WSZYSTKO CO MUSISZ WIEDZIEĆ O KRYPTOWALUTACH

CZASTOPIENIĄDZ

Rozdział 40. Jak nie stracić przez jeden klik

Zacznijmy od zdania, które prostuje najczęstsze nieporozumienie w tej branży.

„Blockchain został zhakowany" jest prawie zawsze błędnym opisem tego, co się wydarzyło.

W większości incydentów sprawca nie łamie kryptografii ani nie przejmuje sieci. Robi jedną z pięciu rzeczy: **przejmuje klucz, oszukuje osobę posiadającą klucz, wykorzystuje błąd aplikacji, przejmuje konto na giełdzie albo nakłania ofiarę do szkodliwej transakcji. To ostatnie jest najczęstsze, napastnik nie musi niczego łamać, wystarczy, że przekona Cię, żebyś sam kliknął.**

Ten rozdział jest o tym, jak to wygląda w praktyce.

Skala i jedna liczba, która wszystko porządkuje

Zestawmy dwie kategorie, bo ich porównanie mówi więcej niż jakakolwiek pojedyncza suma.

Włamania techniczne, czyli exploity, wycieki kluczy, ataki na protokoły, kosztowały według Chainalysis około 2,2 miliarda dolarów w 2024 roku i około 3,4 miliarda w 2025.

Oszustwa, czyli sytuacje, w których ofiara sama wysyła środki pod wpływem manipulacji, to co najmniej 12 miliardów dolarów w 2024 i co najmniej 14 miliardów w 2025, z możliwością wzrostu do 17 miliardów po identyfikacji kolejnych adresów.

Przeczytaj to jeszcze raz. **Ludzie dobrowolnie wysyłają oszustom czterokrotnie więcej, niż wynoszą straty ze wszystkich włamań do systemów.**

Ciekawa jest pierwsza połowa 2026 roku: **207 włamań wobec 83 rok wcześniej, czyli dwa i pół raza więcej.** To rekord. **A wartość skradzionych aktywów spadła w tym samym czasie o 57 procent.**

I ciekawostka potwierdzająca to, co napisałem wyżej: **w ujęciu wartościowym to spadek.** Udział kradzieży z prywatnych portfeli w całej skradzionej wartości spadł z 44 procent do 20. **Incydentów jest dużo więcej, ale pojedyncza ofiara traci mniej.**

Ataków przybywa, kwoty maleją. To znaczy, że celem coraz częściej jest zwykły użytkownik, a nie duży protokół.

I liczba, która pokazuje kierunek: przychody oszustw polegających na **podszywaniu się** wzrosły w 2025 roku o około 1400 procent rok do roku.

Trzy rzeczy, o które nikt nigdy nie poprosi

Zanim przejdziemy do metod, zapamiętaj trzy zdania. **Jeśli zapamiętasz tylko je, unikniesz większości tego, co opiszę niżej.**

Nikt nigdy nie prosi o frazę odzyskiwania. Ani wsparcie giełdy, ani producent portfela, ani „weryfikacja bezpieczeństwa". Konsultant nie potrzebuje Twojego klucza, żeby zdiagnozować problem.

Nikt nigdy nie prosi o przeniesienie środków na „bezpieczny adres". Ta prośba nie istnieje w żadnej legalnej procedurze. Zawsze oznacza kradzież.

Nikt nigdy nie kontaktuje się z Tobą pierwszy w sprawie Twoich pieniędzy. Prawdziwe wsparcie odpowiada na Twoje zgłoszenie. Nie pisze do Ciebie samo.

Cel pierwszy: zdobyć Twoją frazę

To najprostsza droga, kto ma frazę, ma wszystko.

Fałszywe strony. Kopia giełdy albo portfela, do której trafiasz przez reklamę, wiadomość albo wynik wyszukiwania. Strona prosi o zalogowanie, „odblokowanie konta" albo „synchronizację portfela".

Warto tu obalić mit: **kłódka przy adresie niczego nie potwierdza.** Certyfikat oznacza wyłącznie, że połączenie jest szyfrowane, a strona oszusta też może mieć szyfrowane połączenie.

Sygnały: domena różniąca się jedną literą, wejście z reklamy, żądanie frazy, presja czasu. I **sygnał najlepszy ze wszystkich: menedżer haseł nie rozpoznaje domeny. On nie da się nabrać na podobieństwo wizualne.**

Fałszywe aplikacje i rozszerzenia. Kopia znanego portfela, która przy „importowaniu" wysyła Twoją frazę sprawcy. Sygnały: inna nazwa wydawcy niż oficjalna, mała liczba pobrań mimo znanej marki, recenzje napisane w krótkim czasie podobnym językiem, prośba o pełną frazę przy zwykłej aktualizacji, link z reklamy albo z filmu instruktażowego.

Fałszywe wsparcie techniczne. To jest kategoria, która rośnie najszybciej i ma bardzo powtarzalny przebieg.

Piszesz pytanie na forum, w grupie albo w komentarzu. W ciągu kilku minut dostajesz prywatną wiadomość od konta z logo projektu. Konsultant tłumaczy, że trzeba zweryfikować portfel, zsynchronizować węzły, naprawić błąd transakcji albo odblokować wypłatę.

Padają zdania, które warto rozpoznać z daleka:

- „Twoje środki są bezpieczne, ale wymagają ręcznej synchronizacji”,
- „transakcja utknęła i trzeba ją ręcznie zwalidować”,
- „dział techniczny wykrył próbę włamania, musimy przenieść środki”.

Wzór jest zawsze ten sam: autorytet, presja czasu i pozorna pomoc.

Cel drugi: skłonić Cię do podpisu

To jest kategoria, której początkujący w ogóle nie widzą jako zagrożenia, bo nie wygląda na wysyłanie pieniędzy.

Złośliwe podpisy. Trafiasz na stronę rzekomego airdropu, stakingu albo weryfikacji. Łączysz portfel. Strona prosi o podpisanie wiadomości. Zakładasz, że to zwykłe logowanie.

W rzeczywistości podpis może **autoryzować zlecenie, zgodę albo przeniesienie aktywów**, teraz albo za tydzień.

I szczegół, który ratuje pieniądze: **brak opłaty sieciowej nie oznacza braku ryzyka.** Podpis poza łańcuchem bywa darmowy i **nadal ma pełną moc autoryzacyjną.**

Skala jest realna. W operacji ogłoszonej w kwietniu 2026 organy z kilku krajów zidentyfikowały **ponad 20 tysięcy potencjalnych ofiar jednej rodziny kampanii** i zamrożono ponad 12 milionów dolarów, przy schematach wartych ponad 45 milionów.

Nieograniczone zgody dla tokenów. Korzystając z aplikacji zdecentralizowanej, udzielasz kontraktowi prawa do dysponowania Twoimi tokenami. Często na kwotę praktycznie nieograniczoną i bezterminowo.

Ważne dopowiedzenie: to nie jest samo w sobie oszustwo. Wiele legalnych protokołów tak działa, żeby nie kazać Ci płacić za autoryzację przy każdej operacji.

Ryzyko polega na czym innym. Zgoda **pozostaje aktywna**, a kontrakt, któremu jej udzieliłeś, może zostać przejęty za rok. Wtedy tokeny znikają, choć Ty nic nie kliknąłeś.

Dlatego **przeglądaj aktywne zgody co kilka miesięcy i cofaj te, których nie rozpoznajesz.** Pamiętaj tylko, że **cofnięcie zgody nie odzyskuje przeniesionych tokenów, nie pomaga, jeśli sprawca zna Twoją frazę, i musi być wykonane osobno w każdej sieci.**

Fałszywe airdropy. W portfelu pojawia się token, którego nigdy nie kupowałeś, albo dostajesz informację o nagrodzie. Żeby ją odebrać, masz połączyć portfel, podpisać zgodę albo wpłacić „opłatę aktywacyjną”.

Tokeny-pułapki. Kupujesz token, wykres wygląda dobrze, wartość rośnie. Kiedy próbujesz sprzedać, okazuje się, że sprzedaż jest zablokowana albo obłożona absurdalną opłatą. Kontrakt był tak napisany od początku.

Cel trzeci: podmienić adres

Ta grupa jest podstępna, bo Ty robisz wszystko poprawnie, po prostu wysyłasz do niewłaściwej osoby.

Podmiana schowka. Złośliwe oprogramowanie obserwuje, co kopiujesz. Gdy rozpozna ciąg wyglądający na adres kryptowalutowy, zastępuje go adresem sprawcy. Kopiujesz swój adres, wklejasz, widzisz podobny ciąg znaków, zatwierdzasz.

Nie potrzeba tu przejmowania Twojego klucza. **To Ty podpisujesz technicznie prawidłową transakcję na zły adres.**

I rada ważniejsza, niż się wydaje: **sprawdzenie pierwszych czterech znaków nie wystarcza.** Napastnicy potrafią wygenerować adres zgadzający się i na początku, i na końcu. Porównuj cały ciąg, najprościej zeskanuj kod QR albo potwierdź adres na ekranie portfela sprzętowego.

Zatruwanie historii transakcji. Ten atak nie rusza schowka. Manipuluje historią widoczną w Twoim portfelu.

Sprawca obserwuje adresy wykonujące duże albo regularne transfery. Tworzy adres podobny do tego, którego często używasz. Wysyła Ci mikroskopijną kwotę albo bezwartościowy token, dzięki temu jego adres pojawia się w Twojej historii.

Przy kolejnym przelewie kopiujesz adres z ostatniej transakcji. I trafia on nie tam, gdzie myślisz.

Działa to, bo wiele interfejsów **skraca adresy**, pokazując tylko początek i końcówkę. Dwa różne adresy wyglądają wtedy identycznie.

Skala jest udokumentowana. Analiza z 2024 opisała sieć ponad 82 tysięcy adresów-pułapek, do których 2774 adresy ofiar wysłały łącznie **69,7 miliona dolarów.** W jednym przypadku użytkownik wysłał równowartość 68 milionów, **sprawca zwrócił większość po tygodniu, ale nie było to regułą.**

Stąd zasada, którą warto sobie wbić:

Nigdy nie kopiuj adresu odbiorcy z historii transakcji.

Używaj zapisanego, zweryfikowanego adresu albo książki adresowej. Przy nowym odbiorcy potwierdź adres innym kanałem.

Sygnały ostrzegawcze: nieoczekiwany transfer o zerowej lub minimalnej wartości, token, którego nigdy nie kupowałeś, adres podobny do znanego kontrahenta, wiele mikropłatności wokół Twojego dużego przelewu.

Cel czwarty: ominąć Twoje zabezpieczenia

Przejęcie numeru telefonu. Sprawca przekonuje operatora, danymi, dokumentem albo socjotechniką wobec konsultanta, żeby przeniósł Twój numer na kartę SIM sprawcy. Od tego momentu dostaje Twoje SMS-y, w tym kody logowania i resetowania haseł. To dlatego w rozdziale o pierwszym zakupie kazałem Ci wybrać aplikację generującą kody zamiast potwierdzeń SMS-em.

Sygnał jest bardzo charakterystyczny: telefon nagle traci zasięg, choć działa, rachunki są opłacone, karty nie zmieniałeś, a inni w tym samym miejscu mają sieć. Mogą też przyjść wiadomości o wymianie karty albo o zmianie hasła, może też nastąpić nagłe wylogowanie z kont.

Czy zdarza się w Polsce? Tak. W czerwcu 2026 roku Centralne Biuro Zwalczania Cyberprzestępczości poinformowało o rozbiciu grupy, która pozyskiwała dane do takich ataków, przejmowała konta na giełdach i kradła aktywa cyfrowe. Wartość środków wprowadzonych do obrotu przekraczała kilkadziesiąt milionów złotych.

Jeśli zauważysz ten objaw, **zadzwoń do operatora z innego telefonu, zablokuj wszystkie aktywne karty, zabezpiecz pocztę i skontaktuj się z giełdami.** Nie czekaj do rana.

Ryzyko, o którym mówi się najmniej

Krótko, ale musi paść.

W 2025 roku opisano publicznie około **70 ataków fizycznych** wymierzonych w osoby posiadające kryptowaluty, od gróźb i wymuszeń po porwania. Liczba jest prawdopodobnie mocno zaniżona, bo część takich spraw rejestruje się jako rozbój albo wymuszenie, bez osobnej kategorii.

Mechanizm jest prosty i dlatego skuteczny. **Kryptowaluty łączą trzy rzeczy naraz: dużą wartość, przelew, którego nikt nie cofnie, i brak instytucji, która mogłaby cokolwiek zablokować.** Napastnik nie musi niczego wynosić, wystarczy, że zmusi Cię do jednej operacji.

Stąd zasada, którą powtarzam świadomie: **nie mów publicznie, że masz kryptowaluty, i nie podawaj kwot.** Ani w mediach społecznościowych, ani na spotkaniu towarzyskim. **To nie paranoja, tylko jedyne zabezpieczenie przed atakiem, przed którym kryptografia nie chroni.**

Dlaczego jestem tak nieufny

Powiem, skąd u mnie ta ostrożność, bo wynika z czegoś, co z pozoru jest wadą.

Prowadzę kanał na YouTube, więc mój adres e-mail jest publiczny. Efekt jest taki, że codziennie dostaję kilkanaście wiadomości od oszustów: fałszywe propozycje współpracy, linki do „odebrania" tokenów, zaproszenia do projektów, których nie ma.

Przez lata przerobiłem prawdopodobnie każdy istniejący scenariusz.

I paradoksalnie **uważam to za korzyść.** Ktoś, kto dostaje taką wiadomość raz na rok, może potraktować ją poważnie. **Ktoś, kto dostaje piętnaście dziennie, rozpoznaje wzór w trzy sekundy.**

Ale nawet mnie prawie się to przytrafiło.

Raz otworzyłem zainfekowany plik przysłany przez kogoś, kto podszywał się pod współpracę. Kliknąłem, zanim pomyślałem. Uratowało mnie wyłącznie to, że plik nie uruchomił się poprawnie w moim systemie, czyli czysty przypadek, nie moja czujność.

Opowiadam o tym, bo widziałem, jak działa dobra socjotechnika, i wiem, że nie chroni przed nią wiedza, tylko nawyk. Ja mam ten nawyk wyłącznie dlatego, że jestem ostrzeliwany codziennie.

Ty prawdopodobnie nie jesteś. Dlatego zasady z tego rozdziału muszą u Ciebie zastąpić doświadczenie, którego nie masz, i lepiej, żebyś go nie zdobywał w naturalny sposób.

Największa kradzież w historii tego rynku

Pozostaje trzeci mechanizm z listy: **wykorzystanie błędu w oprogramowaniu.** Ciebie dotyczy pośrednio, bo dzieje się po stronie giełd i protokołów. **Ale warto go zobaczyć, bo pokazuje coś, co dotyczy Cię bezpośrednio.**

21 lutego 2025 roku z jednej z największych giełd świata wyprowadzono aktywa warte około półtora miliarda dolarów. To jest największa znana kradzież w historii kryptowalut, a amerykańskie służby przypisały ją grupom powiązanym z Koreą Północną.

Najciekawszy jest jednak sposób.

Nie złamano kryptografii Ethereum. Środki leżały w portfelu wymagającym wielu podpisów, czyli w konstrukcji uznawanej za najbezpieczniejszą z możliwych. Napastnicy zaatakowali **oprogramowanie używane w momencie podpisywania**, tak żeby osoby zatwierdzające widziały na ekranie co innego, niż faktycznie podpisywały.

Zestaw to z dwoma innymi przypadkami, bo układają się w jeden wzór.

W marcu 2022 z sieci powiązanej z popularną grą wyprowadzono 173 600 etherów i 25,5 miliona dolarów w stablecoinach, przejmując kontrolę nad kluczami walidatorów. Miesiąc wcześniej z jednego z mostów zniknęło **około 120 tysięcy etherów** przez błąd w weryfikacji podpisów.

Dostrzegasz, czego w tych opisach nie ma?

W żadnym z nich nie złamano kryptografii. Za każdym razem zawiodło coś obok: oprogramowanie do podpisywania, klucze walidatorów, kod weryfikujący.

To jest dokładnie ten sam wzór, który dotyczy Ciebie, tylko w innej skali. **Nikt nie będzie łamał Twojego klucza. Ktoś spróbuje sprawić, żebyś sam podpisał coś innego, niż myślisz.**

Higiena, która eliminuje większość ryzyka

Zbierzmy to w rutynę, którą da się utrzymać.

- **Adresy stron wpisuj z zakładek.** Nigdy z reklamy, wiadomości ani wyniku wyszukiwania. Dodaj do zakładek raz, przy pierwszej wizycie, i używaj tylko ich.
- **Używaj menedżera haseł.** Nie tylko dla wygody, on nie podpowie danych na fałszywej domenie, więc wykrywa phishing lepiej niż Ty.
- **Uwierzytelnianie aplikacją, nie SMS-em.** Kody zapasowe przechowuj poza telefonem.
- **Osobne hasło do poczty i osobne zabezpieczenie.** Poczta jest kluczem do wszystkiego innego.
- **Osobne urządzenie albo osobna przeglądarka do operacji finansowych.** Nie ta sama, w której otwierasz losowe linki.
- **Przy każdym podpisie przeczytaj, co podpisujesz.** Jeśli nie rozumiesz, nie podpisuj. Brak zrozumienia jest wystarczającym powodem odmowy.
- **Przy portfelu sprzętowym wierz ekranowi urządzenia**, nie ekranowi komputera.
- **Przelew testowy przy każdym nowym adresie.** Powtarzam z rozdziału o pierwszym zakupie, bo to najtańsze ubezpieczenie, jakie istnieje.
- **Przeglądaj zgody dla tokenów co kilka miesięcy.**
- **Rozdziel środki.** Portfel na operacje bieżące i portfel na oszczędności, do którego nie łączysz się z żadnymi aplikacjami.

Zasada, która obowiązuje zawsze

Na koniec jedno zdanie, które streszcza cały ten rozdział.

Pośpiech jest narzędziem napastnika.

Każde „zostało dziesięć minut", każde „konto zostanie zablokowane", każde „musimy natychmiast przenieść Twoje środki" istnieje po to, żebyś nie zdążył pomyśleć.

Prawdziwe instytucje nie działają w ten sposób. Giełda nie zamknie Ci konta, bo nie odpowiedziałeś w kwadrans. Portfel nie wymaga natychmiastowej synchronizacji. Nagroda, która przepada za dwanaście godzin, nigdy nie istniała.

Zawsze możesz się rozłączyć, zamknąć okno i sprawdzić na spokojnie. Jeśli sprawa jest prawdziwa, przetrwa dziesięć minut. Jeśli nie przetrwa, właśnie dostałeś odpowiedź.

Najważniejsze z tego rozdziału

- **„Blockchain został zhakowany" jest prawie zawsze błędnym opisem.** Sprawca przejmuje klucz, oszukuje człowieka albo nakłania go do wykonania prawidłowej technicznie, ale szkodliwej transakcji.
- **Oszustwa są czterokrotnie większym problemem niż włamania techniczne**, co najmniej 14 miliardów dolarów wobec 3,4 miliarda w 2025 roku. Ludzie sami wysyłają środki.
- **W pierwszej połowie 2026 roku padł rekord liczby włamań, 207, przy spadku wartości strat o 57 procent.** Ataków przybywa, kwoty maleją, bo celem jest coraz częściej zwykły użytkownik.
- **Trzy zdania, które chronią przed większością ataków:** nikt nigdy nie prosi o frazę odzyskiwania, nikt nigdy nie każe przenosić środków na „bezpieczny adres", nikt nigdy nie kontaktuje się pierwszy w sprawie Twoich pieniędzy.
- **Brak opłaty sieciowej nie oznacza braku ryzyka.** Darmowy podpis poza łańcuchem może autoryzować przeniesienie aktywów, teraz albo za tydzień.
- **Nigdy nie kopiuj adresu odbiorcy z historii transakcji.** W jednej udokumentowanej kampanii ponad 82 tysiące adresów-pułapek zebrało blisko 70 milionów dolarów.
- **Nie mów publicznie, że masz kryptowaluty.** W 2025 roku opisano około 70 ataków fizycznych, a liczba jest zaniżona.
- **Pośpiech jest narzędziem napastnika.** Jeśli sprawa jest prawdziwa, przetrwa dziesięć minut.