Log in safely with a Web3 wallet signature

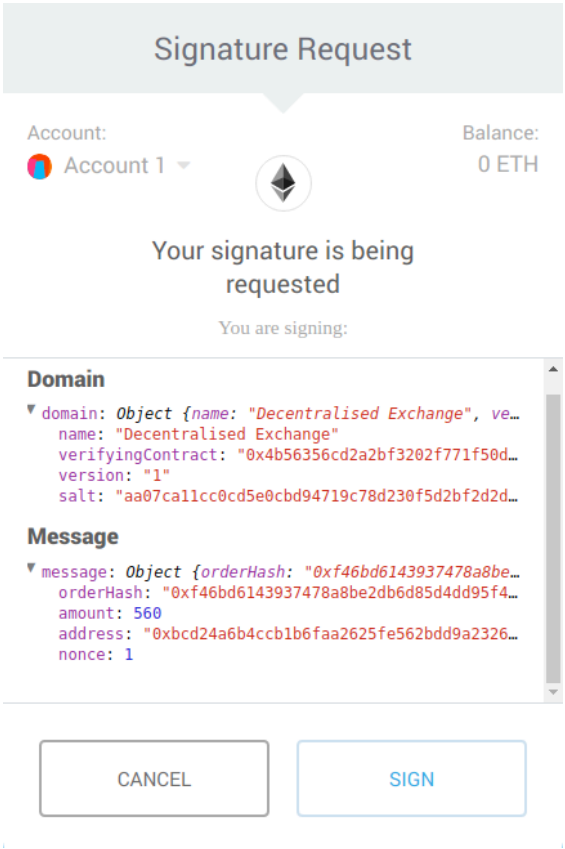
When you hold priceless assets in your wallet, even something as simple as signing in with a Web3 wallet can be a really stressful experience. After all, you can lose everything with one bad move.

In this article we'll learn how to make sure that you can do it safely so you can worry less and enjoy life more 🙂

In essence - logging in safely by signing a message boils down to the following:

1. **Are you on the right page?**
    1. Every time check BOTH:
        1. the address bar of the page you are trying to sign in
        2. the address of the website displayed on transaction window
    2. Make sure you are on the right page and that both domains are exactly the same!
2. **Make sure you are signing a message, not sending a transaction!**
    1. Signing in should never require a blockchain transaction, so if it requests one - cancel.
3. Examine contents of the message to sign:
    1. **Make sure it's plain text**

1. While it is possible to use EIP-712 for signing in - it's unreadable for a non-technical person - it looks like this:



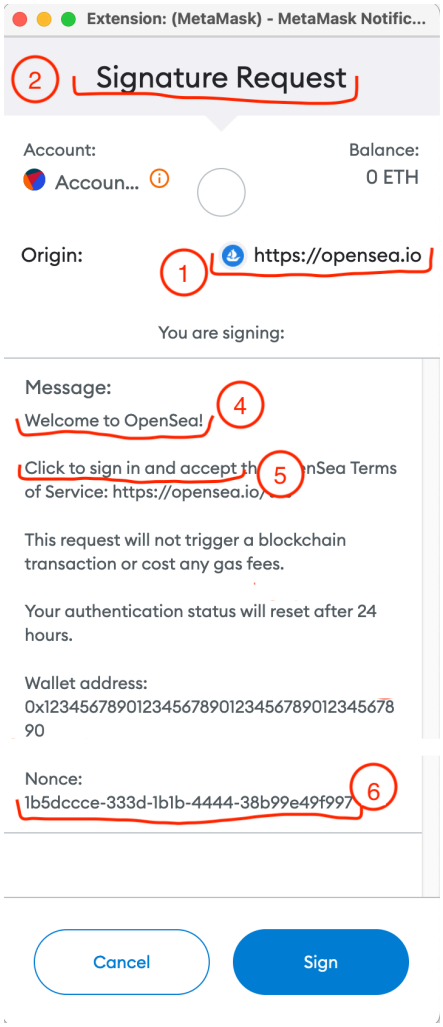
    2. Sure, it's possible that some app uses EIP-712 for login, but it's more probable that someone is trying to trick you into signing a message to transfer ERC-20 coins for example. So it's better to steer away!
2. **Make sure the message refers to the site you want to take the action on**
    1. Phishing websites may try to trick you into signing a message which then they will use to take actions on your behalf!
3. **Make sure the message refers to an action you want to take**
    1. Again, if you wanted to log in but the message says something about changes in the price of your NFT - steer away and cancel.
4. **Make sure it contains a nonce (random number or a date)**
    1. This is a tricky one. Not every app gets this right. If there is no date or a random number in the message then the signed message can be reused over and over.
    2. In this case you're not in immediate danger but you should contact the app's developer to fix their login process. Otherwise if the message gets stolen in some way - the attacker will have the ability to sign in as you forever.
4. **Learn this process by heart and always use it.**
    1. This process shouldn't be used only on untrusted websites.

2. The truth is that websites sometimes get hacked despite best effort and one day even OpenSea may ask you to do something that will make you lose everything.
3. Always treat all websites as untrusted, even if you've used them a thousand times already.

Now that we know the basics - let's see some examples to understand the situation better.

Example 1 - OpenSea

Ok, so let's say you go to https://opensea.io/, then your account and click "settings". OpenSea will want to sign you in



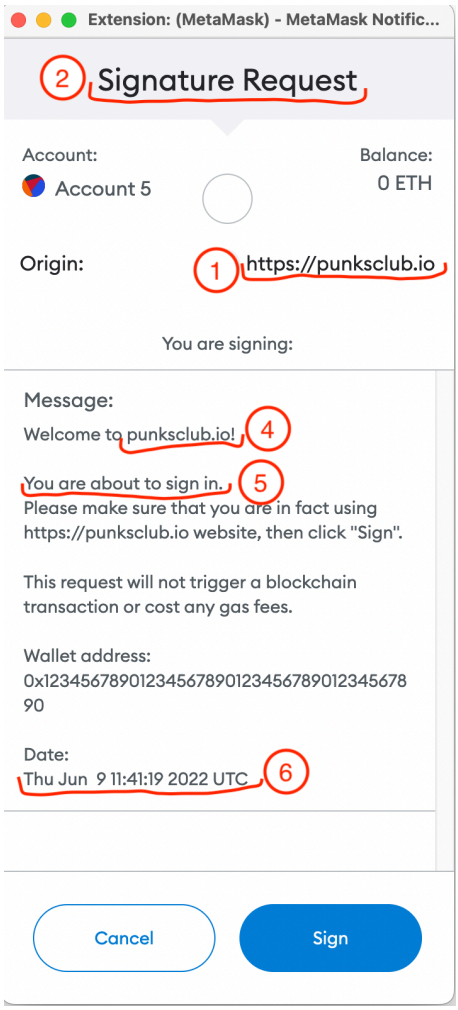
1. Address on both address bar and signing window is right - opensea.io.
2. It's a request for a signature, not to send a transaction.

3. The message is in plaintext - it is human readable. EIP-712 messages look like this and for non-technical person it's hard to understand what they are signing:
4. It refers to OpenSea, so not a chance we are right now being tricked into signing a message for another page.
5. It says that the message will be used for sign in, so we are not being tricked into a message which does something else.
6. Nonce is present, in this case as a random string (well, UUID, but that's technical).

We checked every one of those points so it is safe to sign in.

Example 2 - Punks Club

Another example, let's say we are trying to access [PunksClub.io](). Obviously we are a little bit unsure because we need to sign with an account which holds punks. So let's use our framework to check if all is secure:



So let's go over our checklist again:

1. Address on both address bar and MetaMask window checks out. Be sure to check if there may be a misspelling and if the extension (.io) is right! Be vigilant, hackers will try to trick you.
2. It's a signature request, not a transaction - GOOD.
3. Message again is plaintext, not EIP-712.
4. Message explicitly states that it's about punksclub.io and not - for example - OpenSea or Foundation - GOOD.
5. Action is clearly stated and we are signing in - GOOD.
6. There is a nonce present - this time in form of a date - to prevent reusing signatures - GOOD.

Everything checks out so we are safe to sign in.

Closing words

Hope this helps you stay secure and less anxious.

Remember:

- always use this process, even when you have used the website/app multiple times. It can always get hacked.
- to be secure - all conditions mentioned above must be met. If not all of them are - it's a potential red flag and it's safer to cancel.

Also if you hold valuable assets - then please - get a hardware wallet. And make a backup of the seed phrase (and keep it in a secure place!).

Stay safe!

DM for comments / corrections: https://twitter.com/VoyTechEth