

Forum:[Hack Forums](#)

Thread: [Venus Protocol user suffers \\$13.5M loss from phishing attack](#)

Stanley - September 2, 2025, 3:35 pm

Venus Protocol user suffers \$13.5M loss from phishing attack

Venus Protocol paused the platform to conduct security reviews but said the \$13.5 million loss was not linked to a flaw in its contracts.

https://cointelegraph.com/news/defi-trader-loses-27m-phishing-scam-venus-protocol-pauses?utm_source=rss_feed&utm_medium=rss&utm_campaign=rss_partner_inbound

JoseMar - September 2, 2025, 11:08 pm

(Sep 2, 2025 03:35 PM)Stanley Wrote: [\[CITE\]](#) Venus Protocol user suffers \$13.5M loss from phishing attack

Venus Protocol paused the platform to conduct security reviews but said the \$13.5 million loss was not linked to a flaw in its contracts.

https://cointelegraph.com/news/defi-trader-loses-27m-phishing-scam-venus-protocol-pauses?utm_source=rss_feed&utm_medium=rss&utm_campaign=rss_partner_inbound

So the protocol itself is fine, but the user got phished?. That's somehow even more brutal. You can have the most secure system in the world, and it just takes one tricky link. A \$13.5 million mistake... wow.

sharn - September 14, 2025, 10:55 am

Phishing attacks are becoming more sophisticated, making them harder to detect. Users must remain cautious and skeptical of unexpected requests.

Yanix - September 15, 2025, 6:10 am

Sad to see another huge phishing loss. Even solid platforms like Venus can't protect you from social engineering

Chornaya Magiya - September 15, 2025, 3:03 pm

(Sep 14, 2025 10:55 AM)sharn Wrote: [\[CITE\]](#) Phishing attacks are becoming more sophisticated, making them harder to detect. Users must remain cautious and skeptical of unexpected requests.

Am confused how they pulled this off via phishing

Hackers - September 15, 2025, 4:58 pm

(Sep 15, 2025 03:03 PM)Chornaya Magiya Wrote: [\[CITE\]](#) Am confused how they pulled this off via phishing

There are a number of ways, depending on the victim's setup.

Keep in mind that people are silly and re-use passwords or variations.

They could've phished him elsewhere, gained access to 2FA, got access to a holding contract, withdrawn funds, etc -- I don't know.

It sounds like that if it's "phishing" in the traditional way, there was 2FA or a convenience password (browser wallets for example) in use.

If it's a modern take on the word "phishing", then perhaps they tricked the victim into authorizing a transaction, or signing some sort of access / delegate address.

Really depends - I don't know enough but can think of how a cybercriminal could "phish" in the crypto space.