SHIBA INU

Safeguarding Guide

10.15.2022

Contents

Discord Account Management

Your Discord account provides you with access to many amazing Friendshibs and opportunities! We see you all creating beautiful artwork, fellowships & investments on a daily basis through these accounts.
Let's take a look at what we can do to protect that!

Two-Factor Authentication

Two Factor Authentication means that logging in to your account requires both your password and a passkey only **your** device has access to. Often, this comes in the form of an Authenticator app, such as **Google Authenticator** or **Authy**, Both of these can be installed through Google Play or the Apple Store.

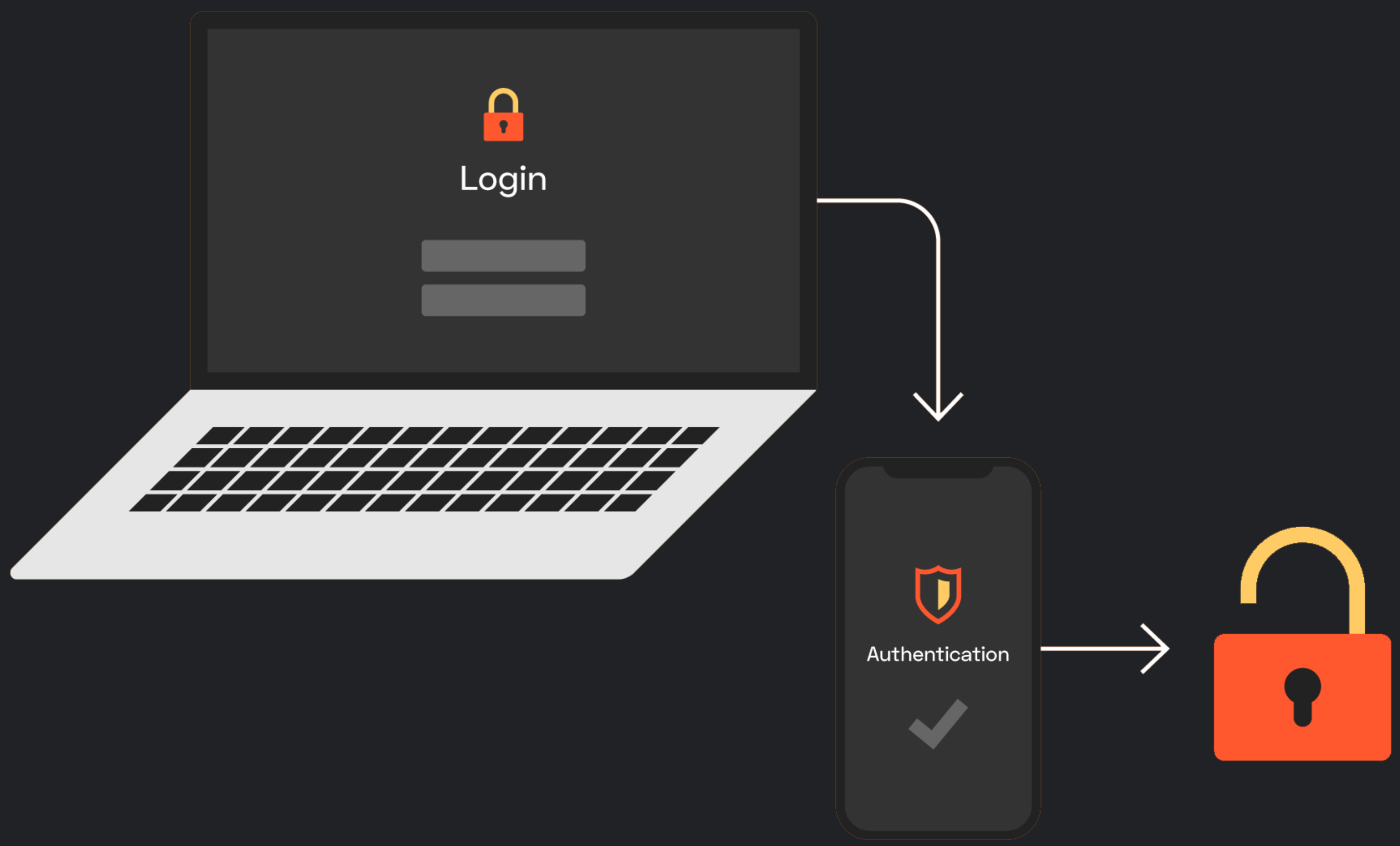
The Two Factor Authentication setting can be found within discord by moving down to the Gear Cog to enter your settings & selecting the top option; 'My Account'. Here you will be able to begin the process to enable Two Factor Authentication.

Google Authenticator

If you're using Google Authenticator, you will choose to either scan a barcode, or enter a key to connect your Discord account. You can select either option, as Discord provides both. Bear in mind, that going with the option of a barcode will require you to have a barcode scanner app installed on your device.

Authy

If you're using Authy, you will need to provide the app with your phone number and E-mail address, once entering this information, a pop up window will appear asking if you want to authenticate your device via text or phone call, do what is best for you.



Most Social Media platforms have options allowing you to enable Two-Factor Authentication, you should consider using it to guard your credentials.

Discord Account Management

SMS Backup

This is useful when you do not have access to your authenticator application when logging in.

SMS Backup works as a second layer of 2FA. If you are unable to access your authenticator, you can log in by requesting a key to be sent to you via Text message. This key will allow a one-time log in.

Backup Codes

Within your safety settings you will find various backup codes that have been generated and allocated to your Discord account to allow bypass of two-factor authentication on log in. You must hold your Discord email address and password if you wish to use a backup code, and usage of each code will eliminate it's usage going forward. If you run out of codes, or wish to reset them, Discord will allow you to generate a table of new codes. Ensure your backup codes are as secure as your email address and password, as they carry as much importance, if not more.

Authorized Apps

When traversing through Discord's many Servers, and interacting with different Bots, access to some will need to be authorized by you. This authorization can allow malevolent forces full access to your account. You should always regularly check which apps have authority within your account, and whether they are still required. Similarly, prior to granting approval to these instruments, you should ensure they are safe to use, the same as you would when connecting a Cryptocurrency wallet to an external website.

Avoiding Phishing Links

Scammers become smarter every day, and as changes are implemented to online services, scammers are always present, silently contemplating how they can exploit you for your information. Phishing links are attempts to trick you into clicking a link, often resulting in loss of personal information & accounts.

It's for this reason that you should scrutinise everything, and always seek legitimacy. Never click links unless it's from someone you trust. There are services online that can check links for you, so that you don't have to visit them yourself, putting yourself at risk.

QR Codes

QR codes are a great way of drawing attention to your website or services. You can scan QR codes using a QR Code scanner to direct yourself to the website or service it represents. Almost all modern phones have the ability to scan QR Codes.

Never scan QR codes from untrusted sources, scammers can embed phishing links within them, and compromise your accounts.

Unexpected Messages

Often within Discord, you may receive messages from someone you don't know. This should always be treated as suspicious, especially in the Shib server as it has over 100,000 members. For what reason would someone want to message you specifically? And, to enlighten you of your mystery crypto winnings? Avoid at all costs.

Malevolent scammers will often try to befriend you & try to acquire information. Often in Crypto, they will provide you with a link to a fake minting site or wallet connecting service.

Normally, members of staff will not try to contact you. If this happens and the account looks like it belongs to a member of staff, always check the 4 digit code at the end of the name, match it with the person you're speaking to within the server.

LINKS FROM UNTRUSTED SOURCES SHOULD NEVER BE OPENED. DELETE THE MESSAGE AND REPORT IT TO THE MODERATORS IF YOU ARE UNSURE. ALWAYS GET EVERYTHING VERIFIED & DO NOT ADD PEOPLE YOU DON'T KNOW.

Scammers & Compromisation

Scammers can be crafty, but they're often careless in self representation. Usually the goal is to obtain money as fast as possible then delete the account and disappear.

Tell-tale signs of a scammer are often:

- They have no profile picture or use a very commonly used one, especially in the case of BOT scammers, these are multiple accounts that are created to post malicious links, they often all share the same profile picture or sometimes a group of specific pictures.
- Slow response times/No response.
- Little participation in public server communication, or statements not related to the current conversation.
- The account has only existed for a short period of time.

What to do if your social media account is compromised.

Sometimes, accounts can unfortunately be compromised, even when you take all precautions to secure them. This is a frustrating situation to be in & steps should be both considered and taken quickly before further damage can be done.

How did they get access? Often access is granted either by the scammer knowing, guessing or obtaining your password by force.

It's also possible they gained access to your Email inbox. You should first ensure your Email address and its backups are secure and that no passwords have been changed by access of E-mail. You should always have a second E-mail address or mobile number connected to your primary E-mail account for Authentication.

Change your password to something more complicated. Your password would probably have been encrypted by the company that holds your details, but if it's a simple password, for example, letters and one or two numbers, it's relatively easy for a hacker to break the password using brute force software. This type of software runs through millions of permutations at lightning speed. Most sites have systems in place to prevent these types of attacks but Hackers are sneaky and often find ways around them.

Scammers & Compromisation

Do not use the same password for everything. Once someone gains access to one account they will have access to them all. It can be difficult to keep track of all these passwords so be sure to have them written down somewhere safe, not electronically!

Monitor Active sessions! Some platforms allow you to see where you're currently logged in and what device you're accessing the platform on, if any of these look suspicious, terminate the session & change your password, (Don't forget, using an VPN will display a different active session than your usual one!).

What to do if your wallet is compromised

Having your wallet compromised is pretty gutting, even more so watching your investments just up and leave out of your wallet. In some cases, the wallet can be re-secured by revoking contract access, but this isn't always the case. You should immediately disconnect from any services you connected to, this should be done frequently. Never leave your wallet connected to a service.

Even if you regain security of the compromised wallet, hackers now know that you could be someone susceptible to their tactics, and searching for the history of your NFT's through social media can allow the scammer to figure out who it is they need to target.

Because of this, often we suggest you create a brand new wallet with separate keys and avoid displaying which NFT's you own. If you like to show them off, keeping your NFT's in a separate wallet from your currency with no transactional history between the two can prevent anyone discovering how much you are holding alongside your NFT's.

Sometimes, the scammer will only target your Cryptocurrency and not your NFT's, this happens either because the scammer hasn't noticed or considered them, is targeting a specific Currency/NFT, or is waiting for you to add gas funds to the account so they can take the gas before you're able to move the NFT. Making transactions with a higher paid gas fee (Higher transaction speed) can beat the scammer when it comes down to a race of draining the account but naturally can cost you a lot of money if you fail.

If the compromised wallet has been drained, get in touch with your local authorities for referral to their Cybercrimes divison, report the theft of your currency and NFT's & notify Opensea of the theft to have the NFT's locked from trading (By doing this you will be required to provide a signed notary from your Lawyer/Solicitor that proves ownership in order to have Opensea unlock them again). In future cases where the scammer is possibly caught, the NFT or Crypto could possibly be returned to you.

In the case of tokens being locked into a service, (Like Shibaswap for example) methods can be used to move ownership of locked funds to another wallet, the following method HERE can be applied in many scenarios by changing the address used in the instructions, to the one for the contract of your locked assets.

VPN

In basic terms, a VPN provides an encrypted server and hides your IP address from corporations, government agencies and would-be hackers. A VPN helps to protect your identity and your data from any prying internet eyes.

VPNs can't make online connections completely anonymous, but they can increase privacy and security. To prevent disclosure of private information or data sniffing, VPNs typically allow only authenticated remote access using tunnelling protocols and secure encryption techniques.

Many VPN services can be paid for on a monthly or yearly basis. Some offer their services for free, usually for a limited amount of data usage.

A VPN can:

- Secure your traffic
- Protect you from phishing
- Keep your crypto activities on the down-low
- Hide your IP Address
- Prevent legal issues
- Unblock geo-restricted coins and trading sites
- Bypass firewalls

Do not only reply on a VPN, though. Ensure alongside protecting your network, you are also using anti-virus, 2-factor authentication, script/ad blockers, and password managers.

Hardware Wallets

A great way to stay safe in crypto is by using a cold wallet, or hardware wallet. These are physical devices that store your private keys offline so they are safe from malware and most exploits. While they are not fool-proof, they securely store your seed phrase and provide a way of externally authorizing transactions for an added level of security. The most popular hardware wallet manufacturers include Trezor and Ledger

Hardware wallets can apply an additional layer of safety to your funds because they minimize the risks that cannot be controlled, such as major data breaches at cryptocurrency exchanges, or malware that exploits zero-day vulnerabilities in mobile and desktop operating systems.

But, to be clear, hardware wallets are not perfectly secure. For instance, last year, hackers broke into the servers of hardware wallet manufacturer Ledger and possibly pushed out malicious firmware updates for Ledger wallets. But these types of supply chain attacks are much harder to pull than phishing scams.

Also, in the past few years, the landscape has evolved much more and hardware wallets have become much easier to use, giving you a nice combination of security and convenience.

Keep your recovery seed safe: Every wallet has a recovery seed, which you can use to restore your keys if you wipe your device or if you lose it and get a new one. You should keep a safe copy of this recovery seed someplace safe, preferably not in your cloud or disk drive.