



# usable security in web3

or the elephant-in-the-metaverse-room

**Antonela**  
MetaMask







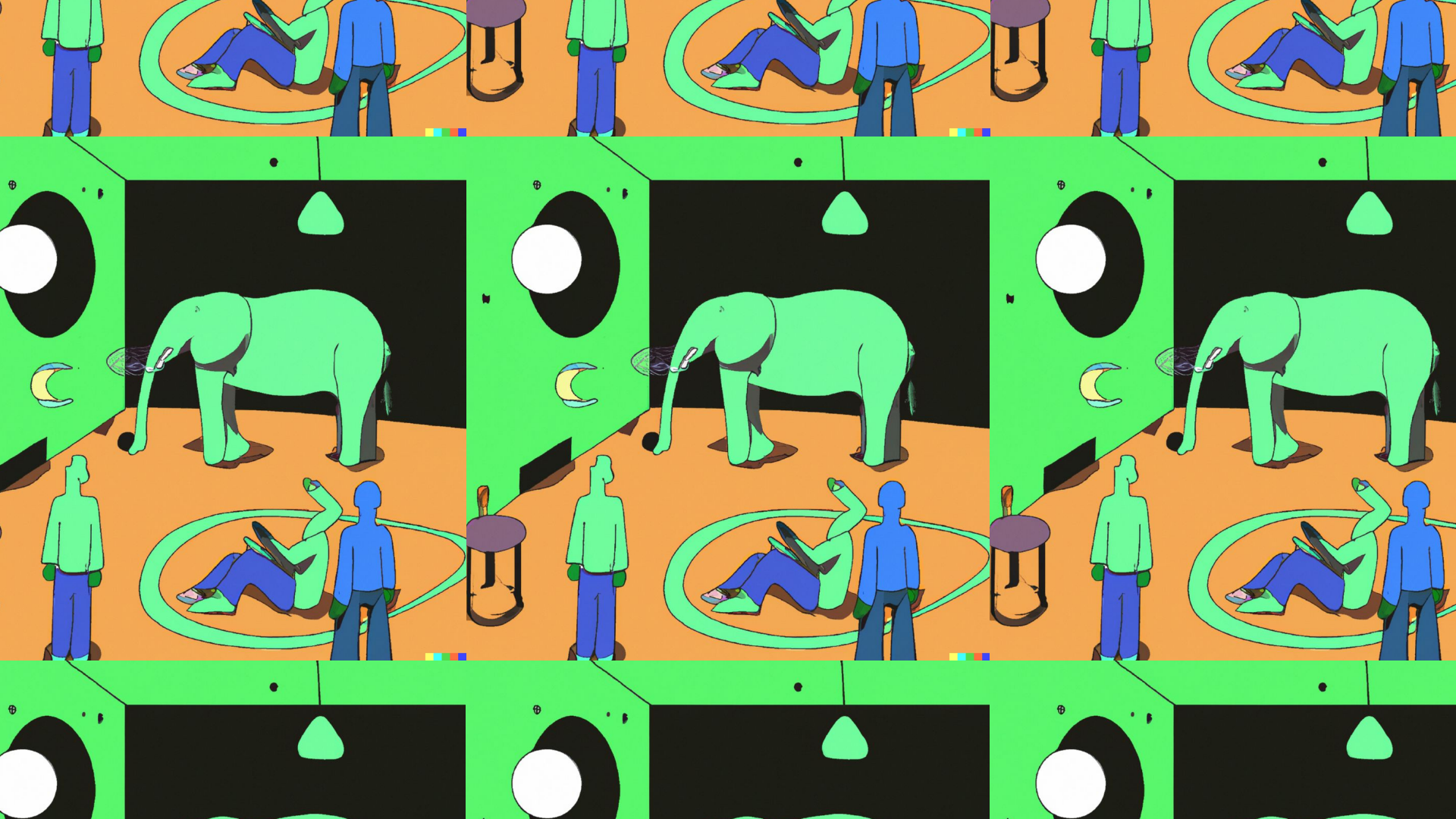




Keys

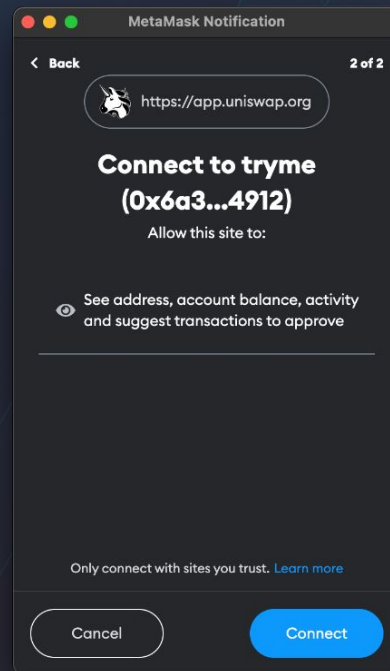
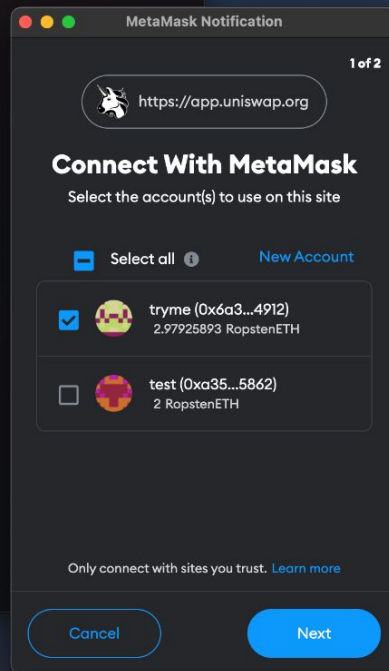
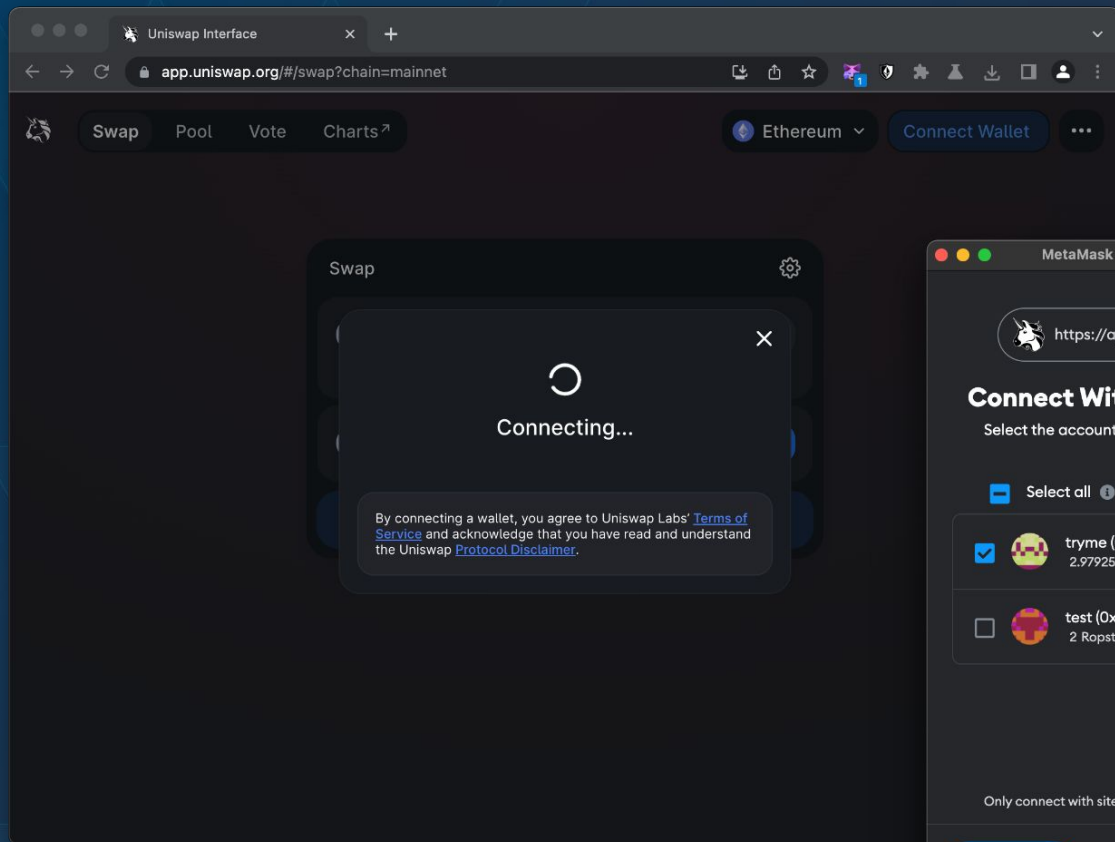
Permissions

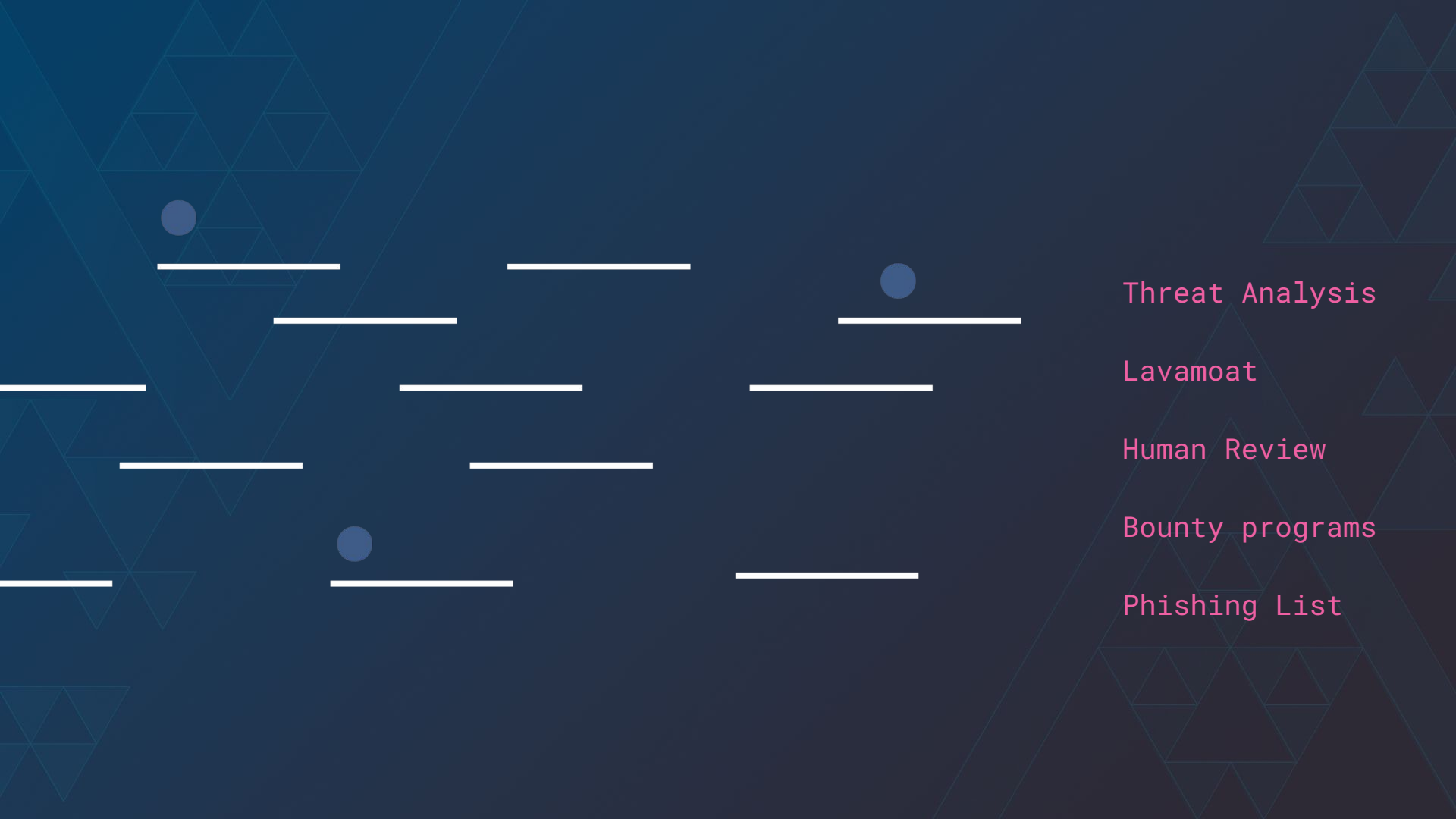




```
const response = await provider.request ({  
  method: 'wallet_requestPermissions',  
  params: [{  
    'eth_accounts': {},  
  }]  
})
```







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



**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?

MetaMask Notification

Ropsten Test Network

tryme

→

New Contract

https://metamask.github.io

CONTRACT DEPLOYMENT

DETAILS

DATA

Estimated gas fee ⓘ

0.00030262

0.000303 RopstenETH

Site suggested

Likely in < 30 seconds

Max fee: 0.00030262 RopstenETH

Total

0.00030262

0.00030262 RopstenETH

Amount + gas fee

Max amount: 0.00030262 RopstenETH

Reject

Confirm

Ropsten Test Network

tryme

→

0x31f...f2Eb

New address detected! Click here to add to your address book.

https://metamask.github.io

0x31f...f2Eb : MINT COLLECTIBLES ⓘ

DETAILS

DATA

HEX

Estimated gas fee ⓘ

0.00013739

0.000137 RopstenETH

Site suggested




Max fee: 0.00013739 RopstenETH

MetaMask Notification

Add Suggested Tokens

Would you like to import these tokens?

A token here reuses a symbol from another token you watch, this can be confusing or deceptive.

Token	Balance
 TST	10 TST
 TST	10 TST
 TST	10 TST

Cancel

Add Token

MetaMask Notification

Ropsten Test Network

tryme

→

0x31f...f2Eb

New address detected! Click here to add to your address book.

https://metamask.github.io

0x31f...f2Eb : MINT COLLECTIBLES ⓘ

DETAILS

DATA

HEX

Estimated gas fee ⓘ

0.00013739

0.000137 RopstenETH

Site suggested

Likely in < 30 seconds

Max fee: 0.00013739 RopstenETH

Total

0.00013739

0.00013739 RopstenETH

Amount + gas fee

Max amount: 0.00013739 RopstenETH

Reject

Confirm

MetaMask Notification

Ropsten Test Network

tryme

→

0x31f...f2Eb

New address detected! Click here to add to your address book.

https://metamask.github.io

MINT COLLECTIBLES ⓘ

DETAILS

DATA

HEX

Estimated gas fee ⓘ

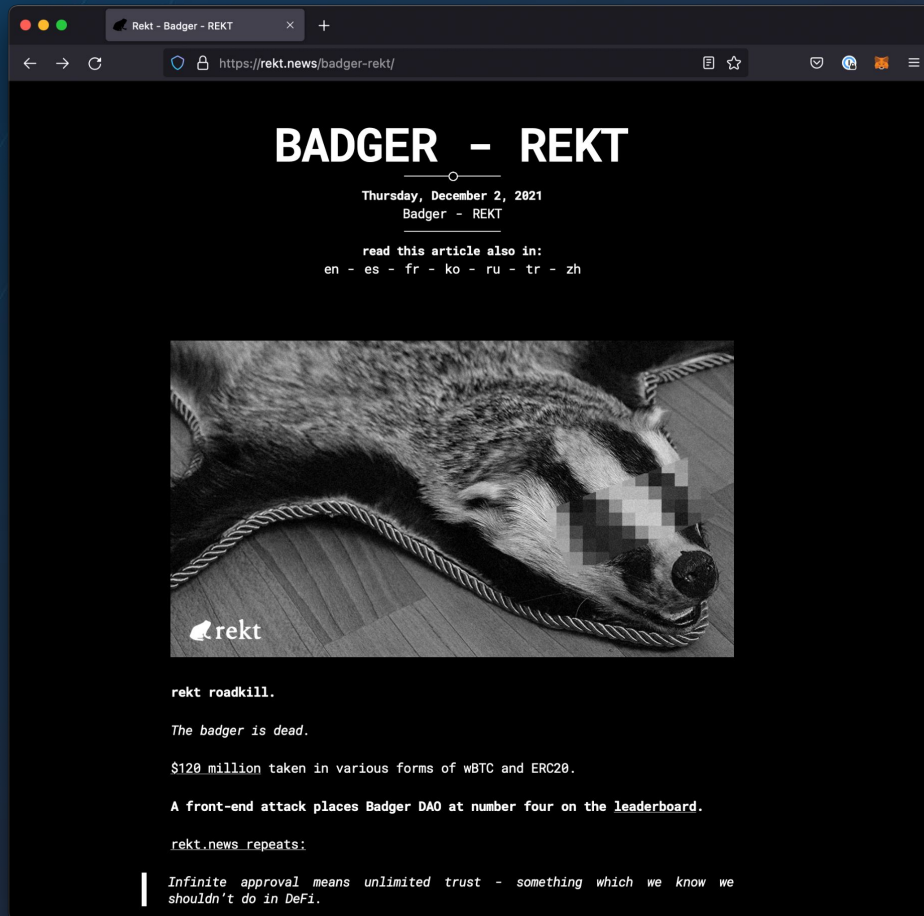
0.00013739

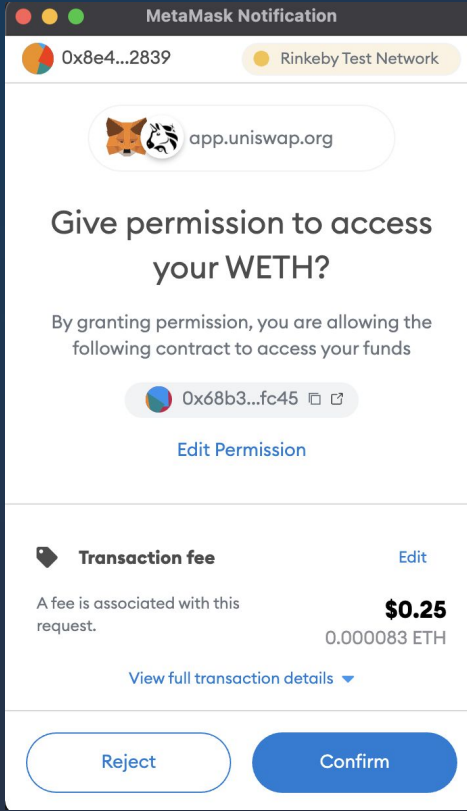
0.000137 RopstenETH

Site suggested

Likely in < 30 seconds

Max fee: 0.00013739 RopstenETH






Current ERC-20




MetaMask




1 of 2

 Ethereum Network  
Account 1

Balance  
200.12 DAI

 <https://app.uniswap.org>

### Set a spending cap for your

 **DAI**  

[Verify contract details](#)

Custom spending cap [Use default](#)

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](#)

Cancel


Next

MetaMask




2 of 2

 Ethereum Network  
Account 1

Balance  
200.12 DAI

 <https://app.uniswap.org>


### Review your spending cap

 **DAI**  

[Verify contract details](#)

Custom spending cap [Edit](#)

900 DAI

Estimated fee  **-\$3.827**

Site Suggested -30 sec Max \$4,172

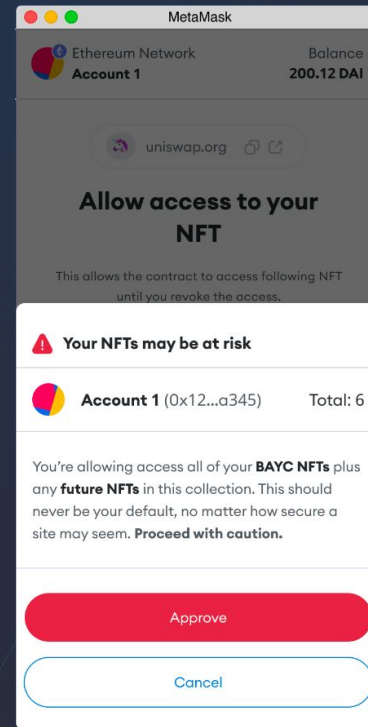
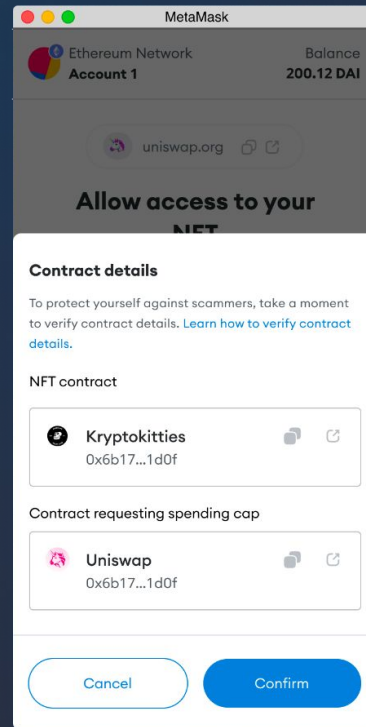
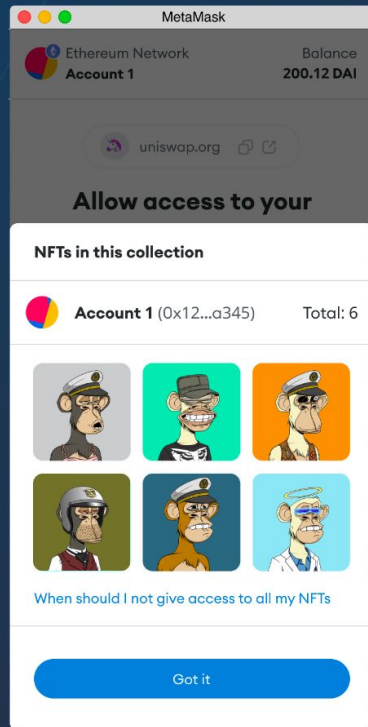
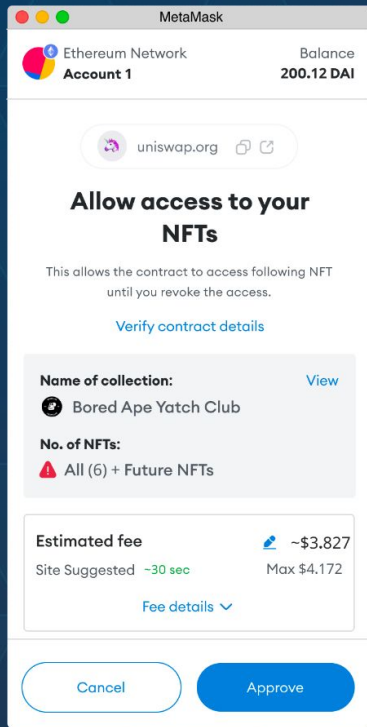
[Fee details](#)

[View details](#)

Cancel

Approve

New ERC-20



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**.

@holantone1a



[hackerone.com/metamask](https://hackerone.com/metamask)

[metamask.io/snaps](https://metamask.io/snaps)

Rethink how the  
information systems to  
which we **delegate trust**  
interact with that  
consent.





Gracias

Antonela

MetaMask



@holantonela