# Free Trial Abuse Prevention Checklist

## Phase 1: Strategy and Foundations

- [ ] Assess the value of your free tier to determine the abuse risk level.
- [ ] Calculate the direct cost of a single abusive user (server, support, etc.).
- [ ] Define your tolerance for user friction versus your need for security.
- [ ] Explicitly prohibit creating multiple accounts in your Terms of Service.
- [ ] Create a clear Privacy Policy that discloses your data monitoring practices.

## Phase 2: Basic Verification and Defense

- [ ] Implement mandatory email verification for all new account signups.
- [ ] Confirm your verification emails are delivered promptly and avoid spam folders.
- [ ] Add a CAPTCHA system (like reCAPTCHA) to your signup form to block simple bots.

## Phase 3: Advanced Detection and Monitoring

- [ ] Add phone number verification as a required step/optional security measure.
- [ ] Integrate OAuth signups (e.g., Google) to link accounts.
- [ ] Log the IP address for every signup and subsequent user login.
- [ ] Use a GeoIP database to flag signups from known VPNs, proxies, or datacenters.
- [ ] Place a unique and persistent cookie to identify returning browsers post-signup.

- [ ] Set up alerts for multiple signups originating from a single IP address in a short period.
- [ ] Monitor for unusual behavior, such as a new account immediately hitting all usage limits.

### Phase 4: Smart Free Plan and Trial Design

- [ ] Identify and limit the high-cost or high-value features in your free tier.
- [ ] Implement clear usage caps on key metrics like API calls, data storage, or number of projects.
- [ ] Consider offering a time-limited free trial instead of a permanent freemium plan.
- [ ] Communicate all trial limitations and expiration dates clearly to the user.
- [ ] Watermark outputs or exports on the free tier to devalue abuse.

### Phase 5: High-Impact Security Measures

- [ ] Evaluate requiring a valid credit card for free trial activation.
- [ ] Integrate a trusted payment partner to handle card validation and authorization holds securely.
- [ ] Develop an internal risk scoring system that flags accounts with multiple suspicious attributes.

### Phase 6: Ongoing Management and Review

Review accounts that have been flagged for suspicious activity. Establish a clear and consistent process for suspending confirmed abusive accounts. Track how your methods impact key metrics like signups and conversion rate.