

Jak nie stracić kryptowalut

Lista kontrolna: czego nigdy nie robić, jak się chronić i co zrobić, jeśli to już się stało.

Czego nigdy nie robić

- 1 **Nigdy nikomu nie podawać frazy odzyskiwania (12–24 słowa) ani klucza prywatnego.** Nie poprosi o nie żadna giełda, pomoc techniczna ani policjant. Kto o nie prosi, chce Państwa okraść.
- 2 **Nigdy nie inwestować za pośrednictwem osoby poznanej w internecie:** w aplikacji randkowej, na Telegramie, WhatsAppie czy Facebooku. Tak zaczyna się większość oszustw, nawet po miesiącach rozmów.
- 3 **Nigdy nie wierzyć w gwarantowany zysk.** „2% dziennie”, „bez ryzyka”, „tylko dziś” zawsze oznaczają oszustwo.
- 4 **Nigdy nie płacić za wypłatę własnych pieniędzy.** Jeśli przed wypłatą żąda się „opłaty”, „podatku” lub „ubezpieczenia”, pieniądze już przepadły.
- 5 **Nigdy nie instalować aplikacji do zdalnego dostępu** (AnyDesk, TeamViewer i podobnych) tylko dlatego, że ktoś o to prosi.
- 6 **Nigdy nie odpowiadać „pomocy technicznej”, która odezwała się pierwsza.** Prawdziwi administratorzy i pracownicy giełd nie piszą pierwsi.
- 7 **Telefon z „banku”, „giełdy” lub „policji”?** Rozłączyć się i samemu zadzwonić na oficjalny numer.
- 8 **Nigdy nie zatwierdzać w portfelu niczego, czego się nie rozumie.** Jedno „Approve” lub „Sign” na fałszywej stronie może opróżnić cały portfel.
- 9 **Sprawdzać cały adres odbiorcy, nie tylko początek i koniec.** Nie kopiować adresów z historii transakcji: oszuści podrzucają tam ładząco podobne adresy.
- 10 **Nigdy nie ufać usługom „odzyskiwania”,** które gwarantują zwrot pieniędzy lub chcą kryptowalut z góry. To drugie oszustwo po pierwszym.

Jak się chronić

- Adres giełdy wpisywać samodzielnie lub otwierać z zakładki. Fałszywe strony pojawiają się w wynikach Google i w reklamach.
- Korzystać z giełdy z licencją na działalność w Państwa kraju lub regionie. Włączyć weryfikację dwuetapową przez aplikację uwierzytelniającą, nie przez SMS.
- Włączyć na giełdzie listę dozwolonych adresów wypłat, aby pieniądze mogły trafiać tylko na zatwierdzone przez Państwa adresy.
- Większe kwoty trzymać w portfelu sprzętowym kupionym wyłącznie u producenta.
- Co jakiś czas sprawdzać, którym stronom portfel nadał uprawnienia, i cofać niepotrzebne (na przykład za pomocą revoke.cash).

Jeśli to już się stało

- 1 **Nic więcej nie płacić** i przerwać kontakt z oszustami.
- 2 **Zabezpieczyć dowody:** identyfikatory transakcji (TxID), adresy, kwoty, godziny oraz zrzuty ekranu czatów i strony.
- 3 **Natychmiast zgłosić sprawę** swojej giełdzie i policji. Najważniejsze są pierwsze godziny: dopóki pieniądze są na giełdzie, można je zamrozić.
- 4 **Jeśli trzeba prześledzić, dokąd trafiły pieniądze,** i przygotować dowody dla policji i giełdy: trailforensics.com.

Trail Forensics nigdy nie prosi o frazy odzyskiwania, hasła ani dostęp do portfela i nie gwarantuje zwrotu pieniędzy.