Uwaga na oszukańcze serwisy internetowe oferujące inwestycje w kryptowaluty i na rynku Forex – Działaj ostrożnie i rozsądnie.

Informacja
Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP o zagrożeniu związanym z ofertami inwestycji na rynku Forex i kryptowalut z dnia 24.03 2021 r.

Co trzeba wiedzieć o oszustwach na rynku Forex i kryptowalut?

Inwestycje w kryptowaluty lub na rynkach Forex co do zasady są legalne. Zauważamy jednak coraz więcej przestępstw, które polegają na oszukańczym działaniu podmiotów pośredniczących w inwestowaniu.

Wariantów wyłudzeń związanych z inwestowaniem w kryptowaluty jest wiele. Przyszli poszkodowani mogą być kuszeni np. udziałem w ekskluzywnych szkoleniach dotyczących inwestowania czy możliwością odbioru fikcyjnej „wygranej" wygenerowanej przez „jakiś" system inwestujący w kryptowaluty lub na rynku Forex. Zamiennie, zamiast inwestycji bezpośrednio w kryptowaluty mogą pojawić się zachęty do inwestowania w rynki Forex czy też zakupy udziałów w nieruchomościach. Zdarzają się również „oferty" pracy związanej z obrotem kryptowalutami. Na rachunki takich osób wpływają skradzione środki, które następnie mogą być przetransferowane poprzez założone na ich dane konta, w kantorach czy giełdach kryptowalut lub Forex.

Przestępcy często działają w zorganizowanej grupie przestępczej. Wykorzystują okres pandemii i kreują nowe scenariusze oszustw, często oparte na strachu przed bezpośrednimi skutkami pandemii, które pogarszają sytuację ekonomiczną ludzi. Najczęściej przestępcy oferują klientom pomoc w inwestowaniu. Proponują na przykład, że będą:

- świadczyć doradztwo inwestycyjne, czyli rekomendować realizację transakcji na rynku Forex za pośrednictwem platform inwestycyjnych,
- zarządzać portfelami klientów, czyli podejmować i realizować decyzje inwestycyjne na ich rachunek.

Niestety skala oszustw jest coraz większa, a pojedyncze transakcje opiewają na coraz wyższe sumy. Przykładowo, odnotowano oszustwa obejmujące jednorazową transakcję na kwotę sięgającą prawie 150 tys. zł.

Jeżeli rozważasz inwestycje, zwróć szczególną uwagę czy podmiot, który prowadzi platformę inwestycyjną lub pośredniczy w nabywaniu i obrocie walutami wirtualnymi (w tym kryptowalutami) ma:

- wymagane zezwolenia w zakresie obrotu instrumentami finansowymi,
- swoją siedzibę w Polsce lub innym kraju UE i innych państw członkowskich UE oferujących takie usługi.

Jeśli tak nie jest, działalność tych podmiotów nie jest uregulowana i nadzorowana w Polsce ani w innym kraju UE. Te podmioty nie mają obowiązku sprawozdawczego zgodnie z wymogami ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu i nie podlegają pod przepisy tej ustawy.

Dlatego, zanim zaczniesz inwestować, zapoznaj się ze wszystkim zasadami, jakie dotyczą tego typu działalności, a szczególnie z zasadami i regulaminami podmiotów pośredniczących w inwestowaniu. Twoje podejrzenia powinno wzbudzić, jeśli w regulaminie znajdziesz:

- bardzo wysokie kwoty prowizji,
- warunek dokonywania ciągłych wpłat na rzecz kolejnych produktów,
- obowiązek uiszczania wysokich składek członkowskich.

Niekiedy wypowiedzenie takiej współpracy jest całkowicie niemożliwe, a chęć inwestycji przeobraża się w walkę o zachowanie ostatnich oszczędności. Właśnie dlatego warto upewnić się, czy dany podmiot ma zezwolenie KNF. Wyszukiwarka podmiotów znajduje się tutaj: *https://www.knf.gov.pl/podmioty/wyszukiwarka_podmiotow*

Inwestując, zachowaj zdrowy rozsądek! Twoją niewiedzę wykorzystują przestępcy, proponując rzekome ułatwienia w inwestowaniu na tych rynkach.

Na co zwracać szczególną uwagę?

Różne scenariusze tego typu wyłudzeń łączą wspólne elementy, które mają zachęcić do szybkiego zarobku. Szczególnie ostrożnie podchodź do ofert „brokerów" w ogłoszeniach i materiałach reklamowych lub kontaktach, zwłaszcza jeśli przeczytasz lub usłyszysz o:

- możliwości szybkich i wysokich zysków dzięki inwestycji w kryptowaluty lub na rynku Forex;
- gwarancji zysku dla „każdego", bez względu na poziom wiedzy o rynkach finansowych;
- pomocy „brokera" i konieczności pierwszej wpłaty (tzw. opłaty rejestracyjnej);
- konieczności instalacji aplikacji (na komputerze lub telefonie), która umożliwia automatyzację operacji związanej z kupnem i sprzedażą kryptowaluty lub operacji na rynku Forex;
- wsparciu telefonicznym analityków w zakresie inwestycji i obsłudze aplikacji;
- konieczności przesłania „brokerowi" skanów (zdjęć) dokumentu tożsamości, selfie z dokumentem tożsamości czy bieżącego rachunku w celu potwierdzenia tożsamości.

Pamiętaj, nie bagatelizuj telefonów i wiadomości z Twojego banku, który próbuje uniemożliwić transakcje powiązane z wyłudzeniami. Zdarzają się przypadki, w których klienci mimo interwencji ze strony banku realizują transakcję.

Zachowaj czujność. Zastanów się chwilę. **Nie ulegaj presji, uważaj na pozornie atrakcyjne oferty** - bezwzględnie **nie działaj pod wpływem chwili.** Miej świadomość, co robisz.

Jak wygląda atak?

- ZACHĘCANIE -

Wyłudzeń dokonują osoby podające się za tzw. „brokerów" inwestycyjnych – pracowników firm zajmujących się pośrednictwem i doradztwem inwestycyjnym.

Działa to w poniższy sposób:

- Oszukańcze firmy ogłaszają swoje usługi za pomocą reklam w mediach społecznościowych, serwisach internetowych oraz aplikacjach mobilnych.
- Osoba zwabiona tymi komunikatami udostępnia w tych mediach swoje dane kontaktowe, które przestępcy wykorzystują następnie do nawiązania kontaktu z przyszłym poszkodowanym.
- Dla przyciągnięcia uwagi i uwiarygodnienia treści w reklamach wykorzystują wizerunki:
  - „przeciętnego Kowalskiego", który szybko zyskał dzięki współpracy z „pośrednikiem", lub:
  - powszechnie znanych i rozpoznawalnych osób, (sportowców, polityków, aktorów, dziennikarzy, celebrytów) bez ich wiedzy i zgody, a przekaz jest zmanipulowany.
- Dzięki współpracy z „brokerem" klienci mają rzekomo osiągać w prosty sposób bardzo szybkie i duże zyski. Znane osoby „ujawniają" to przypadkowo np. podczas programów telewizyjnych czy wywiadów. Opisują to sfabrykowane artykuły wykorzystujące wizerunki znanych osób skopiowane z prawdziwych audycji, dotyczących zupełnie innych tematów. Same artykuły podszywają się pod poczytne tytuły prasowe czy serwisy informacyjne.
- Czasami „broker", reklamując swoje usługi, powołuje się również na rzekomą współpracę z konkretną instytucją finansową. Takie artykuły mogą być później masowo propagowane i udostępniane w serwisach społecznościowych, np. na Facebook-u. Informacje tego typu są często nieprawdziwe i manipulują odbiorcami.

Cel tych działań jest jeden - zwabić przyszłego pokrzywdzonego, klienta banku, wizją szybkiego zarobku i zachęcić do wypełnienia formularza kontaktowego.

- MANIPULACJA KLIENTEM I PROWADZENIE ATAKU -

W kolejnym kroku, z pokrzywdzonym kontaktuje się telefonicznie przedstawiciel „brokera", podający się za „analityka". Mogą to być osoby posługujące się „wschodnim akcentem".

W trakcie kontaktu:

- „Analityk" namawia klienta, aby przekazał opłatę rejestracyjną np. w wysokości 250 EUR, często rozbitą na transze.
- Aby zwiększyć swoją skuteczność, „analitycy" namawiają również do instalacji programów umożliwiających dzwoniącej osobie zdalny dostęp do urządzenia pokrzywdzonego. Ma to rzekomo pomóc w wyjaśnieniu i pokazaniu, jak działa aplikacja do inwestowania oraz w obsłudze zleceń. W rzeczywistości instalowane jest oprogramowanie umożliwiające zdalną kontrolę urządzenia pokrzywdzonego. Pod pozorem tej pomocy pseudo „analitycy" pozyskują od klientów wrażliwe dane, między innymi dotyczące kart płatniczych czy umożliwiające dostęp do bankowości elektronicznej.
- Przestępcy mogą również informować, że będą wypłacać zwrot z inwestycji bezpośrednio na kartę klienta. Proszą pod tym pretekstem o podanie szczegółowych danych karty.
- Bardzo często dochodzi do sytuacji, gdy przestępcy - przy akceptacji pokrzywdzonego - sami inicjują operacje kartami, logują się do bankowości elektronicznej, zrywają lokaty, biorą kredyty i wykonują płatności.
- W początkowym okresie przyszły poszkodowany może obserwować niewielkie „wirtualne zyski" od przekazanej kwoty. Z czasem „analitycy" zaczynają namawiać do zainwestowania

większej kwoty. Może to być np. „super" okazja związana ze zmienną sytuacją na rynku kryptowalut lub Forex.

- Potem może się okazać, że inwestycja była nietrafiona, przy czym „broker" daje szansę na szybkie odrobienie strat i np. proponuje dofinansowanie inwestycji z własnych środków, co ma uwiarygodnić przyszłe zyski z inwestycji. Przy okazji „analitycy" wykorzystują różne techniki manipulacji klientami, np.:
    - Stosują zasadę ekskluzywności – zastrzegają, że oferta jest ograniczona czasowo i tylko dla specjalnych klientów.
    - Używają metody zastraszania – działają nachalnie, dzwonią po kilka razy. Stosują przy tym socjotechnikę polegającą na zaangażowaniu i konsekwencji. Wzbudzają poczucie, że trzeba zrealizować wcześniejszą decyzję.

Mimo tego, że wszystkie opisane działania doprowadzają do sytuacji, gdy poszkodowany traci wszystkie oszczędności, przestępcy nie zaprzestają ataków. Namawiają do brania pożyczek i kredytów, aby odrobić straty. Jest coraz więcej przypadków, w których przestępcy zawierają umowy kredytów np. przez internet, na rzecz niczego nieświadomych klientów.

- WŁĄCZENIE POSZKODOWANEGO W DZIAŁALNOŚĆ PRZESTĘPCZĄ -

Podczas niektórych ataków przestępcy wykorzystują pokrzywdzonego do procederu prania pieniędzy pochodzących z przestępstw (w transferze środków pochodzących z oszustw u innego poszkodowanego):

- Nakłaniają do przelania inwestowanych środków na konta innych osób. Ma to im ułatwić kontynuację inwestowania w związku z rzekomymi działaniami prewencyjnymi podejmowanymi przez niektóre banki.
- W tym samym celu uzgadniają z niektórymi klientami, że na ich rachunek w banku wpłyną środki od innej osoby dla późniejszego przekazania ich dalej. Dzięki temu pokrzywdzony rzekomo będzie mógł łatwiej uzyskać zysk ze swoich „inwestycji" lub odrobić straty.

Więcej o tego typu niebezpieczeństwach przeczytasz tu:

- http://policja.pl/pol/aktualnosci/182302,Operacja-EMMA-5.html?sid=f309c82dc0babb99508f0947e50e7818
- https://zbp.pl/Aktualnosci/Wydarzenia/Nie-zostan-mulem-finansowym.

- ZAKOŃCZENIE „WSPÓŁPRACY" Z „BROKEREM" -

Próby wycofania się od współpracy z „brokerem" lub starania o zwrot jakiejkolwiek części zainwestowanej kwoty najczęściej kończą się całkowitym niepowodzeniem. Jeśli poszkodowany chce to zrobić, dowiaduje się, że nie spełniła zapisów regulaminu. Przykładowo może nie spełnić warunków odnoszących się do aktywności, liczby zleceń, wielkości wpłaconej kwoty, itp.

- FINAŁ -

Koniec jest prawie zawsze ten sam: poszkodowany traci wszystkie oszczędności, niejednokrotnie na jego dane brany jest kredyt lub pożyczka a nawet czasem nieświadomie zostaje włączony w działalność przestępczą.

Co robić w przypadku podejrzenia oszustwa?

Najważniejsze jest zachować sceptycyzm i nie ulegać emocjom. Przed podjęciem jakichkolwiek decyzji związanych z inwestowaniem na rynkach Forex i kryptowalut zadaj sobie pytania:

- **Co wiem** o ryzyku inwestowania na tych rynkach?
- **Czy rozumiem,** na czym polegają inwestycje tego typu?
- **Czy mogę** samodzielnie – z zachowaniem poufności moich danych – realizować operacje na rynkach Forex i kryptowalut?

Odpowiedzi na te pytania powinny ostudzić emocje i przestrzec przed podjęciem zbyt pochopnych działań, na ogół nieodwracalnych.

Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP zalecają między innymi, aby:

- Zapoznać się z informacjami KNF i NBP dotyczącym inwestowania w kryptowaluty – link: https://uwazajnakryptowaluty.pl/;
- Sprawdzać, np. w internecie, wiarygodność instytucji oferującej możliwość inwestowania i osiągania dużych zysków;
- Poszukać informacji w Internecie, czy instytucja zajmująca się tego typu działalnością ma licencję wydaną przez organ nadzoru jednego z krajów Unii Europejskiej;
- Sprawdzić, czy instytucja znajduje się na liście ostrzeżeń KNF – link: https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne;
- Sprawdzić opinie o instytucji w internecie, np. w połączeniu ze terminami „oszustwo" lub „sam". Nie poprzestawaj po znalezieniu jednej strony z opiniami, znajdź kilka. Przestępcy mogą wykorzystywać specjalnie przygotowane dla nich serwisy zawierające jedynie przychylne dla nich, zrównoważone opinie;
- Zapoznać się z Regulaminem usług świadczonych przez „brokera". Zwróć uwagę na to, w jakim kraju jest jego siedziba i gdzie ma siedzibę sąd właściwy w przypadku sporów, jak są ustalane prowizje i opłaty, jak wygląda proces wypłaty środków;
- Nie udostępniać nikomu danych do logowania w bankowości elektronicznej i mobilnej;
- Nie udostępniać nikomu danych poufnych dotyczących swoich kart płatniczych;
- Nie instalować dodatkowego oprogramowania, na urządzeniach z których następuje logowanie do bankowości internetowej;
- Uważnie zapoznawać się z opisem kodów autoryzacyjnych, które wysyłają banki, aby zatwierdzić operację;
- Zachować czujność, gdyby pojawiły się jakiekolwiek propozycje związane z transferem środków pochodzących od innych osób, aby nie współdziałać w przestępstwie;
- Chronić poufność swoich dokumentów oraz wizerunku;
- Pamiętać, że inwestycje wykorzystujące „dźwignię finansową" są zawsze obarczone dużym ryzykiem. Informacja o wysokim ryzyku powinna być przedstawiona w sposób jasny i zrozumiały.

Klienci banków w sytuacjach nietypowych zawsze mają prawo skontaktować się ze swoim bankiem, a w przypadku, gdy podejrzewają, że doszło do popełnienia przestępstwa, powinni zgłosić to na Policji.

Komenda Główna Policji
FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP