usable security in web3
or the elephant-in-the-metaverse-room

Antonela
MetaMask
“Wallets are built around the responsibility of mediating the interactions between untrusted applications and a user’s keys on their computer, getting appropriate consent from the user.”

https://eips.ethereum.org/EIPS/eip-2255
Keys
Permissions
const response = await provider.request({
  method: 'wallet_requestPermissions',
  params: [{
    'eth_accounts': {}
  }]
})
Threat Analysis
Lavamoat
Human Review
Bounty programs
Phishing List
There are no secure systems without consent.
Consent /kən’sent/ 

Noun: Permission for something to happen or agreement to do something.

Verb: Give permission for something to happen.
Freely given
Revokable
Informed
Enthusiastic
Specific

consentfultech.io
Freely given
Revokable
Informed
Enthusiastic
Specific
Freely given
Revokable
Informed
Enthusiastic
Specific
Freely given
Revokable
**Informed**
Enthusiastic
Specific
Freely given
Revokable
Informed
Enthusiastic
Specific
Freely given
Revokable
Informed
Enthusiastic
Specific
If we build a transaction flow grounded in consent, how would it look?
BADGER - REKT

Thursday, December 3, 2021
Badger - REKT

read this article also in:
en - es - fr - ko - ru - tr - zh

rekt roadkill.

The badger is dead.

$120 million taken in various forms of wBTC and ERC20.

A front-end attack places Badger DAO at number four on the leaderboard.

rekt.news repeats:

Infinite approval means unlimited trust - something which we know we shouldn’t do in DeFi.
Give permission to access your WETH?

By granting permission, you are allowing the following contract to access your funds

0x68b3...fc45

Edit Permission

Transaction fee

A fee is associated with this request.

$0.25
0.000083 ETH

View full transaction details

Reject
Confirm
Set a spending cap for your DAI

Custom spending cap: Max

Only enter a number that you're comfortable with the contract accessing now or in the future. You can always increase the token limit later.

View details

Review your spending cap

Custom spending cap: 900 DAI

Estimated fee:
- Site Suggested: 30 sec
- Fee details:

Edit

View details

Cancel Next

Approve
New ERC-721 & ERC-1155
We have the responsibility to **critical think** how to expose the user to a decision that directly affects their digital body.
Balancing security and usability is complex.
@holantonela
hackerone.com/metamask
Rethink how the information systems to which we delegate trust interact with that consent.
Gracias

Antonela
MetaMask

@holantonela