Human Weakness at the Heart of Billion-Dollar Crypto Scams

Infosources™

August 23, 2025

The cryptocurrency world is facing a new wave of fraud and theft, not through the failure of its technology but through the exploitation of its users. Hackers and scammers are increasingly turning to social engineering — manipulating people into revealing sensitive information — to bypass even the most advanced blockchain systems. Billions of dollars have already been lost in 2025 through a mix of phishing, wallet compromises, and large-scale exchange breaches. The common thread is clear: human error and trust are becoming the weakest links in the chain.

A $91 Million Loss in a Single Click

One of the most striking cases came in late May, when a Bitcoin investor lost 783 BTC — worth $91 million — in a single transaction. The attacker impersonated support staff from a crypto exchange and a hardware wallet provider, deceiving the victim into giving up control of their funds. The stolen Bitcoin was quickly moved into Wasabi Wallet, a privacy-focused platform designed to obscure transaction trails, making recovery almost impossible.

> **Info**
> A crypto hardware wallet provider is a company that manufactures and sells physical electronic devices (hardware wallets) designed to securely store the private keys that provide access to your cryptocurrency funds.A hardware wallet provides an ultimate Security, vastly superior to software wallets ("hot wallets") on phones or computers, which are constantly connected to the internet and vulnerable to hacking. As well it is ideal for securely holding large amounts of cryptocurrency you don't need to trade daily. Ledger, Trezor, KeepKey are among major physical wallet providers.

Blockchain investigator ZachXBT, who uncovered the details, emphasized that users should treat every unsolicited email, call, or message as suspicious by default. He also noted that the attack coincided with the anniversary of another major theft, the $243 million Genesis creditor hack, though he ruled out the involvement of North Korea's Lazarus Group in this case.

Old Tricks in New Disguise: Ledger Scam Letters

This latest attack follows a broader trend of social engineering targeting hardware wallet users. In April, scammers mailed physical letters to Ledger customers, dressed up with the company's logo, address, and even reference numbers to look legitimate. The letters urged recipients to perform a "critical security update" by scanning a QR code and entering their 24-word recovery phrase.

For anyone less familiar: that phrase is essentially the master key to a wallet. Whoever has it, has full access to the funds. Ledger immediately warned users that it would never ask for such information. But the scam raised troubling questions, since Ledger's customer database was leaked back in 2020, exposing over 270,000 names, addresses, and phone numbers. The letters show how stolen data can fuel fraud years after the original breach.

Info

Seed phrases (also known as a secret recovery phrase). Just like private keys, seed phrases allow users to recover a wallet. For instance, if the wallet's PIN is forgotten or the respective device is lost or damaged. Seed phrases are a lot more user-friendly than private keys, as they're often 12-24 words. In contrast, private keys typically consist of 64 characters, including upper/lower case letters and numbers. Therefore, seed phrases make it simple to access a wallet when needed. Crucially, seed phrases must never be shared. Anyone with access to the seed phrase can also access the wallet. This is why hackers are constantly on the hunt for seed phrases.

When Code Is No Longer the Weakest Link

The $91 million theft and the Ledger scams are part of a bigger shift. According to Web3 security firm CertiK, more than $2.1 billion has already been stolen in 2025, mostly through phishing, wallet compromises, and human missteps. In contrast to the early years of decentralized finance, when hackers hunted for bugs in smart contracts and protocols, criminals now find it easier to trick people than to break code.

CertiK's co-founder, Ronghui Gu, summed it up: attackers always go for the weakest point. At first, that point was vulnerable code. Now, the vulnerability is people. From elderly investors tricked into sending hundreds of millions in Bitcoin, to seasoned traders misled by professional impostors, the pattern is repeating across the industry.

The Bybit Breach and the Lazarus Factor

This doesn't mean technical exploits are gone. The single largest incident of the year so far was the $1.4 billion hack of the Bybit exchange in February, attributed to North Korea's Lazarus Group. That one case alone accounts for more than 60% of this year's total crypto losses. But outside of such extraordinary attacks, the bulk of thefts are happening not through system flaws but through direct manipulation of users.

Pump.fun: Speculation Amid Decline

While theft and fraud grab the headlines, another story is unfolding on the speculative side of the market. The Solana-based platform Pump.fun, which lets anyone launch a "memecoin" instantly, is rumored to be preparing a $1 billion token sale at a $4 billion valuation, with a 10% airdrop for its community. The reaction has been divisive: some see opportunity in the token launch, while others argue Pump.fun has already turned the crypto market into a casino, where most investors lose money.

The platform has pulled in $677 million in revenue so far, but monthly income has fallen sharply — down from $137 million in January to $46 million in May, a two-thirds decline. At

the same time, memecoins as a whole have lost more than half their market value since December, raising doubts about how sustainable this frenzy really is.

> **Info**
> pump.fun is a cryptocurrency launchpad for the Solana blockchain that enables users to create tokens and trade them immediately on the platform, as well as to launch them onto decentralized exchanges, a process known as "graduation". The platform was launched on January 19, 2024, by Noah Tweedale, Alon Cohen and Dylan Kerler.

A Market Defined by Contradictions

Taken together, these stories highlight the contradictions of the current crypto landscape. On one side, massive loss to scams and social engineering reveal how fragile trust remains, even as the underlying technology grows more robust. On the other, speculative platforms like Pump.fun keep attracting money and attention, despite showing signs of decline.

The industry is caught between its own technological maturity and the very human vulnerabilities that surround it. Billions are being drained not because the math failed, but because people did.