

Forum:[Hack Forums](#)

Thread: [Monero XMR](#)

Btc to 0 - January 17, 2026, 4:59 am

According to Odaily, a victim lost more than \$282 million in LTC and BTC due to a hardware wallet social engineering scam on January 10, 2026, around 23:00 UTC+8. The attacker began converting the stolen 2.05 million LTC and 1,459 BTC into Monero through multiple instant exchanges, causing an increase in XMR prices. Additionally, the stolen BTC was transferred cross-chain via Thorchain to Ethereum, Ripple, and Litecoin.

Mewtwo - January 17, 2026, 5:10 am

(Jan 17, 2026 05:59 AM)Btc to 0 Wrote: [\[CITE\]](#) According to Odaily, a victim lost more than \$282 million in LTC and BTC due to a hardware wallet social engineering scam on January 10, 2026, around 23:00 UTC+8. The attacker began converting the stolen 2.05 million LTC and 1,459 BTC into Monero through multiple instant exchanges, causing an increase in XMR prices. Additionally, the stolen BTC was transferred cross-chain via Thorchain to Ethereum, Ripple, and Litecoin.

As more of these attacks happen, will there ever be a secured way for vulnerable folks to prevent their funds from theft? All it takes is just 12 to 25 words or a private key to financially obliterate someone. If their funds are on an exchange or hedge fund, and a hacker steals the funds, at least there is hope for recovery or reimbursement. Not many folks are too tech savvy and shouldn't be using self custodian wallets for the sake of their wealth.

It's sad to say, but social engineering seems to be a more powerful tool. There could be billions of ways to be creative and trick someone to give their seeds, download malware, send funds to a wallet, or pretend to be an employee. But at the same time, there needs to be a hacker who has private data of customers, who breached websites and collected basic information like emails, names, phone numbers, balances etc. Without this data, there's no SE schemes or ATOs. These breaches happen more frequently because of improper security in place.

Especially now that many websites use API, which is super easy to scrape.

These private data's go for 6 or 7 figures. Only the folks who generated illicit funds like these types of attacks can surely afford to keep buying more private data.

Sadly enough though, there's not much severe penalties for companies to pay up for lawsuits or fines. Even participating in bug bounties, they don't seem to put a high bounty on PPI disclosures, if they even have a program to begin with.

Hackers - January 17, 2026, 5:11 am

interesting, wonder if that helped spark up a buying spree

I see XMR is not in the 700s anymore, down at 622 right now

Money- - January 17, 2026, 5:21 am

Good man , just keep doing that. So that there specific % of folks would earn some pump via XMR.

Puppetmaster - January 17, 2026, 5:56 am

Dude definitely read a lot of books on social engineering xd

SIM-4331310 - January 17, 2026, 7:54 am

What must the person on the other end of the attack feel/live like after this?

Omniscient - January 17, 2026, 8:20 am

Yeah, we got wind of this already. Huge and now there is downward sell pressure on XMR.

SUI-3183372 - January 17, 2026, 9:55 am

(Jan 17, 2026 06:10 AM)Mewtwo Wrote: [\[CITE\]](#) As more of these attacks happen, will there ever be a secured way for vulnerable folks to prevent their funds from theft? All it takes is just 12 to 25 words or a private key to financially obliterate someone. If their funds are on an exchange or hedge fund, and a hacker steals the funds, at least there is hope for recovery or reimbursement. Not many folks are too tech savvy and shouldn't be using self custodian wallets for the sake of their wealth.

I think I'm plenty capable of self-custodianship of my coins. Over 16 years, my only losses are due me intentionally not backing keys up and knowing my risks.

However, why risk it? Why risk a theft or fire or worse locking you out from your wealth?

I'd say about 50-75% of my coins are being held by an insured custodian. This custodian will not release my coins to any addresses but my designated whitelisted addresses, and they will not process a transaction without hopping on video call with me first and verifying numerous aspects of my identity live on call with them. If my custodian loses my coins, I am fully insured for 100% of the value of my losses. My custodian is also a US federally chartered national trust bank, recently securing OCC approval.

As costs around insured custodianship drops, more and more vulnerable individuals should explore it as an option.

Downside is, if I need 100% of my value immediately, my custodian may delay me by hours to days (So far transactions have always been processed within a few hours, but I've never tried to withdraw on a weekend). Edit, just tested, weekend withdrawals are available and are estimated to take 45 mins, not bad.

Tyr - January 17, 2026, 11:43 am

(Jan 17, 2026 06:10 AM)Mewtwo Wrote: [\[CITE\]](#) Without this data, there's no SE schemes or ATOs. These breaches happen more frequently because of improper security in place.

Especially now that many websites use API, which is super easy to scrape.

These private data's go for 6 or 7 figures. Only the folks who generated illicit funds like these types of attacks can surely afford to keep buying more private data.

Sadly enough though, there's not much severe penalties for companies to pay up for lawsuits or fines. Even participating in bug bounties, they don't seem to put a high bounty on PPI disclosures, if they even have a program to begin with.

Fantastically put.