■ CRYPTO & DIGITAL ASSET SCAMS

A Comprehensive Intelligence Report & Educational Guide

Edition 2024 | Volume I

Protecting individuals, investors, and institutions from the fastest-growing category of financial crime in the digital era.

$9.9B	5.6M+	1.5%
Lost in 2024 (est.)	Victims Reported	Recovery Rate

■ This report is compiled from FBI Internet Crime Complaint Center (IC3), Chainalysis Crypto Crime Report, FTC Consumer Sentinel, and global blockchain analytics. All figures are based on reported cases — actual losses are estimated to be 4–10× higher due to severe underreporting.

Prepared for: General Public, Investors, Regulators, Educators
Classification: Educational — Freely Distributable

Table of Contents

01 — Executive Summary

Cryptocurrency and digital asset fraud has become the defining financial crime of the 2020s. Once dismissed as a niche concern, crypto scams now represent the single largest category of financial fraud by total losses reported to global enforcement agencies. In 2024, the FBI's Internet Crime Complaint Center (IC3) recorded estimated losses exceeding **$9.9 billion** in the United States alone — a figure widely acknowledged to represent only 10–25% of actual victimization due to shame, ignorance, and jurisdictional barriers preventing reporting.

The threat landscape has evolved dramatically. Early crypto fraud was typified by crude Ponzi schemes and fake Initial Coin Offerings (ICOs). Today, criminals deploy sophisticated, long-duration social engineering campaigns powered by organized crime syndicates operating from Southeast Asia, Eastern Europe, and West Africa. Artificial intelligence tools now enable voice cloning, deepfake video calls, and hyper-personalized phishing at industrial scale.

This report provides a comprehensive, evidence-based overview of the crypto scam ecosystem: how scams operate, who they target, what the data tells us, and — critically — how individuals and institutions can protect themselves. Knowledge is the most effective defence.

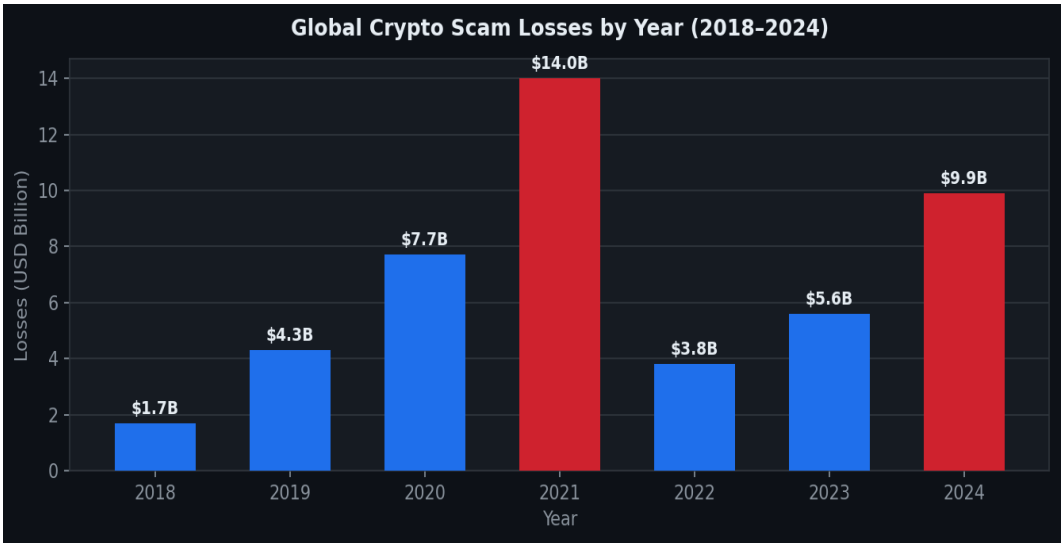

Figure 1: Global reported crypto scam losses 2018–2024. The 2022 dip reflects the broader crypto market crash reducing scam returns; losses rebounded sharply in 2023–2024.

02 — Understanding the Crypto Scam Landscape

Cryptocurrency's fundamental properties make it uniquely attractive to scammers and uniquely dangerous for victims. Understanding *why* crypto is weaponised this way is the foundation for understanding how to defend against it.

Why Crypto Is the Scammer's Preferred Tool

Property	Why Scammers Exploit It
Irreversibility	Once a blockchain transaction is confirmed, it cannot be reversed. There is no equivalent of a credit c
Pseudonymity	Wallet addresses are not inherently linked to real-world identities, making it easy to obscure the desti
Global Reach	Funds can be moved across international borders in minutes, defeating jurisdictional limitations on law
Speed	Transactions settle in seconds to minutes, giving victims almost no window to intervene once funds a
Complexity	Most victims have limited technical understanding of how blockchain works, making them easier to m
Perceived Legitimacy	The widespread media coverage of Bitcoin millionaires makes crypto investment narratives credible a

The Organised Crime Dimension

Modern crypto fraud is not typically the work of lone hackers. The United Nations Office on Drugs and Crime (UNODC) has documented sprawling scam operations in Myanmar, Cambodia, Laos, and the Philippines employing tens of thousands of workers — many trafficked and working under duress. These "scam compounds" operate like corporations, with sales floors, performance targets, training manuals, and HR departments. Individual "operators" may manage dozens of victim relationships simultaneously using scripted playbooks translated into 20+ languages.

■ KEY INSIGHT: The scammer you think is a romantic interest or investment advisor may be a trafficked worker reading from a script in a compound in Southeast Asia, supervised by organised crime and personally earning little of what they steal from you.

03 — The 7 Major Scam Types — In Depth

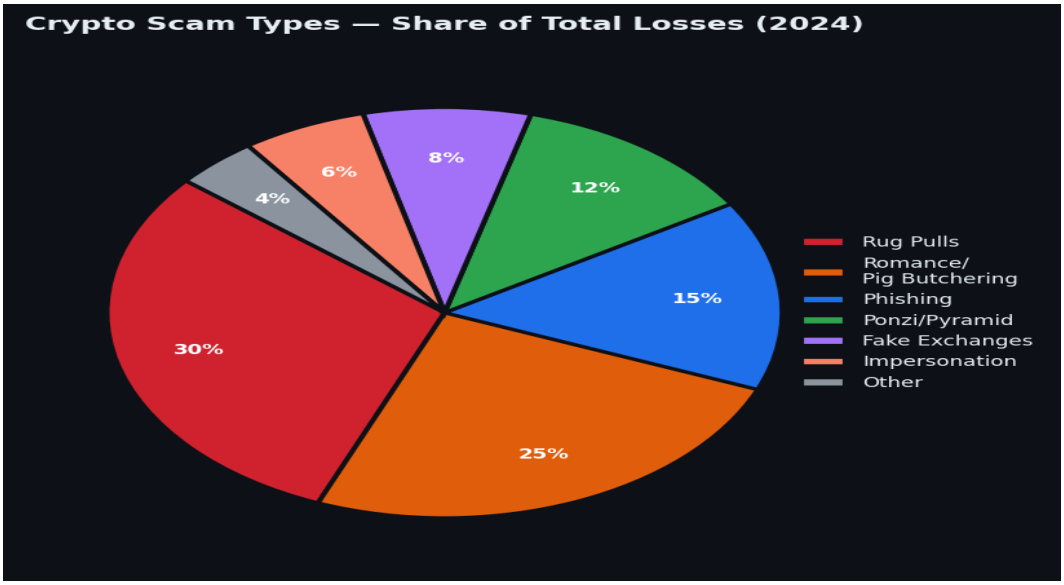

Figure 2: Distribution of crypto scam losses by category (2024 estimate).

■ 1. Rug Pulls

Rug pulls are the defining DeFi (Decentralised Finance) scam. Developers launch a cryptocurrency project, create artificial hype through social media, paid influencers, and fake trading volume, attract investor funds — then abruptly abandon the project and drain the liquidity pool.

- Team anonymity: developers use pseudonyms with no verifiable identity.
- Unaudited smart contracts: code that allows the developers to withdraw funds at will.
- Extreme FOMO marketing: "10,000x guaranteed," limited-time presale pressure.
- Fake partnerships: fabricated relationships with legitimate companies.
- Estimated 2023 losses: $1.1 billion across 1,200+ identified rug pulls.

■ 2. Pig Butchering (Sha Zhu Pan)

"Pig butchering" — a translation of the Chinese criminal slang sha zhu pan — involves months-long relationship building before the financial exploitation begins. The victim ("pig") is metaphorically "fattened" with trust before being "slaughtered." This is now the world's highest-grossing crypto scam category.

- Initial contact via wrong-number text, dating app, or LinkedIn.
- Romantic or friendship relationship built over weeks to months.
- Casual introduction to a "successful" trading platform.
- Small initial investments that appear to generate huge returns.
- The victim invests larger and larger sums; withdrawal is blocked by "taxes" or "fees."
- Average relationship duration before financial exploitation: 4.3 months.

■ 3. Phishing & Impersonation

Phishing attacks trick users into revealing wallet seed phrases, private keys, or exchange login credentials through fake websites, emails, or social media accounts that convincingly mimic legitimate services.

- Fake MetaMask, Coinbase, Binance login pages hosted on lookalike domains.
- Fake "support" agents on social media responding to complaints.
- Email campaigns claiming security breaches requiring immediate verification.
- Seed phrase harvesting through fake wallet recovery tools.
- NFT airdrop scams: free NFT transactions that drain wallets on signature.

■ 4. Ponzi & Pyramid Schemes

Classic investment fraud adapted for crypto. Early investors are paid using funds from new investors, creating the illusion of legitimate returns until the inevitable collapse.

- Guaranteed returns promises (crypto has no guaranteed returns).
- Returns paid in the project's own token, which is worthless.
- Referral commission structures that resemble MLM pyramid schemes.
- Fake "staking" or "yield farming" platforms with fabricated APY figures.
- Notable 2022 example: LUNA/TerraUSD collapse destroyed $45B in value.

■ 5. Fake Exchanges & Wallets

Fraudulent trading platforms that appear fully functional but are designed to steal deposits. Victims can often make small withdrawals initially to build trust, but larger withdrawals are always blocked.

- Professional-looking interfaces cloned from legitimate exchanges.
- "Trading profits" that exist only as numbers on a fake dashboard.
- Customer support who push victims to invest more to "unlock" withdrawals.
- Platforms that disappear entirely once sufficient deposits are accumulated.

■ 6. Celebrity & Influencer Impersonation

Scammers impersonate Elon Musk, MrBeast, crypto influencers, or even create AI-generated deepfake videos of them promoting fraudulent projects or giveaway scams.

- "Send 1 BTC, receive 2 BTC back" giveaway scams — never real.
- Deepfake YouTube livestreams of Elon Musk or other celebrities.
- Fake paid promotion announcements via hacked social accounts.
- AI voice clones used in phone calls to "personally endorse" investments.

■ 7. Smart Contract & Approval Scams

Technical exploits that weaponise how DeFi protocols work. Victims are tricked into signing malicious smart contracts that grant unlimited spending approval to scammer wallets.

- "Token approval" scams: one transaction empties your entire wallet.
- Fake DeFi protocols with backdoors allowing admin fund drainage.
- Clipboard hijacking malware that replaces copied wallet addresses.
- Flash loan attacks and oracle manipulation targeting DeFi protocols.

04 — Pig Butchering: The Billion-Dollar Romance Scam

Pig butchering deserves its own chapter. The FBI has described it as "the most devastating form of crypto fraud" by total victim losses. The 2023 IC3 report attributed over $3.5 billion in losses to this category. The psychological sophistication of these operations makes them effective against intelligent, educated, and financially sophisticated victims.

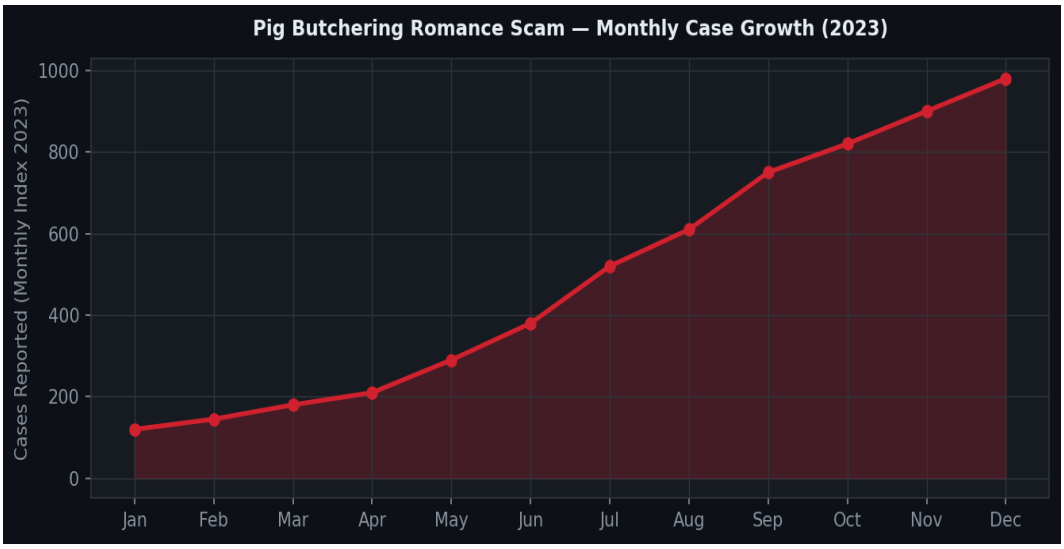

Figure 3: Monthly case report growth of pig butchering scams throughout 2023.

The Anatomy of a Pig Butchering Scam

Stage 1: Contact (Week 1-2)

A message arrives via WhatsApp, Telegram, Instagram, or a dating app. It often appears to be a wrong number: "Hi! Is this Sarah?" When corrected, the scammer is apologetic and charming. They may claim to be a professional — a doctor, entrepreneur, or overseas expat — with an attractive profile photo (often stolen from social media).

Stage 2: Relationship Building (Weeks 2-12)

Daily messages. Good morning texts. Thoughtful questions about your life, your family, your dreams. The scammer mirrors your interests, agrees with your opinions, and makes you feel uniquely understood. This phase can last months. The psychological bond formed is real, even if the person is not.

Stage 3: Introduction (Month 2-3)

Casually, your new friend mentions how they supplemented their income through crypto trading. They're reluctant to discuss it at first — they don't want to seem like they're bragging. Eventually they offer to show you their platform. "Just watch me do it. You don't have to invest anything."

Stage 4: Small Wins (Month 3-4)

You invest a small amount — perhaps $500. You can see it growing on the platform's dashboard. You withdraw $600 to confirm it's real. It arrives. The scammer's platform appears legitimate. This is the "fattening" phase.

Stage 5: Escalation (Month 4-5)

You invest more. The platform shows extraordinary returns. Your "advisor" (often a sophisticated fake trading app) encourages larger deposits. You liquidate savings. Some victims take out home equity loans. The dashboard shows you're a millionaire on paper.

Stage 6: The Slaughter

You request a significant withdrawal. Suddenly there are "taxes," "verification fees," "compliance holds." The platform requires you to pay a percentage of profits upfront before releasing funds. You pay — and the demands continue. Eventually, the platform and your contact disappear.

■ PSYCHOLOGICAL NOTE: Victims of pig butchering often know something is wrong before the end, but the emotional bond prevents them from acting. Scammers exploit cognitive biases including sunk cost fallacy ("I've already invested $200K — I can't stop now"), authority bias, and reciprocity. These are not personal failures; they are the result of skilled psychological manipulation by trained professionals.

05 — How Scammers Operate: The Anatomy of a Scam

Understanding the operational mechanics of crypto fraud helps victims recognise warning signs before irreversible damage occurs.

The Technology Stack

Component	Description	Red Flag
Fake Trading Platform	Custom-built web app showing fabricated balances and trades	Not listed on CoinGecko, CoinMarketCap, or app store
Money Mule Network	Legitimate-looking crypto wallets used to receive and launder proceeds	Wallet has no on-chain history before your deposit
Mixing Services	Tornado Cash-type mixers that obscure transaction trails	Funds sent to anonymous mixer within 24h of receipt
Communication Apps	WhatsApp, Telegram, WeChat preferred for encryption	Pressure to move from mainstream apps to obscure o
AI & Deepfakes	ChatGPT for scripting, voice cloning for phone calls	Inconsistent video quality; refuses live face-to-face cal
Crypto ATMs	Used for initial cash-to-crypto conversion by some victims	ATM with high fees near convenient locations

The Money Flow

Once a victim sends cryptocurrency, it typically moves through three to five wallets within minutes, often passing through a mixing service before being consolidated at an exchange in a jurisdiction with minimal KYC requirements. From there, funds are converted to stablecoins (USDT, USDC) and transferred to criminal infrastructure. The entire process can complete in under four hours, making law enforcement action almost impossible in real time.

Chain analysis firms like Chainalysis and TRM Labs have developed sophisticated graph analysis tools that can trace funds through multiple hops, and have assisted in some high-profile seizures — but this is the exception, not the rule. The technical sophistication required and international cooperation needed means most crypto fraud investigations go cold within weeks.

06 — Who Are the Victims? Demographic Analysis

A common misconception holds that crypto scam victims are exclusively elderly or technically unsophisticated. The data tells a more nuanced and important story.

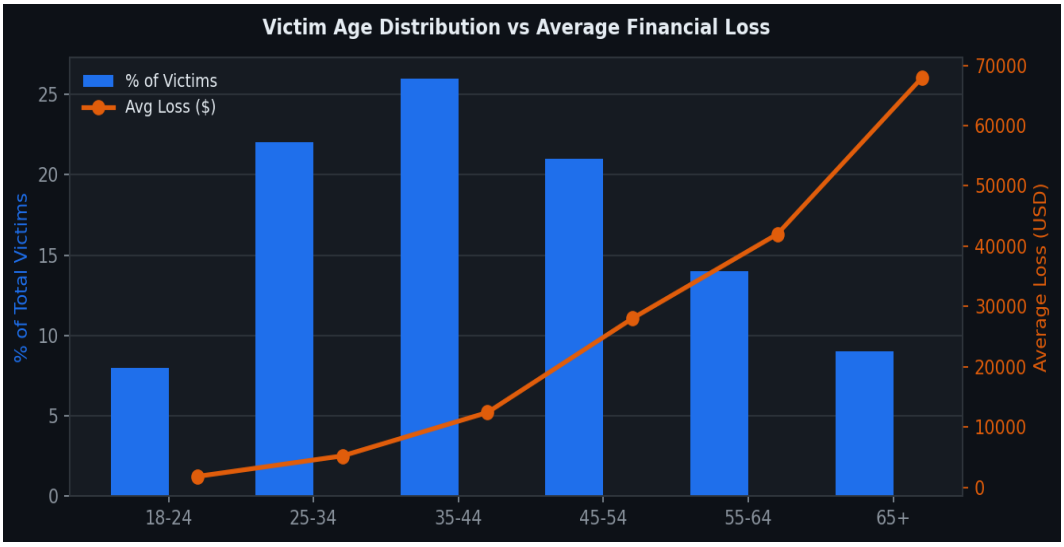

Figure 4: Victim distribution by age group vs. average financial loss per victim. While younger victims are more numerous, older victims lose significantly more per incident.

Key Demographic Findings

Metric	Finding	Source
Highest case count age group	35–44 years (26% of victims)	FBI IC3 2023
Highest average loss age group	65+ years ($68,000 avg loss)	FBI IC3 2023
Gender distribution	57% male, 43% female	FTC Consumer Sentinel 2023
Education level	38% hold bachelor's degree or higher	Stanford Internet Observatory
Prior crypto experience	61% had purchased crypto before	Chainalysis 2024
Reported to authorities	~40% of victims	FTC 2023
Sought mental health support	23% reported lasting psychological impact	Global Anti-Scam Org
Repeat victimisation	12% were scammed more than once	FBI IC3 2023

■ IMPORTANT: High intelligence and financial sophistication do not protect against crypto scams. Many victims are doctors, lawyers, engineers, and executives. Scammers do not target stupidity — they exploit loneliness, optimism, greed, trust, and the very human desire for connection and financial security.

07 — Red Flags: How to Spot a Scam

The following red flags are present in the vast majority of documented crypto fraud cases. A single red flag may have an innocent explanation. Multiple red flags together are a serious warning sign.

■ **Guaranteed or Unrealistically High Returns**	No legitimate investment guarantees returns. Promises of 20%, 50%, or 100%+ monthly returns are impossible in legitimate markets. Even the best hedge funds average 15-20% annually.
■ **Urgency and FOMO Pressure**	"This opportunity closes in 24 hours." "Only 3 spots left." Legitimate investments do not expire. Pressure to decide quickly is a manipulation technique.
■ **Unverifiable Team or Company**	If you cannot find the company registered with a financial regulator, and the team members have no verifiable professional history on LinkedIn or elsewhere, walk away.
■ **Withdrawal Fees and Taxes**	"You need to pay taxes/fees before we can release your withdrawal." This is almost universally a scam. Legitimate platforms deduct fees from withdrawals — they never require additional payments before releasing funds.
■ **Exclusive or Secret Platform**	"My uncle works at a special trading desk." "This platform is only available to private clients." Any platform not listed on major crypto tracking sites (CoinGecko, CoinMarketCap) and not regulated is almost certainly fake.
■ **Romantic Interest Who Mentions Crypto**	An online romantic interest who introduces crypto investment — regardless of how long you've known them — is the single most consistent warning sign of a pig butchering scam.
■ **Recovery Scams**	After losing money, beware of services promising to recover your funds for an upfront fee. This is a secondary scam targeting already-victimised individuals. Legitimate law enforcement and recovery professionals do not charge upfront fees.
■ **Requests to Move to Unusual Apps**	Pressure to move communication from mainstream platforms to obscure apps, or to use specific crypto wallets or platforms you've never heard of.

08 — Case Studies: Real-World Examples

Case Study A: The Romance Scam — $340,000 Lost

A 58-year-old retired nurse from Ohio was contacted via LinkedIn by a man claiming to be a Swiss-American oil engineer. Over four months of daily communication, they developed what she believed was a genuine romantic relationship. He introduced her to a crypto trading platform through which her $15,000 initial investment appeared to grow to $280,000 in two months. When she attempted to withdraw to cover a medical emergency, she was told she owed $47,000 in "profit taxes." She liquidated her retirement account. Total losses: $340,000. The platform vanished three weeks later.

■ LESSON: Multiple red flags present: romance + crypto introduction, extraordinary returns, withdrawal fee. The platform was not registered with any financial regulator.

Case Study B: The Fake Exchange — $1.2M Business Fraud

A small business owner in California moved his company's operating reserves into what appeared to be a premium crypto exchange recommended by a business contact on a professional forum. The exchange showed professional-grade charts and trading data, had a functional mobile app, and processed his first two withdrawals correctly. After depositing $1.2 million, the exchange suddenly required "enhanced verification" and demanded additional funds. All communication ceased within 72 hours.

■ LESSON: The contact who made the recommendation was a paid shill account. The exchange domain was registered six weeks before the first victim contact.

Case Study C: NFT Rug Pull — $50M Project Collapse

Evolved Apes, a 2021 NFT project, raised approximately $2.7 million from buyers before the anonymous developer "Evil Ape" disappeared with all funds. A planned fighting game was never developed. This followed the classic rug pull pattern: anonymous team, unaudited smart contract, community hype, sudden disappearance. Similar patterns played out in dozens of 2021-2022 NFT projects, collectively destroying billions in investor value.

■ LESSON: Despite blockchain transparency allowing full tracking of fund movements, the developer was never identified or prosecuted.

09 — What to Do If You Have Been Scammed

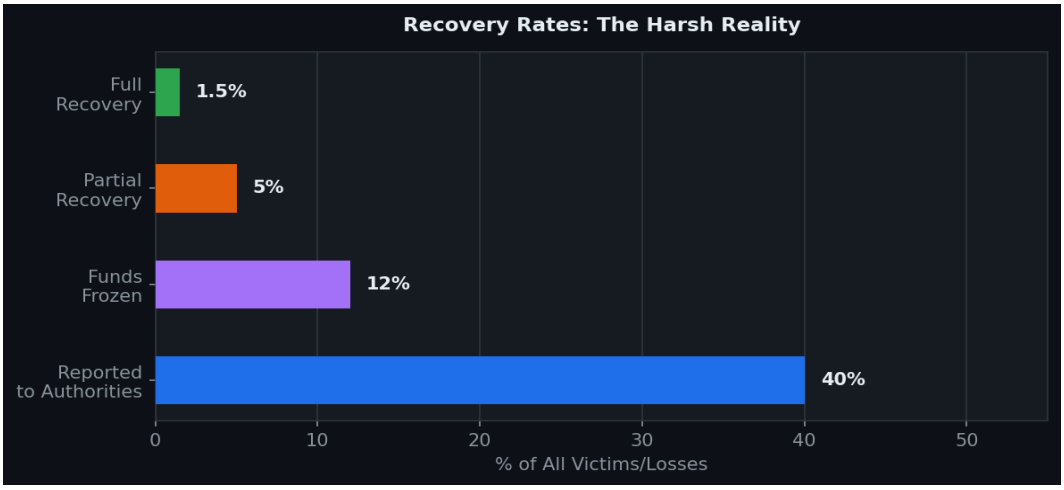

Figure 5: Recovery outcomes across reported crypto scam cases. Most victims never recover funds, making prevention the only effective strategy.

Immediate Actions (Within 24 Hours)

- STOP all further transfers immediately — do not send more funds for "taxes," "fees," or "verification."
- Document everything: screenshots of all communications, the platform URL, wallet addresses used, transaction IDs, email correspondence.
- Contact your bank or card issuer if you used fiat currency to purchase crypto — some chargebacks may be possible within 24-72 hours.
- Do NOT follow advice from anyone connected to the scam about "recovery" — this is almost always a secondary scam.
- Change all passwords and enable 2FA on financial accounts that may have been compromised.

Official Reporting Channels

Agency / Platform	Contact / URL	What to Report
FBI Internet Crime Center	ic3.gov	All internet-based fraud over $1,000
FTC (US)	reportfraud.ftc.gov	General fraud, identity theft
CISA (US Cyber)	cisa.gov/report	Phishing, account compromise
Your State AG	naag.org (directory)	State-level financial fraud
Chainalysis (Private)	chainalysis.com	Provide transaction data to aid tracing
EFCC (Nigeria)	0800-2255-3322	All online fraud involving NGN
Action Fraud (UK)	actionfraud.police.uk	All UK fraud and cybercrime
ACCC (Australia)	scamwatch.gov.au	All Australian scam reports
Interpol	interpol.int/Crimes	Cross-border organised crime cases

■ EMOTIONAL IMPACT: Crypto scam victims often experience grief, shame, anger, and depression comparable to bereavement. These are normal responses to genuine trauma. Contact the Global Anti-Scam Organisation (globalantiscam.org) or your national victim support service — talking to others who have experienced the same can be profoundly helpful. You are not alone and you are not stupid.

10 — Prevention Framework & Best Practices

Prevention is the only reliable protection. The following framework applies to individuals, families, and organisations engaging with cryptocurrency.

Individual Protection

- ✓ Never invest in any platform introduced by someone you have not met in person.
- ✓ Verify every platform on CoinGecko, CoinMarketCap, and your national financial regulator's register.
- ✓ Use only well-known regulated exchanges: Coinbase, Binance, Kraken, Gemini (verify regional availability).
- ✓ Enable 2FA (preferably hardware key, never SMS) on all exchange and wallet accounts.
- ✓ Keep large crypto holdings in cold (hardware) wallets: Ledger, Trezor.
- ✓ Never share your seed phrase or private key with anyone for any reason.
- ✓ Apply the 48-hour rule: wait 48 hours before any investment over $500.
- ✓ Talk to a trusted friend or family member before making significant crypto investments.

Due Diligence Checklist

- ✓ Is the platform registered with a financial regulator in its claimed jurisdiction?
- ✓ Can you independently verify the founding team's professional identity on LinkedIn?
- ✓ Has the smart contract been audited by a reputable firm (CertiK, Trail of Bits, OpenZeppelin)?
- ✓ Is the project's whitepaper technically coherent and written by professionals?
- ✓ Are there independently verifiable reviews from credible crypto journalists (not paid promoters)?
- ✓ Can you withdraw small amounts freely without fees or verification hurdles?
- ✓ Does the project have at least 6 months of transparent on-chain history?

Technical Security Practices

- ✓ Use a dedicated email address for crypto activities never shared elsewhere.
- ✓ Use a hardware security key (YubiKey) for exchange 2FA authentication.
- ✓ Never connect hardware wallets to unknown computers.
- ✓ Regularly review and revoke unused token approvals (revoke.cash).
- ✓ Use browser extensions like MetaMask's phishing detection and EAL.
- ✓ Never click crypto-related links in emails, even from known addresses.

✓ Run transactions through a simulation tool (Tenderly) before signing.

11 — Reporting Agencies & Global Resources

■■ United States

Organisation	Website	Jurisdiction
FBI Internet Crime Center (IC3)	ic3.gov	Primary federal cybercrime reporting
FTC Report Fraud	reportfraud.ftc.gov	Consumer fraud & identity theft
SEC Enforcement	sec.gov/tcr	Securities fraud & unregistered offerings
CFTC Whistleblower	whistleblower.cftc.gov	Commodity & derivatives fraud
FinCEN	fincen.gov	Money laundering concerns

■■ United Kingdom

Organisation	Website	Jurisdiction
Action Fraud	actionfraud.police.uk	National fraud & cybercrime reporting
Financial Conduct Authority	fca.org.uk/consumers/report-scam	Unauthorised financial services
National Crime Agency	nationalcrimeagency.gov.uk	Organised crime

■ Africa / Nigeria

Organisation	Website	Jurisdiction
EFCC Nigeria	efcc.gov.ng	Economic & financial crimes commission
ICPC Nigeria	icpc.gov.ng	Corruption & financial crimes
Interpol NCB Abuja	interpol.int	International cross-border cases

■ Global Resources

Organisation	Website	Jurisdiction
Global Anti-Scam Org	globalantiscam.org	Victim support & education
Chainabuse	chainabuse.com	Blockchain address reporting database
CryptoScamDB	cryptoscamdb.org	Scam address & domain database
Etherscan Token Approval	etherscan.io/tokenapprovalchecker	Revoke dangerous permissions

12 — Conclusion & Key Takeaways

Cryptocurrency represents a genuinely transformative financial technology. Its potential to democratise access to financial services, enable programmable value transfer, and create new economic models is real. But this same potential has been weaponised by criminal networks operating at industrial scale.

The scale of crypto fraud is not a reflection of the technology's fundamental flaws — it is a reflection of human vulnerability to social engineering, the irreversibility of blockchain transactions, and the lag of regulatory frameworks behind technological change. These gaps are being closed, but slowly.

In the meantime, the most effective protection available is knowledge. Understanding how these scams operate, recognising the red flags, applying rigorous due diligence, and maintaining healthy scepticism toward unsolicited investment advice are the behaviours that separate victims from non-victims.

The 10 Rules of Crypto Safety

01. If it sounds too good to be true, it is. Every time.

02. Anyone who contacts you first about a crypto opportunity is a scammer.

03. Your seed phrase is the key to your crypto. Guard it like your life savings — because it is.

04. Regulated, publicly listed exchanges only. If you've never heard of it, don't use it.

05. Never pay fees to unlock withdrawals. This is the clearest possible scam signal.

06. A romantic interest who mentions crypto is a pig butchering scammer.

07. No celebrity is giving away free crypto. All such claims are fraudulent.

08. Do not click links in emails, texts, or social media posts about crypto.

09. Cold storage for savings. Hardware wallets for significant holdings.

10. Talk to someone you trust before every significant investment decision.

The best investment you can make in crypto security costs nothing: share this report. The more people understand how these scams work, the harder they become to execute. Education is the most powerful tool available to reduce the $10 billion per year that organised crime extracts from families, communities, and economies worldwide.

Disclaimer: This report is compiled from publicly available data for educational purposes. Statistics are sourced from FBI IC3, FTC, Chainalysis Crypto Crime Reports, UNODC, and academic research. All figures represent reported cases and should be considered conservative estimates. This document does not constitute legal, financial, or investment advice.