Guide: how to communicate on-chain with an unknown hacker

Last Modified on 05/10/2025 4:52 am EDT

In order to communicate on-chain with an attacker, you will need a non-compromised cryptocurrency wallet and will need to use a wallet application that supports adding a data string to a transaction; not all wallet applications support this.

Wallet applications that do support adding the data string include Metamask, MEW, and Mycrypto as but some examples.

Once you have a wallet you will use for messaging, take the following steps:

1. Draft the message you want to send.

2. Use a Text to Hex conversion tool that converts the message to Hex. Make sure there is no space delimiter (i.e. no spaces between the characters).

3. Open up your wallet, and enter the hacker's address that you want to send the message to as the destination address. You can set the ETH value of the transaction to 0, or alternatively, send a very small amount to draw attention e.g. 0.001 ETH.

4. With most wallet software, you will then need to hit 'advanced' to be able to enter a data string. The data string must be entered in Hexidecimal format, not text format, and **you must add the prefix '0x' to the hexidecimal string**

Example

Message (text):

Please return my money, otherwise I'm going to tell your mom

Message (Hex):

506C65617365207265747572E206D79206D6F6E65792C206F7468657277697365 2049276D20676F696E6720746F2074656C6C20796F757

Data to enter the advanced 'data' field in your wallet to ensure the attacker gets the message:

0x*506C65617365207265747572E206D79206D6F6E65792C206F7468657277697365 2049276D20676F696E6720746F2074656C6C20796F7*

5. Send the transaction. Note, a transaction with an on-chain message consumes more gas, and the longer the message, the higher the gas cost, so make sure you have enough ETH in your wallet to cover gas costs, then go ahead and send the transaction