# OSZUSTWA I WYŁUDZENIA ZWIĄZANE Z KRYPTOAKTYWAMI

## ZACHOWAJ CZUJNOŚĆ I ZADBAJ O SWOJE BEZPIECZEŃSTWO

Szybki rozwój kryptoaktywów i ich cechy charakterystyczne, takie jak: globalna dostępność, szybkość, anonimowość i często nieodwracalność transakcji, implikują ich powszechne wykorzystanie przez cyberprzestępców. Tytułem wyjaśnienia, oszuści i naciągacze stosują wyrafinowane taktyki, takie jak: piramidy finansowe (tzw. *„Ponzi schemes”*), fałszywe możliwości inwestycyjne, bezpłatne oferty w mediach społecznościowych i oszukańcze wiadomości. Ponadto, wykorzystują również oszustwa romantyczne i matrymonialne (tzw. *„romance scams”*), bądź inne podobne metody – polegające na budowaniu relacji i zaufania, aby sięgnąć po środki znajdujące się w Twoim portfelu. Najczęstszą formą komunikacji są media społecznościowe, aplikacje do przesyłania wiadomości, e-maile i nieoczekiwane telefony, które brzmią jak prawdziwe. Istnieje wówczas poważne ryzyko, że można utracić prywatne środki finansowe, bądź to tożsamość i doznać poważnego stresu.

Z tego względu apelujemy o szczególną ostrożność i postępowanie zgodnie z poniższymi wskazówkami:

**Zachowaj czujność wobec potencjalnych oszustw związanych z kryptoaktywami:**
kliknij tutaj, aby dowiedzieć się więcej o różnych rodzajach oszustw (zobacz s. 5-8).

**Rozpoznawaj sygnały ostrzegawcze:**
naucz się rozpoznawać podejrzane zachowania, wiadomości lub oferty (zobacz s. 2).

**Zadbaj o własne bezpieczeństwo i swoich aktywów:**
zabezpiecz swoje dane osobowe (zobacz s. 3).

**Dowiedz się, co zrobić, jeśli padniesz ofiarą oszustwa lub nadużycia**
(zobacz s. 4).

# Sygnały ostrzegawcze

Obietnica, która wydaje się zbyt piękna, aby mogła być prawdziwa.

Nieproszona oferta.

Gwarantowany szybki i wysoki zwrot.

Pilna potrzeba działania (np. ograniczone czasowo oferty, które zmuszają Cię do natychmiastowego działania).

Prośba o dokonanie płatności za pomocą metod niemożliwych do wyśledzenia (np. kryptoaktywa, karty podarunkowe, przelewy bankowe lub przedpłacone karty debetowe).

Zaproszenie do kliknięcia w określony link, zeskanowania kodu QR lub pobrania aplikacji.

Prośba o przesłanie lub udostępnienie kluczy prywatnych i fraz *seed* (tzw. „*seed phrases*" stanowiąca listę słów umożliwiających dostęp do portfela krypto).


Podejrzany lub niepoprawny adres URL.

Logo z niewielkimi zniekształceniami, strona internetowa, która kopiuje wygląd prawdziwej strony internetowej przedsiębiorstwa lub wygląda profesjonalnie, ale nie ma zweryfikowanych danych kontaktowych, informacji na temat rejestracji przedsiębiorstwa, historii lub weryfikowalnej obecności.

Nieznana platforma wymiany.

Podejrzany załącznik - zwłaszcza .exe, .scr, .zip lub plik pakietu Office z włączoną obsługą makr (.docm, .xlsm).

# Kroki, które pomogą Ci się chronić:

## 1 Zanim podejmiesz działanie, zatrzymaj się i zastanów się:

Nie podejmuj pochopnych decyzji dotyczących inwestycji, udostępniania informacji lub klikania w przesłane Ci linki – oszuści celowo wywołują pośpiech. W razie jakichkolwiek wątpliwości, nawet najmniejszych, nie podejmuj działań ani nie inwestuj, a źródło informacji dokładnie zweryfikuj.

## 2 Dokładnie sprawdź źródło:

- Zawsze weryfikuj, skąd pochodzą wiadomości, połączenia, e-maile i linki, nawet jeśli wyglądają na oficjalne, bądź to zdają się pochodzić od znajomych lub rodziny, a zwłaszcza osoby publicznej. Zwróć uwagę na błędy ortograficzne, dziwne adresy URL lub brakujące wskaźniki bezpieczeństwa. Tytułem przykładu, sprawdź, czy link do strony internetowej zawiera literę „s" w „HTTPS", celem upewnienia się, że strona jest bezpieczna. Dodatkowo sprawdź, czy w nazwie firmy nie ma dodanych lub brakujących liter.
- Nie otwieraj linków z niechcianych wiadomości. Instaluj tylko oficjalne aplikacje z zaufanych sklepów z aplikacjami i nie skanuj nieznanych kodów QR.
- Nawet jeśli oferta wygląda na wiarygodną zawsze porównaj ją ze stroną internetową przedsiębiorstwa lub sprawdź, czy konto w mediach społecznościowych jest sprawdzone (np. za pomocą oficjalnych znaczników).
- Skorzystaj z dających się zweryfikować danych kontaktowych, aby dotrzeć bezpośrednio do firmy lub właściwej osoby fizycznej. Nigdy nie polegaj na danych kontaktowych dostarczonych przez osobę, którą podejrzewasz, że może być oszustem. Tytułem przykładu, taka osoba może podawać się za upoważnioną, bądź to wykorzystywać fałszywą stronę internetową naśladująca stronę realnego przedsiębiorstwa. Możesz sprawdzić, czy dostawca kryptoaktywów jest autoryzowany w UE, sprawdzając rejestr ESMA (↖) i do sprawdzenia, czy wydano jakiekolwiek ostrzeżenia, czarne listy, bądź to listę I-SCAN IOSCO (iosco.org/i-scan/).

## 3 Nigdy nie udostępniaj haseł, kluczy prywatnych ani fraz *seed*:

Każdy, kto ma do nich dostęp, może przejąć kontrolę nad Twoimi aktywami. Przedsiębiorstwa działające zgodnie z prawem nigdy nie będą prosić o hasła, czy kody bezpieczeństwa poprzez e-mail, SMS lub telefon.

## 4 Zabezpiecz urządzenia i klucze prywatne:

Używaj silnych i unikalnych haseł dla każdego ze swoich kont , zachowaj hasło w tajemnicy i unikaj ponownego wykorzystania tych samych danych logowania na różnych platformach. W miarę możliwości włącz uwierzytelnianie wieloskładnikowe (↖). Aktualizuj i aktywuj swoje oprogramowanie oraz miej włączoną ochronę antywirusową.

## 5 Zachowaj ostrożność w przypadku nieoczekiwanych ofert inwestycyjnych:

Uważaj na inwestycje obiecujące ogromne zyski. Jeśli coś brzmi zbyt pięknie, aby mogło być prawdziwe- prawdopodobnie tak jest.

## 6 Zastanów się, zanim udostępnisz informacje w mediach społecznościowych:

Grupy czatów, fora, posty w mediach społecznościowych i zdjęcia mogą być cennym źródłem wiedzy dla oszustów. Ujawnianie zbyt wielu informacji o sobie lub prowadzonych przez siebie inwestycjach może sprawić, że staniesz się łatwym celem.

# Co zrobić, gdy staniesz się ofiarą oszustwa lub oszustwa

**Natychmiast wstrzymaj transakcje,**

Aby zablokować dalsze przelewy na podejrzane konta i uniknąć dodatkowych strat. Zerwij kontakt z oszustami – zignoruj ich połączenia i e-maile oraz zablokuj nadawcę.

**Zmień hasła na wszystkich urządzeniach i aplikacjach/stronach internetowych.**

Oszuści kupują w Internecie hasła, które wyciekły, i próbują je wykorzystać na wielu kontach. Zmiana tylko jednego hasła nie jest wystarczająca! Pamiętaj, aby zmienić je wszystkie, aby ci nie mogli ich ponownie wykorzystać.

**Odłącz i cofnij dostęp:**

Cofnij podejrzane uprawnienia w umowie internetowej, która działa automatycznie w technologii blockchain (tzw. „*smart contract*" – inteligentna umowa), aby uniemożliwić oszustom wydawanie Twoich tokenów bez wyrażonej przez Ciebie zgody. Wiele portfeli i eksploratorów technologii blockchain oferuje narzędzia, które pozwalają sprawdzić, które inteligentne umowy mają obecnie dostęp do wydawania Twoich tokenów. Aby to zrobić, możesz:

- skorzystać z zaufanego „narzędzia do sprawdzania uprawnień", które weryfikuje, czy użytkownik lub adres łańcucha bloków jest upoważniony do wykonania operacji.
- przejrzeć listę zatwierdzeń, oraz
- użyć przycisku „cofnij" bezpośrednio z platformy.

**Przenieś swoje środki:**

Jeśli Twój portfel jest zagrożony, natychmiast przenieś pozostałe aktywa do nowego, bezpiecznego portfela.

**Skontaktuj się ze swoim dostawcą kryptoaktywów:**

Jak najszybciej poinformuj swojego dostawcę kryptoaktywów, korzystając z oficjalnych kanałów kontaktu, aby poznać potencjalne, najlepsze opcje zachowania się. Nawet jeśli w większości przypadków cofnięcie transakcji nie będzie możliwe, dostawca może nadal zamrozić konto oszusta (jeśli to znajduje się na jego platformie) i umieścić adres portfela na czarnej liście.

**Zgłoś i ostrzeż:**

Zgłoś incydent policji lub krajowemu organowi nadzoru nad rynkiem finansowym i poinformuj swoją sieć kontaktów (np. przyjaciół i rodzinę), aby zwiększyć ich świadomość.

**Uważaj na oszustwa typu „*recovery room*":**

Wyjaśniając, oszust może skontaktować się z Tobą jako ofiarą oszustwa, twierdząc jednocześnie, że ten jest organem publicznym (np. policją, organem podatkowym lub instytucją finansową) i oferując odzyskanie utraconych pieniędzy pod warunkiem uiszczenia odpowiedniej opłaty. Często jest to kolejna próba oszustwa. Biorąc powyższe od uwagę- pamiętaj, że jednokrotne oszustwo nie uniemożliwia ponownego.

Więcej informacji na temat ryzyka związanego z kryptoaktywami można znaleźć w ostrzeżeniu Europejskich Urzędów Nadzoru (↖) oraz w arkuszu informacyjnym pt. „Kryptoaktywa wyjaśnione: co oznacza MiCA dla Ciebie jako konsumenta" (https://link.europa.eu/BRv4Gn).

Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych, Europejski Urząd Nadzoru Giełd i Papierów Wartościowych, 2025

Luksemburg: Urząd Publikacji Unii Europejskiej, 2025



PDF ISBN 978-92-9407-245-0 doi:10.2853/3094937 DZ-01-25-133-PL-N

# RODZAJE OSZUSTW ZWIĄZANYCH Z KRYPTOAKTYWAMI

## SCHEMAT „*PUMP-AND-DUMP*" LUB „*RUG PULL*"

Widzisz reklamę w mediach społecznościowych lub na stronie internetowej promującej „*ograniczoną czasowo szansę inwestycyjną*" w kryptoaktywa, która rekomenduje inwestowanie w nowy token lub projekt. Po wyrażeniu zainteresowania zakupem zostajesz przekierowany na platformę wymiany kryptoaktywów lub kanał komunikacyjny (np. Telegram, Viber, WhatsApp). Pozornie wiarygodna firma albo osoba fizyczna może Ci obiecywać szybkie lub wysokie zyski, jeśli tylko wystarczająco szybko zainwestujesz. Oszuści wpierw zachęcają do zainwestowania niewielkiej kwoty, a następnie naciskają, abyś zainwestował więcej.

***Co może się zdarzyć:***

*Odkrywasz, że token, w który zainwestowałeś, jest bezwartościowy, a firma lub osoba fizyczna, z którą pozostawałeś w kontakcie, przestaje nagle odpowiadać. Kiedy chcesz wypłacić pieniądze, strona internetowa już nie istnieje, a firma, która nią zarządza jest nieosiągalna. Oszuści sztucznie zawyżali lub wyolbrzymiali kryptoaktywa o niskiej wartości, aby zwiększyć ich wartość („pump"), a następnie sprzedawali posiadane aktywa („dump"), powodując spadek wartości i tym samym straty dla inwestorów. Alternatywnie mogą zamknąć projekt i zniknąć wraz z funduszami („rug pull").*

## OSZUSTWO POLEGAJĄCE NA PODSZYWANIU SIĘ POD INNĄ OSOBĘ

Po opublikowaniu pytania na platformie społecznościowej lub stronie internetowej dotyczącej problemów z portfelem otrzymujesz nieoczekiwaną bezpośrednią wiadomość („*DM*") lub e-mail od osoby podającej się za zaufany kontakt (np. giełdę kryptoaktywów, dostawcę portfela, wsparcie IT, a nawet znajomego). Osoba ta prosi Cię o podanie frazy *seed* (tj. sekwencji słów służących jako centralna kopia zapasowa umożliwiająca dostęp do portfela cyfrowego), hasła lub kluczy prywatnych (automatycznie generowanego kodu kryptograficznego, który potwierdza własność zasobów cyfrowych).

***Co może się zdarzyć:***

*Po udostępnieniu frazy seed, haseł lub kluczy prywatnych oszust wykorzystuje je do kradzieży kryptoaktywów lub innych środków. Należy pamiętać, że utrata kluczy prywatnych powoduje trwałą i nieodwracalną utratę dostępu i własności aktywów. W przeciwieństwie do transakcji bankowych, w przypadku transferów w kryptoaktywach, gdy środki zostaną utracone, ich odzyskanie jest praktycznie niemożliwe.*

## Phishing

Otrzymujesz nieoczekiwaną wiadomość przez pocztę e-mail, telefon, media społecznościowe bądź to w postaci wyskakującego okna internetowego. Rzekomo pochodzi ona od znanego dostawcy kryptoaktywów. Otrzymana wiadomość zachęca Cię do zalogowania się lub pobrania nowej aplikacji. Istnieje możliwość otrzymania również wiadomości e-mail, która wydaje się pochodzić z aplikacji portfela. Nakłania Cię ona do rozwiązania problemu z bezpieczeństwem poprzez kliknięcie linku podanego przez to nieoficjalne źródło lub aktualizację aplikacji.

***Co może się zdarzyć:***

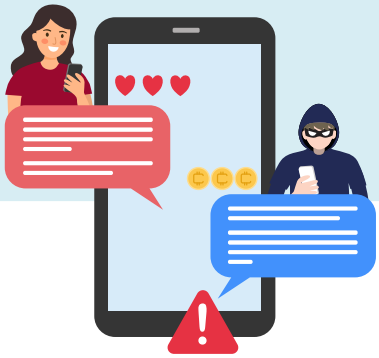
*Klikając link, pobierając aplikację lub skanując kod QR, instalujesz złośliwe oprogramowanie, które umożliwi oszustowi dostęp do informacji i wykorzystanie ich w celu kradzieży Twoich kryptoaktywów lub funduszy.*

## Oszustwo związane z rozdawaniem nagród

W mediach społecznościowych natrafisz na ogłoszenie, w którym firmy oferują rozdawanie kryptoaktywów po dokonaniu niewielkiej inwestycji. Zawiera ono film lub post z fotografiami celebrytów lub znanych marek, które zazwyczaj są fałszywe, bądź to uzyskane bez zgody. Ogłoszenie jawnie obiecuje „podwojenie Twoich kryptoaktywów", jeśli najpierw wyślesz pieniądze. Logo, układ, referencje i użyty język wyglądają profesjonalnie i oficjalnie, podobnie jak strona internetowa, na którą zostajesz przekierowany.

***Co może się zdarzyć:***

*Po wysłaniu kryptoaktywa nie otrzymujesz nic w zamian i tracisz wysłane pieniądze. Rozdanie było fałszywe, a post lub transmisja na żywo podszywająca się pod celebrytów lub firmy została zaprojektowana celem oszustwa i wyłudzenia.*



## Oszustwa inwestycyjne polegające na zbudowaniu relacji i zaufania

Osoba, której nie znasz w rzeczywistości, skontaktowała się z Tobą za pośrednictwem mediów społecznościowych, aplikacji randkowych lub telefonu/SMS-ów. Dąży ona do inicjowania osobistych i romantycznych rozmów, tym samym, starając się zdobywać Twoje zaufanie. Stopniowo jednak kieruje rozmowę na możliwości inwestycyjne, twierdząc, że osiąga ogromne zyski z kryptoaktywów i tym samym zachęca Cię do zainwestowania obietnicami wysokich zysków i niskiego ryzyka. W tym celu pomaga Ci założyć konto i instruuje jak dokonać niewielkiej wpłaty początkowej. Robi to wszystko po to, aby stworzyć wystarczające złudzenie legalności.

Oszuści, chcąc nawiązać z Tobą kontakt, tworzą zatem fałszywe profile internetowe i wykorzystują skradzione lub wygenerowane przez sztuczną inteligencję zdjęcia.

***Co może się zdarzyć:***

*Oszust wyciąga jak najwięcej pieniędzy, a następnie odcina wszelką komunikację i znika. Fałszywa strona internetowa lub aplikacja zostaje wyłączona, uniemożliwiając Ci dostęp do fałszywych inwestycji. W niektórych przypadkach oszuści mogą wykorzystać informacje uzyskane podczas oszustwa, aby zaatakować Twoich przyjaciół i rodzinę oraz dokonać kradzieży tożsamości, co może mieć dla Ciebie konsekwencje finansowe lub prawne (przykładowo - oszust może zidentyfikować skradzione portfele w Twoim imieniu, a Ty możesz zostać pociągnięty do odpowiedzialności za długi lub przestępstwa popełnione w Twoim imieniu, chyba że udowodnisz, że jest inaczej).*

## Piramidy finansowe („*Ponzi schemes*")

Zostajesz zaproszony do udziału w projekcie, który obiecuje stałe, wysokie zyski z inwestycji w kryptoaktywa. Dodatkowo, często są one poparte referencjami lub fałszywymi historiami sukcesu. Program może być przedstawiony jako okazja do marketingu wielopoziomowego, w ramach którego zarabiasz na własnej inwestycji, ale także na rekrutacji innych osób. Wydaje się, że pierwsi inwestorzy otrzymują wypłaty, co zachęca więcej osób do przystąpienia do programu i promowania go.

W rzeczywistości jednak nie ma żadnego biznesu, ani nie osiąga się żadnego zysku. Zamiast tego pieniądze pochodzą wyłącznie z wkładu inwestorów dołączających stosunkowo później. Całość operacji służy do wypłacania zwrotów organizatorom i pierwszym uczestnikom programu.

***Co może się zdarzyć:***

*Gdy tempo nowych inwestycji spadnie, program upada, a Ty, podobnie jak większość uczestników, tracisz swoje pieniądze. Organizatorzy znikają, nie pozostawiając żadnej możliwości odzyskania środków. Struktura wielopoziomowa pomaga w szybkim rozprzestrzenianiu się oszustwa, ponieważ ofiary nieświadomie stają się jego promotorami.*


## MYLĄCE ZNAKI W ADRESIE PORTFELA KRYPTO („ADDRESS POISONING")

Po dokonaniu transakcji zauważasz, że w historii Twojego portfela pojawił się nowy adres. Adres ten wygląda podobnie do adresu, z którym miałeś wcześniej do czynienia. Oszuści mogą sprawić, że fałszywe adresy portfeli pojawią się w historii transakcji, wysyłając niewielką ilość kryptoaktywa z podobnego adresu do portfela. W rezultacie, w historii ostatnich działań portfela lub w automatycznych sugestiach przechowujesz fałszywy adres. Oszuści celowo tworzą takie adresy, zmieniając tylko kilka znaków, często w środkowej części adresu, aby uniknąć wykrycia.

***Co może się zdarzyć:***

*Kiedy próbujesz wysłać kryptoaktywa i kopiujesz niewłaściwy adres z historii portfela, nieświadomie wysyłasz środki do portfela oszusta. Ponieważ transakcje związane z kryptoaktywami są często nieodwracalne, w większości przypadków środki są tracone na zawsze. Oszustwo to opiera się na błędzie użytkownika, wykorzystując nawyk kopiowania i wklejania adresów portfeli bez ich dokładnego sprawdzania.*