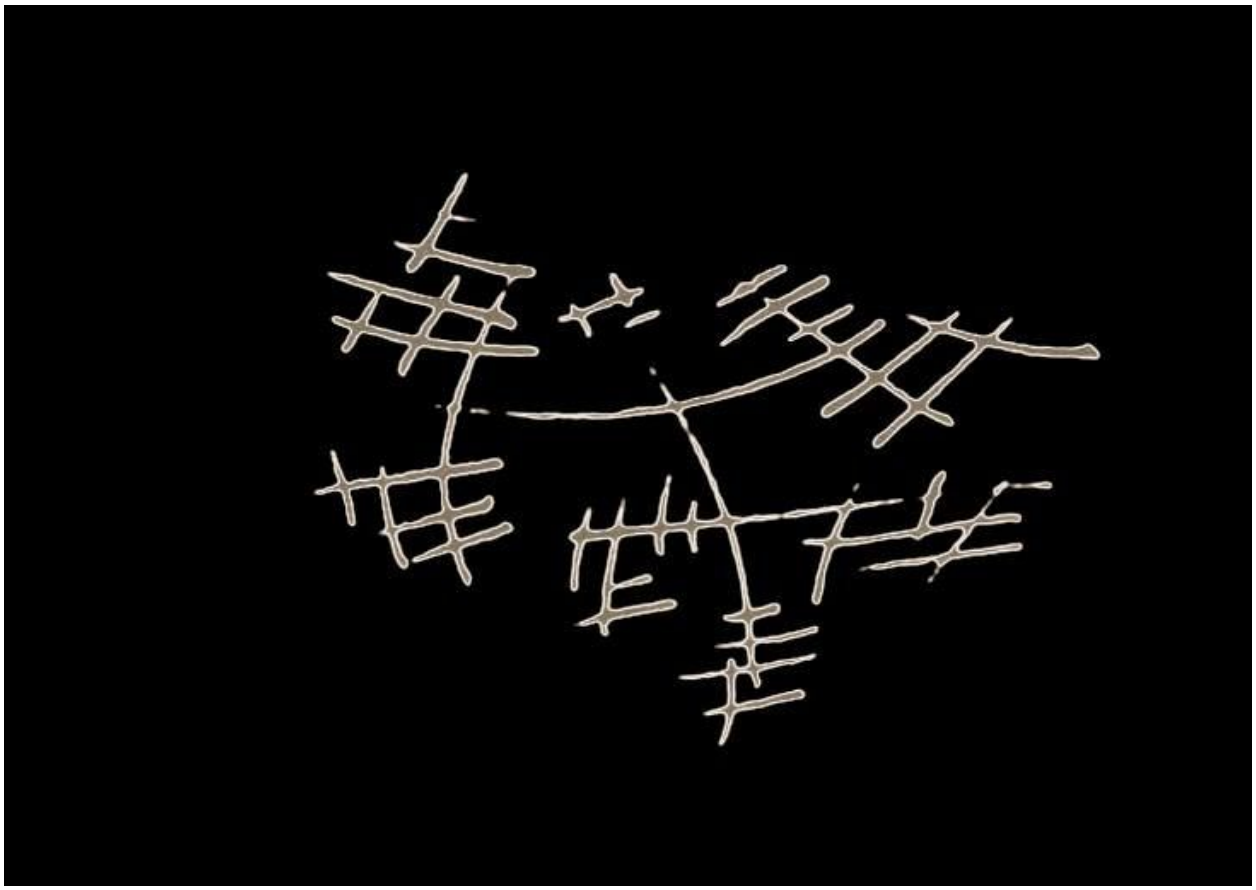
What to Do When Your Web3 Project Discord Server Is Hacked



#How a Security Audit Might Prevent your Discord Server from being Hacked

Greetings dear readers! Today we are going to discuss an unusual question with you, something that we, people who are sometimes far from social networks, have to deal with partly. I am talking about Discord. With its growing popularity and its 350 million users, Discord has now become a magnet for hackers and fraudsters. What can go wrong, you ask? Many things, it turns out — you can even lose your account.

Since I myself specialize in investigating incidents and hacks related to Web3, I often have to deal with it, however, I do everything exclusively on-chain while in Discord a whole world of dangers awaits us. Many attacks are also coordinated, which makes defending against them unusually difficult, why? It's simple:

- Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.

And if we have a coordinated organization against us, we need to be on our guard. This is the only way out that has a real effect. Got scared? Me as well. But let's face it with no fear - if we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

https://youtu.be/uf_JGdkyTEY

Some of the mentioned attacks have already got web-3 life - just remember the very essence of **Eth_sign or Allowance Approve attack** or other popular attacks (there is this list as well) - no wonder that they are used here as part of the scheme.

It's quite another thing with attacks that are specific to Discord - they can be even more dangerous and in my opinion, greatly underestimated. To begin with, I suggest you read the article below to understand the basics of the attacks going on in our industry.

Read:

- An ultimate list of rules any on-chain survivor should follow to stay safe!
- Violent Attack Vectors in Web3: A Detailed Review
- Blue Buttons of Death
- How to store crypto securely — tips from CIA_Officer
- QR Code: An Underestimated Danger

Below, you will see not a typical article, but a systematization of knowledge - SoK, in which I will rely on authors that I myself trust in this matter, and at the end, I will write my conclusions.

Enjoy reading!

#I - Discord server security

Content

Large numbers of spammers can flood your server with low-quality content to distract administrators and moderators from threats, as well as flood your server logs with events such as role assignments and members joining to hide the changes they make. This is sometimes referred to as a server raid. They may also post unapproved links in an attempt to steal community member credentials and tokens. Always configure the following settings to help protect your server from this:

- Choose the **Highest** option in **Safety Setup** so that only Discord accounts with a verified phone number can join your server
- Set up Rules Screening so that all members must perform manual actions before posting messages, decreasing the ability for bots to post unwanted content
- Do not allow **any** users except for moderators and administrators to post links, including bots, unless this is absolutely necessary for verification or security

- Configure the AutoMod feature to **Block Spam Content** in all public channels

Permissions

- Two-factor authentication (using authenticator apps that generate six-digit codes, such as Google Authenticator on Android OS or iOS) should be enabled on every account that can use @mentions or post to announcement channels
- All moderators and administrators should revoke (and not grant) permissions for other apps to administrate your server or post as them
- Try using a test Discord account on your server to post links and perform other actions that can be abusive, or use the View Server as Role feature if your test account can't join your server because it doesn't have a verified phone number

Audit

If you know of an individual or team that can be trusted to secure your server or verify that it has been secured, and you have time to schedule an audit, it's worth the time and cost to have them identify risks. If you want to have a good understanding of what permissions could put your server at risk, the auditor joins you in a screen share so you can make the changes yourself. The auditor should check for the following, and more:

- Bots and integrations that are not widely used, or clones of popular ones
- Webhooks and announcement channel following that can deliver bad content
- Verify that bots can't assign roles that let users post announcements or view private channels

Logs

Designate administrators or senior moderators to monitor logs for administrator activities to see if bots or other administrators are performing suspicious tasks, such as granting elevated permissions. Some bots can post specific log entries to a channel.

Here are some good security tips from Discord folks themselves:

1. Never let yourself be persuaded to reveal your authentication token. With your token, malicious users can sign in and take over your account.
2. Never share any info from the Discord's Developer Console — you likely will never need to open it anyway.
3. Stay away from "Free Nitro" giveaways. "Discord will never ask you to scan a QR code in order to redeem a Nitro code. Do not scan any QR codes from people you don't know or those you can't verify as legitimate."
4. Enable 2-Factor Authentication
5. Help fight scams by using the red "Report Spam" button at the top of DMs.
6. And, yes: never give your password to anyone.

https://youtu.be/DYITjdbZiao

One final important note on human nature. In this piece on the best day-to-day online security practices, the author points out that improving our online security habits comes at a price of human convenience. It is much easier to use the same password for multiple logins, Two-Factor authentication may be annoying, and hardware or smart contract wallets are cumbersome to use.

#II - What to do when your Discord gets hacked

If you're concerned about security threats due to other Discord servers being attacked, or during important times, there are ways to quickly protect your existing community from attacks while focusing on crafting clear announcements and answering questions.

- **Source**

These changes can also be quickly reverted.

- **Pause Invites** for your server in Server Settings > Invites > Pause Invites
- Turn on **Slowmode** for all public channels, with a setting of at least **1 minute**, so that moderators and administrators can keep up with questions... I recommend a Slowmode of **5 seconds** in all public channels at **all** times on most Discord servers
- Temporarily stop members from editing their roles by denying bots permission to **manage roles**, improving security while making your logs clear for audits.

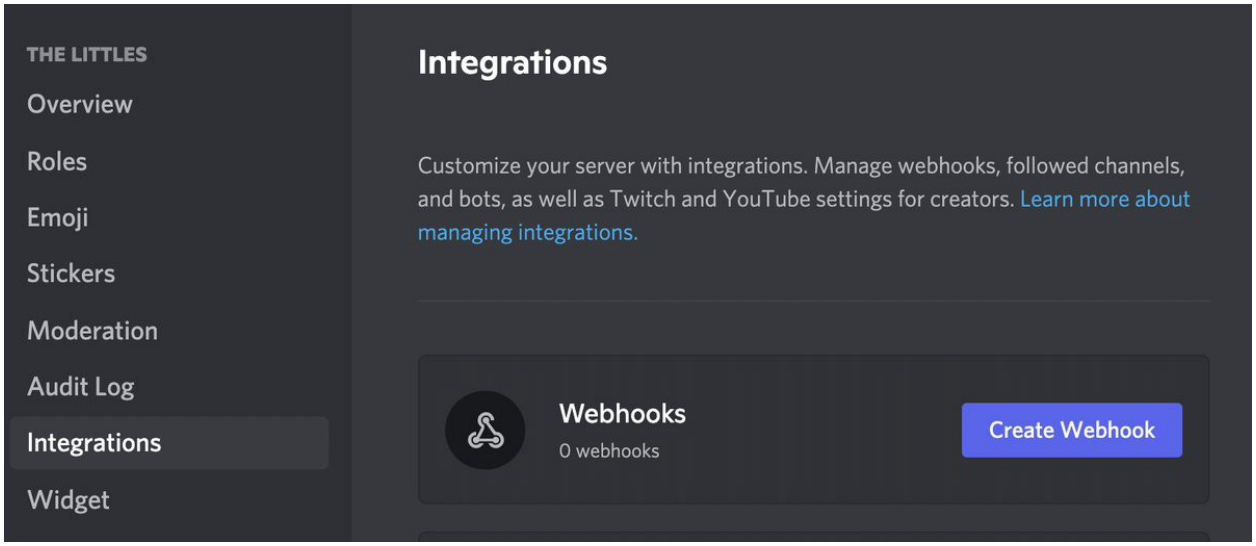
Let us break down each method of protection in detail. For better understanding, after we break down the most unpleasant methods of attack in Discord, some of them will be exceptions and only your caution will save you from them!

Communicate

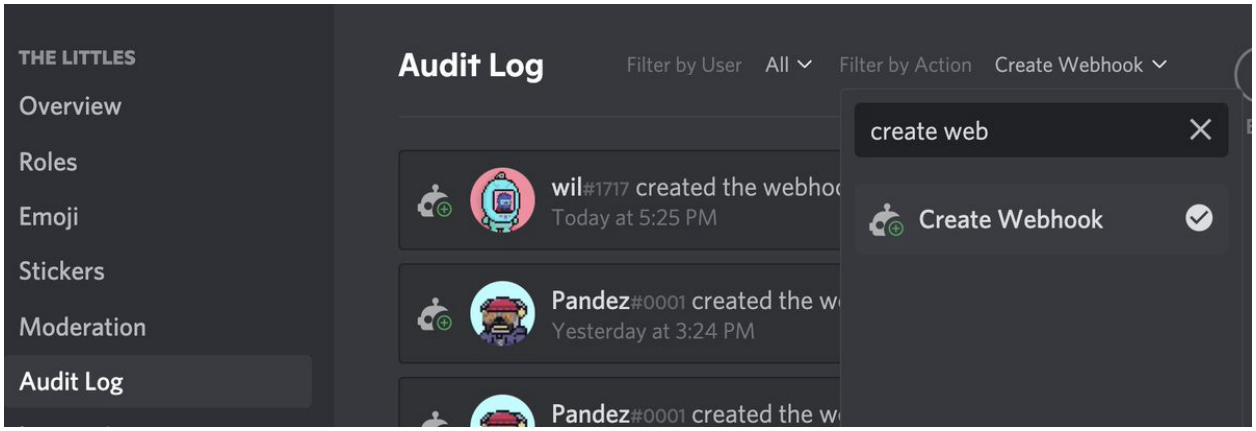
Go on Twitter and tell your community that your discord has been compromised to minimize damage. Oftentimes, hackers close all forms of communication in Discord so no warnings can be sound.

Take control

The majority of hacks now are through something called “webhooks” (See what they are). Basically, a hacker installs a remote control in your home to steal control and post a fake mint site on your channels. Go to your server → server settings → integrations → webhooks → select and delete all. By doing this you should be able to stop the hacker from posting messages. You are not out of the weeds just yet, **you must find the hacker from creating new webhooks**, but how?



Go to your server → server settings → audit log → filter by action (top right) → type in “create webhook”. This will allow u to find out whose account is compromised and who is creating these webhooks. This is where the hackers are. Ban this person for now.



What else the server owner should do?

Make sure you are the server owner. You may not be the person who made the server, but you must tell the creator to transfer ownership to you, so you can take the right actions when things go wrong. Only give permission to a few selected, trusted people.

It’s a fact that if you use Discord for any amount of time in the crypto space, you’ll start getting manual and automated messages from blackhats, fraudsters, and scammers. Sometimes, these are legitimate (though somewhat spammy) messages.

There are a lot of projects in crypto and more are being founded every day. Unsurprisingly, these projects want to try and get the word out about their protocols. But more often than not, these messages fall into three categories:

1. They impersonate a crypto server or a specific individual. It may look like an invite to the SushiSwap server, but it isn't. It may look like Vitalik Buterin himself is DMing you, but he probably isn't. If you're interested in joining the Discord of a project you like, make sure to join that server by finding the link on the project's website or other authenticated social media channels. Don't join the server of a project through a link in a DM.
2. They offer fake giveaways. Scammers know that their DMs come off as spammy, so they want to grab your attention by offering free tokens. This one is trickier because projects airdrop tokens to users all the time, so it's more difficult to tell what is legitimate and what isn't. However, it's always a good idea to ask the admins of that protocol directly whether they are airdropping and whether they are airdropping via Discord DMs. In almost every case, the answer is "No, that's a scam." If you click the link in the scammer's DM and follow the instructions, you often end up ensnared by the scammer.
3. They offer tips on the latest and greatest tokens to buy. These servers are often run by groups of coordinated whales and marketers dupe users with fake alpha and recommended token buys, in order to engineer pumps and dumps. They make money; you lose money.

The above scenarios are the most common you'll experience, and in light of that, it's important to remember some general tips to keep you safe. When you get suspected spam or scam messages, don't just close the DM. Block the user, so you don't get DMs from them again.

https://youtu.be/3GW1QqPNLig

Be careful about clicking links, especially links that have been shortened to hide their final destination. Don't download files, especially executable files, from other users. If you do need to exchange sensitive information with someone, consider using Keybase, which is much more secure and allows for greater independent authentication of a user's account. Those are the basics, which require a healthy dose of common sense in skepticism.

#III - Violent Discord Scam

Recently, a crypto project administrator was attacked by a way of an interesting scheme involving Social Engineering tricks. In this article we analyze how it happened, we look at different Discord scams and we discuss what you can do to protect your identity and your money against these cyber bandits.

- **Source**

Judging from the original tweet, the story goes like this.

1. A scammer picks a target — our victim — who has a presence on a Discord channel.
2. The scammer creates a fake user on the channel impersonating the target.
3. He then starts spamming, scamming, or trash-talking on the channel with the intent to get banned.
4. Discord channel moderators see the mayhem and work to ban this account. Our scammer had skillfully used some known Discord Nitro tricks to manipulate his account user nickname. This way, the channel moderators are fooled into banning the account of the target (and, possibly, the account of the scammer).

5. After seeing that the target is banned, the scammer creates a manipulated image of a fake discussion among the Discord channel's team members about the target's ban.
6. Then, impersonating the channel's moderator, the scammer reaches out to the target via a DM. The target is surprised that he/she has been banned and starts to uncritically accept the words of the scammer who appears to offer help.
7. The scammer fakes urgency insisting that the situation needs to be remedied right now. He asks the target to prove innocence and to come on a Discord call.
8. The scammer convinces the target to share the Discord Web UI computer screen and instructs the target to open Discord Developer Tools and reveal the Discord token. This token can be used to take full control of the account (without the password, and by bypassing the Two Factor Authentication).
9. All this fancy manipulation leads to the scammer gaining full control of the target's Discord account — he can now cause damage to the victim or the victim's company.

So, what happened here? Social Engineering attacks have their own peculiarities. The first point we want to make is that these attacks exploit strong human emotions, such as fear. In our situation the scammer exploited the victim's sense of injustice — "I did nothing wrong."

Second, in order for this attack to succeed the victim had to be rushed. This is the first thing to pay attention to — if you are pushed to give out any information at all, it is a good time to pause.

What else can you look out for when navigating Discord chats? Beware DMs. If you are a heavy Discord user, you likely get invitations via DMs: offers of free token airdrops, invites to exclusive channels, and marketing of all kinds, such as recommended token buys.

Use these working rules of thumb to stay safe:

1. Join Discord servers only via links on companies' sites and authentic long-standing social media pages.
2. When you suspect a scam message, go further than deleting the message — block the user.
3. Pay special attention when opening files — a legitimate business will almost never ask you to open a file. A request may come to you as an invitation to test a game for a prize, for example. Beware. Here is a fresh example of how clicking on an image will send you to a phishing site tricking you into providing your Discord logins. Consider adding an anti-phishing plug-in to your web browser, which will alert you if you get redirected to a phishing site.
4. Watch out for newly minted NFT scams. One victim of a "free" NFT airdrop ruse concluded that "the lesson here is that nothing is free" and "be careful with ANY airdrops you receive. Hiding them is safe."
5. Here is a story of how one company founder narrowly escaped losing all his crypto. His conclusion: when engaging your crypto wallet in some scheme with a new contract, use a burner wallet - a secondary wallet often used to connect temporarily to an NFT minting site. After you obtain the NFT you can then just send it to your real wallet. By holding a minimum amount of funds for a short period of time in this one wallet you thus mitigate your risk of falling prey to a scam.

Check out these attacks:

- twitter.com/paahsecurity/status/1513654317609365514
- twitter.com/mikequeen123/status/1534274373732941830

- www.reddit.com/r/discordapp/comments/ruj8i9/be_warned_theres_this_new_thing_going_around_that
- twitter.com/littlelemonsnft/status/1477923368053706755
- julienvandorland.substack.com/p/the-scr-malware-hack-explained
- therecord.media/nft-creators-tricked-into-installing-malware-in-highly-targeted-attack

---

#IV - General security

Be aware of modern attack methods, carefully read step-by-step my Guide and a Compendium, you don't need a deep understanding of how hacks work exactly but that's important to know how does it look like to be a victim.

Study threat modeling (2) (3) and establish all possible threats even if they seem crazy to you. Being suspicious is always a good thing. After all, fake news only works best with those who carry it to their acquaintances, becoming a kind of donor.

In the same way with attacks, very often you may try to be hacked through acquaintances, pretending to be acquaintances or acquaintances themselves. Always keep this in mind. This world is cruel and dangerous.

#V - Sources

- mirror.xyz/tidus.eth/IkpiXSxTrkm0ZC6Jzd0FspA9ahCmW4MxKsmroVtyVYM
- medium.com/geekculture/what-to-do-when-your-nft-discord-server-is-hacked-for-founders-9a2751d4d066
- medium.com/powerinside-security-lab/how-not-to-lose-your-discord-account-to-a-scammer-%EF%B8%8F-c3e0fb2e50e7
- medium.com/immunefi/how-to-avoid-blockchain-blackhats-on-discord-78e4f278c4a2
- twitter.com/server_forge

Many thanks to the Authors, thank you for your works! @PowerInsideLab, @immunefi, @tidus, @pooria_arab, @Server_Forge ❤️

#Thank you! Stay Safe!

If you want to support my work, please consider donating to me:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A** or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU** - BTC
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**