

TOMASZ ŚLUSARCZYK

Portfel, którego złodziej nie znajdzie

Ukryty portfel na Trezorze — poradnik krok po kroku dla osoby, która nie jest specjalistą od kryptowalut

Spis treści

CZĘŚĆ 0 — ZANIM DOTKNIESZ URZĄDZENIA	3
1. Czego ten poradnik nie robi	4
Trzy rzeczy, których ten poradnik nie robi	4
Czego wymaga od Ciebie	4
Dla kogo to jest	5
Jak czytać	5
2. Przed czym to chroni	6
Ktoś zdobył Twoje urządzenie	6
Ktoś zdobył Twoją kopię zapasową	6
Ktoś stoi obok i patrzy	7
Przed czym to nie chroni	7
Co z tego wynika dla dalszej lektury	7
Koniec fragmentu	10

CZĘŚĆ 0 — ZANIM DOTKNIESZ URZĄDZENIA

1. Czego ten poradnik nie robi

Zacznijmy od zdania, które w większości poradników ląduje na końcu, drobnym drukiem, gdzie nikt go nie czyta.

WAŻNE

Hasła do ukrytego portfela nie da się odzyskać. Nie ma procedury odzyskiwania, nie ma pytania pomocniczego, nie ma wsparcia technicznego, które by pomogło. Producent formułuje to bez owijania: hasła nie można zmienić, usunąć ani odzyskać, a jeśli je stracisz, tracisz dostęp do portfela i do środków, które w nim leżą. To dotyczy również sytuacji, w której **zapisaleś hasło błędnie** — pomyliłeś jedną literę przy przepisywaniu na kartkę i odkryjesz to dopiero za rok.

Przeczytaj to jeszcze raz, bo od tego zależy, czy ten poradnik Ci pomoże, czy zaszkodzi.

Mechanizm, który za chwilę opiszę, jest prosty w wykonaniu — całą procedurę przechodzi się w kilkanaście minut. Jest przy tym skuteczny w sposób, jakiego nie da żadne inne zabezpieczenie dostępne zwykłemu użytkownikowi. Ale jest też **całkowicie bezlitosny**. Nie ma w nim miejsca na „prawie dobrze”. Nie ma trybu awaryjnego. Nie ma nikogo, do kogo można zadzwonić.

Trzy rzeczy, których ten poradnik nie robi

Nie odzyska Twoich środków, jeśli zapomnisz hasła. Nikt tego nie robi. Ani autor, ani producent urządzenia, ani żadna firma oferująca „odzyskiwanie portfeli”. Jeśli ktoś twierdzi inaczej, próbuje Cię okraść.

Nie zamieni słabego hasła w dobre. Rozdział siódmy tłumaczy, jak dobrać hasło i dlaczego akurat tak. Jeśli go pominiesz i wpiszesz imię psa, zbudujesz sobie poczucie bezpieczeństwa, które nie ma pokrycia. To gorsze niż brak zabezpieczenia, bo pod jego wpływem podejmiesz decyzje, których byś inaczej nie podjął — na przykład przeniesiesz do ukrytego portfela wszystko, co masz.

Nie zastąpi ostrożności przy samym urządzeniu i komputerze. Ukryty portfel chroni przed kimś, kto zdobył Twoje urządzenie albo Twoją kopię zapasową. Nie chroni przed sytuacją, w której sam wpiszesz hasło na komputerze przejętym przez złośliwe oprogramowanie. Wrócimy do tego w rozdziale drugim, bo w przypadku Modelu One to ma szczególne znaczenie.

Czego wymaga od Ciebie

Trzech rzeczy, wszystkich wykonalnych w jedno popołudnie.

Kartki i długopisu. Nie notatki w telefonie, nie pliku na komputerze, nie menedżera haseł w chmurze. Powód wyjaśnia rozdział trzynasty i jest to powód techniczny, nie przesąd.

Kilkunastu minut spokoju. Bez pośpiechu, bez dziecka na kolanach, bez rozmowy w tle. Jedna literówka w haśle to inny portfel — a urządzenie Cię o niej nie uprzedzi, bo nie ma jak.

Zgody na to, że przez pierwsze dni będziesz to sprawdzał. Rozdział dziesiąty opisuje test, który wykonuje się przed przeniesieniem oszczędności: wysyłasz najmniejszą kwotę, jaka ma sens, odłączasz urządzenie, wracasz po dwóch dniach i sprawdzasz, czy potrafisz wejść z powrotem. To nie jest przesada. To jedyny moment, w którym pomyłka jest jeszcze odwracalna.

Dla kogo to jest

Dla osoby, która ma kryptowaluty na portfelu sprzętowym i chce, żeby ich zdobycie wymagało czegoś więcej niż zdobycia samego urządzenia albo kartki ze słowami. Nie musisz być specjalistą. Nie musisz rozumieć kryptografii — wystarczy, że przeczytasz rozdziały trzeci i czwarty, które tłumaczą mechanizm w kilkanaście minut.

Nie jest dla osoby, która dopiero zaczyna. Jeśli nie masz jeszcze portfela sprzętowego i nie przeszedłeś nigdy przez zapisywanie frazy odzyskiwania, zacznij od podstaw i wróć tu za kilka tygodni, gdy obsługa urządzenia przestanie być nowością. Ten poradnik zakłada, że wiesz, co to jest fraza odzyskiwania i że masz ją bezpiecznie zapisaną.

Jak czytać

Rozdziały od trzeciego do piątego wyjaśniają, **jak to działa**. Można je przeczytać raz i już do nich nie wracać — ale przeczytać trzeba, bo bez nich procedura z części drugiej będzie ciągiem niezrozumiałych kliknięć, a niezrozumiały ciąg kliknięć łatwo wykonać w złej kolejności.

Rozdziały od szóstego do dwunastego to **procedura**. Do nich wraca się z urządzeniem w rękę. Każdy kończy się listą kontrolną i warunkiem przejścia dalej.

Rozdziały od trzynastego do szesnastego to **utrzymanie i awarie** — co robić za rok, co robić, gdy coś pójdzie nie tak, i co się stanie z Twoimi środkami, gdy Ciebie zabraknie. Ten ostatni temat bywa pomijany. Nie powinien.

Na końcu są załączniki do wydruku: karta procedury na jedną stronę, wzór karty zapisu i lista kontrolna przed przeniesieniem środków.

2. Przed czym to chroni

Zabezpieczenie ma sens tylko wtedy, gdy wiadomo, przeciw czemu jest wymierzone. Inaczej łatwo o dwa błędy naraz: chronić się przed czymś, co nam nie grozi, i zostawić otwarte drzwi tam, gdzie zagrożenie jest realne.

Ukryty portfel odpowiada na trzy konkretne sytuacje.

Ktoś zdobył Twoje urządzenie

Włamanie do mieszkania, kradzież torby, zgubiony bagaż. Złodziej ma Twojego Trezora w ręku.

Bez hasła sytuacja wygląda tak: urządzenie chroni PIN, a po **szesnastu błędnych próbach Model One kasuje się automatycznie**. To realna ochrona i dla większości scenariuszy wystarczająca. Ale opiera się na jednym założeniu — że złodziej ma tylko urządzenie i musi zgadywać PIN.

Z hasłem sytuacja zmienia się jakościowo. Nawet ktoś, kto przejdzie przez PIN, zobaczy portfel podstawowy. Nie zobaczy żadnego śladu, że istnieje drugi. Nie ma listy portfeli, nie ma licznika, nie ma ikonki sugerującej „tu jest coś jeszcze”. Rozdział czwarty tłumaczy, dlaczego tak jest — i dlaczego to nie jest kwestia ukrywania czegoś w pamięci urządzenia, tylko konsekwencja sposobu, w jaki portfele w ogóle powstają.

Ktoś zdobył Twoją kopię zapasową

To scenariusz, o którym myśli się rzadziej, a jest groźniejszy. Kartka ze słowami leży w szufladzie, w sejfie u rodziców, w kopercie w piwnicy. Ktoś ją znalazł — remont, przeprowadzka, ciekawski gość, włamanie do miejsca, o którym byłeś przekonany, że jest bezpieczne.

Bez hasła to koniec. Kto ma słowa, ma środki — urządzenie nie jest do niczego potrzebne.

Z hasłem sama kartka nie wystarcza. Producent stawia to jednoznacznie: dostęp do portfela chronionego hasłem wymaga **obu** rzeczy naraz — poprawnej kopii zapasowej i dokładnie tego samego hasła, którego użyto przy tworzeniu.

UWAGA

To jest ten moment, w którym zabezpieczenie zmienia charakter Twojej kopii zapasowej. Kartka ze słowami przestaje być rzeczą, której ujawnienie kosztuje wszystko. Nadal trzeba jej pilnować — ale jej znalezienie przez obcą osobę przestaje być katastrofą. **Pod jednym warunkiem, który omawia rozdział siódmy:** że hasło jest naprawdę mocne. Słabe hasło ten warunek unieważnia, a poradnik, który by o tym nie powiedział, wyrządziłby Ci krzywdę.

Ktoś stoi obok i patrzy

Najbardziej nieprzyjemny scenariusz i jedyny, w którym technika ustępuje miejsca psychologii. Ktoś zmusza Cię do odblokowania urządzenia.

Producent mówi o tym wprost — mechanizm haseł jest pomyślany między innymi na sytuację napaści. Odblokowujesz urządzenie, pokazujesz portfel podstawowy, oddajesz to, co w nim jest. Napastnik widzi środki, widzi historię transakcji, widzi działający portfel. Nie widzi powodu, by sądzić, że istnieje coś jeszcze.

Warunkiem, żeby to zadziałało, jest **wiarygodność portfela podstawowego**. Pusty portfel z zerowym saldem i bez jednej transakcji nie uspokoi nikogo — przeciwnie, powie wprost, że prawdziwe środki są gdzie indziej. Rozdział jedenasty zajmuje się właśnie tym i opiera się na zaleceniu samego producenta, który podaje gotowy podział: drobne na portfelu bez hasła, część oszczędności pod jednym hasłem, większość pod zupełnie innym.

Przed czym to nie chroni

Trzy sytuacje, w których hasło nie pomoże. Warto je znać, żeby nie budować fałszywego poczucia bezpieczeństwa.

Przed zainfekowanym komputerem w chwili wpisywania hasła. To ograniczenie dotyczy Modelu One szczególnie mocno, bo — inaczej niż w modelach z większym ekranem — **hasła nie da się wpisać na samym urządzeniu**. Wpisujesz je na klawiaturze komputera albo telefonu. Producent mówi wprost: wpisanie hasła na klawiaturze komputera nie ujawnia Twojej frazy odzyskiwania ani kluczy prywatnych, które zostają w urządzeniu — **ale jeśli na komputerze siedzi keylogger, samo hasło może zostać przechwycone**.

Praktyczny wniosek jest prosty i wraca w rozdziale ósmym: hasło wpisujesz na komputerze, któremu ufasz. Nie w kawiarence, nie na cudzym laptopie, nie na maszynie, na której ktoś instaluje losowe programy. Jeśli masz w domu jeden komputer używany do wszystkiego, warto rozważyć, czy do tej jednej operacji nie użyć czegoś czystsze.

Przed Tobą samym. Zapomniane hasło działa dokładnie tak samo jak hasło, którego nigdy nie było. Urządzenie nie odróżnia właściciela od złodzieja — sprawdza tylko, czy wpisano właściwe znaki.

Przed utratą kopii zapasowej. Hasło jest dodatkiem do frazy odzyskiwania, nie jej zastępstwem. Jeśli zgubisz słowa, hasło samo w sobie Ci nie da.

Co z tego wynika dla dalszej lektury

Jeśli Twoim głównym zmartwieniem jest kradzież urządzenia, a kopię zapasową trzymasz w miejscu, do którego naprawdę nikt nie ma dostępu — PIN plus ostrożność mogą Ci wystarczyć i nie musisz nic zmieniać.

Jeśli natomiast któreś z tych zdań brzmi znajomo: „kartka ze słowami leży u rodziców”, „mam kopię w dwóch miejscach i o jednym z nich wie mój brat”, „boję się nie tyle kradzieży, ile tego, że ktoś znajdzie zapisane słowa” — to ukryty portfel jest odpowiedzią na Twój problem. I to odpowiedzią, którą wdrożysz w kilkanaście minut.

PORTFEL, KTÓREGO ZŁODZIEJ NIE ZNAJDZIE

Koniec fragmentu

To była część zerowa poradnika — ta, która mówi, **czego nie robić i przed czym to chroni**. Reszta jest procedurą.

Pełny poradnik to 17 rozdziałów w czterech częściach:

- **Jak to działa** — czym różni się fraza odzyskiwania, PIN i hasło; skąd biorą się portfele i dlaczego ukryty nie zostawia po sobie żadnego śladu; dlaczego urządzenie nigdy nie powie „złe hasło” i dlaczego to jest zaleta, a nie usterka.
- **Procedura** — siedem rozdziałów z listami kontrolnymi i warunkami przejścia dalej: dobór hasła, włączenie funkcji, pierwsze wejście, **test na małej kwocie przed przeniesieniem oszczędności** oraz portfel podstawowy w roli przynęty.
- **Utrzymanie i awarie** — gdzie trzymać hasło, co zrobić, żeby środki nie przepadły, gdy Ciebie zabraknie, jak reagować na pusty portfel i zgubione urządzenie, oraz dziesięć błędów, które kosztują najwięcej.
- **Sześć załączników do wydrukowania** — karta procedury na jedną stronę, wzór karty zapisu hasła, list dla osoby zaufanej, listy kontrolne, słowniczek i wykaz źródeł.

Najważniejszy rozdział poradnika dotyczy **doboru hasła** — bo producent nie podaje w tej sprawie żadnych wytycznych, a od tej jednej decyzji zależy, czy ukryty portfel rzeczywiście chroni. Znajdziesz tam także pułapkę, która dotyczy wyłącznie polskiego czytelnika: **hasło nie może zawierać liter z ogonkami**.

Cały poradnik jest bezpłatny. Nie ma wersji płatnej, nie ma dopłat, nie ma zapisów na listę.

Pobierz komplet — poradnik w PDF i EPUB wraz z załącznikami: <https://sklep.monaltro.pl/>