DOSTAŁEŚ OFERTĘ INWESTYCJI W KRYPTOWALUTY? KTOŚ PROPONUJE CI ŁATWY I SZYBKI ZYSK? UWAŻAJ: OSZUŚCI ATAKUJĄ W INTERNECIE!

Data publikacji 18.02.2021

Jeżeli dostałeś propozycję skorzystania ze świetnej usługi finansowej, ktoś mówi ci o łatwym i szybkim zysku i namawia do inwestowania pieniędzy w kryptowaluty uważaj! Możesz paść ofiarą oszustwa. Przeczytaj koniecznie tekst i podaj go dalej. W ten sposób możemy razem przeciwdziałać oszustom!

Pandemia Covid-19 sprawiła, że bardziej niż wcześniej przenieśliśmy swoją aktywność do świata internetu. W sieci pracujemy, robimy zakupy, uczymy się czy spotykamy się ze znajomymi. Wiedzą też o tym przestępcy, którzy również przenieśli swoją działalność i bezwzględnie wykorzystują ludzkie błędy i często także naiwność. Na szczęście możemy się sami się przed nimi bronić poprzez zasadę ograniczonego zaufania, dużą dozę ostrożności i przede wszystkim poszerzanie własnej wiedzy, na temat tego jak działają przestępcy.

„Zainwestuj w kryptowaluty”- czyli jak działa oszust krok po kroku

W ostatnich latach jednym z wielu rodzajów oszustw w Internecie są przestępstwa związane z namawianiem ofiar do skorzystania z intratnych usług finansowych, które rzekomo mają przynieść łatwy, szybki i duży zysk. Sprawcy dzwonią losowo na różne numery telefoniczne do ofiar lub wysyłają spam na wiele kont e-mail z reklamą swoich usług i czekają, aż ofiara zgłosi się do nich sama. Ostatnio najczęściej występująca usługa finansowa to kryptowaluty.

Legendy, pod którymi działają oszuści mogą być różne. Na przykład:

- szybka oferta inwestycji, która po wpłacie kilkuset złotych pozwoli na ekspresowy zarobek kilku tysięcy
- wprowadzanie ofiary w błąd, że miała kiedyś portfel kryptowalutowy, na którym kilka lat temu było w kryptowalucie kilkadziesiąt złotych, a obecnie „urosło” kilkadziesiąt tysięcy złotych i że inwestor może, a nawet powinien wypłacić te pieniądze na swój rachunek bankowy
- oszuści podają się za pracowników fikcyjnych firm prowadzących działalność inwestycyjną i oferują usługi pomocy w inwestowaniu lub pomocy w przelewaniu rzekomej kryptowaluty na złotówki
- sprawcy informują inwestora, że w celu przeprowadzenia inwestycji albo przelewu należy wykonać ich instrukcje, które m.in. polegają na zainstalowaniu przez niego na swoim komputerze programu komputerowego do obsługi zdalnego pulpitu

Obcy akcent „konsultanta”, „polski” numer telefonu, na który nie można oddzwonić

Bardzo istotną cechą łączącą te oszustwa jest to, że przestępcy podszywający się pod konsultantów firm

inwestycyjnych mówią z obcym, bardzo często wschodnim akcentem. Niemniej ważny jest fakt, że wielu przypadkach oszuści dzwonią do swoich ofiar z numerów telefonicznych, które wyglądają jak polskie numery stacjonarne, np. +48 22 XXX XX XX. Numery te w rzeczywistości działają w ramach telefonii internetowej (VoIP) i mogą być używane przez każdego, z każdego miejsca na świecie. Usługi VoIP pozwalają na konfigurowanie dowolnych numerów, z dowolnymi prefiksami na całym świecie. Polski numer telefonu ma wywołać przeświadczenie o prawdziwości oferty, a wystarczy tylko podjąć próbę oddzwonienia na ten numer, która się nie powiedzie, żeby nabrać wątpliwości.

Zachęta do zainstalowania programu na własnym komputerze

Programem, który najczęściej każą instalować oszuści jest ANYDESK, ale mogą też być inne, które mają taką samą jak on funkcjonalność. Program ten jest legalny, używany na całym świecie przez specjalistów z dziedziny IT, aby łączyć się z komputerami klientów w celu udzielenia zdalnej pomocy w kwestiach technicznych działania komputerów i programów na nich zainstalowanych. Działanie takiego programu polega na tym, że osoba z dowolnego miejsca na świecie może uzyskać dostęp do naszego komputera i używać go tak, jakby była jego właścicielem. Oczywiście program sam w sobie nie jest w stanie zrobić niczego złego, a tylko nieumiejętne i bezkrytyczne korzystanie z tego programu, szczególnie w wyniku namowy przez nieznane nam osoby, którym dajemy nieskrępowany dostęp do naszego komputera prowadzi później do wielu problemów, najczęściej prawnych i finansowych.

Przejęcie konta, kradzież pieniędzy

Oszuści wprowadzają w błąd swoje ofiary, mówiąc np. że program ANYDESK jest potrzebny ze względu na przepisy jakie wprowadziła Komisja Nadzoru Finansowego, że operacja przelewu kryptowaluty na złotówki musi być nagrywana w celu formalnego udokumentowania transakcji. Często zdarza się też, że sprawcy każą instalować ANYDESK pod pozorem wystąpienia problemów technicznych na komputerze lub rzekomym koncie inwestycyjnym ofiary, tłumacząc, że muszą w ten sposób zdalnie rozwiązać te problemy w trakcie, kiedy skuszona „dobrą ofertą" ofiara loguje się do swojego banku i wykonuje wpłatę na rachunek inwestycyjny. Oszust przejmuje kontrolę nad rachunkiem tej osoby, prosi o kody do potwierdzania operacji i dosłownie na oczach ofiary okrada ją z pieniędzy na koncie, nierzadko także generując debet na rachunku bankowym pokrzywdzonego. Często zdarza się także, że oszuści wyłudzają od swojej ofiary dane z dowodu osobistego i wykorzystują je np. do zaciągnięcia kredytu w banku ofiary, podszywając się pod nią samą, robią to także w innych bankach lub firmach pożyczkowych.

Dodatkowo: konsekwencje za udział w praniu pieniędzy

Zdarzają się też przypadki, że przestępcy obiecując prowizje za wykonanie przelewu wykorzystują swoje ofiary do pośrednictwa w ukryciu pieniędzy pochodzących z innych przestępstw. Przelewają na rachunek takiej osoby kwoty pieniędzy, które dalej transferowane są przez posiadacza rachunku na wskazane przez sprawców inne rachunki lub portfele kryptowalutowe, w zamian za obietnicę otrzymania wynagrodzenia za taki przelew. Bywa również tak, że ofiary przekazują dostępy do swojego rachunku bankowego sprawcom, by sami wykonali operację. Przestępcy nie zapłacą żadnej prowizji, sami przeleją kwotę, którą wpłacili na konto ofiary. Przy okazji mogą też ukraść pieniądze, które ofiara miała na swoim rachunku bankowym.

W takiej sytuacji, osoba oprócz tego, że zostanie okradziona z własnych pieniędzy. może też ponieść konsekwencje prawne za pomocnictwo do transferowania pieniędzy pochodzących z przestępstwa czyli mówiąc wprost: za udział w praniu pieniędzy.

Nie tylko kupując, ale również sprzedając w Internecie musimy zachować czujność

W środę (17.02.2021) olsztyńscy policjanci otrzymali informację o próbie oszustwa internetowego. Z relacji zgłaszającego wynikało, że na jednym z portali ogłoszeniowych wystawił on na sprzedaż książki. Do 23-latka na komunikatorze napisał potencjalny kupujący, gdzie podczas konwersacji doszło do finalizacji transakcji. Po chwili sprzedający otrzymał link z rzekomym potwierdzeniem płatności oraz etykietą do wysłania paczki. 23-latek, aby otrzymać pieniądze musiał podać nr kart płatniczej i kod CVV. Po ich wpisaniu na stronie pojawił się błąd i nastąpiło przekierowanie do witryny banku, gdzie mężczyzna wpisał swoje dane do logowania i po tym – znowu wystąpił błąd i nagle pojawiła się strona portalu ogłoszeniowego z informacją o podaniu kodu sms celem potwierdzenia otrzymania wpłaty. 23-latek zorientował się ma do czynienia z oszustem i fałszywymi witrynami internetowymi, ponieważ od dłuższego czasu nie otrzymał smsa z kodem. Mężczyzna wtedy postanowił anulować transakcję, po czym otrzymał informację, że została ona autoryzowana z innego urządzenia mobilnego na kwotę 100 tysięcy złotych. 23-latek

natychmiast zadzwonił na infolinie banku i zastrzegł kartę płatniczą oraz konto bankowego. W ten sposób mężczyzna uniknął utraty swoich oszczędności.

Uwaga na oszustów podszywających się pod pracowników banku

W powiecie piskim policjanci wyjaśniają okoliczności usiłowania oszustwa „na pracownika banku". Dzięki tej metodzie sprawcy są w stanie przejąć dostęp do konta bankowego ofiary i środków na nim zgromadzonych, a nawet wziąć kredyt. Mieszkankę powiatu piskiego próbowała oszukać kobieta podająca się za pracownika banku. Dzwoniąca poinformowała klientkę banku o dokonanym właśnie przelewie z jej konta w wysokości 500 złotych. Sytuacja od razu wydawała się podejrzana, ale „konsultantka" dzwoniła z numeru wyglądający jak ten prawdziwy telefon banku. Dzwoniąca kobieta powiedziała, że istnieje możliwość unieważnienia tej wypłaty poprzez zainstalowanie odpowiedniej aplikacji. Ofiara ściągnęła wskazaną aplikację i postępowała zgodnie ze wskazówkami „pracownika banku". Ofiara najprawdopodobniej pomyliła kod, który należało tam wpisać i aplikacja została zablokowana. Wówczas „konsultant banku" polecił, aby zadzwoniła na infolinię prosząc o jej odblokowanie. Tak też zrobiła. Tam dowiedziała się, że jej konto zostało zablokowane z uwagi na próbę wyłudzenia jej danych oraz złożenia wniosku o kredyt na łączną kwotę 22 900 złotych. Pracownica infolinii poinformowała, że była to próba oszustwa i sprawę należy zgłosić na policję. Funkcjonariusze przyjęli od pokrzywdzonej zawiadomienie o podejrzeniu popełnienia przestępstwa oszustwa na jej szkodę. Policjanci będą teraz prowadzili czynności mające na celu wyjaśnienie sprawy oraz ustalenie i zatrzymanie sprawcy.

Apelujemy o przestrzeganie podstawowych zasad bezpieczeństwa w sieci!

Nie klikajmy bez zastanowienia w nieznane linki! Zachowajmy ostrożność po otrzymaniu linku z przekierowaniem do innej witryny internetowej, szczególnie jeżeli przenosi ona nas do stron logowań do kont bankowych, portali społecznościowych czy aukcyjnych. Jakakolwiek sugestia konieczności ponownego wpisania naszych danych do zalogowania się na danej stronie, powinna wzbudzić naszą czujność. Należy również zweryfikować nadawcę otrzymanej wiadomości. W tym celu można przeanalizować adres strony. Często są one tworzone przez oszustów i do złudzenia przypominają istniejące legalne witryny. Różnić się mogą jednak jedną literą, kropką czy podkreślnikiem.

Pamiętajmy, że zarówno w świecie realnym jak i wirtualnym to my sami w pierwszej kolejności musimy zadbać o bezpieczeństwo naszych danych osobowych oraz finansów.

Nie daj się oszukać!

Co zrobić, żeby nie paść ofiarą oszustów? Pamiętać o zasadach bezpieczeństwa:

- należy kategorycznie odrzucać wszystkie oferty, w których składane są propozycje łatwego, szybkiego i dużego zarobku poprzez kryptowaluty i inne instrumenty
- osoby które nigdy nie zajmowały się inwestowaniem, w tym transakcjami kryptowalutowymi, nie wiedzą jak działa taki produkt i ten rynek, nie mają wystarczającej wiedzy informatycznej pod żadnym pozorem nie mogą podejmować ofert płynących do nich drogą mailową czy telefoniczną, kierując się tylko chęcią osiągnięcia szybkiego zysku
- należy zapoznać się z tym, jak działają te instrumenty, w tym kryptowaluty i programy do obsługi zdalnego pulpitu. Jakakolwiek namowa przez „konsultanta" do zainstalowania programów powinna być powodem do zakończenia rozmowy
- instalować należy tylko narzędzie wskazane przez bank i znajdujące się w jego ofercie, takie jak np. aplikacja moblina na telefon do obsługi rachunku
- każdy, kto mimo grożących niebezpieczeństw chce skorzystać z takich usług, musi dążyć do jak najgłębszej weryfikacji informacji przekazywanych przez konsultanta, np. uzyskać jego imię i nazwisko, nazwę, adres firmy którą reprezentuje, adres e-mail, numer telefonu na który można do nich zadzwonić, dane przełożonego konsultanta, poprosić o dane np. z ewidencji działalności gospodarczej, nr REGON, NIP, dane z KRS. Na uzyskane numery telefonów należy oddzwonić, potwierdzić kto odbierze, poprosić o przesłanie dokumentów dotyczących oferty na maila
- nie należy się zgadzać się na współpracę po pierwszym kontakcie. Trzeba dać sobie czas na przemyślenie i sprawdzić uzyskane informacje np. na stronach Komisji Nadzoru Finansowego, porozmawiać z konsultantem w swoim banku, skontaktować się z Policją i poprosić o pomoc w weryfikacji informacji o ofercie, czy po prostu

sprawdzić informacje w Internecie, np. na stronach o bezpieczeństwie internetowym

- nie można udzielać informacji na temat dostępu do naszego konta, danych do logowania, danych autoryzacyjnych operacji bankowych i naszych danych osobowych żadnej postronnej osobie.

Pamiętajmy, że to my sami jesteśmy w pierwszej klolejności odpowiedzialni za swoje bezpieczeństwo i prawidłowe zabezpieczenie swojego mienia!

(KWP w Olsztynie