

FOUNDATIONS BEFORE YOUR FIRST ACTION

Crypto security

Protect access. Check requests.
Take time to decide.

30-45 minutes · 6 modules · 10 questions

All exercises are completed on paper. No real funds, wallet installation, connections or signatures are required.

Learning path

- 01 Learning map and safe practice
- 02 1. Wallets, exchanges and control of access
- 03 2. Accounts, phishing and false urgency
- 04 3. Network, asset, address and memo
- 05 4. Connecting, signing and approving are different actions
- 06 5. Incident plan and final check

LOGRI CRYPTO SECURITY · 2026-10-31

01 / 06

Learning map and safe practice

What you will learn

By the end, you will be able to distinguish a public address from a secret, recognise a dangerous request, check a transfer route on paper and choose initial steps during an incident. This is a useful foundation before START, HOLD, Radar Practice and GameFi. Allow approximately 30-45 minutes including exercises; you can work in stages.

Read each lesson, write your own solution and only then read the explanation. Platform names A and B, addresses such as "ADDRESS-A" and amounts in the exercises are fictional. The exercises require no wallet installation, exchange registration, dapp connection, message signature, token claim or real transfer. Never send recovery phrases, passwords, codes or keys to the Academy.

Your learning note

Create five rows: what I protect; who controls access; what I check before acting; a reason to stop; where I would seek help. Record categories and decisions, not actual secrets or account addresses. Add to one row after each lesson. Your outcome is a personal procedure you can repeat without a prompt.

The exam has 10 questions, including two mandatory scenario exercises. Passing requires at least 70% overall and both mandatory exercises correct. Reading and practice are free. Sign in to your verified LOGRI account to save completion and obtain a certificate.

How GitBook fits in

The LOGRI wallet reference can help you later find a guide for a chosen network: <https://gamefi-40.gitbook.io/gamefi-40+-docs/wallets>. The safety section is at <https://gamefi-40.gitbook.io/gamefi-40+-docs/bezopasnost-i-skam>. This optional reference is partly in Russian; all required lessons and the exam are provided here in your chosen language. Buying or installing any listed wallet is not required to pass.

02 / 06

1. Wallets, exchanges and control of access

Identify the custody model first

With a custodial service, an operator typically controls the keys and your access depends on its rules and account protection. In a conventional self-custody wallet, keys and the recovery method determine access. Some apps offer Google, Apple or other backup models: first read the official rules for your particular setup. One wallet's instructions cannot be applied to every other wallet.

A public address is used to receive funds and inspect public history. It is not a password, but linking an address to a person exposes some financial privacy. A recovery phrase and private key confer control. An app password may only unlock local storage and may not restore access on a new device.

Secrets stay with the owner

Do not send a recovery phrase or key to an administrator, "support", a bot or a verification form. Do not photograph or store your own phrase in a chat, ordinary note or unprotected cloud. For a self-managed recovery phrase, plan a protected offline backup and consider loss, fire and unauthorised access. Check a real backup only using your wallet's official instructions, never as an Academy exercise.

A hardware wallet changes how keys are stored and actions are confirmed; it does not make a malicious signature safe. A separate experimental wallet helps separate activities, but does not turn an unknown application into a trustworthy one.

Exercise and explanation

Place "public address", "recovery phrase" and "email password" into two columns: may be shared to receive a transfer / must not be given for verification. Answer: only the address, if you accept the privacy consequences. The others are secrets. Then explain in one sentence why changing an app password does not neutralise an already exposed recovery phrase: authority under the old keys remains.

03 / 06

2. Accounts, phishing and false urgency

Protect the access chain

Email is often used to recover other accounts. Use different long passwords, keep them in a reliable password manager, enable available multifactor authentication and review active sessions. Prefer phishing-resistant sign-in methods where supported. An authenticator or SMS code is also a secret and can be tricked out of you. Do not approve an unexpected sign-in request merely because it carries a familiar logo.

Update your system and wallet from a verified source. Do not install an extension sent in a direct message or give a stranger remote access. When support is needed, independently open the official website, find its help channel and verify the contact there. A name, avatar, verified account or large following does not individually prove that a message is genuine.

Check the purpose of the action

HTTPS indicates an encrypted connection, not an honest site operator. Check the full domain after following a link, rather than the label on a button. Advertisements and top search results can lead somewhere unexpected. A saved bookmark is useful only if its original address was verified.

Scenario exercise A

An “admin” contacts you first: “Your certificate is ready. Enter your recovery phrase on the verification page within five minutes or lose the bonus.” Choose your action and name two warning signs.

Explanation: stop, enter nothing, verify through an independently found official channel and report the impersonation. Warning signs include requesting a secret, unsolicited contact and deadline pressure. A LOGRI certificate never requires your recovery phrase or access to funds. Refusing this action successfully completes the exercise; it is not a missed opportunity.

04 / 06

3. Network, asset, address and memo

An address does not describe the whole route

Before a transfer, establish the asset, network, recipient address and any memo or destination tag required by the receiving service. The same ticker may exist on several networks; a similar address format does not establish support for a particular asset or network. Check deposit conditions, minimums and fees on the receiving service's current page. Do not choose a network solely because its fee is lower.

Get the recipient address from a verified recipient source. After pasting, compare the complete address with the original: the first and last characters can reveal some mistakes, but do not replace a full check. Transaction history can contain lookalike addresses placed there by others. Before a real action, also check the amount, fees, network status and deposit availability.

Scenario exercise B

Platform A offers to send a fictional token over network X or Y. Platform B's verified deposit page says "network X only; memo REQUIRED". The draft uses Y and has an empty memo. Is it acceptable to send if the address looks identical?

Explanation: no. Stop, verify B's supported conditions, change the network to X and add the required memo from the verified source. If X or the memo field is unavailable, do not transfer until clarified. An identical-looking address does not resolve the mismatch. This is a conditions-checking exercise, not an invitation to try network Y.

Practice without a transfer

Complete a card: asset - fictional; network - X; address - ADDRESS-A; memo - PRACTICE-MEMO; recipient support - confirmed by the scenario; action - verify the entire route. In real use, a small test transfer may check a particular route, but does not guarantee the next transfer's safety or remove minimums and fees. This course requires no test transfer either.

05 / 06

4. Connecting, signing and approving are different actions

Read the wallet request

Connecting typically shares your selected public address with an app and lets it request further actions. A signature, token spending approval and transaction submission have different consequences. Mechanisms differ across networks and account types. Do not treat every fee-free signature as an ordinary safe login: some signed authorisations can be used later.

Before confirming, establish who requests the action, which contract gains authority, for which token, amount and duration. Compare the request with your intended purpose. If the interface does not explain the data or you do not understand it, reject the request and find the official explanation. A large or unlimited limit increases potential harm. A familiar project name does not remove the need to check the specific request.

Disconnecting is not revoking

Closing a tab or disconnecting a dapp from your wallet is different from cancelling an existing token approval. Permissions must be inspected and revoked separately using official instructions for the network. Revocation may require a network fee; it does not return stolen assets or change an exposed private key. There is no single action that fixes every case.

Exercise and explanation

A fictional app offers a free picture but requests unlimited access to a fictional stablecoin. It then says, "If you change your mind, just close the tab." Write your decision.

Answer: reject the disproportionate request and verify the permission's purpose. Closing the tab does not remove granted authority. A zero signature fee and no immediate debit do not prove an absence of risk. We are analysing a description; connecting a wallet, signing or revoking anything for the exercise is neither allowed nor required.

06 / 06

5. Incident plan and final check

Identify what may have been exposed

If suspicious, stop interacting with the questionable site and do not respond to unsolicited “rescuers”. In a separate note, record the time, domain, request type and public transaction hash if available. Remove secrets and personal details from material shared for assistance. Recovery is not guaranteed; an advance fee for “guaranteed recovery” is a reason to stop.

If an account password was exposed, use a trusted device to open the official service, change the password, end unfamiliar sessions and review recovery methods and MFA. Include email if affected. If a suspicious permission was granted, use the network’s official instructions to inspect and revoke it. These measures address different problems.

If a recovery phrase or private key was exposed, the old access model cannot be considered safe after merely changing a password or revoking one approval. The plan usually requires a new, independently created wallet with fresh keys and protection of remaining assets. Do not enter the old phrase into a rescuer’s “new” form. If there are signs of automated draining, do not blindly fund the compromised address for gas: those funds may also be taken. A real incident needs verified help tailored to the situation.

Final exercise

Write three separate rows: password leaked / suspicious permission / key exposed. Beside each, write the corresponding check from this lesson. Add a personal stop rule: “If I do not understand a request, I do not confirm; urgency does not replace checking.” This is a planning exercise, not an instruction to perform real operations.

Before the exam

Explain address versus secret, password versus recovery, and connection versus approval. Revisit scenarios A and B. The exam assesses decisions under the stated conditions; it does not audit your devices or certify a real wallet as secure.

Sources and scope

Original LOGRI educational text; sources checked on 31 October 2026. Interfaces, recovery methods, permissions and network conditions change: consult current official instructions. EVM mechanisms cannot automatically be applied to Solana, TON or other networks. Neither a wallet nor an exam eliminates every risk. The primary sources below are mostly in English; reading them neither replaces nor blocks the complete course in your chosen language.

Primary sources

- Ethereum: wallet safety: <https://ethereum.org/security/>
- MetaMask: recovery phrase and password: <https://support.metamask.io/start/user-guide-secret-recovery-phrase-password-and-private-keys>
- MetaMask: token approvals: <https://support.metamask.io/transactions-and-gas/transactions/what-is-a-token-approval/>
- MetaMask: disconnecting versus revoking: <https://support.metamask.io/more-web3/dapps/disconnect-wallet-from-a-dapp/>
- Uniswap Labs: signature scams: <https://support.uniswap.org/hc/en-us/articles/40050562560781-Crypto-Wallet-Signature-Scams>
- Solana: security guide: <https://solana.com/learn/staying-safe-on-solana>
- Coinbase: destination tags and memos: <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/destination-tag-memo-faq>
- CISA: four basic online safety habits: <https://www.cisa.gov/sites/default/files/2024-09/Secure-Our-World-4-Easy-Ways-Stay-Safe-Online-Tip-Sheet.pdf>