LESSON 15: SCAMS, SECURITY, PRIVACY, AND IRREVERSIBLE ERRORS

A Prison Professors Self-Directed Course

Estimated time: 70–105 minutes

Educational and Safety Boundary:

> *This lesson provides general education about scams, security, privacy, and digital-asset transactions. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, exchange, network, asset, company, or financial product. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson. Do not contact anyone, open a link, create an account, share personal information, or perform a transaction for any course activity. Never place a real password, private key, seed phrase, authentication code, account number, wallet address, balance, or transaction record in a course response.*

OPENING GUIDANCE

Throughout my years in prison, I learned to slow down before making a decision that could shape my future. Pressure can narrow a person's attention. Excitement can do the same. When someone promises an easy solution, demands immediate action, or asks for secrecy, disciplined thinking becomes a form of protection.

Web3 gives people new ways to exchange value, coordinate communities, and verify public records. The same tools can also be used in dishonest schemes. A scammer may pretend to represent a company, a public figure, a support team, a charity, or a person we trust. The message may look professional. It may use familiar names and accurate public information. It may even point to a real blockchain transaction. None of those features proves that the request is legitimate.

In earlier lessons, I described the independent PP token community and the public treasury associated with the Prison Professors mission. Public blockchain records can help people observe activity connected with a published address. Yet visibility does not prevent impersonation. A dishonest person could copy our name, logo, public address, or community language and then ask someone to send funds, reveal credentials, or visit a false support page. A copied identity is not the same as verified authority.

I encourage you to build a repeatable response before you ever face such a request. Stop. Verify. Seek help. Those three actions create time and distance between an emotional message and an irreversible decision. They also apply beyond Web3—to

employment offers, family emergencies, charitable requests, account warnings, and other claims that arrive through digital communication.

You can practice this judgment without a device. In the offline exercise, you will examine fictional messages, mark warning signs, and explain a safe response. You will not use a working link, contact a sender, disclose information, or move any asset.

PURPOSE AND ESSENTIAL QUESTION

Lesson 15 explains how manipulation can lead a person to reveal sensitive information or authorize an unwanted transaction. It presents common scam patterns, shows how public blockchain records affect privacy, and teaches a cautious response that does not depend on technical expertise.

Essential Question:

» How can a person slow down, verify a digital claim, and protect sensitive information before an error becomes difficult or impossible to reverse?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

» Recognize common patterns in phishing, impersonation, investment, giveaway, romance, support, and recovery scams.
» Identify warning signs such as pressure, secrecy, guaranteed returns, credential requests, and unsolicited contact.
» Explain how public blockchain records can affect personal privacy.
» Describe why some blockchain transactions are difficult or impossible to reverse.
» Apply a Stop, Verify, Seek Help process without visiting a link, sharing credentials, or performing a real transaction.

KEY TERMS

PHISHING

Definition: A deceptive attempt to obtain sensitive information or cause a harmful action by pretending to be a trustworthy person or organization. A phishing message may arrive by email, text, social media, telephone, letter, or another channel.

Sample sentence: The unexpected account warning was a phishing attempt designed to make the recipient open a false sign-in page.

IMPERSONATION

Definition: Pretending to be another person or organization in order to gain trust, information, money, or access. An impersonator may copy a name, photograph, logo, writing style, or public address.

Sample sentence: The copied logo did not prove that the message came from the organization it claimed to represent.

SOCIAL ENGINEERING

Definition: The use of deception, pressure, emotion, or trust to influence a person into revealing information or taking an action. Social engineering attacks people's decisions rather than relying only on a technical weakness.

Sample sentence: The caller used social engineering by creating fear and demanding immediate secrecy.

RECOVERY SCAM

Definition: A scheme in which someone promises to recover money, digital assets, or access lost in an earlier scam, usually in exchange for an advance fee, credentials, or additional payment.

Sample sentence: The person who promised a guaranteed refund for an advance fee was attempting a recovery scam.

PRIVACY

Definition: A person's ability to control or limit access to information about identity, activity, relationships, location, finances, or other personal circumstances. Privacy on a public blockchain is limited because transaction records can often be viewed and analyzed.

Sample sentence: Reusing one public address can reduce privacy by making separate transactions easier to connect.

IRREVERSIBLE TRANSACTION

Definition: A transaction that cannot ordinarily be canceled or reversed after the network accepts and finalizes it. A recipient may voluntarily return funds, but the blockchain usually does not provide a customer-service button that forces a refund.

Sample sentence: The irreversible transaction left little opportunity to correct the wrong destination after finality.

MAIN LESSON

SCAMS TARGET DECISIONS

A scam does not always begin with a technical attack. It often begins with a story.

The story may say that an account will close, a family member faces an emergency, an investment opportunity will disappear, a prize is waiting, a public figure needs support, or a lost payment can be recovered. The sender then gives the recipient a narrow path: act now, keep the conversation private, follow these instructions, and do not verify the claim elsewhere.

The story changes, but the structure often remains familiar:

- Establish trust by using a recognizable name, role, logo, relationship, or shared interest.
- Create emotion through fear, hope, urgency, affection, authority, or embarrassment.
- Reduce independent thinking by demanding speed or secrecy.
- Request value, information, access, or authorization.
- Discourage verification through an established, independent channel.

This structure is social engineering. It exploits ordinary human reactions. Intelligent and experienced people can be deceived when a message reaches them at the wrong time or creates the right emotion. Shame after an error can then keep a victim from asking for help, which gives the scammer more control.

A safer response treats emotional intensity as a signal to pause. The stronger the pressure, the more valuable an independent check becomes.

PHISHING: A FALSE PATH TO INFORMATION OR ACTION

Phishing messages often imitate a bank, exchange, wallet provider, employer, government office, delivery service, charity, or familiar contact. A message may claim that an account has a problem and provide a link or telephone number. The destination may be designed to capture a password, authentication code, seed phrase, identity document, or payment.

Some phishing messages contain obvious errors. Others are polished. Artificial intelligence and copied public information can help a criminal create convincing language, images, audio, or video. A professional appearance cannot establish authenticity.

COMMON WARNING SIGNS INCLUDE:

- An unexpected message about an account, payment, prize, refund, or emergency.
- A request to open a link or attachment before the claim can be checked.
- A sender address, telephone number, or account name that is slightly different from the official one.
- A demand for a password, private key, seed phrase, authentication code, or remote access.
- A threat that delay will cause immediate loss, arrest, closure, or public embarrassment.
- Instructions to bypass ordinary policies or keep the communication secret.

Do not use the contact information supplied in a suspicious message to verify that same message. A false sender can also provide a false support number. Use a known statement, printed policy, official directory, previously verified record, or another independent source.

IMPERSONATION AND FALSE SUPPORT

Impersonation can occur anywhere people communicate. A dishonest account may copy the name and photograph of a founder, celebrity, nonprofit leader, family member, or support representative. It may reply beneath a genuine public post so that the false account appears connected with the real one.

False support agents often look for people who publicly describe a problem. The agent may offer help and then request a seed phrase, private key, screen-sharing session, software installation, or payment to "validate" a wallet. A legitimate service does not need a seed phrase or private key to provide ordinary support. Anyone who receives those credentials can control the associated assets.

Authority should be verified through an established channel. A badge, username, logo, photograph, or confident tone is only part of a presentation. It is not proof of identity.

INVESTMENT AND GUARANTEED-RETURN SCAMS

An investment scam may begin with an unsolicited message, an online relationship, a group conversation, or a convincing-looking platform. The promoter may display supposed profits and allow a small early withdrawal to build confidence. Later, the victim may be asked to deposit more or pay a fee, tax, or security charge before withdrawing. Additional payment can deepen the loss.

WARNING SIGNS INCLUDE:

- Guaranteed profits or unusually high returns with little or no risk.
- Claims that a secret system, automated program, insider connection, or famous supporter removes uncertainty.
- Pressure to act before research or independent advice is possible.
- Instructions to buy or transfer a specific digital asset to an unfamiliar address.
- A dashboard showing profits that cannot be independently withdrawn or verified.
- A demand for new money to release existing funds.

Every investment involves uncertainty. A person who guarantees a return or claims that risk has disappeared is withholding a central truth. Public excitement, a rising price, or a large community does not establish safety, legality, liquidity, or future value.

GIVEAWAY AND ADVANCE-PAYMENT SCAMS

A giveaway scam may claim that a public figure, company, or community will send back more digital assets than the recipient sends first. The scammer may display copied videos, false comments, or a public address that appears active.

A legitimate gift does not require a person to send value first in order to receive a larger amount. A transaction on a block explorer only proves that a transaction occurred. It does not prove that the promotion is honest, that displayed participants are independent, or that a repayment will follow.

Advance-payment schemes use the same logic in other forms. A person may be told to pay a processing charge to receive a prize, grant, inheritance, job, loan, refund, or charitable distribution. The promised benefit becomes a reason to send money before the claim has been verified.

ROMANCE AND RELATIONSHIP-BASED SCAMS

A romance scam develops trust over time. The person may offer attention, affection, spiritual connection, friendship, or plans for a future together. The request for money may come later and may involve travel, medical care, legal trouble, business, or an investment opportunity.

The relationship can feel real because the emotional experience is real for the victim. That does not establish that the other identity or story is genuine. A refusal to meet through a safe, verifiable process; repeated emergencies; requests for secrecy; or pressure to send digital assets should trigger a pause and independent support.

Relationship-based manipulation is not limited to romance. It can involve friendship, mentorship, employment, shared faith, shared incarceration experience, or commitment to a mission. Trust should grow alongside verification, not replace it.

RECOVERY SCAMS CAN FOLLOW THE FIRST LOSS

After a scam, a victim may search for help or post publicly about the loss. A recovery scammer then claims to be a lawyer, investigator, government agent, blockchain expert, hacker, or recovery service. The new scammer may already know details about the first loss and use that knowledge to sound credible.

The recovery offer may require an advance fee, a new deposit, access to an account, or sensitive credentials. It may promise certainty even when the original transfer is irreversible. Paying again can create a second loss.

No private person can force a public blockchain to reverse a finalized transaction. Law enforcement, courts, exchanges, insurers, or other institutions may have lawful processes in some circumstances, but no outcome is guaranteed. A person seeking help should use verified official channels and should not provide credentials or new payments to an unsolicited rescuer.

WARNING SIGNS SHOULD BE CONSIDERED TOGETHER

One unusual detail does not always prove fraud. A legitimate organization may have a deadline. A family member may face a real emergency. A new company may contact a potential customer. The correct response is not automatic disbelief; it is verification proportional to the risk.

Several warning signs together increase concern:

- The contact was unexpected.
- The sender creates urgency or fear.
- The sender requests secrecy.
- The claim promises guaranteed returns, certain recovery, or easy income.
- Payment must be made in digital assets, gift cards, wire transfer, or another hard-to-reverse method.
- The sender requests a password, private key, seed phrase, authentication code, or remote access.
- The sender provides the only method for verifying the claim.
- The explanation changes when questions are asked.
- The sender discourages consultation with family, staff, counsel, or an independent professional.

» More money is required to release funds that supposedly already belong to the recipient.

STOP, VERIFY, SEEK HELP

I recommend a three-part response whenever a digital claim involves money, credentials, identity, access, or urgency.

STOP

Do not reply immediately. Do not open the supplied link, call the supplied number, install software, share a code, or send a payment. If possible, preserve the message without forwarding sensitive information. Time allows emotion to settle and gives reason a chance to return.

Ask: What action is the sender trying to cause? What could I lose if the request is false? Why must I act now?

VERIFY

Check the claim through a channel that the sender did not control. Use previously verified contact information, an official printed statement, a known family contact, an established organizational procedure, or another independent source. Compare more than the display name. Verify the identity, authority, purpose, destination, and requested action.

For a Web3 claim, verification may include checking official documentation, confirming a published address through more than one trusted source, examining what a smart-contract request would authorize, and confirming that the network matches the intended service. A block explorer can support limited verification of public transaction data. It cannot prove the human identity behind every address or the truth of an off-chain promise.

SEEK HELP

Ask a trusted person to review the claim before acting. Depending on the situation, that person may be a family member, institutional staff member, attorney, financial professional, organization representative, law-enforcement contact, or experienced technical professional reached through a verified channel.

Seeking help is a sign of disciplined judgment. A second person may notice pressure, inconsistency, or a hidden assumption that the recipient missed. If a possible scam has already caused a loss, prompt reporting may preserve records and improve the chance that an appropriate institution can respond, even though recovery is not guaranteed.

SECURITY PRACTICES SUPPORT CAREFUL JUDGMENT

Good security does not eliminate deception, but it reduces the opportunities available to an attacker.

USEFUL PRACTICES INCLUDE:

- Use a strong, unique password for each important account.
- Use multifactor authentication when available, and protect authentication codes.
- Keep devices and software updated through trusted channels.
- Store backups of essential information according to a secure, documented plan.
- Limit the personal information posted publicly.
- Review account activity and public addresses without revealing credentials.
- Follow written approval and verification procedures for organizational funds.
- Contact support through an established official path, not through an unsolicited message.

Never share a private key or seed phrase. Do not photograph it for convenience, enter it into an unfamiliar site, send it through email or messaging, or give it to a support representative. A person who receives it may be able to control the associated assets without further permission.

PUBLIC RECORDS AND PERSONAL PRIVACY

Public blockchains are often described as transparent. Depending on the network, a person may be able to view addresses, amounts, token movements, smart-contract interactions, fees, and timing. The record may use an address rather than a legal name, but an address is not automatically anonymous.

An address can become connected with a person or organization through a public post, exchange record, court document, donation page, purchase, data leak, or repeated pattern of activity. Once one connection is known, analysts may compare related transactions and infer relationships or habits. Some inferences will be accurate; others may be wrong.

Reusing one address can make activities easier to connect. Publishing a balance can attract unwanted attention. Combining blockchain data with social-media posts, location information, or other public records can reveal more than any single source.

Privacy therefore requires judgment about disclosure. Do not place real addresses, balances, transaction hashes, account details, or credentials in a course assignment. An organization that publishes a treasury address for transparency should still

avoid revealing private keys, signer identities, device details, backup locations, or procedures that could weaken security.

Transparency and privacy can serve different purposes. A public treasury may support accountability by allowing people to observe certain on-chain activity. The same public record does not reveal every fact about identity, ownership, custody, accounting, intent, or mission use. Responsible communication states what the evidence supports and leaves unsupported claims unstated.

WHY IRREVERSIBILITY CHANGES THE DECISION

Many familiar payment systems have an institution that may pause, dispute, or reverse a transaction under defined rules. A public blockchain usually works differently. After a valid transaction is accepted and finalized, the network generally does not have a central operator who can cancel it because the sender was deceived or chose the wrong address.

The recipient can voluntarily send value back. An exchange may freeze an account under its rules or legal obligations. Law enforcement may investigate. A court may issue an order. None of those possibilities changes the original blockchain record automatically, and none guarantees recovery.

Irreversibility shifts protection toward the period before authorization. The sender should verify the network, destination, asset, amount, action, fee, counterparty, and purpose before signing. A small test transaction may reduce some operational risk in real-world settings, but this course does not ask anyone to conduct one. A test also cannot prove that a counterparty is honest or that a later request is safe.

An urgent message and an irreversible payment method are a dangerous combination. Stop, Verify, Seek Help creates a protective barrier before the network records the decision.

APPLIED SCENARIO: A FALSE PRISON PROFESSORS REQUEST

The following scenario is fictional. It does not describe a verified incident, and it does not reproduce a working address, account, link, or message.

Imagine that a person receives a message from an account displaying the Prison Professors name and logo. The sender refers to the independent PP token community and the public treasury on BNB Smart Chain. The message says that a new “treasury verification program” will double any contribution sent within one hour. It provides an address and says that participants should keep the opportunity private until the verification period closes.

The message uses real public ideas: Prison Professors has a mission, an independent community created a token, and a public treasury address has been discussed. Those facts do not authenticate the new request.

THE WARNING SIGNS INCLUDE:

- Unsolicited contact.
- A copied organizational identity.
- A guaranteed return.
- A one-hour deadline.
- A request for secrecy.
- A hard-to-reverse payment.
- Verification instructions controlled by the sender.

A cautious recipient would stop without replying or sending value. The recipient would verify the claim through established Prison Professors information, such as previously confirmed contact details, rather than any link or number in the message. The recipient could seek help from a trusted person and report the impersonation through an official channel.

If I communicate about the Prison Professors mission, I want people to distinguish our work from independent community activity and from anyone who copies our identity. Prison Professors did not organize, manage, or control the PP token project. Public support for a mission does not give every supporter authority to speak for the organization. Future lessons may continue using the community project as a teaching example, but no course lesson asks a participant to buy a token, send funds, contact a community member, or perform a transaction.

The broader lesson applies to every participant building a Profile. Consistent work can earn attention and support from people we do not yet know. That opportunity also creates a responsibility to protect our name, verify claims, document decisions, and communicate honestly about who has authority.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

BENEFITS OF A DISCIPLINED SECURITY PROCESS

- A pause reduces the influence of urgency, fear, excitement, and embarrassment.
- Independent verification separates a sender's claim from evidence controlled by the sender.
- A second reviewer may identify inconsistencies or risks that one person missed.

» Written procedures help organizations apply the same safeguards repeatedly.
» Limited disclosure reduces the information available for impersonation and targeted attacks.
» Prompt reporting can warn others and preserve evidence for an appropriate institution.

IMPORTANT LIMITATIONS AND RISKS

» A polished message, copied logo, public transaction, or familiar name can still be deceptive.
» Public blockchain records may expose patterns without identifying the full human context.
» An address does not prove who controls it or why a transaction occurred.
» A valid digital signature can authorize a decision made under deception or pressure.
» Finalized transactions may be difficult or impossible to reverse.
» Recovery is uncertain, and a recovery offer can be a second scam.
» Privacy cannot be restored fully after sensitive information becomes public.
» Security tools are less effective when a person voluntarily reveals credentials or bypasses a warning.

COMMON MISCONCEPTIONS

"Only careless people are scammed." Scammers design stories around ordinary emotions and trusted relationships. A repeatable process protects people across experience levels.

"A professional-looking message is authentic." Appearance can be copied. Verify identity and authority through an independent channel.

"A public blockchain proves the entire story." It can show certain on-chain records, but it does not establish every identity, promise, ownership claim, or off-chain event.

"Support needs my seed phrase to fix the problem." Anyone with the seed phrase may gain control. Ordinary support should not request it.

"A guaranteed return removes risk." Guarantees of high or certain profit are a major warning sign.

"Paying one more fee will release my funds." New fees can extend an investment, withdrawal, or recovery scam.

"A verified social-media badge proves the request is safe." Accounts can be copied, compromised, or misunderstood. Verify the specific request elsewhere.

"The blockchain will refund an accidental transfer." A finalized network record usually has no forced-refund feature.

"Privacy means hiding wrongdoing." Lawful privacy protects safety, identity, relationships, and personal autonomy. It can coexist with appropriate accountability.

OFFLINE EXERCISE: MARK THE WARNING SIGNS

Estimated time: 30–35 minutes

Materials: Separate paper and a pencil.

The five messages below are fictional. They contain no working link, real address, telephone number, or account. Do not contact anyone or perform any action described. For each message, complete four tasks:

1. Identify at least two warning signs.
2. Name the emotion or form of pressure the sender may be using.
3. Write a safe response using Stop, Verify, Seek Help.
4. Identify one piece of information that should never be disclosed.

MESSAGE A: URGENT ACCOUNT WARNING

"Security Department: Your account will close in 20 minutes. Confirm your password and six-digit code on the attached page. Failure to respond will permanently lock your funds."

MESSAGE B: FAMOUS SUPPORTER GIVEAWAY

"A well-known Web3 founder is rewarding the first 50 supporters. Send one token now and receive two back. This private offer has been verified on the blockchain. Do not share it until you receive your reward."

MESSAGE C: FRIENDLY INVESTMENT COACH

"I have enjoyed our conversations, and I want us to build a future. My trading system has never lost. Deposit more today so your balance can qualify for withdrawal. The tax must be paid in advance."

MESSAGE D: WALLET SUPPORT

"I saw your public post about a missing transaction. I am an official recovery technician. Send your seed phrase so I can reconnect the wallet. My service charge is due after I confirm access."

MESSAGE E: MISSION IMPERSONATION

"The Prison Professors treasury needs immediate verification. Send a contribution to the address below within one hour and it will be doubled. Keep the address private while the audit is active."

After reviewing all five messages, answer these questions:

- Which warning sign appeared most often?
- Which message might be most persuasive to you, and why?
- How can public information make an impersonation attempt more convincing?
- Why should a person avoid the telephone number or link supplied in a suspicious message?
- How does transaction irreversibility increase the value of pausing before authorization?
- Write a three-sentence personal rule you could use when a digital claim creates urgency.

Important limitation of the exercise: A warning sign is a reason to investigate, not automatic proof that every claim is false. The safe response is to pause and verify through an independent channel without disclosing information or sending value.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which request is the clearest sign of a dangerous support impersonation?
   a. A suggestion to read public documentation
   b. A request for a seed phrase or private key
   c. A reminder to keep software updated
   d. A recommendation to ask a trusted person for help
2. What is the safest way to verify an unexpected account warning?
   a. Use the link in the message because it is faster
   b. Reply and ask the sender whether the message is genuine
   c. Contact the organization through previously verified information

d. Forward the password so support can compare it

3. What can a public blockchain record establish most directly?
   a. Every human identity and motive connected with a transaction
   b. That an investment promise is honest
   c. Certain on-chain activity recorded under the network's rules
   d. That a recipient will voluntarily return a payment

TRUE OR FALSE

» After a finalized blockchain transaction, a sender can ordinarily require the network to reverse it through a customer-service request.

SHORT EXPLANATION

» In three or four sentences, explain how Stop, Verify, Seek Help can protect a person from an urgent impersonation request.

SUMMARY AND PRACTICAL TAKEAWAYS

» Scams often use trust, emotion, urgency, and secrecy to influence a decision.
» Phishing imitates a trusted source to obtain information or cause a harmful action.
» Impersonators may copy names, logos, photographs, public addresses, and accurate public facts.
» Social engineering targets human judgment as well as technical systems.
» Guaranteed returns, unsolicited contact, credential requests, and advance payments are strong warning signs.
» A romance or relationship scam can build trust for weeks or months before requesting value.
» Recovery scammers often target people who have already experienced a loss.
» Never share a password, private key, seed phrase, or authentication code.
» Stop before replying, opening a supplied link, calling a supplied number, or sending value.
» Verify through an independent channel that the sender did not control.
» Seek help from a trusted person or appropriate institution before acting.
» Public blockchain records can support limited on-chain claims but do not prove every identity, promise, or off-chain event.
» A public address is not automatically anonymous, and repeated activity can reveal patterns.

- Finalized blockchain transactions may be difficult or impossible to reverse.
- The fictional Prison Professors example shows how real public information can be copied into a false request.
- No course exercise requires internet access, an account, a wallet, a digital asset, or a real transaction.

The practical lesson is simple: create distance between pressure and authorization. Stop. Verify. Seek help.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- Describe why a scam can persuade an intelligent person.
- Explain the roles of urgency, secrecy, trust, fear, hope, or affection in social engineering.
- Identify three warning signs that would cause you to pause.
- Explain how you would apply Stop, Verify, Seek Help to an unexpected digital claim.
- Describe one independent verification channel you could use without following the sender's instructions.
- Explain why a seed phrase, private key, password, or authentication code must remain confidential.
- Explain how public blockchain records can support transparency while reducing privacy.
- Describe why transaction irreversibility increases the need for review before authorization.
- Use the fictional Prison Professors impersonation scenario to distinguish a real mission from an unauthorized request.
- State the personal rules you will follow to slow down and verify future claims.

Your response should demonstrate reasoning and personal responsibility. Do not open a link, contact a sender, create an account, share personal information, or perform a transaction. Do not include any real password, private key, seed phrase, authentication code, account number, wallet address, balance, transaction hash, transaction detail, or other sensitive information.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 15: Scams, Security, Privacy, and Irreversible Errors, and the date you completed the entry.

Use one of the established Prison Professors Profile methods, subject to your facility's rules:

- Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 15 — [date completed].
- Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
- Send it to an approved family member or supporter who can enter it on your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, real wallet addresses, balances, transaction hashes, transaction details, or other sensitive credentials.