A complete security guide for play-to-earn scholars

Mar 24

Overview

Security is one of the most important aspects one has to take care of when dealing with blockchain and cryptocurrency services. Most of the scholars who start their play-to-earn or play-and-earn journey have never used crypto before and that's exactly why they should pay even more attention to basic security principles.

Why does security matter?

Security in blockchain gaming matters just as much as in real life. Here are a few reasons why:

1. Every blockchain game will have interaction with financial assets at some point. Even if the game is completely free, you will have the chance to collect or win in-game items that can be sold for real money. If you don't know how to keep those assets safe and you're not aware of the numerous scams that exist in crypto, you may lose all of them in a flash. Trust me, there's nothing worse than losing everything you've earned just because you didn't protect yourself enough.

2. The difference between traditional in-game assets and blockchain in-game assets is that the latter ones are stored in a separate wallet from your gaming account. For the first time in history, gaming companies don't possess your in-game assets. They are truly yours. This means that if you lose access to your wallet or you're hacked, all of your assets are gone. I hope blockchains will introduce some ways to restore funds even if you lost access to your seed phrase but right now it's not technically feasible.
3. Understanding the basic security measures will also help you to sleep well and not be afraid that your funds will be stolen when you're awake. This will help to reduce stress and worry. You'll be confident that your assets are safe and you can focus on improving your gaming skills.
4. You never know when you can save somebody's funds. The majority of gamers will not have experience with crypto and blockchains but you will. Sharing your story or even this post can help thousands of people avoid the same mistakes as you already did.
5. Your practical knowledge will help identify potential threats or new phishing attacks. There's nothing more powerful than knowing what to expect.

Best security practices

Below you can see an extensive list of best security practices that every scholar needs to follow. I divided them in sever categories that are equally important.

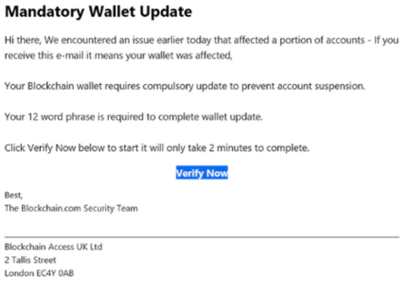
1. Online security practices

Online security in Web3 is the most crucial one. There are so many scams that it's often hard to stay up-to-date. Thus, I took some time and compiled a list of the most common ones to be aware of.

The main goal of fraudsters is to take away your secret phrase and your assets. Don't fall for anything that looks or seems dodgy.

> *Always be cautios and question every single link you click on and every single message you receive on Discord, Twitter, Facebook, TikTok, email, etc. Never share your seed/secret phrase with anyone!*

Fake Support Emails



Mandatory Wallet Update

Hi there, We encountered an issue earlier today that affected a portion of accounts - If you receive this e-mail it means your wallet was affected,

Your Blockchain wallet requires compulsory update to prevent account suspension.

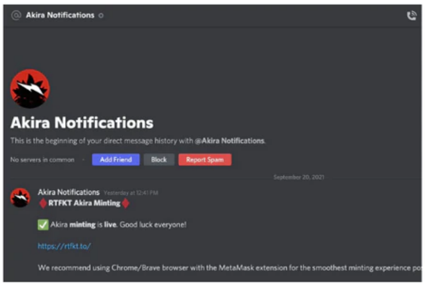
Your 12 word phrase is required to complete wallet update.

Click Verify Now below to start it will only take 2 minutes to complete.

Best,
The Blockchain.com Security Team

Blockchain Access UK Ltd
2 Tallis Street
London EC4Y 0AB

Discord Impersonators



Akira Notifications

This is the beginning of your direct message history with @Akira Notifications.

No servers in common

September 20, 2021

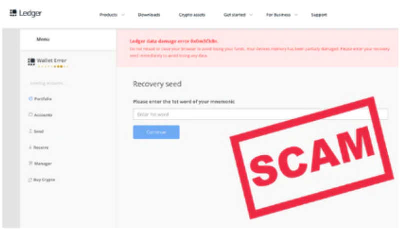
Akira Notifications Yesterday at 12:41 PM
♦ RTFKT Akira Minting ♦

✅ Akira **minting** is **live**. Good luck everyone!

https://rtfkt.to/

We recommend using Chrome/Brave browser with the MetaMask extension for the smoothest minting experience po

Hardware Wallet Scams



Ledger data damage error [illegible]

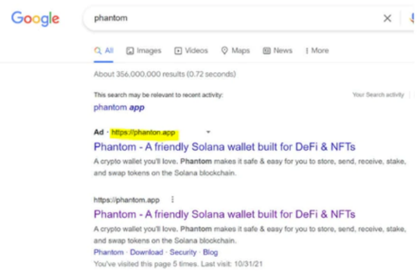
Do not reload or close your browser to avoid losing your funds. Your devices memory has been partially damaged. Please enter your recovery seed immediately to avoid losing any data.

Recovery seed

Please enter the 1st word of your mnemonic

Enter 1st word

Fake Paid Ads



About 356,000,000 results (0.72 seconds)

This search may be relevant to recent activity:
phantom ***app***

Your Search activity

Ad · https://phanton.app

Phantom - A friendly Solana wallet built for DeFi & NFTs

A crypto wallet you'll love. **Phantom** makes it safe & easy for you to store, send, receive, stake, and swap tokens on the Solana blockchain.

https://phantom.app

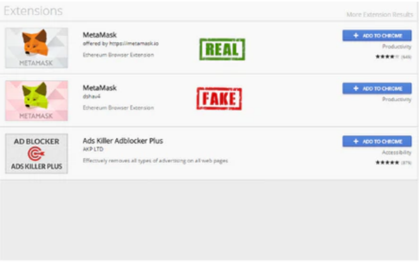
Phantom - A friendly Solana wallet built for DeFi & NFTs

A crypto wallet you'll love. **Phantom** makes it safe & easy for you to store, send, receive, stake, and swap tokens on the Solana blockchain.

Phantom · Download · Security · Blog

You've visited this page 5 times. Last visit: 10/31/21

Fake Browser Extensions



Extensions

More Extension Results

MetaMask
offered by https://metamask.io
Ethereum Browser Extension

Productivity

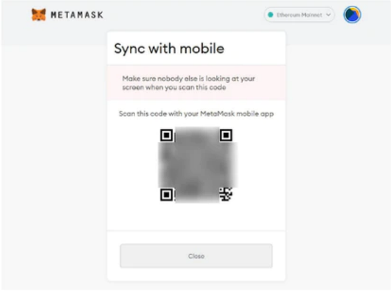
MetaMask
dshav4
Ethereum Browser Extension

Productivity

Ads Killer Adblocker Plus
AKP LTD
Effectively removes all types of advertising on all web pages

Accessibility

Fake Sync with Mobile QR Codes



Sync with mobile

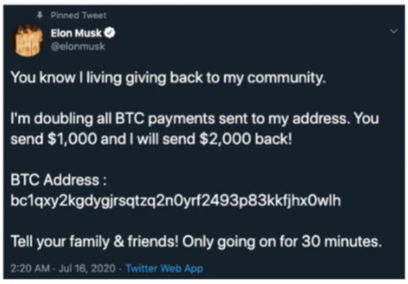
Make sure nobody else is looking at your screen when you scan this code

Scan this code with your MetaMask mobile app

However, hackers don't stop there. They try to catch people with free giveaways, airdrops, covid-19 scams, get rich quick schemes, etc.

> *If it sounds too good to be true, it's a scam.*

Double Your Crypto Scams



Pinned Tweet

Elon Musk @elonmusk

You know I living giving back to my community.

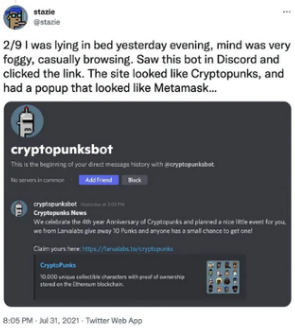
I'm doubling all BTC payments sent to my address. You send $1,000 and I will send $2,000 back!

BTC Address : bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Tell your family & friends! Only going on for 30 minutes.

2:20 AM · Jul 16, 2020 · Twitter Web App

Scam Discord Bots



stazie @stazie

2/9 I was lying in bed yesterday evening, mind was very foggy, casually browsing. Saw this bot in Discord and clicked the link. The site looked like Cryptopunks, and had a popup that looked like Metamask...

cryptopunksbot

This is the beginning of your direct message history with @cryptopunksbot.

No servers in common

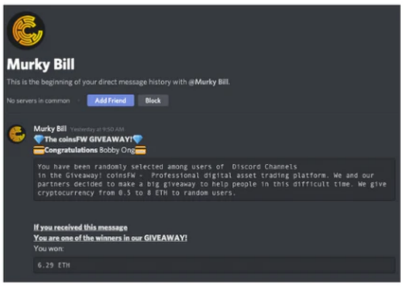
cryptopunksbot Yesterday at 3:03 PM
Cryptopunks News
We celebrate the 4th year Anniversary of Cryptopunks and planned a nice little event for you, we from Larvalabs give away 10 Punks and anyone has a small chance to get one!

Claim yours here: https://larvalabs.to/cryptopunks

CryptoPunks
10,000 unique collectible characters with proof of ownership stored on the Ethereum blockchain.

8:05 PM · Jul 31, 2021 · Twitter Web App

Fake Discord Giveaways



Murky Bill

This is the beginning of your direct message history with @Murky Bill.

No servers in common

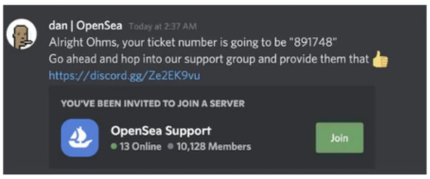
Murky Bill Yesterday at 9:50 AM
💎 **The coinsFW GIVEAWAY!** 💎
Congratulations Bobby Ong

```
You have been randomly selected among users of  Discord Channels
in the Giveaway! coinsFW -  Professional digital asset trading platform. We and our
partners decided to make a big giveaway to help people in this difficult time. We give
cryptocurrency from 0.5 to 8 ETH to random users.
```

If you received this message
You are one of the winners in our GIVEAWAY!
You won:

```
6.29 ETH
```

Fake Discord Groups

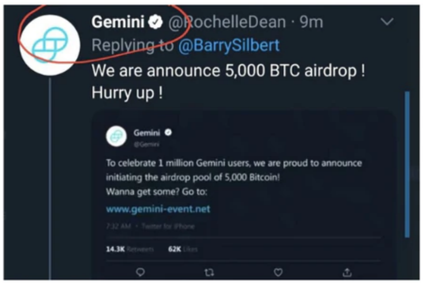


dan | OpenSea Today at 2:37 AM
Alright Ohms, your ticket number is going to be "891748"
Go ahead and hop into our support group and provide them that 👍
https://discord.gg/Ze2EK9vu

YOU'VE BEEN INVITED TO JOIN A SERVER

OpenSea Support
● 13 Online ● 10,128 Members

Fake Aidrops



Gemini @RochelleDean · 9m
Replying to @BarrySilbert
We are announce 5,000 BTC airdrop !
Hurry up !

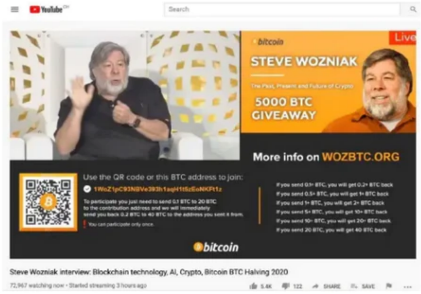
Gemini
@Gemini

To celebrate 1 million Gemini users, we are proud to announce initiating the airdrop pool of 5,000 Bitcoin!
Wanna get some? Go to:
www.gemini-event.net

7:32 AM · Twitter for iPhone

14.3K Retweets 62K Likes

Youtube Stream Scams



Use the QR code or this BTC address to join:
1WoZ1pC93NBVe393h1aqH1t5zEoNKFt1z
To participate you just need to send 0.1 BTC to 20 BTC to the contribution address and we will immediately send you back 0.2 BTC to 40 BTC to the address you sent it from.
You can participate only once.

If you send 0.1+ BTC, you will get 0.2+ BTC back
If you send 0.5+ BTC, you will get 1+ BTC back
If you send 1+ BTC, you will get 2+ BTC back
If you send 5+ BTC, you will get 10+ BTC back
If you send 10+ BTC, you will get 20+ BTC back
If you send 20 BTC, you will get 40 BTC back

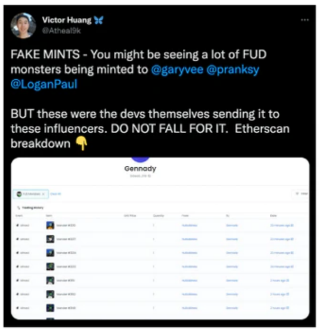
Steve Wozniak interview: Blockchain technology, AI, Crypto, Bitcoin BTC Halving 2020

72,967 watching now · Started streaming 3 hours ago

Lastly, there's a big group of NFT-related scams. It's harder to spot them but they typically use the same tactics: free stuff, fake emails, fake links, fake Opensea collections.

> *Never touch any cheap/trash/garbage NFT that you received for free on Polygon! One signature is enough to drain your entire wallet. This is the most dangerous attack and you should know it!*

Fake NFT Mints

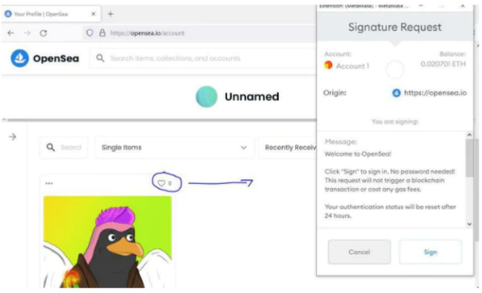


Victor Huang
@Atheal9k

FAKE MINTS - You might be seeing a lot of FUD monsters being minted to @garyvee @pranksy @LoganPaul

BUT these were the devs themselves sending it to these influencers. DO NOT FALL FOR IT. Etherscan breakdown 👇

Garbage Polygon NFTs



Signature Request

Account: Account 1
Balance: 0.020701 ETH
Origin: https://opensea.io

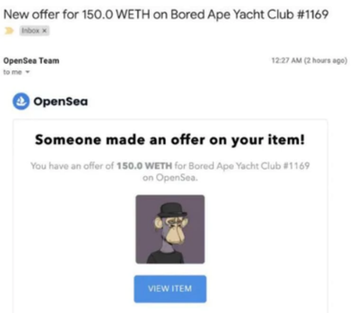
You are signing:

Message:
Welcome to OpenSea!

Click "Sign" to sign in. No password needed! This request will not trigger a blockchain transaction or cost any gas fees.

Your authentication status will be reset after 24 hours.

Fake Opensea Offers



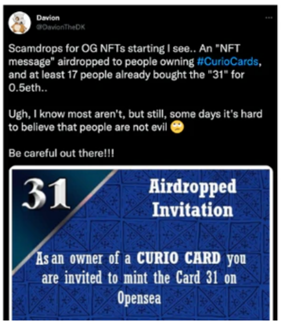
New offer for 150.0 WETH on Bored Ape Yacht Club #1169

OpenSea Team
to me
12:27 AM (2 hours ago)

Someone made an offer on your item!

You have an offer of **150.0 WETH** for Bored Ape Yacht Club #1169 on OpenSea.

OG Invites to Mint NFTs



Davion
@DavionTheDK

Scamdrops for OG NFTs starting I see.. An "NFT message" airdropped to people owning #CurioCards, and at least 17 people already bought the "31" for 0.5eth..

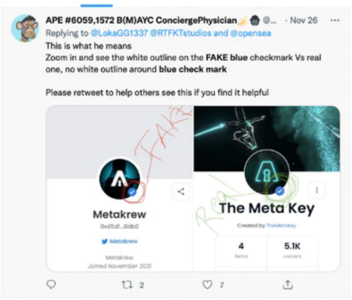
Ugh, I know most aren't, but still, some days it's hard to believe that people are not evil 🙄

Be careful out there!!!

31 Airdropped Invitation

As an owner of a **CURIO CARD** you are invited to mint the Card 31 on Opensea

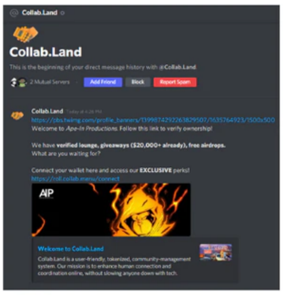
Fake Verified NFT Collections



APE #6059,1572 B(M)AYC ConciergePhysician · Nov 26
Replying to @LokaGG1337 @RTFKTstudios and @opensea
This is what he means
Zoom in and see the white outline on the **FAKE blue** checkmark Vs real one, no white outline around **blue check mark**

Please retweet to help others see this if you find it helpful

Fake CollabLand Links



Collab.Land

This is the beginning of your direct message history with @Collab.Land

Collab.Land
https://pbs.twimg.com/profile_banners/1399874292263829507/1635764923/1500x500
Welcome to *Ape-In Productions*. Follow this link to verify ownership!

We have **verified lounge, giveaways ($20,000+ already), free airdrops.**
What are you waiting for?

Connect your wallet here and access our **EXCLUSIVE** perks!
https://roll.collab.menu/connect

Welcome to Collab.Land
Collab.Land is a user-friendly, tokenized, community-management system. Our mission is to enhance human connection and coordination online, without slowing anyone down with tech.

Actions:

1. Turn off your Discord DMs
2. Create email filters to sort new messages into categories
3. Install Adblock
4. Bookmark all websites that you use daily
5. Remove all browser extensions you don't need or don't use
6. Create new habits:
    - don't click on random links
    - don't share your seed phrase
    - don't send crypto to unknown addresses or people
    - do small transactions before sending large amounts
    - always verify official websites, links, browser extensions, NFT collections
    - don't touch NFTs you got for free

2. Password management security practices

Keeping your passwords safe is a must. Your passwords give access to your personal information and your crypto services. Don't take this lightly! Here are a few things you can do to enhance your password safety:

✅ *Never reuse passwords*

Using the same password exposes you to scenarios where hackers can gain access to multiple websites and services you signed up for. During the years there have been hundreds of accidents that may have leaked your password.

✅ *Use a password manager like 1Password, LastPass, or Bitwarden*

Password managers generate long and strong passwords that you can access anytime from any device in a secure way. You'll need to remember only the master password and the password manager will do the rest for you.

✅ *Use 2FA wherever you can*

I recommend Google Authenticator or LastPass Authenticator apps. Make sure to have a second backup if you use a Google Authenticator app. Otherwise, you may lose access to all of your 2FA services.

✅ *Collect some funds and switch to hardware-based 2FA (e.g. Yubico)*

Those help to upgrade your 2FA to a physical USD device that you will need to authenticate before logging in. This is considered the highest level of security. It's advised to have 2 devices. If you lose the first one, you'll still have access to the backup one.

> *Don't keep your passwords and master key from password manager on your laptop, text or Excel file, phone, GoogleDrive/Dropbox, external hard drive (HDD/SSD), built-in Google or Apple password manager. Files and Google accounts can be compromised or hacked, devices can be corrupted.*

Actions:

- Visit Have I been pwned and enter your email to check if your password has been exposed. If this is the case, make sure to change passwords across all affected accounts.
- Install 1Password, LastPass, or Bitwarden. Store your master password in a secure place offline.
- Move all of your passwords into one of the recommended password managers.

- Remove all of your passwords from built-in Google or Apple password managers and other places. You should not have passwords anywhere else except your password manager.
- Install LastPass Authenticator or Google Authenticator. Add it as the default 2FA option in security settings.
- Turn off SMS authentication on all of your services as it's not secure and can be hijacked.
- Put extra cash every month to buy 2 hardware-based 2FA devices(Yubico, Google Titan, or Thetis). Upgrade your 2FA across all of the services that support hardware-based 2FA.
- Remove your phone number and email as a backup option for your Google (and other) accounts. Use backup codes or 2FA devices.

3. Crypto wallet security practices

All play & earn scholars interact with crypto assets every day. A lot of those players lose in-game assets just as regularly because they don't follow protect their wallet interactions. Make sure you're not one of them.

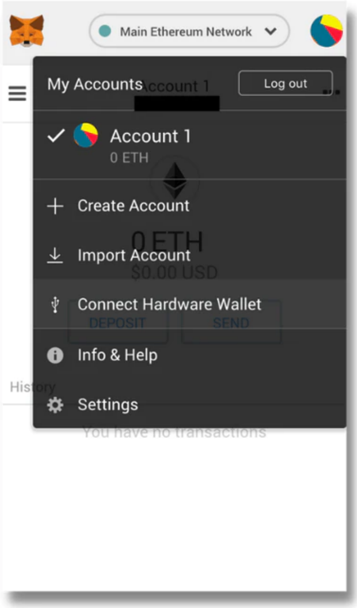
✅ Use a separate browser, browser profile, or laptop for gaming

As a p2e gamer, you should have a second browser that you use strictly for blockchain gaming. If you can afford it, use a new laptop. Such an approach will reduce the risk of massive data collection and potential hacks.

Alternatively, you could create a separate browser profile that you'll be using to play games on. Again, a new browser or laptop would be ideal.

✅ Use a crypto hardware wallet

If you plan to work with crypto in the long-term you must buy a crypto hardware wallet like Trezor or Ledger. These wallets don't have access to the internet and their only function is to sign transactions so you can't install viruses there. Also, you can easily connect a hardware wallet with the Metamask extension.



Main Ethereum Network

My Accounts [redacted] Log out

✓ Account 1
0 ETH

+ Create Account

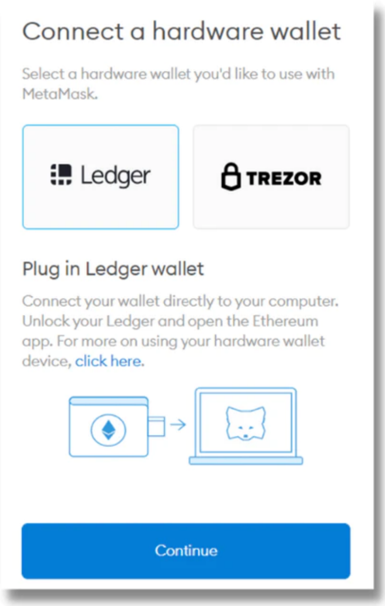
Import Account

Connect Hardware Wallet

Info & Help

Settings

1



Connect a hardware wallet

Select a hardware wallet you'd like to use with MetaMask.

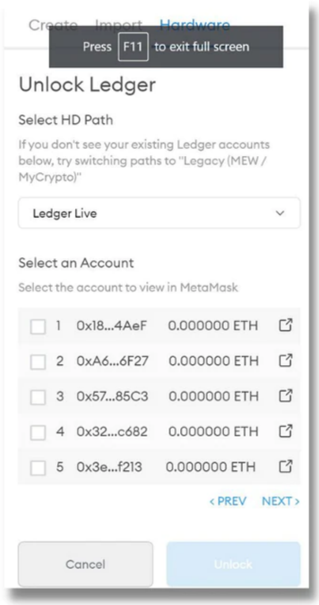
Ledger TREZOR

Plug in Ledger wallet

Connect your wallet directly to your computer. Unlock your Ledger and open the Ethereum app. For more on using your hardware wallet device, click here.

Continue

2



Create Import Hardware

Press F11 to exit full screen

Unlock Ledger

Select HD Path

If you don't see your existing Ledger accounts below, try switching paths to "Legacy (MEW / MyCrypto)"

Ledger Live

Select an Account

Select the account to view in MetaMask

□ 1	0x18...4AeF	0.000000 ETH	
□ 2	0xA6...6F27	0.000000 ETH	
□ 3	0x57...85C3	0.000000 ETH	
□ 4	0x32...c682	0.000000 ETH	
□ 5	0x3e...f213	0.000000 ETH	

‹ PREV NEXT ›

Cancel Unlock

3

Extra tips:

- Apply the same security measures to your seed/secret phrase as for the master password of your password manager: multiple backups, split seed phrase and store it in different locations, never upload/send/store it online or on an external device.
- Store most of the funds in your hardware wallet (also called a cold wallet). Keep small amounts in a hot wallet that is not connected to your hardware wallet. A hot wallet is any wallet that has exposure to the internet: mobile or desktop wallet, Metamask wallet, etc.
- Make all purchases in your hot wallet and only then move the assets to your hardware wallet. You'll be surprised how many hacks have been done by simply purchasing NFTs or in-game assets on phishing websites from a hardware wallet directly.

Actions:

- Install a separate browser (Brave, Chrome, Edge) to play blockchain games. Create a fresh Metamask account on it, don't use it anywhere else. Don't install any extension, login to any service or website that isn't on your playing game list.
- Buy a crypto hardware wallet. Move your crypto funds there.
- Connect your hardware wallet to Metamask in a gaming browser or a separate browser profile.

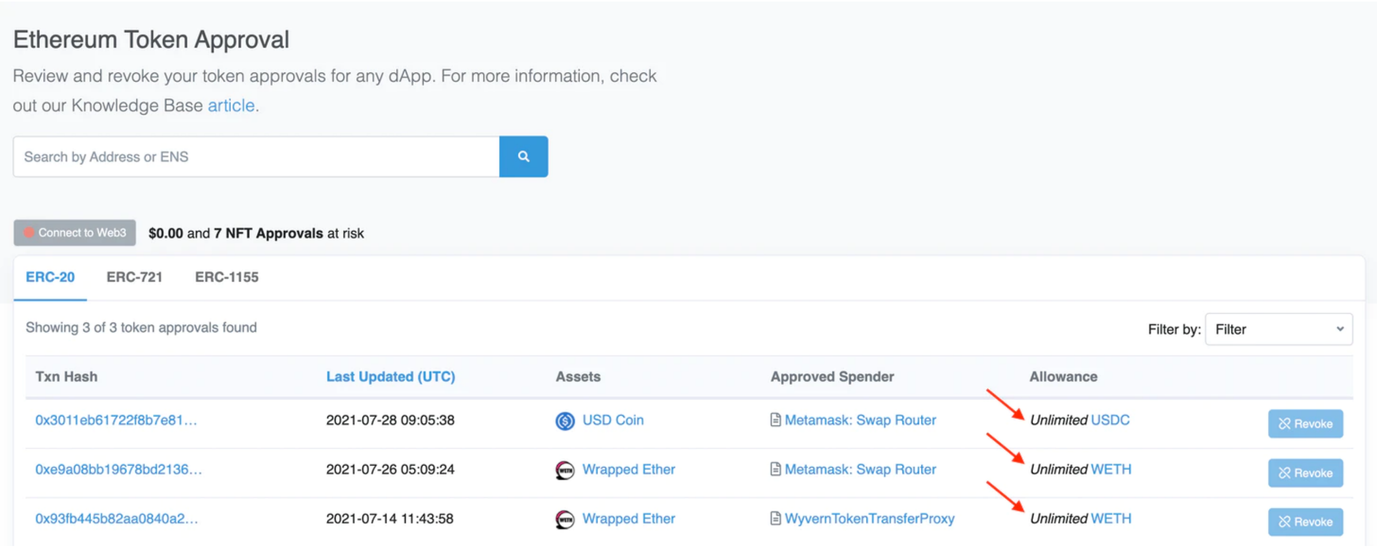
4. Smart contract security practices

✅ Limit smart contract approvals

When you work with tokens on any EVM-compatible blockchain (Ethereum, Avalanche, Fantom, Polygon, Binance Smart Chain, etc.), each transaction requires a token approval before it can be confirmed and sent to the network. This is a security measure that protects Dapp developers and allows the Dapp smart contract to validate the amount of tokens you possess.

Setting a spend limit prevents a smart contract to drain all your tokens (e.g. USDT) if the contract is malicious or has a backdoor. Therefore, always control what permission you give out.

Here’s an example of the wallet that gave permissions to spend an unlimited amount of USDC and WETH respectively.



Ethereum Token Approval

Review and revoke your token approvals for any dApp. For more information, check out our Knowledge Base article.

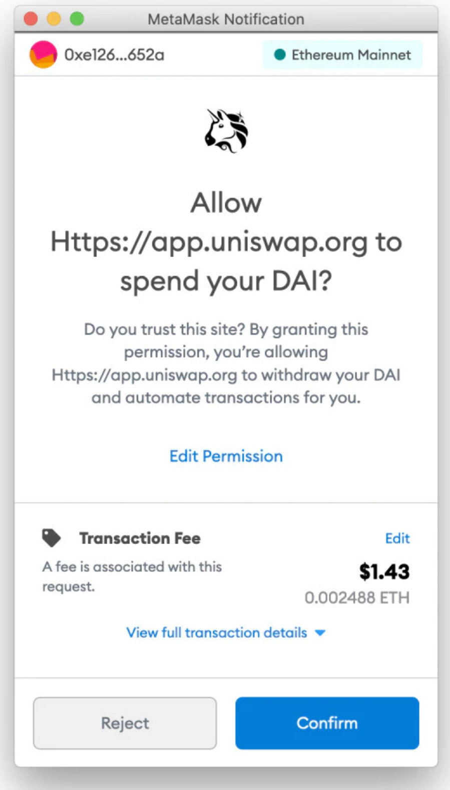
$0.00 and **7 NFT Approvals** at risk

Showing 3 of 3 token approvals found

Filter by: Filter

Txn Hash	Last Updated (UTC)	Assets	Approved Spender	Allowance	
0x3011eb61722f8b7e81…	2021-07-28 09:05:38	USD Coin	Metamask: Swap Router	*Unlimited* USDC	Revoke
0xe9a08bb19678bd2136…	2021-07-26 05:09:24	Wrapped Ether	Metamask: Swap Router	*Unlimited* WETH	Revoke
0x93fb445b82aa0840a2…	2021-07-14 11:43:58	Wrapped Ether	WyvernTokenTransferProxy	*Unlimited* WETH	Revoke

Next time when you need to approve some token, click Edit on Permission and customize the spend limit to the amount of tokens that you want to send.


MetaMask Notification

0xe126...652a

Ethereum Mainnet

Allow Https://app.uniswap.org to spend your DAI?

Do you trust this site? By granting this permission, you're allowing Https://app.uniswap.org to withdraw your DAI and automate transactions for you.

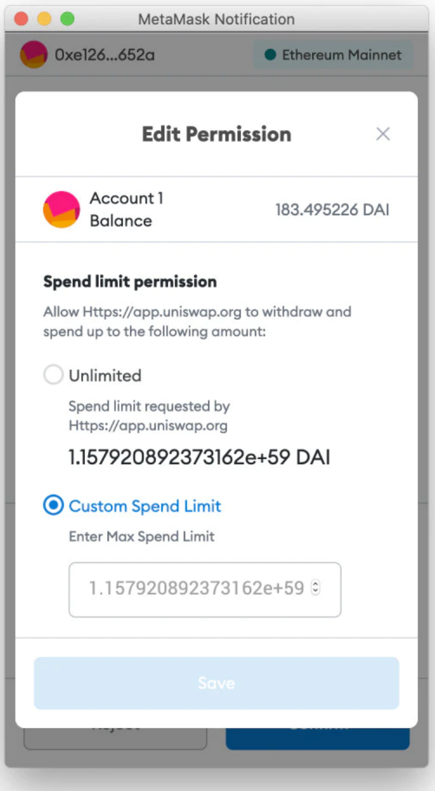
Edit Permission

Transaction Fee — Edit

A fee is associated with this request. $1.43 0.002488 ETH

View full transaction details

Reject | Confirm


MetaMask Notification

0xe126...652a

Ethereum Mainnet

Edit Permission

Account 1 Balance 183.495226 DAI

Spend limit permission

Allow Https://app.uniswap.org to withdraw and spend up to the following amount:

○ Unlimited

Spend limit requested by Https://app.uniswap.org

1.157920892373162e+59 DAI

● Custom Spend Limit

Enter Max Spend Limit

1.157920892373162e+59

Save

Actions:

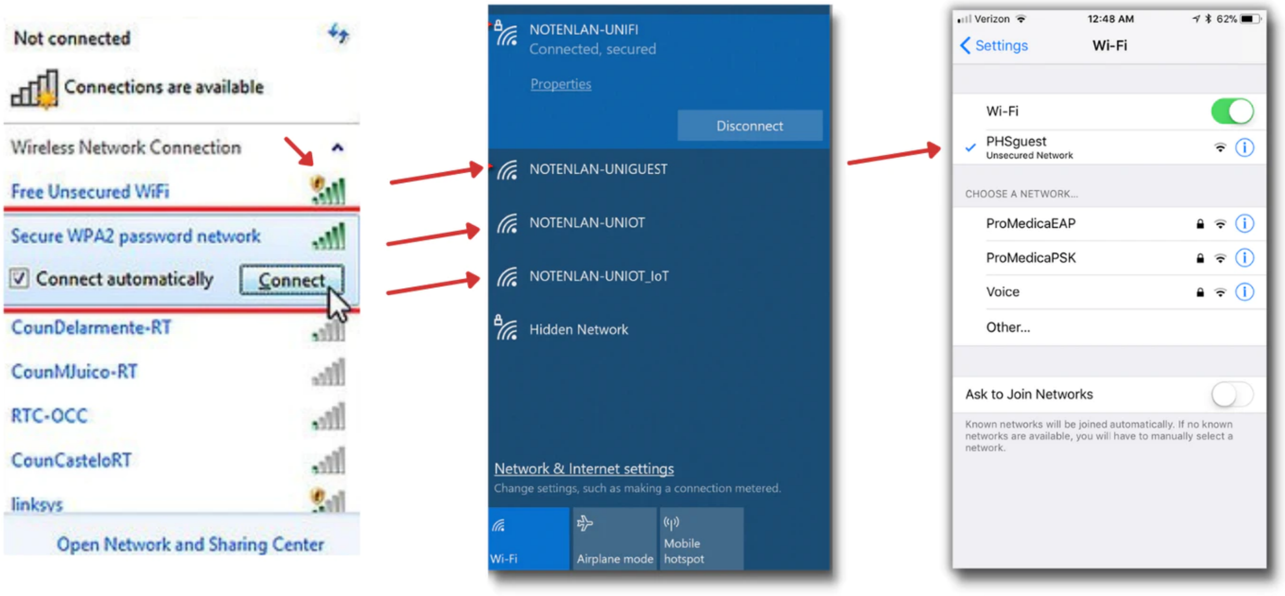
- Go to Ethereum Token Approval, revoke all of your approvals.

5. Laptop/PC/phone security practices

✅ Don't use public WiFi that has an unsecured (open) connection

Your data will be sent in plain text form, which means anyone can read your passwords, login credentials, financial operations, and personal messages.

If WiFi doesn't have a 🔐 sign near their network, it has an unsecured connection. If the WiFi network doesn't have a password, it has an unsecured connection. If the WiFi network has a login and password that you have to open in your browser, it has an unsecured connection. Below are examples of a public open network.



If you need to use the internet asap, use a mobile hotspot instead. Actually, you should prefer this method at all times in hotels, airports, internet cafes, and inexpensive public places.

✅ Do regular antivirus and software checks on your PC and your phone

This one is kind of obvious but you'll be surprised how many people don't perform antivirus scans. You can use a standard Windows Defender or for more advanced checks try MalwareBytes. Fortunately, it's very hard to install external software to MacOS so I don't think you'll have any problems there.

If you have an old computer that you've used for a while, audit all of your installed apps or ideally do a fresh install of your OS. This will clean up all junk software from your device.

Do the same with your mobile, especially if it runs on Android. After you have a clean phone, don't install any apps from external forums, torrents, random resources. Use official marketplaces for all your installs: Play Market or AppStore accordingly.

✅ Never download or open files from strangers

You never know which file will end up installing a keylogger. Never download files with **.zip.exe* extension, they most likely contain viruses. Try to avoid downloading files from Bittorrent but if you have an urgent need, don't open any files that look suspicious.

Actions:

- Always double-check if the network is secured. Remember that 🔐 sign is mandatory.
- Install an antivirus if you don't have one. Set up an automatic weekly scan.
- Configure your Windows laptop to always show the file extension.
- Audit your installed software on both PC and mobile. Remove what you don't use. Ideally, reinstall your OS.
- Disable applications that start on launch that you don't absolutely need.
- Avoid helper tools like a plague, including clipboard managers, auto-upload screenshots, remote desktop apps like Teamviewer, applets for crypto prices, apps from untrusted devs.
- Disable automatic snapshots, backups, screenshots to your cloud storage software (GooglDrive, Dropbox, etc). Turn them off and never turn them back on again.
- Log out of all devices and log in again. Keep track of devices you've been logged into.

I know this all sounds like a lot so try to do one bucket of items each day until you cross all of them. And remember, nothing is more important in crypto that to keep your funds safe.

Cheers,

D