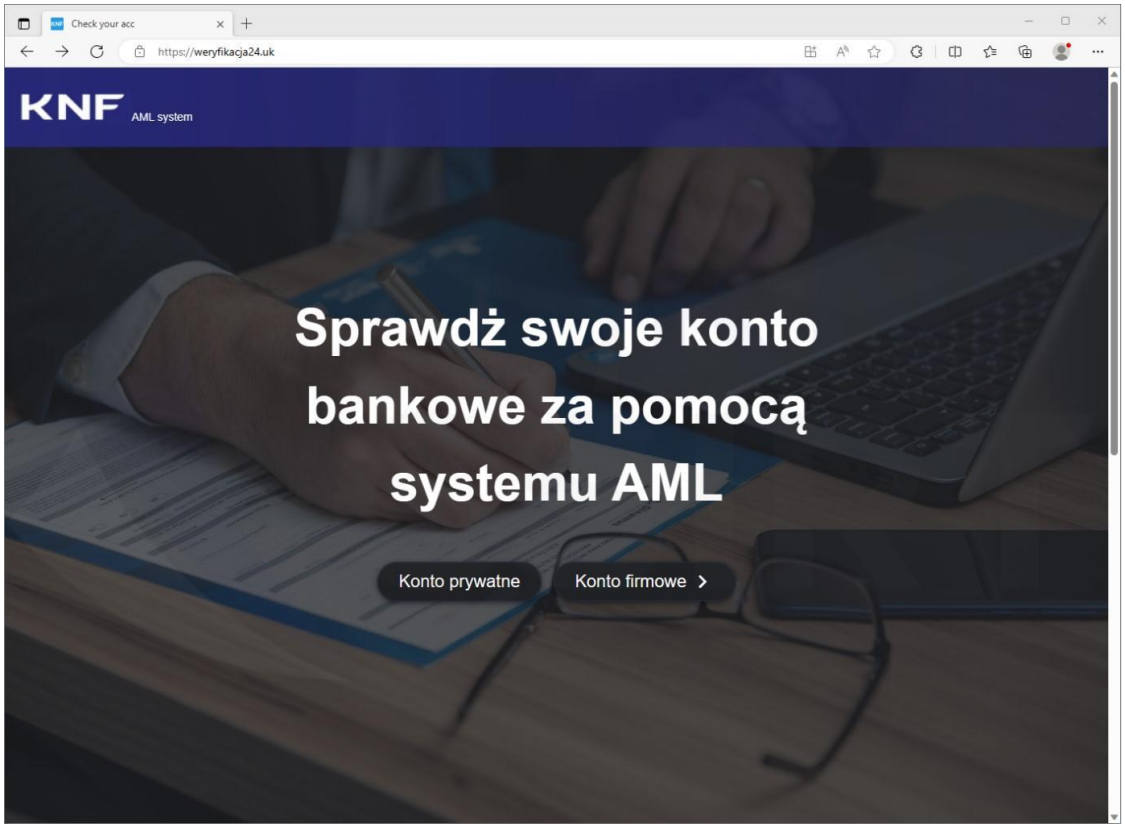
Krok 7
Środki z rachunku osoby oszukanej mogą zostać rozdysponowane przez oszustów w następujący sposób:
• przelewem na rachunek innej osoby poszkodowanej przez oszustów lub słupa,
• przelewem na rachunek zagraniczny,
• przelewem na giełdę kryptowalut,
• płatność kartą na giełdy kryptowalut.
W zależności od scenariusza oszustwa może pojawić się w nim dodatkowy element, jakim jest poproszenie inwestora o przesłanie skanu swojego dowodu osobistego, który może zostać wykorzystany do:
• założenia rachunku bankowego na tak zwaną skradzioną tożsamość,
• zaciągnięcia kredytu/pożyczki krótkoterminowej na dane właściciela dowodu,
• rejestracji konta na giełdzie kryptowalut na podane dane.

Dodatkowe warianty
Zdarza się, że oszuści informują jeszcze, że należy zweryfikować numer rachunku, aby ten nie został zablokowany po wpłacie, rzekomo zarobionej, wysokiej kwoty. W kolejnym etapie przysyłają link do strony phishingowej, wykorzystującej np. wizerunek Komisji Nadzoru Finansowego, aby zwiększyć wiarygodność swoich działań. W formularzu należy podać

dane osobowe oraz wybrać bank, w którym dana osoba posiada rachunek. Następnie następuje przekierowanie do strony przypominającej bankowość internetową banku, w którym osoba ta ma założony rachunek. Podanie na takiej stronie danych logowania do bankowości elektronicznej skutkuje tym, że w ich posiadanie wchodzą oszuści.

Zdarza się również, że osoba poszkodowana trafia na reklamę informującą np. o rzekomym aresztowaniu osób wyłudzających pieniądze i możliwości odzyskania ich. Po kliknięciu w link z reklamy zostaje przekierowana na stronę internetową, na której musi wprowadzić swoje dane osobowe oraz podać informację na jaką kwotę została oszukana. Na kolejnym etapie oszuści kontaktują się z tą osobą próbując w trakcie rozmowy ponownie ją zmanipulować i pozyskać od niej kolejne środki finansowe.

Socjotechnika stosowana przez oszustów w tym schemacie działania pokazuje jak dobrze są oni przygotowani. Jednocześnie osoba, która zostanie przez nich oszukana często jest przez nich manipulowana nawet przez kilka miesięcy biorąc jednocześnie nieświadomy udział w przestępstwie prania pieniędzy.



Przykład strony phisingowej do rzekomej weryfikacji rachunku

Justice - Legal services
Sponsorowane ·

Interpol i policja aresztowały sieć brokerów wyłudzających pieniądze od polskich obywateli!

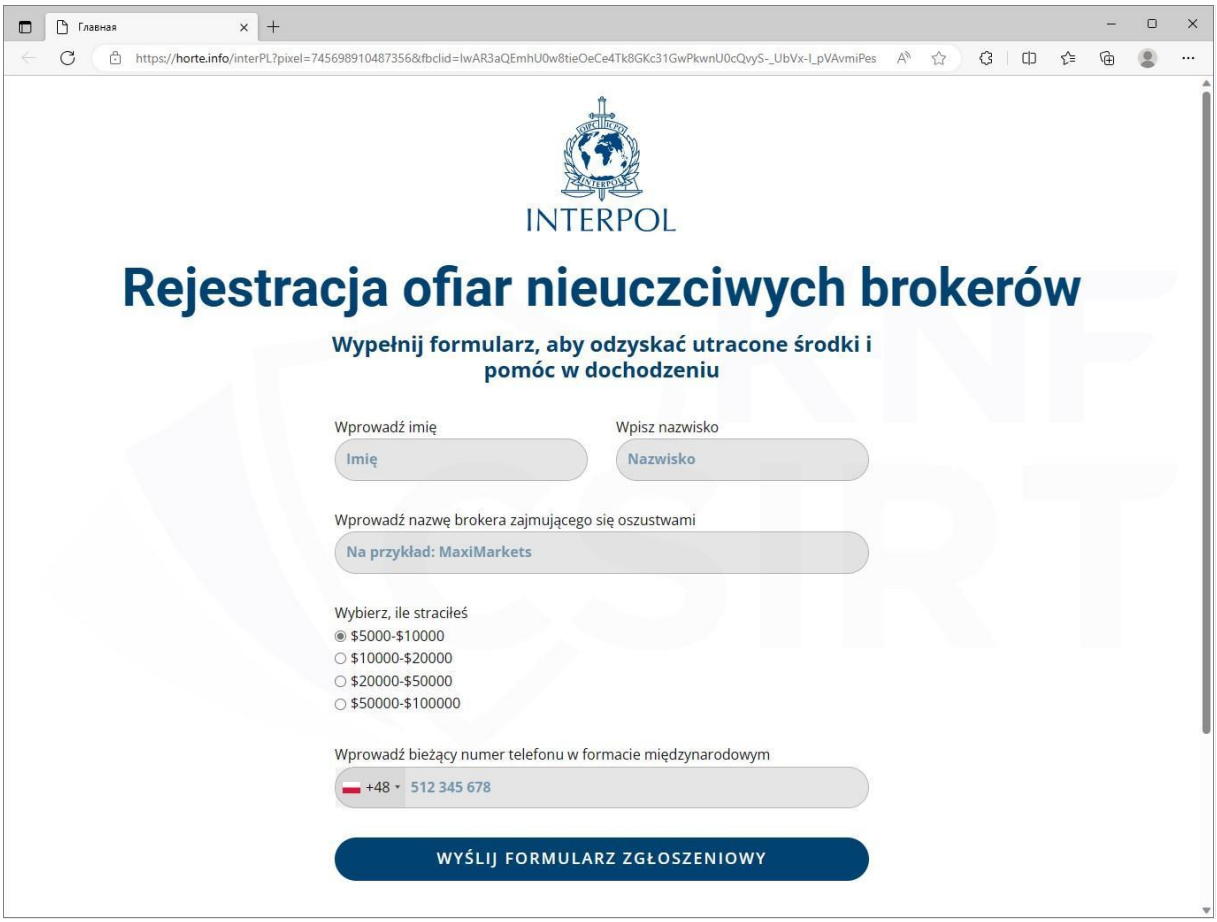
Rejestr ofiar jest tworzony w celu zebrania dowodów i odzyskania utraconych pieniędzy.

Aby zarejestrować się na liście ofiar w celu uzyskania odszkodowania i pomóc w śledztwie, kliknij ten link.

HORTE.INFO
Aby zarejestrować się na liście ofiar w celu uzyskania odszkodowania i pomóc w...

Dowiedz się więcej

Przykład reklamy fałszywej inwestycji



Kilka podstawowych zasad bezpieczeństwa:

- przede wszystkim kieruj się zasadą ograniczonego zaufania – nigdy nie masz pewności kto może znajdować się po "drugiej stronie" w sieci,
- nigdy nie loguj się do bankowości internetowej po tym jak zainstalowałeś aplikacje do zdalnego zarządzania pulpitem i przekazałeś do niej kod osobie trzeciej,
- nigdy nie podawaj osobie trzeciej kodów SMS autoryzujących operacje bankowe,
- zawsze dokładnie czytaj komunikaty i sprawdzaj transakcje, które potwierdzasz w aplikacji mobilnej lub za pośrednictwem kodów SMS, w szczególności zwróć uwagę na numer rachunku odbiorcy i kwotę realizowanej operacji,
- jeżeli realizujesz przelew na rachunek firmy oferującej inwestycje lub na giełdę kryptowalut to zwróć uwagę, że dane odbiorcy przelewu nie powinny być danymi osoby fizycznej.

Cyberoszuści wykorzystują wizerunki polityków, sportowców, artystów, a także instytucji państwowych i znanych firm. Mogą podszyć się pod dowolny numer telefonu.

Zachęcamy do śledzenia profilów CSIRT KNF w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook, na których pojawiają się informacje o najnowszych działaniach cyberoszustów.