Uwaga na oszukańcze serwisy internetowe oferujące inwestycje w kryptowaluty i na rynku Forex – Działaj rozsądnie. Nie ulegaj złudnym wizjom dużego i szybkiego zysku oferowanym przez przestępców!!!

Informacja
Prokuratury Krajowej, Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP o zagrożeniu związanym z ofertami inwestycji na rynku Forex i Bitcoin z dnia 10 lipca 2020 r.

Szanowni Państwo,

W trosce o bezpieczeństwo Państwa środków oraz danych ostrzegamy przed próbami wyłudzeń związanych z inwestowaniem na rynkach kryptowalut i Forex. Przestępcy wykorzystują trudny czas, jakim jest pandemia, wymyślając coraz to nowe scenariusze oszustw, często oparte na strachu przed bezpośrednimi skutkami pandemii przekładającymi się na sytuację ekonomiczną osób przebywających w Polsce.

Należy zaznaczyć, że inwestycje w kryptowaluty lub na rynkach Forex, co do zasady są legalne. Jednakże zanim zaczniemy inwestować warto zapoznać się ze wszystkim zasadami jakie dotyczą tego typu działalności. Podstawową zasadą jest, że można dużo zyskać, ale też można wszystko stracić! Nie ma zysków bez ryzyka, a w tym przypadku ryzyko jest bardzo wysokie! Rzekome ułatwienia w inwestowaniu na tych rynkach wykorzystują przestępcy, którzy oferuję pośrednictwo w takich inwestycjach.

Na co zwracać uwagę?
W różnych scenariuszach tego typu wyłudzenia wykorzystywane są wspólne elementy mające zachęcić do szybkiego zarobku. Szczególnie ostrożnie należy podchodzić do ofert „brokerów", w ogłoszeniach i materiałach reklamowych lub gdy skontaktuje się z Tobą informując o:

- możliwości uzyskania szybkich i wysokich zysków dzięki inwestycji w kryptowaluty lub na rynku Forex;
- gwarancja zyski dla „każdego", bez względu na poziom wiedzy o rynkach finansowych;
- pomocy „brokera" i konieczności dokonania pierwszej wpłaty (tzw. opłaty rejestracyjnej);
- konieczności instalacji aplikacji (na komputerze lub telefonie), dającej możliwość automatyzacji operacji związanej z kupnem i sprzedażą kryptowaluty lub operacji na rynku Forex;
- wsparcie telefoniczne analityków w zakresie inwestycji i obsłudze aplikacji;
- konieczność przesłania „brokerowi" skanów (zdjęć) dokumentu tożsamości, selfie z dokumentem tożsamości, czy jakiegoś bieżącego rachunku w celu potwierdzenia tożsamości.

Gdy spotkasz się z tego typu informacjami – **bądź czujny. Zastanów się chwilę.** Zachowaj zdrowy rozsądek i dużo ostrożności. **Nie ulegaj presji, nie daj skusić się pozornie atrakcyjnymi ofertami,** bezwzględnie **nie działaj pod wpływem chwili.** Bądź świadomy co robisz i co się wokół Ciebie dzieje.

Jak wygląda atak?

- ZACHĘCANIE -

Wyłudzeń dokonują osoby podające się za tzw. „brokerów" inwestycyjnych – pracowników firm zajmujących się pośrednictwem i doradztwem inwestycyjnym. Firmy te ogłaszają swoje usługi za pomocą reklam w mediach społecznościowych, serwisach internetowych oraz aplikacjach mobilnych. Dla przyciągnięcia uwagi i uwiarygodnienia treści w reklamach wykorzystywane są wizerunki „przeciętnego Kowalskiego", który szybko zyskał dzięki współpracy z „pośrednikiem", lub wizerunek 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 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 powołując się również na rzekomą współpracę z konkretną instytucją finansową. Takie artykuły mogą być później masowo propagowane np. w serwisach społecznościowych, np. w Facebook'u. Informacje tego typu są często nieprawdziwe a ich celem jest manipulacja klientami.

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

- MANIPULACJA OFIARĄ I PROWADZENIE ATAKU -

W kolejnym kroku z ofiarą kontaktuje się telefonicznie przedstawiciel „brokera", podający się za „analityka". Mogą to być osoby posługujące się „wschodnim akcentem". Ofiara jest namawiana do przekazania opłaty rejestracyjnej np. w wysokości 250 EUR, często rozbitej na transze.

Dla zwiększenia swojej skuteczności „analitycy" namawiają do instalacji programów umożliwiających dzwoniącej osobie zdalny dostęp do urządzenia ofiary. 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 ofiary. Pod pozorem tej pomocy w obsłudze zleceń pseudo „analitycy" pozyskują od nieświadomych ofiar wrażliwe dane między innymi dotyczące kart płatniczych, dane umożliwiające dostęp do bankowości elektronicznej. Bardzo często dochodzi do sytuacji, gdy przestępcy przy akceptacji ofiar sami inicjują operacje kartami, logują się do bankowości elektronicznej, zrywają lokaty, biorą kredyty i inicjują płatności.

W początkowym okresie ofiara może obserwować niewielkie „wirtualne zyski" od przekazanej kwoty. Z czasem „analitycy" zaczynają namawiać do zainwestowania większej kwoty. Może się wiązać z np. „super" okazjami związanymi ze zmienną sytuacją na rynku kryptowalut lub Forex. Po początkowym czasie może się okazać, że inwestycja była nietrafiona, przy czym „broker" daje szanse na szybkie odrobienie strat. Może pojawić się oferta, że jeśli ofiara wpłaci kolejna kwotę to „broker" ze swojej strony również przekaże część środków by powiększyć inwestowaną kwotę. Przy okazji „analitycy" wykorzystują różne techniki manipulacji ofiarą.

W konsekwencji doprowadzają do sytuacji, gdy ofiara traci wszystkie oszczędności. Także i wtedy przestępcy nie zaprzestają ataków i namawiają do brania pożyczek i kredytów w celu odrobienia strat.

- WŁĄCZENIE OFIARY W DZIAŁALNOŚĆ PRZESTĘPCZĄ -

Podczas niektórych ataków przestępcy nakłaniają do przelania inwestowanych środków na konta prowadzone w innym banku. Ma to im ułatwić kontynuację rzekomego inwestowania w związku z rzekomymi działaniami prewencyjnymi podejmowanymi prze niektóre banki. W tym samym celu

uzgadniają z niektórymi ofiarami, że na ich rachunek w banku wpłyną środki od innej osoby dla późniejszego przekazania ich dalej. Dzięki temu będą mogły łatwiej uzyskać zysk od swoich „inwestycji" lub odrobić straty. W rzeczywistości w ten sposób ofiara zostanie wykorzystana do procederu prania pieniędzy pochodzących z przestępstwa (w transferze środków pochodzących z kradzieży u innej ofiary) i sama staje udziałowcem przestępstwa. Więcej o tego typu niebezpieczeństwach przeczytasz tu – linki:

- 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. W momencie kierowania takiego żądania ofiara dowiaduje się, że nie zostały spełnione przez nią zapisy Regulaminu odnoszące się np. do aktywności, liczby zleceń, wielkości wpłaconej kwoty, etc. W Regulaminie „brokera" znajdują się też często zapisy uprawniające go do swobodnego ustalania wysokości „opłat" i „prowizji".

Wariantów wyłudzeń związanych z inwestowaniem w kryptowaluty jest wiele. Ofiary mogą być nęcone 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 i mają być następnie przetransferowane poprzez założone na ich dane konta w kantorach czy giełdach kryptowalut lub Forex.

- FINAŁ -

Koniec jest prawie zawsze ten sam: ofiara traci wszystkie oszczędności, niejednokrotnie zmuszona jest wziąć kredyt lub pożyczkę a niekiedy nieświadomie sama zostaje włączona w działalność przestępczą.

Jak się przestrzec przed atakami tego typu?

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

- **Co wiem** o ryzyku inwestowania na tych rynkach?
- **Czy rozumiem** na czym polegają inwestycje tego typu?
- Czy jestem w stanie bez uszczerbku na poufności moich danych dokonać **samodzielnie** operacji na rynkach Forex i kryptowalut?

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

W przypadku, gdybyś natrafił na tego typu informacje, Prokuratura Krajowa, Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP wskazują, że dobrą praktyką jest w takich sytuacjach:

- Zapoznanie się z informacjami KNF i NBP dotyczącym inwestowania w kryptowaluty – link: https://uwazajnakryptowaluty.pl/;

- Sprawdzanie, np. w Internecie wiarygodność instytucji oferującej możliwość inwestowania i osiągania dużych zysków;
- Nieudostępnianie nikomu danych do logowania w bankowości elektronicznej i mobilnej;
- Nieudostępnianie poufnych danych kart płatniczych;
- Niedopuszczanie do instalowania dodatkowego oprogramowania, na urządzeniach z których następuje logowanie do bankowości internetowej lub mobilnej;
- Uważne zapoznawanie się z opisem kodów autoryzacyjnych wysyłanych z banków w celu zatwierdzania operacji;
- Bycie czujnym w przypadku pojawienia się jakichkolwiek propozycji związanych z transferem środków pochodzących od innych osób – nie stań się współudziałowcem przestępstwa;
- Ochrona poufności swoich dokumentów oraz wizerunku;
- Zwrócenie uwagi, że inwestycje wykorzystujące „dźwignię finansową" są zawsze obarczone dużym ryzykiem i informacja o tym powinna być przedstawiona w sposób jasny i zrozumiały;
- Instytucja zajmująca się tego typu działalnością nie musi być zarejestrowana w Polsce, ale powinna posiadać licencję wydaną przez organ nadzoru jednego z krajów Unii Europejskiej – poszukaj o tym informacji w internecie;
- Sprawdź, czy instytucja znajduje się na liście ostrzeżeń KNF – link: https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne;
- Sprawdź opinie o instytucji w internecie, np. w połączeniu ze terminami „oszustwo" lub „scam". 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;
- Zapoznaj 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, jaki są ustalane prowizje i opłaty, jak wygląda proces wypłaty środków.

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

Prokuratura Krajowa
Komenda Główna Policji
FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP