Level 2

Topic 3: DIGITAL WALLET FUNDAMENTALS

Point 1: The Admin Will Never Direct Message You First

Real admins never message you first in private. If someone sends you a direct message offering help out of nowhere, treat it as a scam. Scammers watch Telegram groups, and the moment you mention a problem, they create a lookalike profile with the same photo and name to pretend to be support. Make it your habit to ask questions only in the public group, and if you truly need help, click the verified username to start the DM yourself. If an uninvited helper appears in your DMs, block and delete immediately with no discussion

Point 2: Emotional Pressure: Fear and Urgency

Scammers try to manipulate your emotions by rushing you, claiming the flip is about to happen, or telling you your assets will disappear unless you act right now. They want you to panic and move faster than you can think. Remember your motto: there is no train you are going to miss. If something is safe and real, it will still be safe in ten minutes, ten hours, or twenty-four hours. Take a breath, slow down, and verify everything in the official group chat.

Point 3: Clone Groups and Fake Communities

Scammers often create clone groups that look almost identical to the official chat with the same logos and descriptions, using them to announce fake token sales or send people to dangerous links. Protect yourself by joining groups only through official links sourced directly from trusted Academy channels. If a group feels quiet, unfamiliar, or overly aggressive with offers, treat it with extreme caution.



Point 4: Take Control of Your Telegram Invites

To stop getting pulled into strange Telegram groups you never joined, lock down your privacy settings right away. Open Telegram on your phone, go to "Settings", "Privacy and Security", scroll down to invites, and select "Nobody". You can also switch on "Archive and Mute". Choosing "Nobody" means people must send you an invite link and you choose whether to join, locking the front door against unwanted spam and fake rooms.

Point 5: "Activation of a QFS Account" and "Quantum Ledger”

Any message, website, or form directing you to activate a QFS account, register for a Quantum Ledger, or deposit funds to keep your money safe is an outright scam. There is no extra registration or link that magically makes your wallet safer. If a site demands personal details like a Driver's License or Passport, asks you to pay a fee to qualify, or tells you to deposit now to unlock QFS benefits, close the page straight away and walk away.

Point 6: Look alike Domains and Fake Tokens

Scammers use lookalike websites and domain names that change just one letter, number, or file ending like dot co instead of dot com. Always double-check official domains and read every single letter of a domain name before adding it to your wallet.

Point 7: Fake Tokens and Copycat Assets

On decentralized networks, anyone can create a token sharing a popular name, so always check the listed domain against official channel posts and ask in the chat before completing any trade.

Point 8: Your Secret Key and Recovery Phrase: The Master Vault: What You Must Never Share

Your Secret Key and Recovery Phrase are the master keys to your vault, and if someone else has them, they have complete control over your wallet. LOBSTR does not hold your key—it is just a tool to access the Stellar network, meaning only you hold your key. No admin or team member will ever ask for your keys. Store them offline on paper in a secure private location, and never type them into random websites, social media, or private messages anywhere.



Point 9: Account vs Wallet: Knowing What is Compromised

There is a difference between an account compromise and a wallet compromise. If your main LOBSTR username, email, or password is breached, all wallets under that account are at risk, and creating a new wallet inside that same account does not fix the problem. If your main login feels compromised, stop using that account entirely, create a brand-new LOBSTR account with a fresh email and strong password, move your remaining funds, and enable strong security.

Point 10: Hacking on Your Browser

If you are using LOBSTR on your computer, never step away without logging out first, as browser-based wallet compromises happen when sessions are left open. If you see suspicious activity happening in real-time, log off, shut down your browser immediately, and turn off your computer. Consult a computer expert to secure your machine and never open a new account using a compromised browser.

Point 11: Turning on Two-Factor Authentication (2FA) in LOBSTR

Two-factor authentication adds a second lock so that even if someone guesses your password, they cannot get in without a code from your phone. Navigate to "Settings" and "Security" in LOBSTR to Two-factor authentication. When the authenticator app gives you a backup key, do not screenshot it—write it down on paper and store it offline safely. Enter your password, backup key, and app code to finish enabling 2FA so every login requires a secure one-time code

Point 12: Password Managers: Make your Passwords Strong

Protect your digital life by using password managers to generate and store strong, unique passwords inside an encrypted vault, stopping you from reusing the same password across email, Telegram, and wallets. Never autofill passwords carelessly. Remember that all safety measures are at the discretion of the investor, and practicing these calm, deliberate daily habits ensures you protect your position every step of the way.

Questions and Answers

Q1: What is the golden rule regarding admins and project owners and private messages on Telegram?

Answer: Real admins and project owners never message you first in private. If someone sends you a direct message offering help out of nowhere, treat it as a scam, block them, and delete the message immediately with no discussion.

The Difference: Scammers watch Telegram groups and create lookalike profiles with the same photos and names to impersonate support the moment you mention a problem. **By asking questions only in the group and starting DMs yourself with verified usernames**, you prevent fake support profiles from compromising your position.

Q2: How should you handle messages or people that try to invoke fear, panic, or urgency regarding your digital assets?

Answer: Remember your motto—there is no train you are going to miss even if you wait ten minutes, 10 hours or twenty four hours. **Take a breath, slow down, and verify everything in the official group chat.**

The Difference: Scammers try to manipulate your emotions by claiming your assets will disappear or that you must register instantly to rush you past your defenses. **Real, safe opportunities will still be secure hours later, giving you time to think clearly instead of reacting under stress.**



Q3: How can you protect yourself from fake clone groups and copycat communities?

Answer: Join groups only through official links sourced directly from trusted Academy channels, and treat unfamiliar or overly aggressive rooms with extreme caution.

The Difference: Scammers build clone groups mimicking official chats down to the exact logo and description to push fake token sales and bad links. **Sticking strictly to verified channel links ensures you never walk into a fraudulent trap.**

Q4: Which privacy setting should you change on Telegram to stop strange rooms from pulling you into chats without your consent?

Answer: Open Telegram, go to "Settings", "Privacy and Security", scroll down to "Invites", and select "Nobody".

The Difference: Leaving invites options open in Telegram allows random rooms to pull you into spaces pushing scam links and fake tokens. Switching your setting to "Nobody" or "My Contacts" locks the front door so you only enter rooms you actually choose to join.

Q5: How should you respond to any website or form demanding money or deposits to activate a QFS account or register for a Quantum Ledger?

Answer: Recognize it as an outright scam, close the browser page straight away, and walk away.

The Difference: There is no extra registration, fee, or link required to make your wallet safer. Any site demanding personal documents like a driver's license or passport, or asking for deposits to unlock special benefits, is simply trying to steal your funds.



Q6: What is the proper habit for checking domain names before adding an asset or interacting with a link?

Answer: Always double-check official domains, read every single letter of the domain name, and verify it against official channel posts.

The Difference: Scammers register lookalike domains changing just one letter, number, or file ending like dot co instead of dot com. Because anyone can create tokens with matching names on decentralized networks, checking the exact domain protects you from copycat assets.

Q7: What makes your Secret Key and Recovery Phrase the absolute master keys to your vault, and how must they be stored?

Answer: They control full access to your wallet. If someone else gets them, they have complete control over your funds without needing your permission. **They must be stored offline on paper in a secure private location and never shared digitally.**

The Difference: LOBSTR does not hold your key; it is only a tool to access the Stellar Network, meaning only you hold your keys. **Storing them offline on physical paper ensures that no website, social media platform, or private message can ever expose your wealth.**

Q8: What must you do immediately if your main LOBSTR username, email, or account password has been compromised?

Answer: Stop using that compromised account entirely, create a brand-new LOBSTR account with a fresh email and strong password, move your remaining funds, and enable strong security.

The Difference: Compromising your main login puts every wallet under that account at risk, and creating a new wallet inside an already compromised account does not fix the underlying breach. Moving to a fresh account secures your remaining assets away from hackers.



Q9: How can you protect your wallet from browser-based hacks when using a computer?

Answer: Always log off when finished, never step away leaving your session open, and **immediately shut down your browser and computer if you notice suspicious real-time activity.**

The Difference: Leaving your wallet open on a browser leaves you vulnerable to hackers accessing your active session. **Turning off your computer and consulting a computer expert ensures your environment is safe before trying to access your accounts again.**

Q10: Why is enabling Two-Factor Authentication (2FA) essential for your digital security, and how must you handle its backup key?

Answer: 2FA adds a second lock requiring **a one-time code from your phone. You must write down the back up key and store it safely offline. Do not take a screen shot.**

The Difference: Even if someone guesses your password, they cannot get into your account without your phone's code. Protecting the backup key on physical paper keeps your secondary recovery method entirely out of reach from hackers.

Q11: How do password managers protect your digital life, and what rule should you follow regarding autofill?

Answer: Password managers generate and store strong, unique passwords inside an encrypted vault so you never have to memorize them or reuse the same password across platforms, and you should never autofill passwords.

The Difference: Reusing passwords across email, Telegram, and wallets creates a single point of failure if one service is breached. Using a password manager isolates each login with high-level complexity while keeping your vault secure.