Extended Context

Extended Context on Unofficial FTC Discord Compromised

On November 26th, 2025, at roughly 4:30 PM EST, the FTC Discord staff team was made aware that our server owner of the Unofficial FIRST Tech Challenge was targeted in a phishing hack. The vast majority of the mod team quickly rushed for an emergency meeting, and created a new server to continue where we left off. Maintaining the incredible FTC community we had on the old server is our #1 priority, and we are incredibly thankful to moderators on the Unofficial FRC server for joining forces with us as we push for normalcy.

Come join us at our new location! → discord.gg/ftc

After we were notified of the hack in the late afternoon, an emergency meeting was called where we tried our absolute best to recover the account and server. For over 7 hours, there was extensive debate and discussion to explore the best course of action, in an attempt to recover both the account and the server.

Our first course of action was resolving this through official means. We contacted Discord support through quite literally every single medium that was possible. We went through official Discord support (tickets and phone calls), and even DMing the Discord X account, to name a few.

We were optimistic that some venue would come through, but unfortunately, we vastly overestimated the amount of time available to us. There were many decisions to be made in little time:

1. Should we make an announcement regarding the compromisation of the account? But if we make the announcement too early, we might notify the malicious actor and start the attack sooner.
2. Should we silently migrate the custom invite link? Doing so may send an email notification to the malicious actor, and start the attack sooner.
3. Should we begin to prune, ban, or otherwise remove people from the old server in order to preemptively protect them from a raid? Doing so would lead to too many unresolved questions that we would not be equipped to handle.

With too many unknowns, there was not a clear, undisputed path to action. We began to create a backup server for migration. Channels were transferred, content was archived, and new verification procedures were beginning to be implemented in order to prevent a server raid.

We thought we had at least a day.

- **At 10:07 EST,** the compromised account made their first interaction in #general-robotics, with the default "Wumpus Wave" sticker. Moderators on that meeting that were meticulously scanning all of the compromised accounts activity (through messages and the audit log) noticed immediately, and we were a little panicked.
- **At 10:08 EST,** the compromised account began removing permissions from the three administrators. Immediately, we had to execute the decisions we had made just an hour or two prior.
- **At 10:11 EST**, there was a systematic pruning of a small number of inactive server members in order to minimize the users affected by the attack
- **At 10:15 EST,** the moderation team quickly boosted the new server in order to gain access to the custom invite link.
- **At 10:21 EST,** the custom invite link of the old server was removed, and the custom invite link of the new server changed by FTC Discord staff who still had permissions to do so.

Immediately after we had access to the **discord.gg/ftc** link, moderators pinged everyone on the old server (a message that was later deleted by the hackers), and the transition to the new server began. Unfortunately, the verification pipeline into the new server was ratelimited, as well as some permissions not being properly set up. This led to a massive delay in people being able to access the new server, which will be resolved in the upcoming days.

This is what we're doing differently to prevent such a scenario from occurring again:

1. We are in the process of making a new, inactive account with every level of authentication enabled, with credentials given only to one user in order to prevent token stealing attacks.
2. We will be bringing in bots to create periodic backups of the server to preserve the content and history of the server.
3. We will be restructuring permissions for moderators to be able to act more rapidly in response to a similar scenario.

Finally, a thank you to all of the people who helped us throughout this process. Thank you to the staff team from the Unofficial FRC Discord server; thank you to community members who archived what they could from the old server; thank you to those who sent us kind suggestions and were understanding in a time of chaos; and finally, thank you to every single member of the community for your continued patience and understanding.

— hextanium and jersicwa, on behalf of the entire FTC Discord Staff team