

ОСНОВА ПЕРЕД ПЕРШОЮ ДІЄЮ

Криптобезпека

Захисти доступ. Перевірй запити.
Дій без поспіху.

30-45 хвилин · 6 модулів · 10 запитань

Усі вправи виконуються на папері. Реальні кошти, встановлення гаманця, підключення та підписи не потрібні.

Маршрут навчання

- 01 Карта курсу та безпечна практика
- 02 1. Гаманець, біржа та межі доступу
- 03 2. Акаунти, фішинг і хибна терміновість
- 04 3. Мережа, актив, адреса та мето
- 05 4. Підключити, підписати й дозволити - різні дії
- 06 5. План під час інциденту та підсумкова перевірка

LOGRI CRYPTO SECURITY · 2026-10-31

01 / 06

Карта курсу та безпечна практика

Чого ти навчишся

Наприкінці курсу ти зможеш відрізнити публічну адресу від секрету, розпізнати небезпечний запит, перевірити маршрут переказу на папері та обрати перші дії під час інциденту. Це корисна база перед START, HOLD, Radar Practice і GameFi. Час із завданнями - орієнтовно 30-45 хвилин; можна проходити частинами.

Спочатку прочитай урок, потім запиши рішення завдання своїми словами й лише після цього відкрий розбір. Усі назви платформ А і В, адреси «АДРЕСА-А» та суми у вправах умовні. Вправи не потребують встановлення гаманця, реєстрації на біржі, підключення dapp, підпису повідомлення, отримання токена чи реального переказу. Жодних seed-фраз, паролів, кодів або ключів до Академії надсилати не потрібно.

Твоя навчальна нотатка

Створи п'ять рядків: що захищаю; хто контролює доступ; що перевіряю перед дією; причина зупинки; куди звернуся в разі помилки. Записуй категорії та рішення, а не реальні секрети чи адреси власних рахунків. Після кожного уроку доповнюй один рядок. Результат - особистий порядок дій, який можна повторити без підказки.

Наприкінці - 10 запитань, зокрема два обов'язкові ситуаційні завдання. Для успішного результату потрібні щонайменше 70% і обидва обов'язкові завдання без помилок. Читання та практика доступні безкоштовно. Для збереження результату й сертифіката увійди до свого підтвердженого акаунта LOGRI.

Як пов'язаний GitBook

Довідник гаманців LOGRI допомагає згодом знайти посібник для обраної мережі: <https://gamefi-40.gitbook.io/gamefi-40+-docs/wallets>. Розділ безпеки: <https://gamefi-40.gitbook.io/gamefi-40+-docs/bezopasnost-i-skam>. Цей додатковий довідник частково російськомовний; увесь обов'язковий матеріал курсу та іспит розміщені тут обраною мовою. Купувати чи встановлювати перелічені гаманці для складання іспиту не потрібно.

02 / 06

1. Гаманець, біржа та межі доступу

Спочатку визнач модель зберігання

У кастодіальному сервісі ключі зазвичай контролює оператор, а твій доступ залежить від його правил і захисту акаунта. У звичайному самостійному гаманці доступ визначається ключами та способом відновлення. Деякі застосунки пропонують вхід через Google, Apple або інші моделі резервування: спочатку прочитай офіційні правила саме свого варіанта. Не можна переносити інструкцію одного гаманця на всі інші.

Публічну адресу використовують для отримання коштів і перегляду відкритої історії. Вона не є паролем, але зв'язок адреси з людиною розкриває частину фінансової приватності. Seed-фраза та приватний ключ надають повноваження керування. Пароль застосунку може лише розблокувати локальне сховище й не завжди відновлює доступ на новому пристрої.

Секрети залишаються у власника

Не надсилай seed-фразу чи ключ адміністратору, «підтримці», боту або у форму перевірки. Не фотографуй і не зберігай власну фразу в чаті, звичайній нотатці чи незахищеній хмарі. Для моделі з власною seed-фразою продумай захищену офлайн-копію та ризик втрати, пожежі або доступу сторонніх. Перевіряти реальну резервну копію слід лише за офіційною інструкцією свого гаманця, не у вправі Академії.

Апаратний гаманець змінює спосіб зберігання й підтвердження, але не робить шкідливий підпис безпечним. Окремий гаманець для експериментів обмежує змішування завдань; він не перетворює невідомий застосунок на надійний.

Завдання та розбір

Розподіли «публічна адреса», «seed-фраза», «пароль пошти» на дві колонки: можна повідомити для отримання переказу / не можна передавати для перевірки. Відповідь: лише адресу, якщо погоджуєшся з наслідками для приватності. Решта - секрети. Потім одним реченням поясни, чому зміна пароля застосунку не знешкоджує вже розкриту seed-фразу: повноваження за старими ключами зберігаються.

03 / 06

2. Акаунти, фішинг і хибна терміновість

Захисти ланцюг доступу

Пошта часто використовується для відновлення інших акаунтів. Застосовуй різні довгі паролі, зберігай їх у надійному менеджері, вмикай доступний багатфакторний захист і перевіряй активні сеанси. Віддавай перевагу стійким до фішингу способам входу, якщо сервіс їх підтримує. Код із застосунку чи SMS також є секретом: його можуть виманити. Не підтверджуй неочікуваний запит входу лише тому, що на ньому знайомий логотип.

Оновлюй систему та гаманець із перевіреного джерела. Не встановлюй розширення з особистого повідомлення й не надавай незнайомцю віддалений доступ. Коли потрібна підтримка, відкрий офіційний сайт самостійно, знайди канал допомоги там і зістав звернення. Ім'я, аватарка, верифікація акаунта чи велика кількість підписників окремо не доводять справжність повідомлення.

Перевіряй призначення дії

Значок HTTPS означає шифрування з'єднання, а не чесність власника сайту. Перевір повний домен після переходу, а не підпис кнопки. Реклама й перші результати пошуку можуть вести не туди, куди очікуєш. Збережена закладка корисна лише тоді, коли вихідну адресу перевірили.

Ситуаційне завдання А

Тобі першим пише «адмін»: «Сертифікат готовий, за п'ять хвилин введи seed-фразу на сторінці перевірки, інакше втрапиш бонус». Обери дію та назви дві тривожні ознаки.

Розбір: зупинитися, нічого не вводити, перевірити повідомлення через самостійно знайдений офіційний канал і повідомити про підробку. Ознаки: вимога секрету, ініціатива незнайомця й тиск строком. Для сертифіката LOGRI не потрібна seed-фраза або доступ до коштів. Відмова від такої дії - правильне виконання завдання, а не втрачена можливість.

04 / 06

3. Мережа, актив, адреса та мемо

Адреса не описує весь маршрут

Перед переказом потрібно узгодити актив, мережу, адресу отримувача та, якщо цього вимагає сторона отримання, мемо або destination tag. Один тикер може існувати в кількох мережах, а схожий формат адреси не означає підтримку потрібного активу чи мережі. Умови введення, мінімуми й комісії перевіряють за поточною сторінкою сервісу отримувача. Не обирай мережу лише через меншу комісію.

Отримуй адресу з перевіреного джерела отримувача. Після вставлення порівняй повну адресу з оригіналом: перші й останні символи допомагають помітити частину помилок, але не замінюють повну перевірку. Історія переказів може містити схожі адреси, залишені сторонніми. Перед реальною дією додатково перевіряють суму, комісію, стан мережі та можливість зарахування.

Ситуаційне завдання В

Платформа А пропонує надіслати навчальний токен мережею Х або Y. На перевірній сторінці введення платформи В написано: «лише мережа Х; мемо ОБОВ'ЯЗКОВЕ». У чернетці обрана Y, мемо порожнє. Чи можна надсилати, якщо адреса виглядає однаково?

Розбір: ні. Зупинися, звір підтримувані умови В, виправ мережу на Х і додай потрібне мемо з перевіреного джерела. Якщо Х або поле мемо недоступні - переказу немає до з'ясування. Однаковий вигляд адреси не усуває невідповідність. Це завдання на перевірку умов, а не запрошення пробувати мережу Y.

Практика без переказу

Заповни картку: актив - навчальний; мережа - Х; адреса - АДРЕСА-А; мемо - НАВЧАЛЬНЕ-МЕМО; підтримка отримувачем - підтверджена умовою; дія - звірити весь маршрут. У реальній роботі невеликий пробний переказ може перевірити конкретний маршрут, але не гарантує безпеку наступного й не скасовує мінімуми або комісії. Для цього курсу навіть пробний переказ не потрібен.

05 / 06

4. Підключити, підписати й дозволити - різні дії

Читай запит гаманця

Підключення зазвичай повідомляє застосунку обрану публічну адресу та дозволяє запитувати подальші дії. Підпис, дозвіл витрачання токенів і надсилання транзакції мають інші наслідки. У різних мережах і типах акаунтів механізми відрізняються. Не вважай будь-який підпис без комісії звичайним безпечним входом: деякі підписані дозволи можуть бути використані пізніше.

До підтвердження з'ясууй, хто запитує дію, який контракт отримує повноваження, для якого токена, на яку суму та строк. Зістав запит зі своєю метою. Якщо інтерфейс не пояснює зміст даних або ти його не розумієш, відхили запит і знайди офіційний опис. Великий або необмежений ліміт збільшує можливу шкоду. Знайоме ім'я проєкту не скасовує перевірку конкретного запиту.

Відключення не дорівнює відкликанню

Закрити вкладку чи відключити dapp від гаманця - не те саме, що скасувати раніше виданий дозвіл на токени. Перевірка та відкликання дозволів виконуються окремо за офіційною інструкцією для обраної мережі. Відкликання може потребувати мережевої комісії; воно не повертає вже вкрадене та не змінює розкритий приватний ключ. Однієї дії для всіх випадків немає.

Завдання та розбір

Умовний застосунок пропонує отримати безкоштовну картинку, але просить необмежений доступ до навчального стейблкоїна. Потім заспокоює: «якщо передумаєш, просто закрій вкладку». Запиши рішення.

Відповідь: відхилити неспівмірний запит і перевірити призначення дозволу. Закриття вкладки не знімає видані повноваження. Нульова комісія за підпис і відсутність списання одразу не доводять відсутності ризику. Ми аналізуємо опис; підключати гаманець, підписувати чи відкликати щось для завдання не можна й не потрібно.

06 / 06

5. План під час інциденту та підсумкова перевірка

Визнач, що могло бути розкрито

За підозри припини дії із сумнівним сайтом і не відповідай «рятівникам» в особистих повідомленнях. В окремій нотатці зафіксуй час, домен, характер запиту й наявності публічний хеш операції. Прибери з матеріалів для звернення секрети та персональні дані. Повернення коштів не гарантоване; вимога попередньої оплати за «гарантоване повернення» - привід зупинитися.

Якщо розкрито пароль акаунта, з довіреного пристрою відкрий офіційний сервіс, зміни пароль, заверши чужі сеанси та перевір способи відновлення й MFA. Якщо зачеплено пошту, включи її до перевірки. Якщо видано підозрілий дозвіл, скористайся офіційною інструкцією мережі для його перевірки й відкликання. Ці заходи вирішують різні проблеми.

Якщо розкрита seed-фраза або приватний ключ, стару модель доступу не можна вважати безпечною після простої зміни пароля чи відкликання одного approval. План зазвичай потребує нового незалежно створеного гаманця з новими ключами й захисту решти активів. Не вводь стару фразу в «нову» форму рятівника. За ознак автоматичного виведення не поповнюй скомпрометовану адресу навання заради комісії: можуть вивести й ці кошти. Для реального інциденту потрібна перевірена допомога щодо конкретної ситуації.

Підсумкове завдання

Склади три окремі рядки: пароль витік / дозвіл підозрілий / ключ розкрито. Навпроти кожного запиши відповідну перевірку з уроку. Додай особисте правило зупинки: «Не розумію запит - не підтверджую; поспіх не скасовує перевірку». Це вправа на планування, не команда виконувати реальні операції.

Перед іспитом

Поясни відмінності адреси й секрету, пароля та відновлення, з'єднання й approval. Повтори два сценарії А та В. Іспит перевіряє рішення за описаними умовами; він не проводить аудит твоїх пристроїв і не засвідчує безпеку реального гаманця.

Джерела та межі

Оригінальний навчальний текст LOGRI; джерела перевірено 31.10.2026. Інтерфейси, способи відновлення, дозволи й умови мереж змінюються: звіряй поточні офіційні інструкції. Механіки EVM не можна автоматично переносити на Solana, TON або інші мережі. Ні гаманець, ні іспит не усувають усіх ризиків. Первинні джерела нижче переважно англомовні; їх читання не замінює та не блокує повний курс обраною мовою.

Первинні джерела

- Ethereum: безпека гаманця: <https://ethereum.org/security/>
- MetaMask: відновлення та пароль: <https://support.metamask.io/start/user-guide-secret-recovery-phrase-password-and-private-keys>
- MetaMask: дозволи токенів: <https://support.metamask.io/transactions-and-gas/transactions/what-is-a-token-approval/>
- MetaMask: відключення та відкликання дозволів: <https://support.metamask.io/more-web3/dapps/disconnect-wallet-from-a-dapp/>
- Uniswap Labs: небезпечні підписи: <https://support.uniswap.org/hc/en-us/articles/40050562560781-Crypto-Wallet-Signature-Scams>
- Solana: посібник із безпеки: <https://solana.com/learn/staying-safe-on-solana>
- Coinbase: мемо та destination tag: <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/destination-tag-memo-faq>
- CISA: базовий захист в інтернеті: <https://www.cisa.gov/sites/default/files/2024-09/Secure-Our-World-4-Easy-Ways-Stay-Safe-Online-Tip-Sheet.pdf>