Happy to hear that EIP-3074 ("AUTHCALL") is going forward.

The question I have in mind is how EIP-3074 prevents phishing? I looked up some old AUTHCALL examples (likely outdated), and most of them seem to be a normal EIP-712 message.

An example here:

[

image

1752×1862 132 KB

](https://ethresear.ch/uploads/default/original/2X/5/5368dc978cd0a5d9e4faeddc2d67c5ef3ff91d4c.jpeg)

[

image

2168×2152 390 KB

](https://ethresear.ch/uploads/default/original/2X/1/112061eb401698e3860a7fb2b15b3dd864a04ed6.png)

If AUTH/AUTHCALL allows the user to delegate her wallet to any smart contract with a single signed message, isn't this a large phishing risk? Or am I misunderstanding something here, and there are going to be some security measurements not signing arbitrary AUTH/AUTHCALLs?

- Currently Ethereum has ~600 wallets as listed on WalletConnect website, there are likely couple of hundreds more
- Phishing is the largest security problem in the Ethereum ecosystem, where approve(), permit() and Permit2 phishing cause $70M/month losses to Ethereum users, causing more damage than hacks and rug pulls, or any other attack vector
- Legacy wallet dev teams do not have resources to build transaction simulators or other such security measurements to prevent new phishing vectors
- EIP-3074 specification does not discuss this problem, does not give any UX guidelines for wallet and Dapp developers, and so on, so it feels there might be a risk here