# Crypto Compromise – Data Breaches and Security Scenarios

**Author** josh
**Date** 2024-04-21

## Overview

Unfortunately, data breaches happen. Any company, service, or piece of software may experience compromise at some point. Engineering secure software is a difficult challenge despite the best efforts of developers, and hackers continue to evolve their tactics. But what happens when there is a data breach, and what are some ways that an attacker can use stolen data to steal valuable information or even money? In this article, we'll discuss two examples of data breaches that effect the cryptocurrency world in particular. We will discuss what kind of data can be stolen, how the compromise can effect users, and what individuals can do to mitigate those effects on their security.

## Password Manager Breaches and Crypto Theft

The first breach in our list is that of *LastPass*, a cloud password manager. LastPass (and other password managers) allow users to securely store, generate, and autofill passwords and other secrets for various services. The user specifies a *master passphrase* that only they know, which is used as a key to encrypt the *password vault* using strong encryption. In order to access the secrets inside, a user must specify that master passphrase to decrypt the data inside.

This allows users to store lots of long, strong, randomly generated passphrases that a user could not remember on their own. A password manager is an excellent security tool for this reason, as it prevents password reuse and allows the use of stronger passphrases. However, the security of the *master passphrase* is critically important. If the vault uses strong, properly implemented encryption such as AES, the only way for an attacker to gain access to the data inside is to guess the password.

In August of 2022, LastPass experienced a breach where the *encrypted vaults* were stolen from LastPass. LastPass and other password manager companies don't know or store your master passphrase, just the encrypted vaults. The attackers now have snapshots of those vaults from the time of compromise. But what does that mean for users? In order to gain access to the secrets stored inside, the attackers must try to *crack* the password using something like a brute-force or dictionary attack. This does take a lot of computing resources, but in some cases is quite worth the reward.

Unfortunately, some users did not use the best master passphrases possible. Those compromised vaults, in some cases, contained a juicy reward for the attackers – cryptocurrency

seed phrases! Some users of LastPass that stored *seed phrases* in their vaults have had their cryptocurrency stolen as a result, as anyone that has the seed has access to the coins.

It is absolutely critical that users of any password manager generate a very long, strong, high entropy *passphrase* to protect their vault. The master passphrase, in this case, is the weakest link in the chain. Compromise the passphrase, compromise the vault and all the secrets inside. It's also important if you're the victim of such a breach to be proactive. Move your secrets to a new platform, rotate the secrets (seed phrases, passwords, etc.) to *new* ones, and choose a new master passphrase. Active management of your data can mitigate the effects of such a compromise.

## Crypto Company Email Leaks

Another, perhaps more straightforward data breach to understand occurred with *CoinMarketCap*, a cryptocurrency market information platform. The *emails* of over 3 million users were exposed – no passwords, just emails. It might seem that this is a relatively tame breach, as the attackers cannot directly crack and takeover accounts without a password breach.

However, emails allow a common vector of attack to flourish – *phishing*. One of the most effective ways for an attacker to compromise a user account isn't technical, it's human. Phishing is the act of tricking a user into giving up information that they shouldn't such as a *password* or a crypto *seed phrase*. If your email is included in a data breach such as CoinMarketCap's, it tells hackers something about you – that you use or are interested in cryptocurrency.

As such, attackers have used emails in this breach to send out all sorts of crypto-related phishing emails – pretenting to be CoinMarketCap, Coinbase, Gemini, Metamask, and other crypto services, coins, airdrops, and more. Victims of this breach have been targeted with these wide-ranging phishing emails in the hope that user inadvertendly gives up a seed phrase, a password, or signs a malicious contract. In this case, it's critical that users have *awareness* about phishing. Users should know what to look for when it comes to phishing – a sense of urgency, a too good to be true offer, coming from a different email than expected, and more. Again, active awareness and self-education is a key to preventing compromise.

## Awareness and Activity

Breaches happen in the digital world, and crypto-related breaches can be particularly devastating as they have financial consequences. Two examples include the breach of password managers containing seed phrases or exchange credentials, and email breaches that make users the target of sophisticated phishing attacks. In both cases, *active awareness* are important for user security. Taking the time to educate yourself about phishing may prevent falling victim to theft. If a user knows they've been compomised in a password manager breach, taking the time to rotate credentials and choose a new master passphrase can help avoid loss.