

Discord Safety

How to Protect Yourself on Discord

Almost all NFT projects use Discord to connect with their communities. Therefore, scammers target Discord to try to access your cryptocurrency and NFTs. This is called social engineering. Scams aren't new, and the saying "if it is too good to be true, it probably is," still applies. But we are here to help! We have some handy tips on best practices to stay safe in the digital space of NFTs.


The first thing you MUST do is:

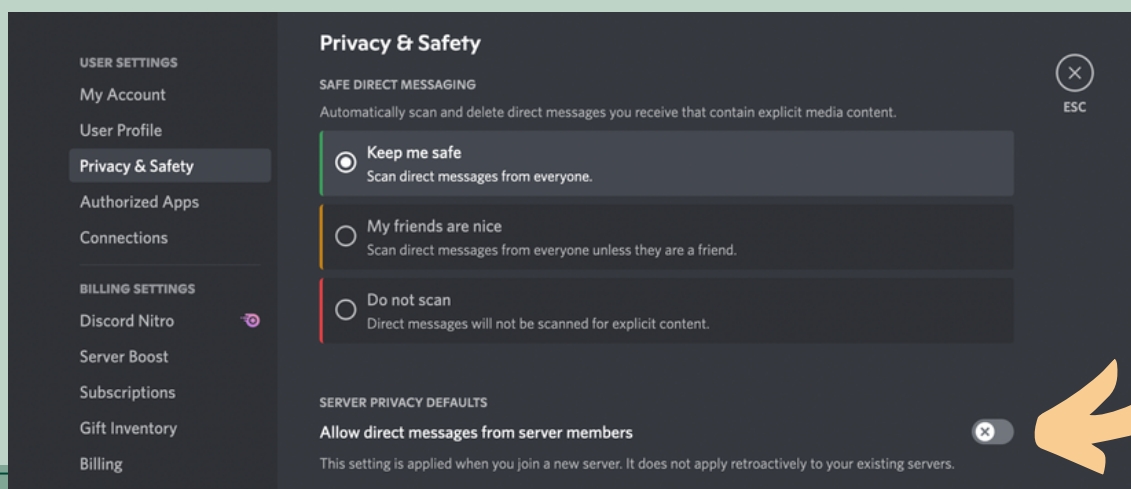
1

Turn off your Discord direct messages (DMs)

Most communities you join on Discord will say this from the outset: "we will NEVER direct message you."

A lot of scams are happening via Discord direct messages, so it is best practice to turn off this setting. If you want to connect with someone individually, go to Twitter.

- User Settings  → Privacy & Safety →
 - Make sure 'Allow direct messages from server members' is switched off.
 - This may be a good time to check a few other settings. I have everything OFF.



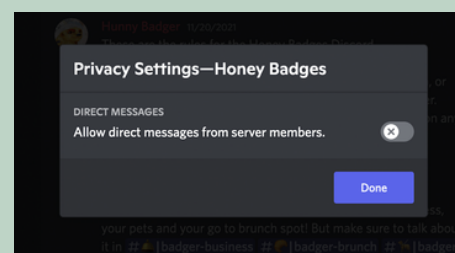
Discord Safety

Reminder: Your public wallet address is the hash of numbers and letters (an Ethereum wallet starts with 0x.....). Your seed phrase is the series of randomly generated words that you were given when you set up your wallet. You only ever need it if you are setting up your wallet on a new device, and you initiated it.

1 continued....

When you turn direct messages off, this will apply to all new servers and communities that you join. However, it won't apply retrospectively to ones you've joined earlier. To fix this:

- Right click on any existing servers' image → Privacy Settings
- Make sure 'Allow direct messages from server members' is switched off.



2 Look for RED FLAGS

How to identify a Discord scam. (This also applies to other social media you use)

1. **Impersonations** – these scams often impersonate Admins or Mods of a server. Team members will never directly message you on Discord. If you think they have, go back to the community channel, and ask them directly. Some common scammers pose as community support; this is social engineering. If you need help, it is better to open a support ticket in the community channel.
2. **Prizes** – 'You're the lucky winner.' 'This is a secret mint.' 'This is the last chance to get in.' Or other bold claims of making huge profits, if you just act now. It's too good to be true, trust us! These scams are relying on you to get excited and forget basic safety practices.
3. **Links and Pictures** – don't click on anything you were direct messaged. Especially if you weren't expecting it. Some common scam links include links to other Discords, links to an allow list for a big project or a blank image that won't load. Don't click them.
4. **Spelling Mistakes** – and typos. It is probably a scam.
5. **Issues with your account** – 'Your account has been compromised.' These types of direct messages are trying to use fear to get you to act in a hurry.
6. **Seed Phrase** – No one needs this from you! Ever! You can share your wallet address in community channels. You use your wallet address to mint NFTs or get airdrops. It is like an email address. Your seed phrase is the private password, which should never be shared with anyone.

Discord Safety

3

Links on Discord:

Many community channels won't let you post links, and it's best practice not to click on them. The exceptions are links that the project leads, or moderators, have marked specifically in the community channels for minting, roadmaps, websites, or other social media.

- If you are unsure, just ask.
- If a server is compromised, the links that are put in the chat can be compromised too. It is best practice to be cautious.

4

Server Hacks:

This occurs when a scammer gains control of an administrative user's account (like a Mod) and locks out other team members. Once this has occurred, they can post realistic looking announcements and scam links. Your best protection is to pause and think before you click any links. If a Discord gets compromised, the project will often send out information on Twitter, and there will often be warnings in other communities. Check there first.

Use a Strong Password - If you do get compromised on Discord, immediately change your password.

Verify your email address - This is important for the next step.

Set up Two Factor Authentication (2FA) - this adds an additional method of verification when you log in, such as a code received on your mobile phone.

(To set up 2FA, you have to have added your phone number and verified your email address. Discord will allow you to create accounts without this, but it's safest to enable 2FA.

Settings → My Account → Enable 2FA)

For more on Discord security, this course provides templates, bot recommendations, and extra security tips, especially for project founders and moderators.