DISCORD SECURITY

How To Stop Account Takeovers On Discord

Plain-English how-to. ~10 minutes. Stops the most common Discord scams cold.

Discord is the social glue of modern gaming — and attackers know it. A compromised Discord account is a launching pad: scammers use it to message every friend, every server, asking for 'help' or pushing fake giveaways. Trust gets weaponized.

Discord token-stealer malware has become a small industry. A single click on an infected file, mod, or 'free Nitro generator' can lift the session token from your computer in seconds — bypassing your password and even your 2FA.

By the end of this guide your Discord account will have authenticator-app 2FA, DMs locked down to friends, no risky linked apps, and a recovery plan if anything goes wrong.

Quick snapshot

What you'll learn	Lock Discord with 2FA, DM controls, app review, and safe-mode habits.
Skill level	Beginner-friendly · Teen-appropriate
Time required	10 minutes
What you'll need	Discord login, your phone with an authenticator app
Risk if you skip this	Account takeover, scam DMs sent to every friend, malware spread
PDF kit	■ Download at the bottom of this page

Why this matters

Discord uses long-lived session tokens stored locally on your computer. Info-stealer malware specifically targets these tokens — a successful infection grants instant access without needing your password or 2FA prompt.

Once an attacker has your account they typically: (1) DM every friend with a phishing link or fake 'help me, I'm locked out' plea, (2) drop the same link into every server you mod, (3) sell or rent the account.

The fix is layered: authenticator-app 2FA blocks password-based attacks; DM controls reduce attack surface; safe download habits stop the token-stealer infection itself.

Before you start

Install an authenticator app (Authy, Microsoft Authenticator, Google Authenticator) on your phone. Avoid SMS-only 2FA — Discord supports both but app is far safer.

Have 10 minutes uninterrupted and your password manager open to generate a strong unique password if your current one is weak or reused.

Be ready to write down the backup codes Discord generates — these are your only way back in if you lose your phone.

Step 1 — Enable authenticator-app 2FA

User Settings → **My Account** → **Enable Two-Factor Auth**. Scan the QR code with your authenticator app. Enter the 6-digit code to confirm.

Discord then shows **backup codes** — print them, save in your password manager, or both. These are critical for recovery.

Step 2 — Add SMS as backup (optional but useful)

After enabling app-based 2FA, you can add SMS as a backup. **Settings** → **My Account** → **Add a phone number**.

Caveat: SMS is weaker than app-based 2FA. Use it only as backup, never as primary.

Step 3 — Lock down DMs from non-friends

Settings → **Privacy & Safety** → **Allow direct messages from server members** → **Off**. This stops random server members from DMing you with phishing.

Also turn on **Keep Me Safe** to filter explicit content and DMs from non-friends.

Step 4 — Review and revoke linked apps

Settings → **Authorized Apps**. Revoke anything you don't actively use. Many people have dozens of apps connected from bot servers years ago — each is a potential foothold.

Re-authorize only the ones you actively need (Twitch sub bot, music bot, etc.). Anything else gets deauthorized.

Step 5 — Set up account recovery email with its own 2FA

Your Discord email is your reset path. **Settings** → **My Account** → **Email** should point to an inbox YOU control and that has 2FA enabled.

If your Discord email is the same as your gaming, banking, or work email, the attack surface multiplies. Consider a dedicated email for high-value gaming accounts.

Step 6 — Set a unique strong password

Settings → **My Account** → **Change Password**. Generate a 20+ char password in your password manager. Never reuse the password from any other site.

Old Discord passwords have appeared in breach dumps. If you've used Discord for years on the same password, treat it as compromised and rotate now.

Step 7 — Avoid Discord token-stealer malware

The top infection vector: 'free Discord Nitro generator,' 'cheat for game X,' 'mod pack from anonfiles' — all common token-stealer delivery methods. Never run executables from untrusted sources.

If you must download mods or game tools, use only verified developer sites. Scan with VirusTotal first if unsure. Keep Windows Defender or another endpoint protection enabled.

Step 8 — Set up a recovery plan

Write down your backup codes and recovery email in a place you'll remember. Configure a 'I am compromised' message you can send via another platform if needed.

Tell your closest friends the rules: if my Discord ever asks you to send money, click a sketchy link, or share your Steam login, it's not me. Pre-agreement keeps your network from getting phished too.

PRO TIP

Discord Tokens Live On Your PC.

Token-stealer malware bypasses 2FA entirely by grabbing the local session token.

Never run unknown .exe or .scr files — even from a 'friend' who may also be compromised.

Keep Windows Defender (or your AV) up to date.

If 'a friend' DMs an unsolicited file, verify in voice or another platform before opening.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Use Discord in a non-admin Windows account

Limits the damage if a token-stealer somehow runs. Daily-driver Discord on a standard user, not admin.

Trade-off: occasional UAC prompts.

Power-user upgrade #2 — Run Discord in a separate browser profile

Use Discord via web in a sandboxed browser profile instead of the desktop app. Tokens are scoped to that profile.

Trade-off: misses some app features (push-to-talk on global hotkey, voice quality).

Power-user upgrade #3 — Use a hardware key for the linked email

Discord 2FA stops at the app. Your email is the recovery channel — protect it with FIDO2.

Trade-off: ~$30 hardware key.

Power-user upgrade #4 — Subscribe to Discord's security blog

discord.com/safety publishes regular threat advisories. Quick read, occasional value.

Trade-off: occasional email.

Power-user upgrade #5 — Audit each server's roles you hold

If you mod or admin a server, you're a higher target. Mod accounts need stronger security than user accounts.

Trade-off: 5-minute review.

Power-user upgrade #6 — Set Discord to wipe credentials on every quit

More advanced: configure Discord to not persist tokens. Requires logging in every session — annoying but secure.

Trade-off: more frequent logins.

Common mistakes & pitfalls

Mistake — Using SMS-only 2FA on a server-admin Discord account.

Fix — SIM swaps target high-value moderators. Authenticator app or nothing.

Mistake — Clicking 'free Nitro' or 'gift link' DMs.

Fix — All scams. Real Nitro gifts come through Discord's gift system in-app.

Mistake — Reusing your Discord password.

Fix — Breach dumps include Discord. Unique random passwords only.

Mistake — Leaving 'allow DMs from server members' on.

Fix — Drastically increases phishing exposure.

Mistake — Running mod packs / cheat tools from anonymous sources.

Fix — Top vector for token-stealer infections.

Mistake — Trusting a friend's urgent DM without verifying.

Fix — Their account may be compromised. Voice-verify or use another channel.

Mistake — No backup codes saved.

Fix — Lose your phone = lose your account.

Pro tips

Pro tip 1. If a friend asks for 'urgent help with $20 or login on this site,' call them voice. Always.

Pro tip 2. Set a status that says 'I never DM links — if you got a link from me, ignore' for an extra layer of friend protection.

Pro tip 3. Use Discord's **Streamer Mode** to hide tokens/IDs from your screen when sharing.

Pro tip 4. Server boost or Nitro? Manage via Settings, never via DM-linked sites.

Pro tip 5. Once a year, do a 'connections' audit: every linked app gets reviewed.

Frequently asked questions

My Discord is sending scam DMs to all my friends. What now?

Change password from a trusted device, sign out everywhere (Settings → Authorized Apps → Sign out devices), enable 2FA if not already, and run a full antivirus scan. Tell friends not to click anything.

Can Discord recover my account if I lose my 2FA app?

Yes, via Discord Support (support.discord.com). You'll need your backup codes ideally; without them, recovery is harder but possible.

Are bots safe to add to my account?

Verified bots (with Discord's checkmark) are generally safe. Unverified bots could request more permissions than they need — review carefully.

Is the Discord desktop app safer than the browser?

Browser version (especially in a clean profile) is slightly more isolated. Desktop app has more features.

What does 'token logging' mean?

Malware that reads your locally-stored Discord session token, then sends it to an attacker who logs in as you — bypassing password and 2FA.

Should I share my Discord ID publicly?

Username + tag is fine. The Discord user ID (long number) is also harmless. What matters is locking the account, not hiding the ID.

Can I have two Discord accounts?

Yes — Discord supports account switching. Useful for separating personal and stream/community accounts.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

1. Enable authenticator-app 2FA and save backup codes.
2. Lock DMs to friends only.
3. Revoke unused authorized apps.
4. Recovery email has its own 2FA.
5. Use a unique strong password.
6. Never run .exe from untrusted sources.
7. Voice-verify urgent friend asks.
8. Quarterly audit of connections + permissions.

Mini glossary

Discord token: Local session ID that authenticates your account.

Token logger: Malware that steals the token, bypassing 2FA.

Nitro: Discord's paid subscription with extra features.

Bot: Automated user-like account that adds features to servers.

Streamer Mode: Hides sensitive info from your screen during screen-share.

Backup code: One-time use code that lets you sign in without your authenticator.