THE ALASKA CRYPTO SAFETY GUIDE

Avoid Scams • Set Up Safely • Verify Projects

For Alaskans, by Alaskans.

Created by Alaska Crypto Financial

Version 1.3

Alaska Crypto Safety Guide

A practical onboarding guide for wallets, swaps, and staying secure on-chain.

Prepared by Alaska Crypto Financial | Version 1.2

Important disclaimer. This e-book is provided for educational purposes only and does not constitute financial, legal, or tax advice. Crypto and DeFi carry significant risk, including total loss of funds. You are responsible for your own decisions and security practices. Never share your seed phrase with anyone. If someone asks for it, it is a scam.

How to use this guide

If you are brand new, start with Quick Start, then complete the Onboarding Checklist. If you already use wallets, skip to Transaction Safety, Verify Tokens & Pools, and DeFi Hygiene.

Table of contents

Quick Start: the 10 rules that prevent most losses

Most crypto losses are not "hacks." They are mistakes, rushed clicks, and social engineering. These 10 rules cover the highest-impact behaviors.

• Slow down. If you feel urgency, it is probably a scam.

• Never share your seed phrase or private keys. Not with "support." Not with friends. Not with anyone.

• Verify tokens by mint address, not by name/logo.

• Use official downloads only. Bookmark official wallet and swap sites.

• Treat links as hostile. Type the URL or use bookmarks; ignore ads and reply-links.

• Send a small test transaction before sending a large amount.

• Review approvals: what am I signing, and what permissions am I granting?

• Separate wallets: a "daily" wallet for small balances and a "vault" wallet for savings.

• Enable strong account security: unique passwords, 2FA, and SIM-swap protection.

• If something goes wrong, stop. Do not keep clicking. Preserve evidence and revoke approvals.

High-value anti-scam line (include in every post and chat): Always verify a token by its mint address (not the name or logo). If the mint doesn't match, don't buy.

Onboarding Checklist

Use this as your baseline "done-right" setup before you buy, swap, or interact with DeFi.

Install a wallet safely

• Download from the official app store or official website only.
• Verify you are on the correct domain before installing (no extra letters, no dashes).
• Create a new wallet and write the seed phrase down offline.

Backups that actually work

• Write the seed phrase on paper (or a dedicated metal backup).
• Store backups in two separate secure locations (fire/theft resilience).
• Do not store seed phrases in screenshots, notes apps, email drafts, or cloud storage.

First funding steps

• Buy SOL/crypto via a reputable on-ramp or exchange; send to your wallet.
• Start with a small amount for learning (fees + first swaps).
• Double-check the receiving address character-by-character (or scan QR).

First swap safety

• Use known aggregators/DEXs (example: Jupiter).
• Paste the token mint address (do not rely on search by name).
• Start small and confirm the output token is correct before increasing size.
• Set conservative slippage; if a swap requires unusually high slippage, stop and investigate.

Ongoing habits

• Use bookmarks for wallet, explorer, and swap tools.
• Keep only spending money in the daily wallet.
• Review connected apps/permissions regularly and revoke what you do not recognize.

Seed Phrase & Key Management

Your seed phrase (recovery phrase) is the master key to your funds. If anyone gets it, they can drain your wallet, and you typically cannot reverse it.

Non-negotiables. Never type your seed phrase into a website, Google Form, Discord DM, or "wallet verification" page. Legitimate services will never ask for it. If someone asks, it is a scam.

Recommended setup for most people

• Daily wallet: for small balances and routine swaps.
• Vault wallet: for long-term holding (used rarely).
• Optional: hardware wallet for the vault (adds physical confirmation).

Storage best practices

• Write the seed phrase clearly. Use block letters. Avoid smudging.
• Make two backups. Store in separate secure locations.
• Do not "test" the seed phrase by entering it into random tools; test only by restoring into your official wallet app on a clean device (offline if possible).
• Do not share your screen or camera when the seed phrase is visible.

If you already exposed your seed phrase

Assume the wallet is compromised. Create a brand-new wallet on a clean device and move funds immediately. Then review and revoke connected app permissions from the old wallet.

Device & Account Security

Your wallet is only as safe as the device and accounts around it. Many compromises happen through email, SIM swaps, fake support, or malware - not through "breaking the blockchain."

Passwords and 2FA

• Use a password manager and unique passwords for email, exchanges, and social accounts.
• Turn on 2FA everywhere. Prefer authenticator apps or security keys over SMS when possible.
• Protect your primary email account like it holds your bank vault - because it often does.

SIM swap defense

• Ask your mobile carrier to add a SIM-swap/port-out PIN (account takeover protection).
• Do not rely on SMS codes for high-value accounts if alternatives exist.
• Be cautious with public personal info (birthday, address, phone) that attackers use for verification.

Computer and browser hygiene

• Keep your OS and browser updated; enable automatic updates.
• Install wallet extensions only from official sources; avoid look-alike extensions.
• Limit browser extensions; each one is a potential attack surface.
• Use separate browser profiles: one for crypto, one for daily browsing.
• Avoid downloading pirated software; it is a common malware delivery method.

Rule of thumb. If a site asks you to "fix" a wallet issue by entering your seed phrase, it is not fixing anything. It is draining your wallet.

Transaction Safety

Every transaction is a signed instruction. Signing is consent. Your job is to understand what you are consenting to before you approve.

Before you send funds

• Confirm the receiving address from an independent source (not a DM).
• Send a small test amount first, then the full amount.
• Watch for clipboard malware: paste the address and verify the first/last 4-6 characters match.
• Assume transactions are irreversible once finalized.

Before you connect a wallet to a site

• Use bookmarks or type the URL; do not click "sponsored" ads for swap sites.
• Read the wallet prompt carefully. If it requests unexpected permissions, cancel.
• If you do not understand the transaction, do not sign it.

Approvals, delegates, and permissions (plain-English)

Many chains use permissions that allow a dApp to move tokens later (sometimes called approvals, delegates, or allowances). Even if a permission was granted yesterday, it can be used tomorrow. Review and revoke connected apps/permissions regularly inside your wallet settings or trusted permission tools.

Verify Tokens & Pools

Token names and logos are easy to copy. On-chain identifiers are not. Always verify a token and its pool using explorers and exact addresses.

The 3-step verification method

Step 1: Get the official mint address from a trusted source (project website, pinned post, verified account).
Step 2: Open the mint on an explorer and confirm the address matches exactly.
Step 3: When swapping, confirm the selected token mint matches the mint you verified.

> Anti-scam reminder. If the mint address does not match, it is not the token - no matter what the logo says.

Tip: For your own token/project, publish the mint address in one consistent place (website + X bio + pinned post) so users can verify quickly.

Swap Safety (Jupiter + Raydium style)

Swapping is the most common activity for new users - and also the most common point of failure. Most problems come from phishing sites, wrong token selection, or signing a malicious transaction.

Safe swap workflow

• Use official tools and bookmarks (example: Jupiter, Raydium).
• Paste the mint address to select the token (do not rely on name search).
• Start small and confirm output before increasing size.
• Set conservative slippage. If a swap requires unusually high slippage, stop and investigate.
• Avoid unknown routes/programs unless you understand the risk.

What to watch on the confirmation screen

• Am I on the correct domain?
• Is the input token correct?
• Is the output token correct (mint match)?
• Is the amount correct (watch decimals)?
• Are fees reasonable?
• Does the transaction mention unknown programs or permissions I didn't expect?

Common trap: fake swap sites. Scammers buy ads and create look-alike pages for wallet and swap tools. The URL is the giveaway. Bookmark official sites and avoid clicking ads.

DeFi Hygiene (advanced users)

As you move from basic swaps into DeFi, the risk becomes more about permissions, smart-contract risk, liquidity risk, and operational discipline. Use this section as your "advanced checklist" to stay clean on-chain.

1) Wallet isolation and compartmentalization

• Keep a dedicated DeFi wallet separate from your savings/vault wallet.
• Use separate wallets for: daily spending, DeFi experimentation, and long-term holding.
• Treat new dApps like untrusted software until proven otherwise; start with small limits.

2) Approval hygiene (the #1 DeFi habit)

• Prefer permissions that are limited in amount and scope when available.
• Review connected apps/approvals monthly (or after every new dApp).
• Revoke anything you do not recognize or no longer use.
• If a dApp requires broad or unlimited permissions without a clear reason, do not proceed.

3) Signature hygiene and transaction simulation

• Read transaction prompts - do not "click through."
• Be suspicious of transactions that include many instructions unrelated to what you intended.
• When possible, simulate or preview transactions using trusted tools before signing.
• If a site asks you to sign repeatedly, slow down and verify what is changing.

4) Slippage, MEV, and execution risk

• High slippage can hide bad pricing or route manipulation. Use conservative slippage settings.
• MEV and bots can worsen execution during volatile moments. Avoid swapping large size in thin liquidity.
• If price impact is high, break trades into smaller chunks or wait for better liquidity.

5) Liquidity pools and yield risk

• Providing liquidity can lead to impermanent loss; returns are not guaranteed.
• New pools can be manipulated; avoid pools with suspiciously high yield and low transparency.
• Verify token mints and pool addresses before depositing liquidity.

6) Stablecoins and bridge discipline

• Stablecoins can depeg. Treat them as "low volatility," not "no risk."
• Bridges add another failure point. Use reputable bridges only, and keep bridged balances small.
• Confirm you are using the official bridge domain; phishing is common.

7) Operational discipline (what pros do)

- Keep a written "official links list" and use bookmarks only.
- Update devices regularly and keep crypto activity in a separate browser profile.
- Keep your vault wallet offline as much as possible (hardware wallet recommended).
- If you run a team: use multisig for treasury funds and document who can sign what.

Advanced default response. If anything feels off: pause. Do not sign. Do not continue the conversation. Navigate to the official site from a bookmark, verify addresses, and ask questions publicly in the official community channel.

Scam Watch: the most common traps

This section is designed to make you hard to scam. Most attacks follow predictable scripts.

Fake support DM
Someone messages you pretending to be Phantom, Jupiter, Raydium, Solscan, or the project team. They push you to "verify" your wallet, "sync" your account, or "fix" a stuck swap. They ask for your seed phrase or want you to sign a transaction.

Airdrop bait
You receive tokens you didn't ask for and a link to "claim." The claim site drains your wallet when you connect or sign.

Giveaway / doubling scam
"Send 1 SOL and receive 2 SOL back." No legitimate project runs giveaways like this.

Look-alike tokens
A token uses the same name/logo as a real project. The mint address is different.

Malicious links in comments
A scammer replies under a real post with a fake link and urgency (limited time, last chance).

Scam Watch: advanced attacks and red flags

As you move from basic swaps into DeFi, the risk becomes more about permissions, smart-contract risk, and advanced social engineering.

- Drainers disguised as "mint," "claim," "staking," or "verification" pages.
- Fake browser extensions that replace addresses or capture seed phrases.
- Rug pulls and liquidity pulls on new tokens/pairs.
- Fake "investment groups" promising guaranteed returns.
- Screenshots-based scams (edited transaction confirmations, fake balances).
- AI deepfakes and voice cloning that impersonate founders, influencers, or support.
- Fake support chatbots that walk you into signing malicious transactions.

AI-powered scams and impersonation (what to do)

AI makes scams look professional and "legit." Use verification - not appearances - as your security control.

- Do not treat video/audio as proof. Verify via official channels you already know.
- If you get an urgent call, hang up and call back using an official number you find yourself.
- Do not trust screenshots as proof; rely on explorers and your wallet activity.
- If pushed to DMs, stop. Ask publicly in the official community channel.

The safest default response. Pause. Do not click. Do not sign. Do not send. Navigate to the official site from a bookmark, verify addresses, and ask questions publicly. If uncertain, walk away and revisit later.

If You Think You've Been Scammed

Speed matters. The goal is to stop further loss, protect remaining funds, and preserve evidence.

Immediate actions (first 10 minutes)

• Disconnect your wallet from the site and close the browser tab.
• If you signed something you did not understand, assume risk is ongoing.
• Move remaining funds to a new wallet (created on a clean device) if you believe your wallet is compromised.
• If malware is suspected, stop using the device for crypto until it is cleaned or rebuilt.

Stabilize and document (same day)

• Take screenshots of the site, the transaction prompt, and any DMs/emails (do not share your seed phrase).
• Save transaction signatures/links from the explorer.
• Review connected apps and revoke anything you don't recognize.
• Change passwords for email and exchanges; rotate 2FA; add carrier port-out protection.

Do not pay "recovery" services. After a scam, criminals often follow up with fake recovery agents who promise they can retrieve funds for a fee. This is a second scam. Treat it as hostile.

Resources and Official Links

Bookmark these sites. Navigate by bookmarks - not by ads, DMs, or random search results.

Safety rule: Always verify AKSOL by the mint address 2ENXn…wvSK (not the name/logo). If the mint doesn't match, don’t buy.

Resource	Official link
Wallet (official)	Phantom official site Phantom download page
Swap (simple)	Jupiter swap Raydium swap
Verify on-chain	Solscan - AKSOL mint Solscan - Raydium pool/pair
Chart / price	DEXScreener - AKSOL/SOL
Alaska Crypto Financial	Website Support: akcyptofinancial@gmail.com X / updates Community: r/AlaskaCryptoHub Discord

Quick QR access (optional):

DEXScreener chart

Solscan mint page

Glossary (Definitions)

Quick definitions to help you read token pages, swaps, and security warnings.

Term	Definition
Address	Public destination for tokens. Looks like a long base58 string.
Approve	Grant a smart contract permission to spend tokens from your wallet.
DEX	Decentralized exchange. A swap venue like Jupiter, Raydium, Orca.
dApp	Web/app that interacts with smart contracts using your wallet.
Explorer	Blockchain search tool (Solscan) to verify token mints, accounts, and transactions.
Faucet	Free testnet tokens (devnet). Not for mainnet.
Gas / Fees	Transaction fees paid to the network (SOL on Solana).
Hardware wallet	A physical device that stores keys offline for strong security.

Glossary (Definitions)

Term	Definition
HODL	Slang: hold long-term through volatility.
Liquidity	How easily you can buy/sell without moving the price much.
Liquidity pool	A pool of tokens used for swaps; provides trading liquidity.
Mint address	Unique identifier for a token. Treat it as the token's true ID.
Phishing	Fake sites/messages that trick you into revealing secrets or signing malicious transactions.
Seed phrase	12-24 words that restore your wallet. Anyone who has it can take everything.
SIM swap	Attack where someone takes over your phone number to intercept codes/resets.
Slippage	Allowed price movement during a swap. High slippage can hide bad pricing.

Glossary (Definitions)

Term	Definition
Stablecoin	Token designed to track a stable value (often $1).
Staking	Locking tokens to support a network/app to earn rewards.
Token account	Account that holds a specific token in your wallet.
Token symbol	Short label (AKSOL) - can be faked. Always verify mint.
Verify	Cross-check mint + pool addresses on Solscan/DEXScreener before swapping.
Wallet	App that holds keys, signs transactions, and stores your tokens.
Yield	Return earned from staking, lending, or providing liquidity. Higher yield usually means higher risk.

AKSOL Verification Card

Use this page to verify AKSOL before you swap. If anything does not match, stop.

Safety rule: Always verify AKSOL by the mint address `2ENXn…wvSK` (not the name/logo). If the mint doesn't match, don’t buy.

AKSOL Verification Card	

1) Your AKSOL identifiers (most important)	AKSOL token mint address (verify every time):
	`2ENXnAQFQAhQ5kF49SSj9Jm4tPb2fShYs4DDuVdtwvSK`
	
	Raydium pool / pair address (AKSOL/SOL):
	`BMCgy8EkKiqEtQNjx88CqdUd6u4Y15QCCCDBqNoUMNVb`

2) Verify on-chain (Explorer links)	Solscan - AKSOL token (mint) page Solscan - Raydium pool/pair address page
3) Track price + chart (public)	DEXScreener - AKSOL/SOL chart (pair)
4) Where users can swap (public, simple)	Jupiter swap (paste mint to find AKSOL) Raydium swap (paste mint to select the token)
5) Wallet download (official only)	Phantom official site Phantom download page

Pro tip: Save the mint + pool addresses in your notes and verify them again anytime you reinstall a wallet or use a new device.

Stay Connected

If you want updates, education, and Alaska-focused crypto conversations, here are the official channels.

Stay connected	
Website	https://alaskacrypto.financial
Support	akcyptofinancial@gmail.com
X / updates	https://x.com/AKCFinancial
Community	r/AlaskaCryptoHub
Discord	https://discord.gg/m7F6ZX88

Next steps
1) Save the Resources page as a bookmark.
2) Share this guide with someone new to crypto.
3) If you have questions, ask them in r/AlaskaCryptoHub (public and searchable).