sierpień 2022

OSTRZEŻENIE PRZED ZAGROŻENIAMI
- próby oszustw inwestycyjnych

Ponownie ostrzegamy przed próbami oszustw, których częstym motywem są inwestycje w kryptowaluty oraz na rynkach Forex. Dodatkowo w ostatnim okresie pojawiają się motywy powiązane z inwestycjami w przedsięwzięcia realizowane przez spółki państwowe (np. PKN Orlen).

Typowy schemat działania oszustów:

1) ktoś (rzekomy „doradca" lub „broker") kontaktuje się telefonicznie, e-mailem lub przez media społecznościowe i:
    a. oferuje szansę zainwestowania w „jedyną w swoim rodzaju okazję" lub informuje o konieczności rozliczenia zysków z inwestycji (np. w kryptowaluty);
    b. oferuje pomoc w inwestowaniu - proponując, że będzie:
        - świadczyć doradztwo inwestycyjne, czyli rekomendować realizację transakcji na rynku Forex za pośrednictwem platform inwestycyjnych;
        - zarządzać portfelem klienta, czyli podejmować i realizować decyzje inwestycyjne na jego rachunek.
2) oszuści często brzmią wiarygodnie i mają wiedzę, która może uśpić czujność ofiary, np. operują liczbami czy prognozami zysków, a także podają przykłady znanych osób, które osiągnęły znaczące zyski z podobnych przedsięwzięć;
3) oszust dąży do tego, aby na urządzeniu (komputerze, telefonie, itp.) ofiary zostały zainstalowane odpowiednie programy (np. AnyDesk, TeamViewer, itp.) - rzekomo mają one ułatwić ofierze inwestowanie i/lub rozliczenie zysków, a także bieżący kontakt z „doradcą" (np. wyjaśnianie i prezentowanie, jak działa aplikacja do inwestowania oraz zasady obsługi zleceń). W rzeczywistości najczęściej są to programy, które umożliwiają oszustowi zdalne korzystanie z urządzenia ofiary i wyłudzenie poufnych danych;
4) można również natknąć się na ogłoszenie dotyczące inwestycji w Internecie lub w mediach społecznościowych z obietnicą szybkiego zysku – często tego typu ogłoszenia podszywają się pod logo znanych instytucji i/lub korzystają w sposób nieuprawniony z wizerunku znanych osób.

Wariantów wyłudzeń związanych z inwestowaniem jest wiele – stoją za nimi wyspecjalizowane grupy przestępcze. Przestępcy mogą oferować np. udział w ekskluzywnych szkoleniach dotyczących inwestowania, czy możliwość odbioru fikcyjnej „wygranej" wygenerowanej przez „jakiś" system inwestujący w kryptowaluty lub na rynku Forex. Zamiennie, zamiast inwestycji w kryptowaluty, mogą pojawić się zachęty do inwestowania w rynki Forex, czy też nabycie udziałów w nieruchomościach. Zdarzają się również „oferty" pracy związanej z obrotem kryptowalutami - wówczas na rachunki ofiary wpływają skradzione środki, które następnie mogą być przetransferowane poprzez założone na ich dane konta, w kantorach czy giełdach kryptowalut lub Forex.

Jak można rozpoznać próbę oszustwa?

Oferta inwestycyjna może być oszustwem, jeśli rzekomy „doradca" lub „broker":

1) dzwoni wielokrotnie lub często kontaktuje się za pomocą portali społecznościowych albo kanałem e-mail;
2) oferuje możliwości szybkich i wysokich zysków dzięki inwestycji w kryptowaluty lub na rynku Forex;
3) informuje o gwarancji zysku dla „każdego", bez względu na poziom wiedzy o rynkach finansowych lub wskazuje na „ekskluzywność" oferty i jej ograniczenie wyłącznie do wąskiej grupy klientow;
4) powołuje się na przykłady inwestycji, na których zyskały znane osoby;
5) nakłania do podjęcia szybkiej decyzji, aby nie stracić okazji;
6) oferuje wsparcie w obsłudze transakcji poprzez program do obsługi zdalnej (np. AnyDesk lub TeamViewer) i/lub poprzez kontakt telefoniczny;
7) informuje o pomocy „brokera" i konieczności dokonania pierwszej wpłaty (tzw. opłaty rejestracyjnej);
8) informuje o konieczności przesłania skanów (zdjęć) dokumentu tożsamości, selfie z dokumentem tożsamości, danych dotyczących rachunku bankowego, czy też dostępów do elektronicznych kanałów

dostępu i/lub danych kartowych, w celu potwierdzenia tożsamości i przyspieszenia rozliczania zysków z transakcji.

Przypominamy:

- przy inwestowaniu pieniędzy **ZAWSZE** stosuj metodę ograniczonego zaufania:
  - jeżeli nie rozumiesz oferty, **ZAWSZE** poproś o jej ponowne i dokładne wyjaśnienie;
  - jeżeli nie masz pewności i nie ufasz firmie, **NIGDY** niczego nie podpisuj i na nic się nie zgadzaj;
  - **NIGDY** nie ulegaj presji - uważaj na pozornie atrakcyjne oferty. Nie działaj pochopnie, pod wpływem chwili i emocji;
  - jeżeli rozważasz inwestycje, **ZAWSZE** zwróć szczególną uwagę czy podmiot, z którym nawiązujesz współpracę jest wiarygodny i ma wymagane zezwolenia do prowadzenia takiej działalności;
  - zanim zaczniesz inwestować, **ZAWSZE** zapoznaj się ze wszystkim zasadami i ryzykami, jakie dotyczą tego typu działalności, a szczególnie z zasadami i regulaminami podmiotów pośredniczących w inwestowaniu.
- **NIGDY** nie instaluj żadnego dodatkowego oprogramowania ze źródła, którego nie znasz lub na prośbę nieznanej Ci osoby - w szczególności jeśli jest to urządzenie (komputer, telefon, itp.), którego używasz do korzystania z bankowości elektronicznej;
- **ZAWSZE** zachowaj ostrożność jeżeli ktoś prosi Cię o zainstalowanie oprogramowania umożliwiającego zdalny dostęp do urządzenia (np. AnyDesk, TeamViewer, itp.) – pamiętaj, że umożliwia ono połączenie do urządzenia i dostęp do przechowywanych danych;
- **ZAWSZE** bądź ostrożny przy podawaniu danych telefonicznie i staraj się potwierdzić tożsamość rozmówcy – w przypadku jakichkolwiek wątpliwości zakończ rozmowę;
- jeśli treść rozmowy wyda Ci się podejrzana i niestandardowa, a osoba dzwoniąca wymaga szybkiego podjęcia działań (np. podania danych, instalacji oprogramowania, podania kodów SMS, itp.) **NIEZWŁOCZNIE** zakończ rozmowę;
- jeśli podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie, **NIEZWŁOCZNIE** skontaktuj się z Bankiem informując o zaistniałym zdarzeniu;
- **NIGDY** nie podawaj przez telefon nadmiarowych informacji, nie zdradzaj szczegółów swoich transakcji, ani innych danych podlegających ochronie;
- **NIGDY** nie udostępniaj nikomu danych do logowania w bankowości elektronicznej i mobilnej oraz danych poufnych dotyczących swoich kart płatniczych;
- **ZAWSZE** zachowuj ostrożność przy otwieraniu linków i korzystaniu z nieznanych portali internetowych - nie klikaj w podejrzane reklamy i nie korzystaj z ofert obiecujących bardzo wysokie i pewne zyski;
- **ZAWSZE** czytaj szczegółowo informacje z Banku (w szczególności treść wiadomości SMS, powiadomień i żądań autoryzacyjnych) – **ZAWSZE** zwracaj uwagę na to, co autoryzujesz;
- **ZAWSZE** chroń poufność swoich dokumentów tożsamości oraz wizerunku;
- **ZAWSZE** zachowaj czujność, gdyby pojawiły się jakiekolwiek propozycje związane z transferem środków inwestycyjnych pochodzących od innych osób, aby nie współdziałać w przestępstwie.

Więcej informacji o tego typu zagrożeniach znajdziesz tutaj:

- informacje KNF i NBP dotyczące inwestowania w kryptowaluty - https://uwazajnakryptowaluty.pl
- lista ostrzeżeń publicznych KNF - https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne
- komunikat Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP - https://zbp.pl/Aktualnosci/Wydarzenia/Uwazaj-na-oszukancze-serwisy-internetowe,-ktore-oferuja-kryptowaluty-i-inwestycje-na-rynku-Forex.
- ostrzeżenie PKN Orlen - https://www.orlen.pl/pl/ostrzegamy