Level 2

Topic 3. Stellar Wallet - Safety and Security

Part 1: Opening

Beth: Welcome back to the Maga Academy. You are doing something powerful by taking time to learn about safety and security before you move money. Think of the Stellar Network like a new city; it is exciting, but you need to know which streets are safe.

Sam: I am glad we are doing this. This is very important topic for the MAGA Academy community. Beth and I are here today to share with you ways to protect and keep your wallets safe.

Beth: The goal is to build simple habits that keep you safe. Let us start with Telegram.



Part 2: Core Content

Point 1: The “Admin will Never Direct Message you First”

Sam: Here is our first rule; Real admins never message you first in private. On Telegram, you will often hear the term "DM," which means direct message, a private chat that does not appear in the public group. If someone sends you a direct message, offering help out of no where, treat it as a scam.

Beth: Scammers watch Telegram groups. The moment you say you are confused or mention a problem, they create a look alike profile with the same photo and name, as a real admin. Then send you a direct message. They do this, pretending to be "support."

Sam: So, to a beginner, they look exactly like the project leaders or an admin. If a direct message is sent to you first, then that, is your big warning sign.

Beth: Exactly, make this your habit; Ask questions only in the group, not in private DMs. If you truly need one on one help, you click the verified username in the group and start the DM yourself. If someone DMs you first saying, "I am support," you block, and delete. In Telegram, simply hold down their name, until the green check shows, go to the Telegram menu at the top. Click the three dots. Then a menu will show up, Click "Block user". No discussion.

Sam: So, if a "helper admin" appears in your private DMs without asking, treat it as a scam, block and delete.

Beth: Exactly. They also create the same USER ID, and add it to another field like BIO, and if you only look quickly, you think that it is an admin's USER ID. Make sure you check this field. If it is not in the USER ID section, you block and delete. No discussion. You do not owe strangers your time, your data, or your keys.

Sam: Definitely check that the scammer, hasn't used the admin's USER ID in the BIO field. Always go to the chat, tag the admin in the chat, and ask if they sent you a direct message. Do not respond to the direct message until you receive an answer in the chat. The answer will always be NO. But ask anyway. Block and delete. There are also scammers who impersonate high profile names or the owner of the Telegram channels, like The President of the United States, Melania, Whiplash, General Flynn, or Elon Musk.

Beth: This would definitely be our alert, these are busy people with very busy roles, they are NOT messaging you. Treat it as a scam, and block, and delete. No discussion.

Point 2: Emotional Pressure: Fear and Urgency

Beth: Scammers use your emotions. They might say things like:

- "The flip is about to happen and I'm here to keep your assets safe", Or
- "You need to register with this website link quickly". Or
- "you need to send me your tokens, and I will send them back safely to you". Or
- "Do you have other funds in other locations? I can help protect those for you as well". Or
- "your assets will disappear if you do not follow my instructions right now". Or
- "you don't need to check with a friend, or in the channel I am here to help you"

Sam: They want you to panic, they want you to stay engaged with them and they move faster than you can think. Any Direct message that says "do this right now, I can help you." is a red alert! So, if you feel rushed, stressed, or pressured, alarm bells will ring for you. Time to slow down and validate who you are speaking to in the group chat.

Beth: That's right Sam! Our motto is: 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 even twenty four hours. Take a breath, slow down and verify.

Point 3: Clone Groups and Fake Communities

Sam: Sometimes you may notice you are in groups that look like copies of a real community.

Beth: Yes, this can happen. Scammers create clone groups that look almost identical to the official chat, same logo, similar name, similar description. Then they announce fake token sales or "special offers" that send people to bad links.

Sam: Your safety checklist: Join groups only through official links from a trusted Telegram official channel. If a group feels quiet and new, or full of aggressive offers, treat it with caution.

Point 4: Take Control of Your Telegram Invites

Beth: A lot of people tell us, "I keep getting pulled into strange Telegram groups that I never joined." Some of those rooms exist, only to push fake tokens or scam links. Let's turn that off. Now!

Sam: On your phone: Open Telegram. Tap "Settings" "Privacy & Security". Scroll down to "Invites" and select, "Nobody". Now go to "Archive and Mute" and switch to the right to it is on. If you choose "My Contacts", only people you already know can add you. If you choose "Nobody", people must send you an invite link. and you choose whether to join.

Beth: That feels like locking the front door. Now you will only be in rooms you actually decided to enter.

Sam: Exactly. And if you ever find yourself in a group you do not recognize, you can tap the group name and choose "Leave Group". You always have the right to leave a channel.

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

Beth: I've heard people getting messages directing them to activate a QFS account. I've also heard some people mention. I need to set up a QFS account to keep my money safe and or register for a "Quantum Ledger".

Sam: I need you to hear me clearly. This is an outright scam! Any website or form that asks you to pay money or deposit funds to "activate" your QFS account or "register for a QFS ledger" is a scam designed to take your deposit. There is no extra registration or link that magically makes your wallet safer.

Beth: If a site says enter your personal details, verify your drivers license or passport, or address, "pay this fee to qualify" or "deposit now to unlock special QFS benefits,". You close the page straight away and walk away.

Point 6: Look alike Domains

Sam: Another quiet trick is the look alike website. Also called the domain name. With the stellar network, all tokens have a domain name, that the token is linked to. For example, XLM is stellar.org. Scammers register a domain that looks almost exactly like the real one, but they change one small detail: one letter, one number, or the ending, .co instead of .com.

Beth: Your habit needs to be always double check official domains. Read every letter of the domain name, before you add it to your wallet. If a link arrives from a stranger or a random DM, do not click it. Go to the official Telegram channel and check the domain name there.

Sam: On decentralized networks, anyone can create a token and name it after a popular project. That means you might see multiple assets with almost the same name.

Point 7: Fake Tokens and Copycat Assets

Beth: Before you click Buy, check the domain listed for the token. Compare it against the project's official posts on their Telegram channel. If there is any doubt, stop and ask in the official community chat before you add a token, or before you complete any trade.

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

Beth: Let us talk about the wallet itself. The two most important things you must protect.

Sam: Your Secret Key and Recovery Phrase are the master keys to your vault. If someone has your Secret Key and your Recovery Phrase, that person does not need your permission. That person now has control over your wallet. Some people think contacting LOBSTR will help them. LOBSTR doesn't hold your key. It is just a tool to access the Stellar Network. Only you, hold your key.

Beth: Key principles. No project owner, admin, or project team member will ever ask for your Secret Key or Recovery Phrase. You never ever type it into random websites, chats. or social media. You never ever type them into a private message to anyone on any platform including Telegram, text message, WhatsApp, or Facebook. You share absolutely nowhere. You store it offline, on paper and keep it safe, in a secure private location.

Sam: If you ever type your Secret Key or Recovery Phrase into an unknown site, you have handed that person Your money. It's like giving someone your bank card or a signed blank check.

Beth: That is correct. Your money is gone. If this happens you need to start a brand-new wallet, new username or email address and password.

Point 9: Account vs Wallet: Knowing What is Compromised

Sam: There is a difference between account compromise. and wallet compromise.

Beth: If someone has your main LOBSTR login, username. or email, plus password or passkey. Then, all wallets under that account are at risk. Creating a new wallet inside a compromised account does not fix the problem. If someone only saw one specific wallet Secret Key, that wallet is unsafe. But other wallets created separately, with different Secret Keys can still be safe.

Sam: So, if your main login feels compromised, stop using that account. Create a brand-new LOBSTR account with a new username or new email address, and strong new password. Move any remaining funds to the new account and a fresh new wallet. Enable strong security and never reuse old passwords.

Beth: Yes exactly. That is the process. If this is required, stay calm and focused and follow the process.

Point 10: Hacking on Your Browser

Sam: If you are using, LOBSTR on your computer, always log off when you have finished. Never step away from your computer leaving it logged in. Always log out first.

Beth: There are instances of hackers accessing wallets through the browser. You are more vulnerable to this if you leave your wallet open on your computer.

Sam: If you are online and you see this happening real time, log off and shut the browser immediately and turn your computer off. Speak to a computer expert to improve the security on your computer.

Beth: If you do get hacked from your browser, do not open a new account using the same browser. The hackers will take those funds too. Speak to a computer expert to improve the security on your computer.



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

Sam: Two-Factor Authentication. This adds a second lock. Even if someone guesses your password, that person still cannot get in without a code from your phone.

Beth: Here is how to navigate to Two-Factor Authentication in LOBSTR. Click on the three bars at the top left of your LOBSTR screen, then go to "Settings", Go to "Security". Find "Two-Factor Authentication" and click on "Disabled". This will start your process for enabling Two-Factor Authentication. Follow the steps to complete, if you want to implement this level of security. The Two-Factor Authentication app will come with a key.

Sam: Do not screenshot it. Write that backup key down on paper. Store it offline, and keep it safe, in a secure private location. Enter your LOBSTR password, the backup key, and the code from your authenticator app, then click Enable 2FA.

Beth: After this, each login will require the one-time code from your phone.

Point 12: Password Managers: Make your Passwords Strong

Sam: The next topic is password manager. There are apps that are built to generate and store, strong unique passwords inside an encrypted vault.

Beth: They create complex passwords that you do not have to memorize. They stop you from using the same password across email, Telegram, and wallets.

Sam: Also, never autofill a password.

Beth: All safety measures are at the discretion of the investor. These are all recommendations and as usual an investor must do their own research.



Part 3: Closing

Daily habits and Final Protocols

Sam: Now we will summarize these points. To keep your money and tokens safe and secure, ensure you follow these guidelines.

Beth: Never react under pressure. Never take direction from anyone when stressed.

Sam: Nothing is urgent.

Beth: Only Direct Message support first. Never correspond with an admin who messages you first. It is always a scammer.

Sam: Domains look like websites. Check domains at least twice before adding any domain to your wallet.

Beth: Keep your Recovery Phrase in a safe, secure, private location and never share with anyone.

Sam: Never add more wallets to a compromised account - start a new account with username or new email address and password.

Beth: Be mindful of safety guidelines when using a browser.

Sam: For additional security add Two-Factor authentication and use password managers.

Beth: Never transfer XLM to an unknown person or account. An admin will never ask you to send them XLM.

Sam: Never provide your private information including address, license and passport to anyone on Telegram or in a website link.

Beth: Stay tuned. We will soon have our own dedicated reporting center where members will be able to report scams and suspicious activity directly.



Sam: Now MAGA Community. This information is very important. This is your safety and security checklist, Block anyone who DMs you first and asks for keys, codes, or private information. Delete suspicious chats and links. Do not let them sit in your inbox. When you need help, you always go to the official T channel and group chat. Click the known admin username. Confirm that no one is asking for your Secret Key, or Recovery Phrase.

Now you can use Telegram and your wallets with clear boundaries. You know what to ignore, what to double-check, and what steps to take if something feels wrong.

Beth: That is the goal. You are not just investing in assets; you are investing in your safety habits. Thank you for learning with us today. Join us in the MAGA Academy chat if you have any questions.

Sam: Protect your position and only trust channels and admins you can verify.