БАЗА DEFI · УРОК 6

Безопасность: как не потерять свои деньги

В вводном уроке были пять правил. Здесь разберём, как именно у людей крадут крипту, как устроить хранение так, чтобы одна ошибка не стоила всего, и что делать, если что-то уже случилось.

ЧТО ВЫ ПОЙМЁТЕ

1. Какими кошельками пользоваться и как не поставить подделку
2. Как разложить деньги по трём кошелькам
3. Шесть схем, на которых теряют деньги чаще всего
4. Какие риски остаются, даже если вы всё делаете правильно
5. Что делать в первые 15 минут, если кошелёк взломали

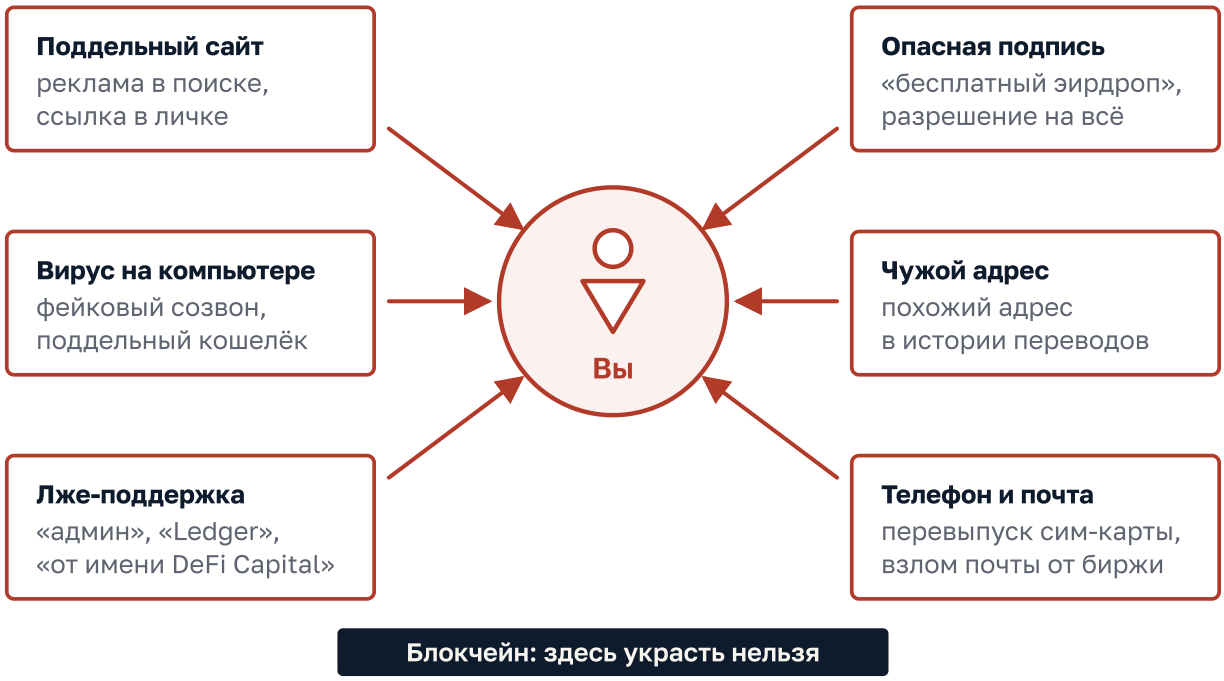
ВЕСЬ КУРС

ВВОДНЫЙ — С чего начать
УРОК 1 — Откуда берётся доход
УРОК 2 — DeFi. Депозиты и займы
УРОК 3 — Пулы ликвидности
УРОК 4 — Пулы с диапазоном
УРОК 5 — Сборка стратегии
УРОК 6 — Безопасность

ГДЕ НА САМОМ ДЕЛЕ ТЕРЯЮТ

01 Взламывают не блокчейн, а человека

Блокчейн Ethereum за всю историю не взломали ни разу. Деньги уходят в тех местах, где участвует человек: его устройство, его подпись, его доверие к сообщению.



ХОРОШАЯ НОВОСТЬ

Почти все эти схемы ломаются об одну и ту же привычку: остановиться и проверить, прежде чем нажать.

КАК УСТРОЕН УРОК

Сначала хранение (разделы 02-07), потом шесть схем кражи (08-13), остальные риски (14-15) и план, если что-то случилось (16).

КОРОТКО

Ваш главный риск не взлом протокола, а момент, когда вы сами нажимаете «Подписать» или «Установить».

ХРАНЕНИЕ · ВЫБОР

02 Какими кошельками пользуемся мы

Кошельков сотни, но для вашей работы хватит двух-трёх. Список короткий нарочно: чем меньше программ, тем меньше мест, где можно ошибиться.

В БРАУЗЕРЕ

Rabby
основной: показывает, что спишется до подписи

MetaMask
запасной, самый известный

rabby.io
metamask.com

только с этих сайтов

АППАРАТНЫЙ КЛЮЧ

Ledger
самый распространённый

Trezor, Keystone
тоже подходят, все три работают в паре с Rabby

ledger.com
trezor.io · keyst.one

покупать только там

НЕ СТАВИМ

- кошелёк «с бонусом» или «с доходом 2% в день»
- кошелёк, который посоветовали в чате
- всё, что прислали ссылкой или файлом
- «обновлённую версию» из письма

Телефон: для мелочи можно мобильный Rabby или MetaMask. Крупные суммы на телефоне не держим.

ПОЧЕМУ RABBY

Перед каждой подписью он показывает, сколько и каких монет спишется, и предупреждает о подозрительных сайтах и адресах. Это главная защита от схем из разделов 08-10.

ОДИН КОШЕЛЁК В БРАУЗЕРЕ

Не ставьте несколько кошельков-расширений сразу: они перехватывают друг у друга запросы, и легко подписать не в том окне.

КОРОТКО

Rabby для работы, аппаратный ключ для основных денег. Всё остальное не нужно, а значит, не нужно и рисковать.

ХРАНЕНИЕ · УСТАНОВКА

03 Как не поставить поддельный кошелёк

Самый быстрый способ потерять всё: поставить копию кошелька и ввести в неё сид-фразу. Копии выглядят один в один и иногда лежат даже в официальных магазинах приложений.

Правильный путь

Адрес сайта из урока → или от нас, не из поиска
Официальный сайт → rabby.io, ledger.com
Кнопка «Скачать» → ведёт в магазин сама

Опасный путь

Поиск «rabby wallet» → первая строка: реклама
rabby-wallet.app → похожий адрес
«Введите сид-фразу» → деньги уйдут

Признак подделки: новый кошелёк сразу просит ввести сид-фразу. Настоящий предлагает создать кошелёк, а слова просит, только если вы выбрали «восстановить».

РЕАЛЬНЫЙ СЛУЧАЙ, АПРЕЛЬ 2026

В Mac App Store появилось поддельное приложение Ledger Live. Оно просило ввести сид-фразу «для синхронизации». Около 50 человек потеряли в сумме примерно $9,5 млн.

МАГАЗИН ПРИЛОЖЕНИЙ

Не гарантия. Смотрите имя разработчика, число скачиваний и отзывов. Надёжнее перейти в магазин по ссылке с официального сайта.

ФАЙЛЫ И ССЫЛКИ

Никаких .apk, архивов и «новых версий» из Telegram, почты и личных сообщений.

«СРОЧНО ОБНОВИТЕ»

Письмо или окно с таким текстом почти всегда фишинг. Обновления приходят через магазин или само приложение.

КОРОТКО

Кошелёк ставим только по ссылке с официального сайта. Сид-фразу вводим только при восстановлении и только в проверенное приложение.

ХРАНЕНИЕ · РАСКЛАДКА

04 Три кошелька вместо одного

Если все деньги на одном адресе, одна неудачная подпись забирает всё. Разложите их по трём кошелькам с разной ролью, как дома: сейф, кошелёк в кармане и мелочь на чай.



ПРОПОРЦИИ ПРИМЕРНЫЕ

Точную раскладку под вашу стратегию согласуем в плане. Главное правило: на рабочем лежит только то, что сейчас в работе.

ЗАЧЕМ ОДНОРАЗОВЫЙ

Если сайт окажется ловушкой, вы потеряете $50, а не капитал. Одноразовый адрес создаётся в Rabby за минуту.

КОРОТКО

Сейф, карман и мелочь. Незнакомый сайт видит только мелочь, а сейф видит только проверенные протоколы.

ХРАНЕНИЕ · АППАРАТНЫЙ КЛЮЧ

05 Аппаратный ключ: купить и настроить

Аппаратный ключ защищает, только если он настоящий и вы сами создали на нём сид-фразу. Подменённое устройство хуже, чем никакого: вы спокойны, а ключ уже у мошенника.

1 **Покупать только на официальном сайте производителя**

ledger.com, trezor.io, keyst.one. Не на маркетплейсе, не «с рук», не у перекупщика со скидкой. Ссылку на сайт берите из этого урока.

2 **Сид-фразу создаёт само устройство при первом включении**

Если в коробке лежит карточка с уже вписанными словами или «пин-кодом от продавца», это подделка. Устройство не подключать, написать нам.

3 **Пин-код на устройстве, слова на бумаге или металле**

Пин защищает, если устройство украли. Сид-фраза нужна, если оно сломалось или потерялось: по ней всё восстанавливается на новом.

4 **Адрес и сумму сверяйте на экране самого устройства**

Экран компьютера может показать что угодно, если на нём вирус. Экран ключа подделать нельзя. Совпадает с тем, что вы хотели? Тогда нажимайте.

5 **Приложение к ключу тоже только с официального сайта**

Ledger Wallet (бывший Ledger Live), Trezor Suite. Поддельные версии этих приложений встречаются в поиске и даже в официальных магазинах.

6 **Письмо «ваш Ledger нужно перепроверить» от производителя**

Утечки баз покупателей были, и по этим адресам рассылают письма и даже посылки с «новым устройством». Производитель никогда не просит сид-фразу и не присылает устройства без заказа.

КОРОТКО

Ключ с официального сайта, слова создаёт он сам, подтверждаете вы, глядя на его экран, а не на экран компьютера.

ХРАНЕНИЕ · СИД-ФРАЗА

06 Где хранить сид-фразу, чтобы не потерять и не отдать

У сид-фразы два врага: огонь, вода и забывчивость с одной стороны, чужие глаза с другой. Хорошее хранение защищает от обоих сразу.

Варианты хранения

Бумага в надёжном месте	✓ годится	боится воды и огня
Металлическая пластина	✓ лучше всего	переживёт пожар и потоп
Две копии в разных местах	✓ обязательно	дом и второе надёжное место
Фото на телефоне	✗ нельзя	фото уходят в облако
Заметки, почта, облако	✗ нельзя	взлом аккаунта = потеря денег
«Избранное» в мессенджере	✗ нельзя	хранится на чужом сервере
Менеджер паролей	✗ не для крупных сумм	их тоже взламывают

КОДОВОЕ СЛОВО (PASSPHRASE)

Аппаратный ключ умеет добавить к сид-фразе ещё одно ваше слово. Тогда найденных 24 слов мало. Но забудете слово, и доступ потерян навсегда. Включаем только вместе с нами.

ЕСЛИ С ВАМИ ЧТО-ТО СЛУЧИТСЯ

Без сид-фразы родные не получат доступ, и помочь им никто не сможет. Подумайте заранее, кто и как её найдёт: например, запечатанный конверт у нотариуса или в банковской ячейке и инструкция близкому человеку.

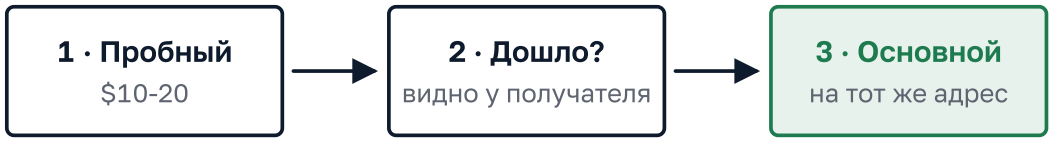
КОРОТКО

Металл или бумага, две копии в разных местах, ничего цифрового. И план, как сид-фразу найдут близкие, если вас не будет рядом.

ХРАНЕНИЕ · ПЕРЕВОДЫ

07 Сначала маленький перевод, потом основной

Перевод в блокчейне нельзя отменить. Отправили не на тот адрес или не в ту сеть, и вернуть деньги может только получатель, если захочет. Поэтому первый перевод на любой новый адрес всегда пробный.



Как сверять адрес

нужный: **0x7a3f 9c21 e4b8 … 51d0 c91e**

похожий: **0x7a3f 0b77 a2f1 … 9e43 c91e**

Начало и конец совпадают, середина другая. Сверяйте **середину тоже**, хотя бы 4-6 символов.

АДРЕСНАЯ КНИГА

Адреса, на которые вы переводите регулярно (биржа, свой холодный кошелёк), сохраните в Rabby один раз после пробного перевода. Дальше выбирайте из книги, а не копируйте.

СЕТЬ

При выводе с биржи сеть выбирайте ту, о которой договорились (урок 0, раздел 07). Пробный перевод проверяет и адрес, и сеть сразу.

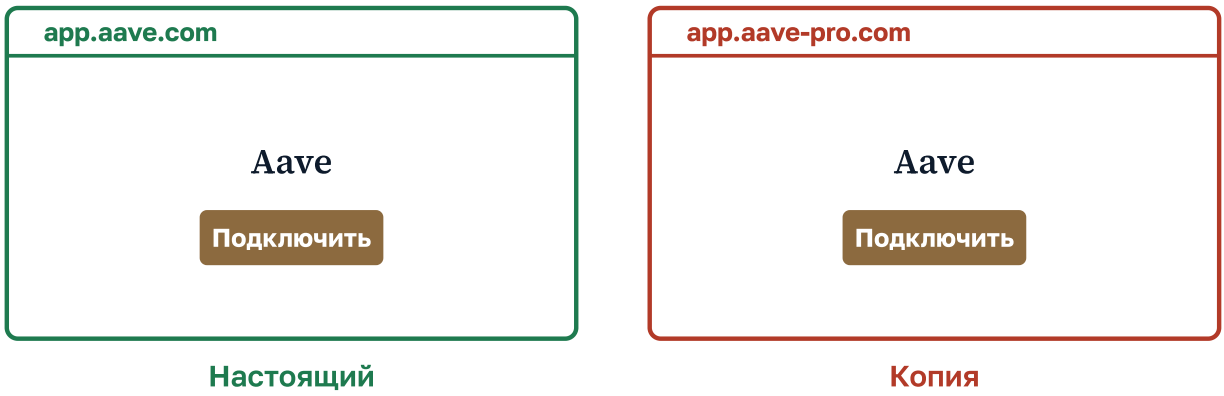
КОРОТКО

Новый адрес: пробный перевод, проверили, потом основной. Пробный стоит центы, ошибка стоит всю сумму.

СХЕМА КРАЖИ 1 ИЗ 6

08 Поддельный сайт

Мошенники копируют сайт протокола до последнего пикселя и приводят на него людей: рекламой в поиске выше настоящего сайта, ссылкой в комментарии, в личном сообщении или в поддельном аккаунте проекта.



Настоящий

Копия

Внешне не отличить. Отличается только **адрес в строке браузера**, и то на одну букву, дефис или окончание.

ЗАКЛАДКИ

Каждый протокол, с которым работаем, в закладках браузера. Заходим только оттуда, никогда через поиск.

RABBY ПРЕДУПРЕДИТ

Rabby помечает незнакомые сайты и известные фишинговые адреса. Красное окно в Rabby: закрыть вкладку, ничего не подписывать.

ССЫЛКИ В TELEGRAM И X

Даже от «официального» аккаунта. Аккаунты проектов взламывают и публикуют с них ссылки на копии.

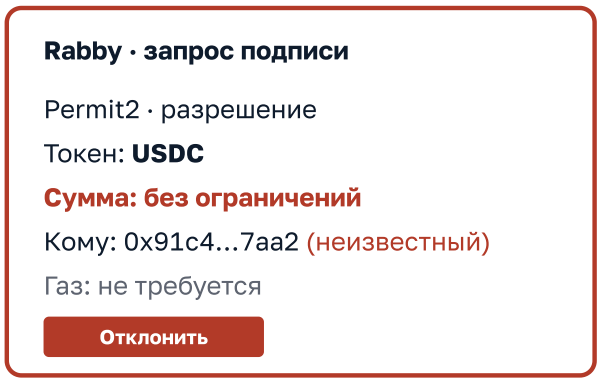
КОРОТКО

Протоколы открываем только по закладке. Ссылка из поиска, комментария или сообщения считается поддельной, пока не доказано обратное.

СХЕМА КРАЖИ 2 ИЗ 6

09 Подпись, которая забирает всё

Ворам не нужна ваша сид-фраза, если вы сами подпишете им разрешение. Такая подпись часто ничего не стоит и выглядит безобидно: «подтвердите вход», «получите эирдроп», «проверка кошелька».



Что здесь опасно

«Без ограничений»
получатель сможет забрать все ваши USDC в любой момент

«Кому» не протокол
неизвестный адрес вместо Aave, Uniswap и т. п.

«Газ не требуется»
подпись бесплатна, но это не значит, что она безопасна

Новое с 2025 года: подпись может передать управление кошельком чужому контракту. Rabby пишет «delegation» или «upgrade account». Такое подписываем только с нами.

СЛОВА-ТРЕВОГА

Permit, Permit2, Approve, SetApprovalForAll, «unlimited», «без ограничений», delegation. Увидели и не ждали: отклонить и спросить нас.

УБОРКА РАЗ В МЕСЯЦ

Старые разрешения отзывайте в Rabby, раздел Approvals (или revoke.cash). Отзыв стоит газ, зато вчерашний протокол завтра не станет дверью к вашим деньгам.

КОРОТКО

Бесплатная подпись не значит безопасная. Читайте, кому и сколько вы разрешаете. Непонятно, значит «Отклонить».

СХЕМА КРАЖИ 3 ИЗ 6

10 Подмена адреса

Вы перевели деньги на биржу. Через минуту в истории кошелька появляется перевод на $0 с адреса, который начинается и заканчивается так же, как адрес биржи. Расчёт на то, что в следующий раз вы скопируете адрес из истории.

История кошелька

Отправлено	`0x3b8e…a41f`	**−5 000 USDC**	ваш перевод
Получено	**`0x3b8e…a41f`**	0 USDC	**ловушка**

Адреса совпадают по первым и последним символам. Целиком они разные.

Родственник схемы: вирус в буфере обмена

Вы скопировали адрес, а вирус подменил его при вставке на свой. Защита та же: сверить вставленный адрес целиком, включая середину, и смотреть на экран ключа.

ПРАВИЛО

Никогда не копируйте адрес из истории переводов. Только из адресной книги Rabby или из самой биржи, раздел «Пополнить».

СТРАННЫЕ МЕЛКИЕ ПОСТУПЛЕНИЯ

Переводы на $0, монеты, которых вы не покупали, «подарочные» токены: не трогать, не продавать, не переходить по ссылкам в их названиях.

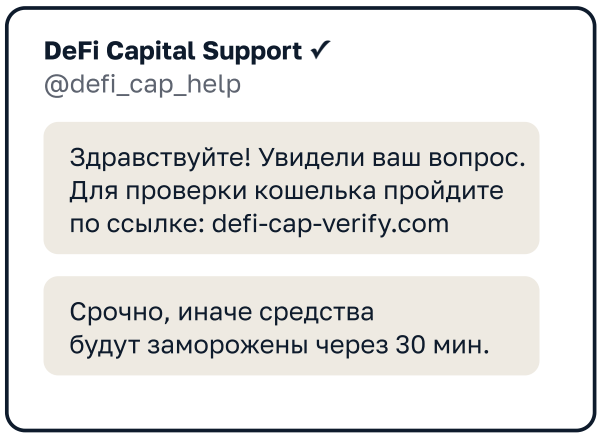
КОРОТКО

История кошелька не адресная книга. Адрес берём только из сохранённого контакта или из источника, и сверяем середину.

СХЕМА КРАЖИ 4 ИЗ 6

11 Лже-поддержка и «мы от DeFi Capital»

Вы задали вопрос в чате, и через минуту вам в личку пишет «администратор». Или звонит «служба безопасности биржи», или приходит письмо от «Ledger». Цель всегда одна: чтобы вы открыли ссылку, поставили программу или назвали слова.



Признаки обмана

- пишут первыми
- галочка и логотип в аватарке
- ссылка или файл
- срочность и угроза
- просьба подписать, «проверить», назвать слова или показать экран

одного признака достаточно

КАК РАБОТАЕМ МЫ

Мы **никогда не пишем первыми со ссылкой**, не просим сид-фразу, не просим подписать что-то «для проверки» и не просим показать экран. Сомневаетесь, что пишем мы: напишите сами в известный вам контакт и спросите.

ЗВОНОК «ИЗ БАНКА ИЛИ БИРЖИ»

Положите трубку и перезвоните по номеру с официального сайта. Настоящая служба этому не мешает.

УДАЛЁННЫЙ ДОСТУП

AnyDesk, TeamViewer, «демонстрация экрана для помощи» по просьбе незнакомца: нет, ни при каких условиях.

КОРОТКО

Настоящая поддержка не пишет первой и никогда не торопит. Срочность в сообщении сама по себе признак мошенника.

СХЕМА КРАЖИ 5 ИЗ 6

12 Вирус под видом созвона, работы или программы

Сейчас самые дорогие кражи начинаются не с подписи, а с установки. Человеку назначают деловой созвон, предлагают работу или интервью, и для этого нужно «поставить программу». Программа ворует ключи браузерного кошелька и пароли.

1 **«Созвон не работает, обновите Zoom по ссылке»**

Ссылка ведёт на копию сайта Zoom или Teams, а «обновление» оказывается вирусом. Другой вариант: во время созвона просят дать управление экраном. Созвоны только по ссылке из официального приложения, ничего не скачивать из чата, управление не давать.

2 **«Тестовое задание: скачайте проект и запустите»**

Работа, партнёрство или «документ по вашему портфелю» с файлом или архивом. На компьютере с кошельком такое не открываем.

3 **Взломанные программы и «бесплатные» версии платных**

Пиратские сборки, «активаторы», моды для игр: частый способ доставки вирусов, ворующих кошельки.

4 **Лишние расширения браузера**

Расширение видит всё, что происходит на странице. В профиле для крипты только кошелёк, больше ничего (урок 0, раздел 01).

ПОЧЕМУ ТУТ СПАСАЕТ АППАРАТНЫЙ КЛЮЧ

Вирус может украсть ключ браузерного кошелька, но не может вытащить ключ из аппаратного устройства и не может нажать на нём кнопку. Поэтому основная сумма живёт в «сейфе» (раздел 04).

КОРОТКО

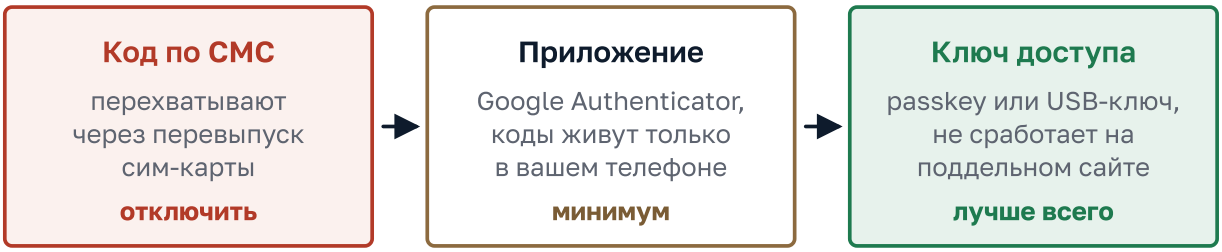
На компьютере с кошельком ничего не устанавливаем по чужой просьбе. Срочный созвон, работа или документ не причина.

СХЕМА КРАЖИ 6 ИЗ 6

13 Телефон и почта: ключ к бирже

Если на бирже вход подтверждается кодом из СМС, то ваша сим-карта и есть ключ от счёта. Мошенник по поддельной доверенности перевыпускает сим-карту на себя, получает код и выводит деньги.

Двухфакторная защита: от слабой к сильной



Плюс на бирже: **белый список адресов вывода**.
Вывод только на сохранённые адреса, а новый адрес заработает через 1-2 дня.

ОТДЕЛЬНАЯ ПОЧТА

Для бирж и кошельков отдельный адрес почты, который нигде не светится и не используется для рассылок.

ПАРОЛИ

Разные на каждой бирже, длинные, в менеджере паролей. Один пароль на всё означает, что утечка где угодно откроет биржу.

ОПЕРАТОР СВЯЗИ

Попросите у оператора запрет на перевыпуск сим-карты без вашего личного визита, если он это предлагает.

КОРОТКО

На бирже: никаких СМС-кодов, приложение или ключ доступа, отдельная почта и белый список адресов вывода.

РИСКИ БЕЗ МОШЕННИКОВ

14 Что может сломаться, даже если вы всё делаете правильно

Часть рисков от вас не зависит. Их нельзя убрать до нуля, но можно сделать так, чтобы одна поломка не задела весь капитал.

Протокол	Сайт протокола	Мост	Биржа
ошибка в коде, через которую выводят деньги	код цел, но сайт подменили, и он просит не то	переводы между сетями, исторически самое взламываемое	взлом, банкротство или заморозка счёта
Снижаем: старые протоколы с аудитами и годами работы	**Снижаем:** читаем подпись, сверяем на экране аппаратного ключа	**Снижаем:** мосты только по нашей схеме, деньги там не держим	**Снижаем:** на бирже только то, что сейчас покупаем или выводим

ПРИМЕР

В феврале 2025 года у биржи Bybit украли около $1,5 млрд в ETH. Протоколы и блокчейн были ни при чём: злоумышленники подменили интерфейс, через который сотрудники подписывали перевод, и те подписали, не видя, что именно. Это тот же риск, что на странице 09, только у профессионалов.

РАЗНЕСЕНИЕ

Поэтому капитал стоит не в одном протоколе и не в одной сети. Как именно разносим, решаем в плане стратегии (урок 5).

СТЕЙБЛКОИНЫ

Тоже риск: стейбл держится на $1, пока его эмитент или механизм работает. Мы держим только крупные стейблы.

КОРОТКО

Ноль риска не бывает. Бывает так, что одна поломка задевает небольшую часть денег, а не всё.

ТИШИНА

15 Чем меньше о вас знают, тем вы целее

Крипта требует не только цифровой, но и обычной осторожности. Нападения на держателей крипты вживую, с угрозами и похищениями, участились: по данным CertiK, в 2025 году таких случаев было 72, на 75% больше, чем годом раньше. Чаще всего страдают те, кто сам рассказывал о своих деньгах.

1 Не показывайте суммы

Скрины баланса, «сколько я заработал», рассказы в соцсетях и малознакомым людям. Адрес кошелька с крупной суммой, однажды показанный, видят все и навсегда.

2 Не связывайте адрес с собой публично

Не используйте один и тот же адрес для работы, публичных сборов и личных переводов знакомым.

3 Аккуратно с базами клиентов

Утечки клиентских баз бирж и магазинов кошельков случаются. Поэтому физическое устройство и бумага с сид-фразой не должны лежать вместе и на виду.

4 Кошелёк для показа

Отдельный кошелёк с небольшой суммой, который можно показать под давлением. Жизнь дороже денег: если вам угрожают, отдайте.

5 Близкие знают правила

Члены семьи тоже получают «звонки из банка». Расскажите им про лже-поддержку (раздел 11).

КОРОТКО

Тихий держатель крипты в безопасности. Суммы, скрины и рассказы о доходе делают из вас цель.

ЕСЛИ ЧТО-ТО СЛУЧИЛОСЬ

16 Первые 15 минут после взлома

Подписали что-то не то, ввели слова на подозрительном сайте или видите перевод, которого не делали. Счёт идёт на минуты: часто вор забирает не всё сразу, и остальное можно спасти.



Сид-фраза попала к чужим?

Тогда кошелёк потерян навсегда, даже если деньги пока на месте, и отзыв не поможет. Создайте новый кошелёк на чистом устройстве и переведите туда всё, начиная с самого дорогого.

ВТОРАЯ ВОЛНА МОШЕННИКОВ

После взлома вам обязательно напишут «специалисты по возврату средств», «блокчейн-детективы» или «юристы». Они берут предоплату и исчезают. Вернуть украденную крипту за деньги никто не может. Обращаемся только к нам и в полицию.

КОМПЬЮТЕР

Если подозреваете вирус, кошелёк с этого компьютера больше не используйте. Новый кошелёк создавайте на другом устройстве.

ЗАЯВЛЕНИЕ

Сохраните адреса, ссылки и переписку. Это нужно для заявления в полицию и для бирж, которые иногда замораживают украденное.

ИТОГ УРОКА

17 Пять вопросов перед каждой подписью

ЧЕК-ЛИСТ «ПЕРЕД ПОДПИСЬЮ»

- ☐ Я открыл этот сайт из своей закладки, а не по ссылке?
- ☐ Я сам начал это действие, меня никто не торопил?
- ☐ Я понимаю, что спишется и кому я даю разрешение?
- ☐ Сумма разрешения ограничена, а не «без ограничений»?
- ☐ Адрес и сумма на экране аппаратного ключа совпадают с задуманным?

Хотя бы одно «нет»: отклонить и спросить нас. Отмена бесплатна, ошибка нет.

ПРОВЕРЬТЕ СЕБЯ: ПОДПИСАЛИ БЫ?

1 **«Админ» в личке присылает ссылку, чтобы «верифицировать кошелёк»**

Нет. Пишут первыми со ссылкой только мошенники (раздел 11).

2 **Сайт эирдропа просит бесплатную подпись Permit на USDC без ограничений**

Нет. Бесплатная подпись может отдать все ваши USDC (раздел 09).

3 **Новый кошелёк из магазина приложений сразу просит ввести сид-фразу**

Нет. Это признак подделки (раздел 03). Удалить приложение.

4 **Вы переводите на биржу и берёте адрес из истории переводов**

Нет. Адрес только из адресной книги или из самой биржи (раздел 10).

5 **Вы открыли Aave по закладке, вносите 1 000 USDC, Rabby показывает −1 000 USDC в Aave**

Да. Сайт из закладки, вы начали сами, сумма и получатель понятны.

ЗАПОМНИТЬ ОДНОЙ ФРАЗОЙ

Деньги в крипте теряют в одну секунду спешки. Остановиться и проверить всегда дешевле, чем исправлять.