The Scammers Who Stole $9.9 Billion in 2024 Were Not Hackers -- They Were Storytellers

Pig Butchering. Fake Exchanges. Approval Phishing. Wallet Drainers. The Eight Scam Types and the One Rule That Stops All of Them. -- Q2 2026

In 2024, crypto scammers stole approximately $9.9 billion from victims globally -- a figure that represents not a single dramatic hack of a major exchange or protocol but the accumulated result of thousands of individual deceptions, each one targeting a person who trusted the wrong message, clicked the wrong link, or believed the wrong promise. The Chainalysis 2025 Crypto Crime Report confirmed that the dominant scam category by stolen value is not technical exploits but social engineering -- the art of manipulating human psychology to convince people to voluntarily hand over their assets or the access credentials that protect them. The most sophisticated scam operation documented in 2024 was not a team of elite hackers who broke into exchange systems. It was a network of organized criminal compounds -- primarily in Southeast Asia -- where tens of thousands of workers, many of them trafficking victims themselves, spent months building fake romantic relationships with victims across the world before slowly convincing those victims to invest in fraudulent crypto platforms that would steal everything they deposited. This category of crime -- called pig butchering because the criminals fatten their victims with trust before slaughtering them financially -- generated an estimated $3.6 billion in 2024 alone. The technical complexity of most crypto scams is low. The psychological complexity is high. The scammers who stole $9.9 billion in 2024 understood human nature better than they understood cryptography. They exploited loneliness, greed, urgency, and trust -- the same vulnerabilities that con artists have exploited for centuries. The difference is that crypto transactions are irreversible. When your bank account is defrauded, your bank can often reverse the transaction. When your crypto wallet is drained, the blockchain is permanent. There is no customer service number to call. There is no chargeback. There is no appeal. The protection has to happen before the transaction, not after. This report gives you the complete framework for understanding how crypto scams work and the specific practices that protect your assets.

01 -- PIG BUTCHERING: THE MOST DANGEROUS SCAM IN CRYPTO HISTORY

Pig butchering -- known in Mandarin as sha zhu pan, meaning slaughtering the pig -- is the most financially devastating scam category in the crypto ecosystem, responsible for billions of dollars in annual losses and an estimated tens of thousands of victims globally in 2024 alone. Understanding how pig butchering works in detail is the most important scam education any crypto investor can receive, because the scam is so psychologically sophisticated that victims frequently do not realize they have been scammed until after they have lost everything.

The pig butchering scam begins with an unsolicited contact -- a wrong number text message, a LinkedIn connection request, a dating app match, or a random social media message -- that appears innocent and coincidental. The scammer introduces themselves as an attractive, successful individual who made contact by apparent accident. Over the following days, weeks, or months, the scammer builds a genuine-seeming relationship with the victim -- asking questions, sharing personal details, expressing romantic interest, and establishing emotional trust through consistent, attentive communication.

Once the emotional relationship is established, the scammer casually mentions that they have been earning exceptional returns through a crypto investment platform that a family member or financial advisor introduced them to. They are not pressuring the victim to invest -- they mention it as an aside, something they have been doing quietly that has been going very well. Over subsequent conversations, the scammer shares screenshots of impressive returns, explains that the platform uses a sophisticated trading algorithm, and eventually offers to help the victim set up an account and make their first investment.

The victim deposits a small amount -- $500 or $1,000 -- and sees immediate returns on the fraudulent platform. Encouraged, they deposit more. The platform shows growing balances. When the victim tries to withdraw a small amount, it works -- the scammers allow early withdrawals to build confidence. As the victim deposits larger amounts, the scammer introduces a tax requirement, an insurance fee, or a withdrawal verification payment that must be paid before the funds can be released. The victim, having already invested their savings and emotionally committed to the relationship, pays the additional fee. The platform then becomes inaccessible and the scammer disappears. Everything is gone.

> ***PIG BUTCHERING PATTERN: Unsolicited contact appears innocent. Weeks or months of relationship building. Casual mention of crypto investment platform. Small successful withdrawal to build confidence. Escalating deposits. Withdrawal fee trap. Platform disappears. $3.6 billion stolen in 2024 alone. The entire scam depends on emotional trust built before any financial request is made.***

02 -- THE EIGHT SCAM TYPES EVERY CRYPTO INVESTOR MUST RECOGNIZE

Beyond pig butchering, the crypto scam landscape in 2026 includes seven additional major categories that every investor needs to be able to recognize on sight. Each category exploits a different psychological vulnerability and requires a different defensive response.

Phishing attacks are the most common scam type by volume -- emails, text messages, and social media messages that impersonate legitimate exchanges, wallets, or support services and direct victims to fake websites where they enter their login credentials or seed phrases. A phishing email from what appears to be Coinbase asking you to verify your account will have a URL that looks almost identical to coinbase.com but contains a subtle misspelling -- coinba5e.com, co1nbase.com, or coinbase-support.com. Every crypto exchange in the world will never ask you to enter your seed phrase on a website.

Approval phishing is a more technically sophisticated variant where scammers trick victims into signing a malicious blockchain transaction that grants the scammer unlimited access to the victim wallet. Approval phishing typically occurs through fake DeFi platforms, fake NFT minting sites, or malicious

links sent through Discord and Telegram. The transaction the victim signs looks like a routine DeFi interaction -- connecting a wallet to a platform. The actual transaction grants the scammer token approval to transfer all assets in the wallet. Chainalysis estimated that approval phishing stole approximately $2.7 billion in 2023.

Fake exchange scams involve fraudulent platforms that mimic legitimate exchanges and accept deposits that can never be withdrawn. The fraudulent exchange typically ranks highly in search results through paid advertising, has a professional-looking website, and may even allow small withdrawals initially to build victim confidence. The platform becomes inaccessible or imposes withdrawal requirements that cannot be met once a significant deposit has been made.

Rug pulls are scams where the developers of a crypto project -- a new token, an NFT collection, or a DeFi protocol -- abandon the project and take investor funds after building sufficient hype and liquidity. The project is marketed aggressively, early investors see price appreciation that creates FOMO, and a wave of new investors buy in at higher prices. The developers then sell their own holdings simultaneously, crashing the price, and disappear with the funds.

Giveaway scams impersonate prominent crypto figures -- Elon Musk, Michael Saylor, Brian Armstrong, Vitalik Buterin -- and promise to double any crypto sent to a specific wallet address as part of a promotional giveaway. The victim sends crypto expecting to receive twice the amount back. Nothing is returned. These scams operate primarily through fake YouTube livestreams, fake Twitter accounts with verified-looking profiles, and fake news articles. No legitimate crypto figure has ever run a send me crypto and I will send you back double promotion.

SIM swapping is a sophisticated attack where a scammer convinces your mobile carrier to transfer your phone number to a SIM card the scammer controls. Once the scammer has your phone number, they can intercept SMS-based two-factor authentication codes and reset your exchange account passwords. SIM swap attacks have stolen millions of dollars from high-profile crypto investors and are particularly dangerous because they bypass the security measures that most investors believe protect them.

Malware and clipboard hijacking attacks install software on your computer that monitors your clipboard and replaces crypto wallet addresses you copy with the addresses of the attacker. When you intend to send Bitcoin to your hardware wallet, you copy your wallet address, and the malware silently replaces it with the attacker address. You paste what you believe is your own address and send the Bitcoin to the attacker. Always verify the full wallet address character by character before confirming any transaction.

03 -- THE ONE RULE THAT STOPS ALL SCAMS

Every crypto scam in existence -- pig butchering, phishing, approval phishing, fake exchanges, rug pulls, giveaway scams, SIM swapping, malware -- ultimately depends on one of three actions by the victim: sharing their seed phrase or private keys with someone else, sending crypto to an address they have not independently verified through multiple channels, or signing a blockchain transaction without understanding exactly what it authorizes.

The one rule that stops all scams is this: your seed phrase never leaves your possession, you never send crypto based on a message you received rather than a decision you independently made, and you

never sign a transaction you do not fully understand. This rule sounds simple. Its consistent application eliminates virtually all crypto scam vulnerability.

Your seed phrase -- the 12 or 24 word recovery phrase that controls access to your self-custody wallet -- is the master key to every asset in that wallet. Anyone who has your seed phrase has your assets. No legitimate exchange, wallet provider, support service, or financial advisor will ever ask you for your seed phrase under any circumstances. If anyone asks you for your seed phrase, they are a scammer. This is not an exaggeration. It is an absolute rule with no legitimate exceptions. Write your seed phrase on paper, store it in a physically secure location, and never type it into any website, application, or message for any reason.

The verification principle applies to every crypto transaction. Before sending any amount of crypto to any address, verify that address through a channel completely independent of the message that provided it. If someone sends you a wallet address through Telegram, verify it through the official website of the service, through a phone call to the verified number, or through a face-to-face confirmation. The extra 60 seconds of verification has never cost anyone their assets. The failure to verify has cost many people everything.

> ***THE ONE RULE: Your seed phrase never leaves your possession. Never send crypto based on a message you received. Never sign a transaction you do not fully understand. These three practices eliminate virtually all crypto scam vulnerability. No legitimate service will ever ask for your seed phrase. If someone asks for your seed phrase they are a scammer. No exceptions.***

04 -- HARDWARE WALLETS: THE PHYSICAL BARRIER THAT STOPS REMOTE ATTACKS

A hardware wallet is a physical device -- typically a USB-sized device from manufacturers Ledger or Trezor -- that stores your private keys in a secure chip that is never exposed to your computer or the internet. When you want to send crypto from a hardware wallet, the transaction is signed inside the device using the private key stored in the secure chip, and only the signed transaction is transmitted to the blockchain. The private key itself never leaves the device.

The hardware wallet physical security model defeats every remote attack category in the crypto scam landscape. A phishing website that captures your exchange password cannot access assets in a hardware wallet. Malware that monitors your clipboard cannot sign transactions without physical confirmation on the hardware wallet device. A SIM swap that compromises your phone number cannot authorize hardware wallet transactions. Approval phishing requires you to physically confirm the transaction on the hardware device -- giving you a moment to review what you are signing before it is authorized.

Ledger hardware wallets are the most widely used in the world with over 6 million units sold. The Ledger Nano X supports over 5,500 cryptocurrencies and connects to your computer via USB or Bluetooth. The Trezor Model T is the primary alternative with a touchscreen interface and open-source firmware that allows independent security auditing. Both devices cost approximately $70 to $200 and provide security infrastructure that is appropriate for any portfolio size -- from a beginner with $500 in crypto to an

institutional investor with $10 million in holdings.

The CLARITY Act Section 605 confirmed in permanent federal statute that every American has the legal right to hold their own crypto in a self-hosted wallet for lawful purposes. Hardware wallets are the most secure implementation of that right. Buying a hardware wallet and moving your long-term holdings off exchange is the single highest-impact security improvement most crypto investors can make in 2026.

05 -- TWO-FACTOR AUTHENTICATION AND ACCOUNT SECURITY BEST PRACTICES

For assets held on exchanges -- the trading float you keep for active transactions -- two-factor authentication is the most important account security practice. Two-factor authentication requires a second verification step beyond your password when logging in or withdrawing funds. The three types of two-factor authentication available on most exchanges are ranked here from weakest to strongest.

SMS-based two-factor authentication -- where a code is sent to your phone number -- is the weakest form of 2FA because it is vulnerable to SIM swap attacks. If a scammer can convince your mobile carrier to transfer your phone number to their SIM card, they can intercept your SMS verification codes. Do not use SMS-based 2FA for any exchange that holds significant crypto assets. Most major exchanges now allow you to disable SMS 2FA in favor of stronger alternatives.

Authenticator app-based two-factor authentication -- using Google Authenticator, Authy, or Microsoft Authenticator -- generates time-based one-time passwords that are stored on your device rather than sent via SMS. Authenticator app 2FA is significantly more secure than SMS 2FA because it is not vulnerable to SIM swapping. The codes exist only on your physical device. Enable authenticator app 2FA on every exchange account you use and back up your authenticator codes securely in case you lose your device.

Hardware security key authentication -- using a YubiKey or similar FIDO2 hardware key -- is the strongest form of 2FA available. A hardware security key is a physical USB device that you plug in or tap against your phone to verify your identity. It cannot be phished because the authentication is tied to the specific website domain -- a fake Coinbase website cannot use your YubiKey authentication because the domain does not match. For investors with significant exchange holdings, a hardware security key is the gold standard of account security.

06 -- RED FLAGS: THE WARNING SIGNS THAT IDENTIFY EVERY SCAM

The most practical scam protection is the ability to recognize the warning signs that are present in every scam, regardless of its specific category. Training yourself to identify these red flags and treat them as automatic stop signals eliminates the cognitive vulnerability that scammers exploit.

Urgency is the most universal scam red flag. Scammers create artificial time pressure because they know that victims who have time to think, research, and consult with others will often recognize the scam before completing the transaction. Any message that includes phrases like this offer expires in 24 hours, you must act now to protect your account, or your funds will be seized if you do not respond

immediately is almost certainly a scam. Legitimate financial services do not require instant decisions under artificial deadlines.

Guaranteed returns are the second universal red flag. No legitimate investment offers guaranteed returns. Bitcoin, Ethereum, Solana, and every other crypto asset can decline in value. Any platform or person who promises you a specific return -- 1% per day, 20% per month, double your money in 30 days -- is running a scam. The promised returns may be paid initially using funds from new victims -- the classic Ponzi structure -- but the platform will eventually collapse and take all remaining deposits with it.

Unsolicited contact that escalates to financial requests is the pig butchering red flag. If someone contacts you without prior relationship -- through any channel -- and over time introduces a financial opportunity, treat the entire interaction with maximum skepticism regardless of how genuine the relationship feels. The months of relationship-building in pig butchering scams are specifically designed to make the eventual financial request feel trustworthy. The feeling of trust is the product of deliberate manipulation.

07 -- CONCLUSION: THE BLOCKCHAIN IS PERMANENT -- YOUR PROTECTION MUST COME FIRST

The $9.9 billion stolen from crypto investors in 2024 was not lost to technical failures. Blockchain technology did not fail. The cryptography did not break. The consensus mechanisms were not compromised. The assets were lost because human beings were deceived into taking actions that transferred those assets to criminals -- actions that the blockchain faithfully recorded and made permanent.

The irreversibility of blockchain transactions is simultaneously the property that makes crypto valuable as a censorship-resistant store of wealth and the property that makes crypto security non-negotiable. Your bank can reverse a fraudulent transaction. The blockchain cannot. Your protection must happen before you sign any transaction, not after.

The complete security framework this report has presented -- recognizing pig butchering and the seven other major scam types, applying the one rule that stops all scams, using a hardware wallet for long-term holdings, enabling authenticator app 2FA on exchange accounts, and training yourself to recognize the red flags of urgency, guaranteed returns, and unsolicited financial requests -- is not complex or expensive to implement. It requires awareness, discipline, and the consistent application of a small number of practices that experienced crypto investors follow as second nature. Proverbs 4:7 says wisdom is the principal thing -- therefore get wisdom. In crypto security, wisdom means understanding that no one will ever contact you with a genuinely good deal that requires your immediate action. The deals that protect your wealth are the ones you initiate yourself, with full understanding, through verified channels. Everything else is a scam.

> ***9.9 billion stolen in 2024. Most losses from social engineering not technical hacks. The one rule: seed phrase never leaves your possession, never send crypto based on a received message, never sign transactions you do not understand. Hardware wallet for long-term holdings. Authenticator app 2FA for exchange accounts. Red flags: urgency, guaranteed returns, unsolicited contact. The blockchain is permanent. Protection must come first.***